Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1	Page 87 of 291	Annexure-8 / Scope of Work	3. Sizing & Scalability Requirements	Sl. No. 15 SOC Solution - Cyber Range	Existing: Under Estimated Future Sizing (For 5 years) Participants: 5/ batch Hours: 40 hours per year When opting for **Cyber Range as a Service (CRaaS)** with a **yearly subscription** limited to **5 people per batch** and **40 hours per year**, the platform's utilization is minimal. The upfront investment covers the entire year, but usage is restricted, leading to underutilization of the service. Change: Under Estimated Future Sizing (For 5 years) Participants: 5/ batch Hours: 40 hours per month In contrast, using **CRaaS for 5 people per batch** with up to **40 hours per month** results in a more efficient and cost-effective use of the platform. With monthly access, the bank can conduct more frequent training sessions, increase hands-on experience for participants, and maximize the platform's value by leveraging it throughout the year instead of limited annual sessions. This provides greater flexibility and better return on investment.	Bidder to refer Corrigendum-2.
2	Page 155,156 of 291	Annexure-8 / Scope of Work	14. Scope of Work for Proposed services	c) Cyber Range	Addition: Cyber Range SaaS solution should support 50 or more users logging in simultaneously to play individual exercises. Each user should be able to engage in the same or different threat scenarios concurrently, without impacting the configurations, settings, or gameplay rules on other users' machines.	Bidder to comply with RFP terms and conditions.
3	Page 245 of 291	Annexure-17 / Bill of Material	Table 2) Price for NGSOC Services	Sl. No. 3 Solution/Service - Cyber Range	Existing: Qty mentioned is Participants: 5/ batch Hours: 40 hours per year Change: Qty should be 1	Bidder to refer Corrigendum-2.
4	NA	NA	Bid Submission Timelines	Bid Submission Timelines	Requesting Bank to kindly extend the Bid Submission timelines to at least 4 weeks from the date of releasing the Pre-bid response.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
5	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines	A. SIEM, SOAR & UEBA Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	Are these log sources & applications to be integrated with SIEM during the Implementation phase itself. Kindly clarify the number of log sources to be integrated for the implementation sign-off for SIEM, SOAR & UEBA.	Yes, log sources & applications to be integrated with SIEM during the Implementation phase itself. The details will be shared with selected Bidder.
6	NA	General Query	General Query	General Query	Requesting Bank to define the implementation sign-off for the below solutions: 1. SIEM, SOAR, UEBA & PCAP 2. TIP 3. EDR 4. Anti-APT 5. Anti-DDoS 6. PIM 7. NBA 8. VM, BAS, ASM & DAST 9. Brand Monitoring	Bidder to comply with RFP terms and conditions.
7	93	Annexure-8 : Scope of Work	5. Manpower Requirement & 6. Manpower Roles and Responsibilities	5. Manpower Requirement & 6. Manpower Roles and Responsibilities Annexure-17 : Bill of Material	We see that the count of L1, L2 & L3 resources mentioned in Section 5 (Manpower Requirement) for each of the security technologies is not matching with the resources/shift count mentioned in section 6 (Manpower Roles and Responsibilities) & in Annexure-17 : Bill of Material. Kindly clarify.	Bidder to refer Corrigendum-2.
8	93	Annexure-8 : Scope of Work	5. Manpower Requirement	Threat Management	Requesting Bank to increase the Threat Management resources count for the following as this is a 24x7 operations & we need to factor for weekly-off for the resources on rotational basis. L1 - From 12 to 17 L2 - From 5 to 9	Bidder to refer Corrigendum-2.
9	93	Annexure-8 : Scope of Work	5. Manpower Requirement	Endpoint Security	As Endpoint Security consists of EDR, DLP & Deception technologies, we request Bank to include dedicated resources for DLP. Requesting Bank to also share the volume of DLP tickets handled currently.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
10	94	Annexure-8 : Scope of Work	5. Manpower Requirement	Network Security	As Network Security comprises NBAD, Anti-APT & Anti-DDoS technologies, requesting Bank to have 4 L2 resources (2 for NBAD, and 2 for Anti-APT & Anti-DDoS) for these technologies.	Bidder to refer Corrigendum-2.
11	94	Annexure-8 : Scope of Work	5. Manpower Requirement	PIM Specialist VM, BAS, ASM & DAST	Requesting Bank to consider the following additional resources for handling these security technologies. PIM - 2 x L1 VM, BAS, ASM & DAST - 2 x L1	Bidder to refer Corrigendum-2.
12	26	7. Payment Terms	7.1 Payment Terms for Solutions and Hardware	7.1.1	We propose the Bank to pay the full GST to be paid upfront upon the delivery of Hardware / Software delivery.	Bidder to comply with RFP terms and conditions
13	26	7. Payment Terms	Hardware cost (including OS & associated Softwares) 40%	After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.	We assume that the payment will be made for the installation and commissioning of software (OS) and hardware, excluding the integration and testing of the technologies (SIEM, UBA). Kindly clarify. Here software means the OS and not the solution software like SIEM / UBA, etc. We would request bank to pay this money on hardware installation in the rack / POST.	Bidder to comply with RFP terms and conditions.
14	26	7. Payment Terms	10% After completsion of warranty period and submission of BG equivalent amount		We assume this should be or , either the bidder wait for the entire warranty period and then collect the money or the bidder can submit 10% BG to collect the money in advacne	Bidder to comply with RFP terms and conditions
15	26	7. Payment Terms	Additional		As per RFP the payment terms are split into 30%, 40%, 20% and 10%, however when we generate invoice we need to pay the GST on entire amount we request bank to pay the GST in full when the first invoice is generated	Bidder to comply with RFP terms and conditions
16	26	7. Payment Terms	Additional		We anticipate that full payment will be made for the supply of licenses for the existing technologies such as DLP, NBAD, DDOS and Tenbale.	Bidder to comply with RFP terms and conditions.
17	26	7. Payment Terms	7.1 Payment Terms for Solutions & Hardware	After completion of training and on submission invoices duly acknowledge by the Bank's Officials i.e., 3 months post sign off.	We request the bank to release 20% of the payment upon completion, sign-off, and training, rather than waiting for three months after the sign-off.	Bidder to comply with RFP terms and conditions
18	27	7. Payment Terms	License cost per Year	100% After complete delivery of license and on production of relevant documents like delivery signoff and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment.	Request Bank to revise this clause as, 100% After complete delivery of license ~~and on production of relevant documents like delivery signoff~~ and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
19	27	7. Payment Terms	AMC/ ATS	Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	Request Bank to release AMC/ATS money annually in advance against submission of additional PBG of equivalent value.	Bidder to comply with RFP terms and conditions
20	27	7. Payment Terms	3. One time implementation cost	30% on successful implementation in UAT	Kindly clarify the significance of the UAT environment here, do you have UAT setup for all the solutions, if not we request you to pls pay this on delivery and submission of invoice	Please read this clasue as : On successsful completion of User Acceptance Test
21	NA	NA	NA	Additional Query	Requesting Bank to charge the penalties on monthly charges only for the manpower services & not on AMC / other charges.	Bidder to comply with RFP terms and conditions.
22	20	6.Penalties/ Liquidated Damages	6.1	Uptime Penalty	As per our understanding, the solution components are in HA at DC & DR. Hence the downtime of the repective solutions should be considered only when its all components at both sites are down. Kindly confirm the above understanding.	Bidder to comply with RFP terms and conditions.
23	20	6.Penalties/ Liquidated Damages	6.1	Note: Penalty will not be applicable, if the down time is caused due to any Bank dependency or planned and approved downtime. However, the bidder shall work in tandem with Bank and its existing System Integrator (SI) to resolve such issues and make the solution up & running. Above LD is applicable for the following solutions SIEM, SOAR, UEBA, EDR, PIM, Anti-DDoS, Anti -APT and for other NG SOC solutions/services minimum uptime of 90 percent to be maintained, else flat 20% of monthly NGSOC operations charges will be levied .	Request Bank to limit the max penalties to 10% on monthly services invoice (this is only for manpower services and not including AMC / other OEM cost)	Bidder to refer Corrigendum-2.
24	21	6. Penalties/ Liquidated Damages	6.1.2. The maximum penalty levied shall not be more than the 100% of the monthly charges payable to NG SOC services operations.	6.1.2. The maximum penalty levied shall not be more than the 100% of the monthly charges payable to NG SOC services operations.	Requesting Bank to cap the maximum penalty to only 10% of the monthly SOC operations (manpower) charges.	Bidder to refer Corrigendum-2.
25	28	7.2	Payment Terms for Services	SaaS solutions like Threat Intel , ASM , BAS, Cyber Range , etc	We request bank to pay 100% upon activation of subscritpion services from the OEM's since these are SaaS services OEM will start the billing from activiation of services	Bidder to comply with RFP terms and conditions.
26	21	6.Penalties/ Liquidated Damages	6.3	Penalty on Non Retrievability of Historical logs/data	Max penalty capping is not defined. Requesting Bank to limit penalties to 10% on monthly basis.	Bidder to comply with RFP terms and conditions.
27	233-236	Annexure-10	Technical Scoring		NDA clients, please accept Mask PO and CA certificate	Bidder can mask pricing part.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
28	22	6.Penalties/ Liquidated Damages	6.4.Penalty on Service levels during Operations phase	Manpower services	Request Bank to exclude this clause for Non availability of resource due to medical emergency / unforeseen situations	Bidder to comply with RFP terms and conditions.
29	25	6.Penalties/ Liquidated Damages	6.11.	Penalties/Liquidated damages of delay in Takedown of fraudulent mobile/Web apps specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Request Bank to cap the penalty or define the maximum penalty	Bidder to refer Corrigendum-2.
30	25	6.Penalties/ Liquidated Damages	6.12.Penalties/Liquidated damages of failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	A genuine act of defacement on Bank's websites should be detected within 15 minutes of the incident. Penalty at the rate of 10% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 15 minutes but less than 1 hour. In case of response time more than 1 hour the penalty at the rate of 20% of quarterly payment of website scanning services will be charged. If the response time is more than 24 hrs, penalty at the rate of 100% of quarterly payment of website scanning services will be charged .	Request Bank to cap maximum Penalty to 10% instead of 100%.	Bidder to refer Corrigendum-1.
31	25	6.Penalties/ Liquidated Damages	6.17.	Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions attributable to the staff of the selected bidder.	Request Bank to cap the penalty 10% of monthly invoice as maximum penalty is not defined	Bidder to comply with RFP terms and conditions.
32	57	20.Protection of Data:	20.3.	The BIDDER/VENDOR/ SERVICE PROVIDER is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Bidder/Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information	Request Bank to remove this clause as SI will adhere to Canara Bank's policies, processes and guidelines.	Bidder to comply with RFP terms and conditions.
33	112	7	7.Scope of Work for Bidder/ System Integrator (SI)	Bidder / System Integrator (SI) should provide health reports and utilization details that may affect the day-to-day normal functionality of existing IT infrastructure.	Can we leverage Bank's existing tool for Health and Performance monitoring for NGSOC tools?	Bidder to comply with RFP terms and conditions.
34	113	7	7.Scope of Work for Bidder/ System Integrator (SI)	The Bidder shall take over operations and management of the currently running CSOC setup till NGSOC implementation is completed.	We assume that there will be no SLA monitoring during the transition and operation of the existing CSOC, also can this be supported by existing bidder as the tools are already deployed by them and we will be on the journey to migrate them to new tools	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
35	115	9	NGSOC Operations	Bidder must ensure that for each security incident, the solution should provide real-time remediation guidance .	Request Bank to modify this caluse as: Bidder must ensure that for each P1, P2 security incident, the solution should provide remediation guidance .	Bidder to comply with RFP terms and conditions.
36	74	Annexure-2 Pre-Qualification Criteria	Pre-Qualification Criteria	15. The proposed SOAR solution should have been implemented satisfactorily in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids	Requesting Bank to clarify that the credentials will be from OEM for this criteria.	Bidder to refer Corrigendum-2.
37	74	Annexure-2 Pre-Qualification Criteria	Pre-Qualification Criteria	16. The proposed UEBA solution should have been implemented in two Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Requesting Bank to clarify that the credentials will be from OEM for this criteria.	Bidder to refer Corrigendum-2.
38	74	Annexure-2 Pre-Qualification Criteria	Pre-Qualification Criteria	17. The Bidder should have implemented/ managed the EDR solution in single entity of Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Requesting Bank to consider amending this clause as below: The Bidder should have implemented/ managed the EDR / XDR solution in single entity of Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Bidder to refer Corrigendum-2.
39	20	6.1 Uptime Penalty	Solution (NGSOC Solutions and other Security Solutions and Services) Uptime (Individual systems at DC/ DR)	Bidder shall ensure that a minimum 99.90% uptime of the solution is maintained monthly (which includes all the components of the solutions as a whole).	Bidder request bank to calculate the uptime qtrly instead of monthly	Bidder to comply with RFP terms and conditions.
40	21	6	Penalties / Liquidated Damages	Section from 6.1 till 6.20	we request bank to pls limit the max penalty as 10% of the monthly invoice	Bidder to refer Corrigendum-2.
41	235	Annexure-10	Technical Evaluation Criteria	S.No 9. ""The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India 500 privileged users with more than 5 clients - Score of 5 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2"	We request bank to consider 500 users / 5000 devices as some OEM have licensing mechanism on no. of devices and not numnber of users	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
42	49	12.4	12.4.After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one-month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled		We request bank to cap the max liability to 10% of the total contract value	Bidder to comply with RFP terms and conditions
43	56	SECTION G - GENERAL CONDITIONS	15. Training and Handholding:	15.1. Bidder/ Vendor/ Service Provider shall provide necessary knowledge transfer and transition support to the satisfaction of the Bank. The deliverables as indicated below but not limited to:	We request bank to define number of training sessions (for eg 2 trainings in a year) and no. of participants (may be 5)	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
44	57	18	18.Hiring of Bank Staff or Ex-Staff: existing/ ex/retired employee of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the Bidder/VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory guidelines/HR policies of the Bank.		This should be limited to existing employees and for a term of contract. Independent hiring should be permitted.	Bidder to comply with RFP terms and conditions
45	57	20.3	20.3.The BIDDER/VENDOR/ SERVICE PROVIDER is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Bidder/Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information		We request bank to remove this clause as this might not be solely applicable to the bidder	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
46	58	22	Indemnity	22.1.3.Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER.	We request bank to remove this clause as this might not be solely applicable to the bidder	Bidder to comply with RFP terms and conditions.
47	58	22	Indemnity	22.6.The limits specified in above clauses shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or loss caused due to breach of confidential obligations or applicable data protection laws or commission of any fraud by the bidder or its employees or agents or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.	We request bank to limit the liability to maximum of the total contract value, we also request bank to limit only to the employees deployed on this project and not for the entire organization	Bidder to comply with RFP terms and conditions.
48	63	32	Social Media Policy		This is restricted to the extent it is applicable to the scope to be delivered	Bidder to comply with RFP terms and conditions.
49	64	35	Bidder Conformity	35.2.Bidder should ensure to adhere applicable regulatory guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Vendor will be liable to bank for any event for security breach and leakage of data/information	We request bank to amend this and restrict the cases applicable to bidder alone	Bidder to comply with RFP terms and conditions.
50	84	2	Scope of work	q.The proposed solutions implemented by the Bidder should adopt evolving threats and technological advancements, including quantum computing.	Quatum computing is still evolving and is covered in multiple phases like Discovery and then QKD solution , we request bank to keep the clause out of the current scope	Bidder to comply with RFP terms and conditions.
51	103		Project Manager Responsibilities	11. Ensure policies and procedures are regularly reviewed and updated to reflect changes in the threat landscape and organizational needs and 13. Develop and implement long-term strategies to enhance the effectiveness and efficiency of the SOC	As per RACI, bank is accountable however under PM job desc PM is responsible we request bank to remove this from PM scope	Bidder to comply with RFP terms and conditions.
52	109	7	Scope of work	•Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months	We request bank to keep this in existing vendor scope as the new bidder would have migrated the solutions to new OEM's	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

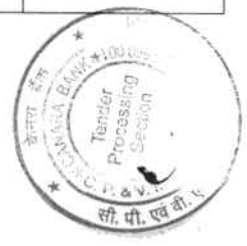
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
53	112	7	Scope of work	•The different components of NGSOC should be integrated with existing Bank's infrastructure like LDAP/Active Directory - Microsoft, IT Service Management -Service Now, Aruba-NAC, DLP-Forcepoint, NTP, TACAS, AV-TrendMicro, DAM-Oracle AVDF or any other Bank's existing /proposed solutions. etc. The Bidder should provide the detailed architecture of NGSOC, and other solutions being offered. The architecture to be deployed must be approved by the Bank	Bidder will integrate latest solutions howevr any legacy / non compatible solutions will be out of scope	Bidder to comply with RFP terms and conditions.
54	112	7	Scope of work	•Bidder and OEMs should ensure close collaboration with all necessary third parties & other OEMs. Any requirements from the Bank for customization, enhancement and other device/solution administration-related activity required in the supplied solutions to deliver seamless, fully functional integration, custom and native parsers, connectors, incidents management and related workflows, native and custom playbooks, alerts fine-tuning, notifications, dashboards, reporting, customization of default templates, additional remediation efforts etc. shall be undertaken by the Bidder at no cost to the Bank during the Contract period, even in case of extension of timelines for the commission of NGSOC due to any reason and such extension would be at the sole discretion of the Bank	We request bank to limit to the scope and bandwidth of the team involved onsite , any additional connector etc requried from 3rd party for integration etc will not be in bidders scope	Bidder to comply with RFP terms and conditions.
55	114	9	NGSOC Operations	•Bidder shall ensure that all logs (raw or normalized) data must remain within the Bank's premises (within jurisdiction of India). Under no circumstances these data must travel / store / processed / disclosed outside Bank's premises without Bank's consent	Since some solutions are provided on SaaS data might flow out of banks premises , we request bank to accept this clause as SaaS providers will have their setup beyond Banks premises	Bidder to refer Corrigendum-2.
56	115	9	NGSOC Operations	•Bidder must ensure that for each security incident, the solution should provide real-time remediation guidance	We will provide the support as soon as possible as there is an onsite team to respond to any incidents, howver it might not be always real time as it might need 3rd party / OEM support hence request bank to amend this clause and the overall SLA & Penalty does covert this	Bidder to comply with RFP terms and conditions.
57	115	9	NGSOC Operations	•The Bidder should implement required solutions for local log retention supported by log analysis tool for offline monitoring and reporting	Bank to let us know the log retention solution wise so that we can plan the storage accordingly and also inform SaaS vendors.	Log retention for all the solutions to be maintained for six months unless it is mentioned elsewhere in the RFP.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
58	130	VIII	DAST	•The Bidder will be responsible for actionable remediation steps for each identified vulnerability, including references to best practices and relevant security standards	Remidiation will be in bank scope and this might involve multiple bank (applications, mobille apps team) , hence pls remove this from bidder scope, however bidder will coordiatne / followup with required owners for closure	Bidder to comply with RFP terms and conditions.
59	149	b)	Other service & requirements	b)The incident will be closed only after successful takedown. Selected OEM/Bidder should have the reach on their own or through official business partnerships to take up closure/ mitigation measures on phishing sites anywhere in the world. Specify bidder connects exist with how many countries to take legal and other appropriate actions	Bidder will help bank with required inputs, however legal procdeeings will be in bank scope	Bidder to comply with RFP terms and conditions., (in case of any inputs from Bank, same has to be conveyed to Bank before acceptance of purchase order for takedown services)
60	NA	Additional clause	NA	NA	We request bank to share the current ticket count in SIEM + UBA , this will help us to arrive at the overall managed services efforts	Bidder to comply with RFP terms and conditions.
61	NA	Additional clause	NA	NA	we request bank to add additional manpower in the required matirx only for hardware (compute / storage / OS / DB) managed services	Bidder to comply with RFP terms and conditions.
62	161	16	16.System Integration Testing (SIT) and User Acceptance Testing (UAT)	10.The Installation will be deemed as incomplete if the solution is not operational or not acceptable to the Bank after acceptance testing / examination. The installation will be accepted only after complete commissioning of all solutions covered under this RFP. The date of commencement of contract will be the date when the Bank accepts all solutions covered under this RFP. The contract tenure for the solutions covered under this RFP will commence after acceptance by the Bank.	Different solutions have different start date , we request bank to state the managed services start date clearly We also understand bank wants the bidder to run the earlier installed solutions for a specific period till the new solutions are live, in that case does bank need the entire manpower strength as asked in the RFP or can we work with a lean team.	Bidder to comply with RFP terms and conditions.
63	158	a. other general terms	Implementation & Integration	(c)The support for all the solutions proposed should be provided for a minimum of 5 years post go live of all components in the solution. The Updates/ Upgrades for medium and low risk/threat should be implemented within 60 days of release of the same. For critical and high upgrades / updates, implementation to be implemented within 15 days of release or as per the Bank's policy.	We request bank to define the start date of managed services as multiple solutions have different start date	Bidder to comply with RFP terms and conditions.
64	109	7	Scope of work	•Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months	We request bank to clarify this 6 months of support , will this start with the overall 5 years managed services, if not then where do we capture this cost in commercials sheet	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
65	14	14.1.3	Indemnity	14.1.3.Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the Vendor/Service Provider	We request bank to pls delete this as this might not be solely for the actions done by the bidder	Bidder to comply with RFP terms and conditions.
66	95	6	Manpower roles & responsibilites	SOC Locations: the resources shall be deployed at both primary and DR SOC situated in bengaluru and mumbai respectively	We request bank to pls provide the breakup of how many resources are required in which location	This will be shared to succcessful bidder
67	NA	NA	NA	General Query	Please help us with number of service accounts to be managed by PIM This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder
68	NA	NA	NA	General Query	Understanding Bank is retaining the existing DLP, NBAD, DDoS and VM solutions. To ensure everyone gets fair inputs for all existing solutions, suggest Bank to obtain commercials from respective OEMs directly & share with the successful bidder and consider in overall TCO.	Bidder to comply with RFP terms and conditions.
69	22	6.4. Penalty on Service levels during Operations phase	Incident Response	Penalty applicability	We understand that the penalties mentioned in this section are applicable only for Threat Management solutions (SOC operations), and not applicable to Brand Monitoring services. Kindly confirm.	Bidder to comply with RFP terms and conditions.
70	24	6.9 to 6.12	Penalties / Liquidated Damages	Penalty applicability	The peanlties meniotned in these sections are applicable only for Brand Monitoring services. Kindly confirm.	Bidder to comply with RFP terms and conditions.
71	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	7. Solution should contain Generative AI based automatic/ custom use case rules builder based on Analyst prompt.	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-2.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

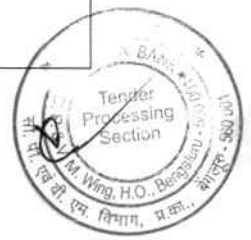
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
72	170	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	76. The proposed solution must allow access to the rules written in Sigma/Generic SIEM and EDR/XDR query languages. It supports common data schemas of SIEM along with the integration with content service to directly deploy rules from threat detection marketplace.	Request you to kindly elaborate the appropriate use case for the proposed clause. Also request this clause to be removed as it does not make relevance with regards to the SIEM requirements	Bidder to comply with RFP terms and conditions.
73	171	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	85. The platform should Query-less search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values	Request to modify the clause as "The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values"	Bidder to refer Corrigendum-2.
74	173	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	125. The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, offense, and the generic APIs.	Offense is a vendor-specific terminology. Request you to remove this clause	Bidder to refer Corrigendum-2.
75	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Security Incident and Event Management (SIEM)	Additional Points	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
76	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Security Incident and Event Management (SIEM)	Additional Points	Machine learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Bidder to comply with RFP terms and conditions.
77	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Security Incident and Event Management (SIEM)	Additional Points	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period. Use Case: Referencing old data for predictive analytics, proactive monitoring etc.	Bidder to comply with RFP terms and conditions.
78	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Security Incident and Event Management (SIEM)	Additional Points	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre-defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	Bidder to comply with RFP terms and conditions.
79	165	Annexure-9 Functional and Technical Requirements Security Incident and Event Management (SIEM)	Security Incident and Event Management (SIEM)	Additional Points	The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
80	176	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	9. The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Request to kindly modify this to "The solution shall have 400+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost"	Bidder to refer Corrigendum-1
81	177	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	17. AI Capabilities: a. Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc.	Request you to modify this to "Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department etc." This is specific to a single vendor	Bidder to refer Corrigendum-1.
82	177	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	18. The solution should suggest contextual between incidents using machine learning.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-1
83	177	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	19. The solution should provide shift management feature to upload shift schedule of users in any suitable format.	Request this clause to be removed as it is specific to a single vendor	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
84	178	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	31. The platform shall have threat visibility and investigation depth, speed and consistency with AI based automated analysis of EDR, NDR and SIEM telemetry sources	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-2.
85	178	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	38. The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console as in when required.	Request you to modify this to "The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console/cli as in when required."	Bidder to refer Corrigendum-2.
86	179	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	41. The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-2.
87	179	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	49. The solution must provide a visual workflow editor that is based on BPMN-Business Process Model and Notation to enforce sequencing of incident response activities	Reqest to modify the clause as "The solution must provide a visual workflow editor to enforce sequencing of incident response activities" since this is specific to a single vendor	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
88	182	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	Annexure-9 Functional and Technical Requirements Security Orchestration and Automation (SOAR)	92. The solution must maintain a database of incidents. The user must be able to search this database using the embedded Elasticsearch. Please describe how your solution meets this requirement.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-2
89	183	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	2. Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Request the bank to confirm that the UEBA solution in the RFP should perform both user and entity behavior analytics since it is not explicitly mentioned	Yes, UEBA solution in the RFP should perform both user and entity behavior analytics.
90	183	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	7. The solution shall have native integration available with leading SIEM, SOAR and ITSM solutions such as IBM, Palo Alto, ServiceNow, BMC Remedy etc.	This contradicts #2. Request to remove this clause	Bidder to refer Corrigendum-2
91	184	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	16. UEBA should activate a rules for a set of users until a specified condition or specified time window.	Request you to kindly clarify the use case for this as this does not makes sense for UEBA Solution	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
92	185	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	22. Network Traffic and Attacks D/DoS Attack Detected Honeytoken Activity Capture, Monitoring and Analysis Program Usage	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-2.
93	185	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	25. Solution must have network forensic analysis solution as integrated part of offering.	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-2.
94	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	27. Critical Applications Critical Commands execution on SWIFT Servers - success/ failed Critical Password Retrievals From Unauthorized Accounts Critical Server Rooms/Locations Access Attempts By Non-Admin Users	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
95	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	29. Defense Evasion - T1070 - Indicator Removal on Host - Unauthorized audit logs modification	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
96	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	30. Defense Evasion - T1484 - Group Policy Modification - Account created and deleted in short interval of time	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
97	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	31. Defense Evasion, Persistence - T1108 - Redundant Access - Potential Account Misuse: Disabled Account	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
98	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	32. Direct RDP access of Windows server	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
99	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	37. Interactive Login Detected From Service Accounts on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
100	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	38. Intranet/Internet Activity Via Rare /unauthorized User Agents	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
101	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	39. IOC Compromise Activity Followed By Security risk found-in End point	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
102	186	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	40. Malware / Ransomware Activity Detected - External Facing Hosts	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
103	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	42. PIM Bypass	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
104	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	43. Ransomware behavior on Critical servers via botnets	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2
105	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	44. Rare Malicious PowerShell Scripts Downloads on Critical Servers	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2
106	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	45. SMB Traffic / Sessions on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2
107	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	47. Suspicious Activity Detected From Non-Compliant Device / Host	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
108	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	48. Suspicious Kerberos RC4 Ticket Encryption	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
109	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	49. Terminated User Activity on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
110	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	50. Testing-Defense Evasion - T1484 - Group Policy Modification - Unauthorized self-privilege escalation - User Context	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
111	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	55. VIP Accounts Monitoring - Watchlists	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
112	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	56. Web Access-Potential Person of Concern	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
113	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	57. Web Access-Potentially Unwanted Software Accessed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
114	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	59. Web Traffic / EDR Alert - Malicious File Download Followed by High Severity EDR Virus Alert	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
115	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	60. Windows - scheduled task created by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
116	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	61. Windows logon-Terminated User Activity	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
117	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	62. Windows- registry value was modified by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
118	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	63. Potential Flight Risk: Unusual Visits to Job Sites	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
119	187	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	71. The solution should provide Identity Access Analytics use cases along with Access Outliers, Access Clean-up, Dormant Access, Orphan Account Analysis & Terminated Account Access monitoring. The Remediation should happen via Risk Based certifications from the UEBA tool itself.	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
120	188	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	Annexure-9 Functional and Technical Requirements User Entity Behavioral Analysis (UEBA)	77. The solution should have inbuilt platform support for automation of routine L1/L2 activities.	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-2.
121	184	Annexure-9 Functional and Technical Requirements	User Entity Behavioral Analysis (UEBA)	Additional Points	The UEBA solution should not require internet access to upade any machine learning models	Bidder to comply with RFP terms and conditions.
122	184	Annexure-9 Functional and Technical Requirements	User Entity Behavioral Analysis (UEBA)	Additional Points	The UEBA solution should not need a seperate data lake and should be able to fetch data from SIEM	Bidder to comply with RFP terms and conditions.
123	19	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5.3 Uptime	The selected bidder should consider high-availability (active-passive) at DC & DR with RPO of 15 minutes and RTO of 120 minutes.	Request the bank to modify this too active- active high availability with zero RPO and RTO. This is to make sure that there are no challenges with the bank during DC and DR drills and audits as performed by RBI	Bidder to refer Corrigendum-2.
124	216	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	9. The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	20 Gbps from Day 1, scale upto 40 Gbps with active-active cluster. We request to consider 20 Gbps from Day 1 and 40 Gbps using Cluster solution.	Bidder to refer Corrigendum-2.
125	216	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	12. The proposed solution must be deployed in span mode on day one and also should support inline blocking mode with automatically block inbound exploits, malware, and outbound multi-protocol callbacks.	Is inline mode required from Day 1 or this is a future requirement. Kindly clarify	Solution should support Inline-Monitoring mode and Out of Band (Span) mode from day one.
126	218	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	22. Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations with all licenses and dependencies included in the solution.	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
127	220	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	40. The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2.
128	221	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	53. The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.		Query is not clear.
129	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	The Sandbox solution should support at-least 5000 File submissions per day and should be upgradable to higher file submissions in future with additional licenses.	Bidder to comply with RFP terms and conditions.
130	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	The proposed sandbox solution should be able to track for network I/O to raw disks and any modification to MBR made by the samples during the dynamic analysis. Justification: MBR is the most critical part of the windows system as it stores the information on where the OS is there on disk and to be loaded. Modifications to this can corrupt the entire system thus it is very important for sandbox to check for this.	Bidder to comply with RFP terms and conditions.
131	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	The proposed sandbox solution should allow user to manually interact with the sample within the analysis environment while the analysis is taking place. Justification: Manualy interaction by admin on malware sample in analysis environment facilitate them with simulating real user scernarios and help in inverstigating the malware with various behvaioural indicators and develop the response strategries without infecting the end user machine	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

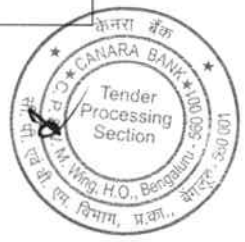
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
132	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	A video recording of the malware analysis should be made and be able to have playback and download capability for further analysis. curity expertise to interpret reports. Justification: Video Playback of sample execution helps the admins to better visualise the analysis and triggers leading upto the file being flagged.and gaining valuable insight into the behaiour of file. It also serves as a great evidence to be submiited to other teams for their consumption for reporting purposes	Bidder to comply with RFP terms and conditions.
133	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	The sandbox solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed. Justification: Allowing admin's/incident responders to have the capability to interact with the malware sample execution helps them to understand the every samples behvaiour and its impact on the system	Bidder to comply with RFP terms and conditions.
134	165-232	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	The sandbox must have capability to Analyze more than 800+ highly accurate and actionable advanced behavioral indicators. Justification: A detonation engine works on by detecting a behvaiour and matching it against the baseline behvaiour data that the sytem has in order to determine whether it is clean or bad. Thus a sandbox which is a behvaioural detection engine working on by detonating files in controlled environment. thus the higher number of behvaioural indicators ensures the higher catch rate and efficay of sandbox	Bidder to comply with RFP terms and conditions.
135	228	Annexure-9 Functional and Technical Requirements	Anti-APT - Technical Requirement	Additional Points	AntiAPT solution must have static and dynamic analysis capabilities. Dynamic Analysis solution should have a file processing capability of 50K files per day in case solution scans all the files or 5K file per day if solution scans only unknown/zero-day files.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
136	125	12. Scope of Work for Proposed Solutions	III.Security Orchestration, Automation and Response (SOAR)	The solution should ensure that time between MTTD and MTTR should be improved gradually. Further, the vulnerability window should be within the tolerable time limit of the Bank.	We understand there is a tolerable limit for vulnerability, Please elaborate what is the expectation in relation to Vulnerability in SOAR and what is the tolerable limit in terms of timeline?	As per the defined SLA for updates/ upgrades documented in the RFP.
137	125	12. Scope of Work for Proposed Solutions	III.Security Orchestration, Automation and Response (SOAR)	The bidder shall develop custom integration as necessary within the defined timeline.	The expectation is to build custom integration in SOAR within defined timeline, please clarify what is the timeline? What type of custom integration are expected? How many custom integration are expected?	Defined timeline will be mutually agreed between bank and SI. Bidder to comply with RFP terms and conditions.
138	125	12. Scope of Work for Proposed Solutions	III.Security Orchestration, Automation and Response (SOAR)	Bidder to perform periodic backup and store in a secure storage.Bidder to fix the gaps identified by OEM or Auditor as part of the assessment · Bidder to build incident and alert layout.	The expectation is to perform periodic backup and storage, Please clarify whether you want to have backup of alerts or raw logs? Please clarify for what timeline is the storage required?	Bidder to comply with RFP terms and conditions.
139	130	12. Scope of Work for Proposed Solutions	VII. Threat Intelligence Platform (TIP)	Bank is procuring Centralized Cyber Threat Intelligence Platform solution for which Bidder has to provide the services which includes but not limited to the following:	Please clarify whether the requirements mentioned below are in relation to Threat Intel Management as a platform or as a service?	Threat Intelligence Platform (TIP).
140	130	12. Scope of Work for Proposed Solutions	VII. Threat Intelligence Platform (TIP)	Perform periodic validation of integration, data flow, and automation configurations.	Please clarify what is the frequency of periodic validation?	Frequency of periodic validation is as and when required by the bank.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
141	174	Annexure-9 Functional and Technical Requirements	Packet Capture	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	The current technical specifications appear to reference the ingestion of logs, which is not directly relevant to packet capture (PCAP) solutions. For PCAP systems, only packet data and metadata related to ingested packets are applicable. We respectfully request that the specification be revised as follows to better reflect the requirements of a PCAP system: "The proposed Packet capture solution shall have capabilities to integrate with the proposed SIEM solution in both DC and DR. The OEM shall have the capacity to capture traffic at 10 Gbps and retain packet-like data and associated metadata for 7 days. Adequate storage shall be provisioned accordingly. The PCAP solution should also support both automated and manual mechanisms for selectively discarding, masking, or filtering packets based on their security relevance (e.g., customer PII, SPDI, or other classified information as per the Bank or Regulatory guidelines), to optimize storage.	Bidder to refer Corrigendum-2.
142	174	Annexure-9 Functional and Technical Requirements	Packet Capture	The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance with minimum 4 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 2*1/10G management port.	We propose the use of a Network Packet Broker to ingest traffic from multiple vantage points with various port configurations. To better reflect this approach, we respectfully request revising the clause as follows: "The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/outflow of data in the DC. The proposed solution should be a dedicated hardware with 4 X 10 Gig SFP+ and 2 X 1/10G management ports. For environments requiring traffic capture from more than four vantage points, a dedicated Network Packet Broker should be proposed." This revision allows for more flexibility in network design and ensures effective capture across multiple vantage points without compromising performance or expandability.	Bidder to refer Corrigendum-2.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
143	174	Annexure-9 Functional and Technical Requirements	Packet Capture	The proposed packet capture solution should be a dedicated Hardware appliance, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports	Kindly consider the suggested points to secure enough storage on the proposed hardware: "The proposed packet capture solution should be a dedicated Hardware, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the dedicated hardware and the storage should utilize Self-Encrypting Drives (SED). Should have required OEM approved storage to scale upto 20Gbps throughput without the need to integrate with other storage solutions".	Bidder to refer Corrigendum-2.
144	175	Annexure-9 Functional and Technical Requirements	Packet Capture	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should be a native feature of SIEM for sharing of network data (Packet + Meta data) in real time .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	Given the critical need to protect customer privacy, particularly with respect to Personally Identifiable Information (PII), Sensitive Personal Data or Information (SPDI), and other classified information, we recommend limiting payload data capture to only suspicious and malicious traffic. This approach ensures that sensitive data is not unnecessarily captured and stored, aligning with privacy regulations and best practices. We respectfully request revising the clause as follows: "The proposed packet capture solution should be able to perform real-time monitoring and network traffic analysis to identify threats. The solution should feature Deep Packet Inspection (DPI) to provide visibility into all layers of the OSI stack (L2 to L7), including application payload data, but only for suspicious and malicious traffic. The solution should create indexes for payload objects as required and not just rely on header information." Additionally, the solution should provide network traffic insights by: a. Classifying protocols and applications b. Performing deep-packet inspection c. Supporting cross-correlation for analysis and aggregation d. Reconstructing sessions and analyzing artifacts e. Previewing artifacts and malicious attachments	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
145	175	Annexure-9 Functional and Technical Requirements	Packet Capture	Solution should provide meaningful artefacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files from Deep packet Inspection. Post reconstruction, solution should be able to do object extractions from sessions like pcaps, zip files, office documents, media, embedded malicious attachments etc.	In consideration of maintaining customer privacy and safeguarding Personally Identifiable Information (PII), Sensitive Personal Data Information (SPDI), and any classified information, we propose a modification to the specifications regarding payload data capture. We request that the requirement for comprehensive payload data capture for all traffic be adjusted to only include the storage of payloads associated with suspicious or malicious traffic for further analysis. We recommend rephrasing the specification as follows: "The solution should provide meaningful artifacts such as FTP data files, JavaScript, and .Net files derived from Deep Packet Inspection. After reconstruction, the solution should be capable of performing object extractions from sessions, including PCAPs, zip files, office documents, media files, and embedded malicious attachments." This amendment will help ensure compliance with privacy regulations while still delivering the necessary analytical capabilities.	Bidder to comply as per GeM Bid/ RFP terms and conditions.
146	175	Annexure-9 Functional and Technical Requirements	Packet Capture	The solution should have the capability to extract data/ files from the captured network packets	We propose the following modification to enhance the specification: "The solution should possess the capability to extract data / malicious files from the captured network packets. Additionally, the solution should include the functionality for comprehensive host investigations, as well as session and packet analysis on the captured packets and any generated alerts." This revision ensures that the solution not only extracts relevant data but also provides crucial investigative capabilities that are essential for effective threat analysis.	Bidder to refer Corrigendum-2
147	175	Annexure-9 Functional and Technical Requirements	Packet Capture	The solution should have the functionality to reconstruct and replay the network packets which will help to identify the entire transaction	We recommend the following modification to the specification: "The solution should have the functionality to reconstruct or complete packet analysis or replay the network packets which will help to identify the entire transaction." This adjustment underscores the importance of all three capabilities for a thorough understanding of network interactions and transaction integrity.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
148	124	Annexure-9 Functional and Technical Requirements	PCAP	Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload &header as well (like TLS 1.3) etc.	We recommend the following modification to the specification: "Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload & header as well".	Bidder to refer Corrigendum-2.
149	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		We strongly recommend that the bank insists on a dedicated solution that fully delivers all PCAP specifications and use cases outlined above. It is crucial to note that PCAP is inherently resource-intensive, requiring significant processing power, storage, and management capabilities. By integrating PCAP functionality as a subset of a Security Information and Event Management (SIEM) system or any other solution, the bank risks diluting the effectiveness and performance of both systems. Advantages of a Dedicated PCAP Solution: 1. Optimal Performance: A dedicated PCAP solution ensures that the capture, storage, and analysis of packet data occur without interference from other applications, leading to more reliable performance. 2. Comprehensive Coverage: Focusing exclusively on PCAP capabilities allows for a more thorough and targeted approach to data capture and incident investigation, enhancing security monitoring. 3. Scalability: Separating the PCAP solution facilitates better scalability, enabling the bank to adapt to growing data needs without compromising the functionality of a combined system. 4. Simplified Management: A dedicated solution streamlines management and maintenance, reducing complexity and	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

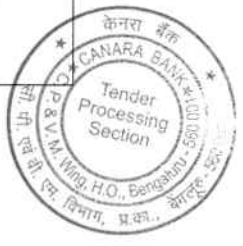
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
150	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		The PCAP solution should be capable of capturing network traffic and flexibility to use tools to read / extract pcap files on the device itself rather than downloading it to local machine. This will ensure that the pcap file irrespective of its size can be opened directly on the device which otherwise requires the file to be downloaded and opened using tools. If the file size is large than 1GB, then the local machine / workstation struggles to open the file. Thus it is essential for the pcap to be opened on solution itself without having to download it for quick forensic investigations, security analysis, and integration with other network-based security tools. The solution should support manual export of captured packets or the ability to forward them to external security systems for further analysis.	Bidder to comply with RFP terms and conditions.
151	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		Given the criticality of real-time threat detection and the need for deep packet analysis, we suggest bank to consider the following requirement: - Zero-Day Threat Detection: The solution must be capable of identifying and mitigating zero-day threats as they emerge, ensuring proactive protection against emerging cyberattacks. - Retrospective Analysis: The system should allow for in-depth examination of captured packets, enabling the extraction of valuable metadata for subsequent analysis by an analytics engine. - Packet Storage and Analysis: The solution must have robust capabilities for storing, extracting, and analyzing packets, providing essential insights for incident response and threat intelligence.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
152	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		Considering the criticality and agility for precise packet retrieval, we request bank to consider the following: - Efficient Indexing and Searching: The solution must have robust indexing and searching capabilities to allow for quick and easy location of specific packets based on a wide range of criteria. - Comprehensive Search Support: The system should support search functionality not only at the network layer (Layer 3 and Layer 4) but also at the application layer (Layer 7), including protocols such as HTTP, DNS, DB, LDAP, and others. - Search Criteria: The solution should support searching based on various criteria, such as time, links, IP addresses, port applications, protocols, and any other relevant attributes.	Bidder to comply with RFP terms and conditions.
153	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		Proposed PCAP tool should have capability to ingest packets from all type of application footprint, On Premise, Public Cloud or Private Cloud, so we request to add this clause. "The PCAP solution should support for capturing and storing data from (but not limited to) multiple network segments, VLANs, network locations, etc. The solution must be capable of supporting Public or Private Cloud infrastructure deployment using industry standard ecosystems. The solution should support deployment into Public Cloud platforms like Amazon Web Services (AWS), Microsoft Azure environments, Google Cloud, etc. The solution should be capable of capturing traffic on Private Cloud, Containers, Dockers & other virtual Infrastructure without the need of third party components. > Microsoft Hyper-V > VMware's ESX, NSX-V & NSX-T > OpenStack > Ubuntu/KVM"	Clause added. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
154	165-232	Annexure-9 Functional and Technical Requirements	Additional Points to Consider for PCAP Solution		We recommend that the requirement for an advanced PCAP solution with real-time threat detection capabilities be included as part of this RFP. The solution should be able to detect and analyze the following incident categories (but not limited to): - Suspicious communication over non-standard ports - Data exfiltration attempts - Command and Control (C2) communications - The use of The Onion Router (TOR) - SSH communication with monitored countries - Privacy VPN usage detection - Reconnaissance activities - Detection of unknown Domain Generation Algorithm (DGA) attacks These capabilities are crucial for ensuring proactive security and effective threat mitigation. We believe incorporating this into the solution requirement will significantly enhance your ability to detect and respond to advanced threats in real-time.	Bidder to comply with RFP terms and conditions.
155	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
156	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-2



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
157	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-2
158	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
159	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-2
160	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-2
161	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
162	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-2.
163	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-2.
164	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-2.
165	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2.
166	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
167	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
168	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
169	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
170	228	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
171	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2.
172	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
173	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-2.
174	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
175	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
176	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
177	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
178	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
179	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2.
180	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-2.
181	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2.
182	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-2.
183	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
184	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
185	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum 2
186	24	6.9.	Penalties/Liquidated damages on failure to resolve incidents like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents)	The selected bidder should resolve the incidents reported. The selected bidder shall be -liable to pay Liquidated damages at the rates specified below subject to a cap of 20% of quarterly payment of in scope service. Resolution time Penalty Amount Within 480 minutes No Penalty 480 to < 540 minutes 3.00% on Basic invoice value of Quarterly payment 540 to < 600 minutes 5.00% on Basic invoice value of Quarterly payment	We request removal of this clause as resolution may involve takedown or assistance from Bank's internal teams to validate/isolate/patch issues that are identified. This SLA is unreasonable given dependencies.	Bidder to comply with RFP terms and conditions.
187	24	6.10.	Penalties/Liquidated damages of delay in Takedown of phishing sites specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.50 per takedown More than 48 hours, but less than 72 hours Rs.100 per takedown More than 72 hours Rs. 150 per takedown	We request modification of the same as - More than 48 hours, but less than 72 hours Rs.50 per takedown More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours Rs. 150 per takedown	Bidder to comply with RFP terms and conditions.
188	25	6.11.	Penalties/Liquidated damages of delay in Takedown of fraudulent mobile/Web apps specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.100 per takedown More than 48 hours, but less than 72 hours Rs.500 per takedown More than 72 hours Rs. 1000 per takedown	We request modification of the same as - More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours, but less than 168 hours Rs.500 per takedown More than 168 hours Rs. 1000 per takedown	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
189	25	6.12.	Penalties/Liquidated damages of failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	A genuine act of defacement on Bank's websites should be detected within 15 minutes of the incident. Penalty at the rate of 10% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 15 minutes but less than 1 hour. In case of response time more than 1 hour the penalty at the rate of 20% of quarterly payment of website scanning services will be charged. If the response time is more than 24 hrs, penalty at the rate of 100% of quarterly payment of website scanning services will be charged.	We request modification as - A genuine act of defacement on Bank's websites should be detected within 4 hours of the incident. Penalty at the rate of 1% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 4 hours but less than 6 hours. In case of response time more than 6 hours the penalty at the rate of 2% of quarterly payment of website scanning services will be charged. If the detection time is more than 24 hrs, penalty at the rate of 5% of quarterly payment of website scanning services will be charged. The Total Penalty levied cannot exceed 10% of the Quarterly Payment (Pro-Rata) for the tool.	Bidder to refer Corrigendum-2.
190	28	7.2.2.	Payment Terms for Services	Payment shall be released quarterly in arrears after completion of implementation of the SOC Services mentioned in the RFP and acceptance of the same by the Bank Officials for the respective Assignment.	We request modification to - Payment shall be released yearly in advance after completion of implementation of the Tool. Additionally, the subscription Date starting from the date of implementation and acceptance by the Bank).	Bidder to comply with RFP terms and conditions
191	146	(i)	Early Phishing Detection	Monitoring spam traps to detect phishing mails.	This is a email security tool capability. Canara Bank would be have subscribed to a dedicated e-mail security solution that covers Spam Traps use case. Today, there are several techniques used by spammer/defrauders that evade Spam Traps like using Spam Trap detection services (ex. www.zerobounce.net). We request this clause to be removed as it is an ineffective method to detect phishing campaigns. Monitoring Typo-squatted domain reginstrations, Monitoring Social Media platforms/Darkweb discussions, IRCs (Telegram/Discord) for any targetted phishing campaigns and blocking indicators associated with phishing infrastructure is a much effective way to defend phishing campaigns.	Clause stands deleted. Bidder to refer Corrigendum-2.
192	148	(m)	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:	Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	There is no legally obliged entity hosting forums and content on the dark web. Owing to this, there is no takedown possible of Dark Web Mentions or data leaks. We request the bank to remove this clause.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
193	149	(c)	Brand Protection and Monitoring:	Search engines (like Google, Yahoo, Bing etc.) and Generative AI (like chat GPT, Open AI, Gemini etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including but not limited to Truecaller and JustDial.	Kindly elaborate Generative AI monitoring scope. As Generative AI LLMs are trained on specific datasets and are susceptible to poisoning as well. The technology is still in the early days and each Generative AI platform provides unique answers. We request this to be removed from the scope as there isn't a reliable method to monitor GenAI platforms. Tracking of Branch Addresses when the Bank has over 9,000+ branches is not technically feasible and Google Maps enables any user to place a location marker and register a business. Post merger with Syndicate Bank, there are thousands of Canara Bank's Nitya Nidhi Deposit (NND) Scheme Collection agents who would have registered their business. An army of manual analysts would be needed to verify and takedown these addresses. This use case is challenging to address and beyond automation or AI capabilities to monitor.	Bidder to comply with RFP terms and conditions.
194	150	(c)	Attack Surface Monitoring:	The proposed solution shall identify potentially orphaned applications, and services.	We seek clarity from the Bank if "Orphaned applications" refers to shadow IT or dangling DNS records.	Bidder to comply with RFP terms and conditions.
195	151	(q)	Attack Surface Monitoring:	The proposed solution shall be able to validate the Current IP attribution is using DNS, Netblock, and Keywords to improve accuracy.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
196	151	(t)	Attack Surface Monitoring:	The proposed solution shall be able to do Active Banner Grabbing and advanced search based on banners to detect any vulnerable version and provide reports as mentioned earlier.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
197	151	(w)	Attack Surface Monitoring:	The proposed solution shall be able to perform Network-level Risk scanning to identify misconfigured servers, services, and devices.	We request the Bank to define "devices".	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
198	153	c)	Other Services & Requirements:	The solution shall provide correlation capability and actionable intelligence with respect to historical reference to threats.	We request the Bank to elaborate the use case.	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
199	154	b)	Service Level Agreements	Alert within 20 minutes of attack/compromise/down/not reachable.	This is a WAF/IPS/IDS/SIEM/Application Monitoring/EDR/MDR/NAC use case. We request the same to be removed from the scope.	Bidder to comply with RFP terms and conditions.
200	154	d)	Service Level Agreements	Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident and fraudulent mobile apps within 24 hours.	We request this to be modified to - Take down of Phishing Site within 48 hours of detection and fraudulent mobile apps within 72 hours.	Bidder to refer Corrigendum-2.
201	154	f)	Service Level Agreements	Resolution of Trojan incidents with 24 hrs of detection.	This scope is beyond the scope of Threat Intelligence Services. We can alert of any Trojan Incident leading to data leak and it being available on the Dark Web or Freemium/Premium portals/marketplaces.	Clause stands deleted. Bidder to refer Corrigendum-2.
202	NA	NA	Propose Addition of Clause		As a Best Practice - we suggest the Threat Intelligence Platform and Threat Intelligence Services to be subscribed from different OEMs/Vendors. Several Indian Government entities/PSUs have adopted this approach for better coverage.	Bidder to comply with RFP terms and conditions.
203	142	14. SoW for Proposed Services	Threat Intelligence Services Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage	Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Yes, ask is about threat intel services.
204	145	14. SoW for Proposed Services	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/tools/exchange knowledge for banks brand	Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.
205	146	14. SoW for Proposed Services	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	Kindly elaborate the scope.	Bidder to refer Corrigendum-2.
206	200	V.Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% Yo-Yo Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

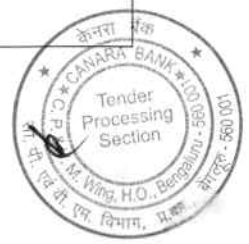
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
207	204	V.Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be trated as 1 application)
208	136		DLP	Additional Points	Our understanding is that Data Classification is not in the scope of this RFP, pls. clarify	Bidder to comply with RFP terms and conditions.
209	136		DLP	Additional Points	We would like to understand if Bank would like to have training and certification on DLP directly from Forcepoint at Administration or System Engineer level. Bank may include specific requirements on the same like number of trainees and if training is required every year as Bank team changes every few years.	Bidder to comply with RFP terms and conditions.
210	136		DLP	Additional Points	We would like to understand if Bank wants to have Annual Health Check and review directly from OEM professional Services team for the DLP Solution	Bidder to comply with RFP terms and conditions.
211	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should have MFA capabilities of SMS, Email or Application based authenticator (TOTP). If the solution does not have in-built feature, then the OEM should provide additional tool to meet the objective without any additional cost. It should have an inbuilt authentication for Biometrics and must integrate with Bank's existing biometric solution	Kindly provide details on Bank's existig biometrics solution ? Is it FIDO compliant and which is the OEM ?	Bidder to refer Corrigendum-2
212	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.	Kindly provide list of applications and application platform for which this capability is required ? Also request to clarify the number of application for BOQ.	The list of applications will be provided to selected Bidder, however the number of applications is 50.
213	204	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should be able to provide rotation capabilities at scale (across technologies)	Kindly provide the ist of technologies for which require credentials rotation capabilities	Bidder to comply with RFP terms and conditions.
214	206	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution must enforce auto- rotation for each password/ key before the default expiry of custom expiry date of the keys/ certificate.	Kindly mention the type of keys/certificates. Kindly clarify the count of such certificates to arrive at BOQ .	Bidder to refer Corrigendum-2
215	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution shall have feature to manage system and application-level privilege accounts. OEM to support application integration	Kindly provide list of applications for integrationg to PAM	Bank will provide the details to the selected Bidder.
216	243	Annexure 17	Bill of Material	User Licenses Cost	For PIM Solution which is subscription based, how do we represent costing in the table	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
217	251	Annexure 17	Bill of Material	Table 5) AMC/ATS Cost for items mentioned in Table- 1 and Table- 2	For PIM solution which is subscription based, it will be spread across all the 5 years and there is no separate licenses and AMC costing how do we represent the 4th and 5th year costing in this table?	Bidder to refer Corrigendum-2.
218	255	Annexure 17A	Optional Cost	Optional cost for PIM Solution - Cost per Additional 100 IDs (in bundles)	The cost for additional 100 IDs meaning cost for additional users? Also is this licenses cost per year?	Yes, the cost for 100 IDs meaning cost for additional users
219	27	Payment terms	License cost	100% After complete delivery of license and on production of relevant documents like delivery signoff and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment	Kindly consider license cost from date of delivery as the start of the term of contract period	Bidder to comply with RFP terms and conditions.
220	27	Payment terms	License cost	100% After complete delivery of license and on production of relevant documents like delivery signoff and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment	Kindly consder US $ fluctuation variation factor for yearly annual invoicing	Bidder to comply with RFP terms and conditions.
221	86	Annexure 8 - SOW	3. Sizing and scalability requirement	12. PIM - 1500 users licenses requirement	Pls share the profiles of these 1500 users - are they all Bank's internal employees, or vendor resources, What other profiling details can you share of these 1500 users - Networki team, DB team, App team, admins, super admins, approvers, etc	Bidder to comply with RFP terms and conditions.
222	201	Annexure-9	Technical Specifications of each SOC Solutions: (V) PIM	The solution shall have redundancy to failover in DC and DR both in HA in case the primary solution goes down. All the required hardware, software, OS, storage and required licenses shall be provided by the bidder.	Kindly provide the maximum concurrent sessions required in order to recommend appropriate hardware requirement.	Bidder to comply with RFP terms and conditions.
223	71	Annexure 2	Pre-Qualification Criteria	The Bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.	Bidder requests to modify the clause only for OEM and Class-I or Class-II criteria to be removed.	Bidder to comply with RFP terms and conditions
224	73	Annexure 3	Pre-Qualification Criteria	OEM should have provided on- prem SIEM solution should have been implemented at least 1,00,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Request Bank to modify the clause as below: OEM should have provided on- prem SIEM solution should have been implemented at least ~~1,00,000 EPS~~ 70,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
225	110	Manpower Roles and Responsibilities - Resource Cost	To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored - 1.SOC Resource for All the services L1 - Rs. 6 Lakhs per year. L2 - Rs. 10 Lakhs per year. L3 - Rs. 20 Lakhs per year. 2. SOC Project Manager Resource - Rs.25 Lakhs per year. 3. SOC Automation Engineer (L3) - Rs.25 Lakhs per year.	To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored - 1.SOC Resource for All the services L1 - Rs. 6 Lakhs per year. L2 - Rs. 10 Lakhs per year. L3 - Rs. 20 Lakhs per year. 2. SOC Project Manager Resource - Rs.25 Lakhs per year. 3. SOC Automation Engineer (L3) - Rs.25 Lakhs per year.	Bidder requests the below modification to the floor limit for resource cost as below: L1 - Rs. ~~6~~ 10 Lakhs per year. L2 - Rs. ~~10~~ 20 Lakhs per year. L3 - Rs. ~~20~~ 30 Lakhs per year. 2. SOC Project Manager Resource - Rs.~~25~~ 50 Lakhs per year. 3. SOC Automation Engineer (L3) - Rs.~~25~~ 30 Lakhs per year. Note: Revised price benchmarking is based on industry standards for experienced and qualified SOC specialists.	Bidder to comply with RFP terms and conditions.
226	17	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.4.Implementation Phase	The SI shall ensure that 100% of the resources deployed at the Bank shall be on the payroll of the primary SI.	Request Bank to modify the clause: All L1 resources and 50% of L2 resources to be on contract and L3 on bidder's payroll.	Bidder to comply with RFP terms and conditions.
227	234	PIM point 9 in scoring	Annexure-10 Technical Evaluation Criteria	The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India 500 privileged users with more than 5 clients - Score of 5 500 privileged users with more than 2 clients and up to and including 5 clients - Score of 2	Seeking clarification on if 500 for each client or to be considered as total of 500 for 5 clients	Privileged users for each client. Bidder to refer Corrigendum-2
228	234	EPS point 8	Annexure-10 Technical Evaluation Criteria	The Bidder should have the experience in implementing or managing SIEM Solution in Organization(s) in India 1 lakh EPS with 2 clients - Score of 5 1 lakh EPS with 1 client - Score of 2	Seeking relaxation to 70K ePS for both the references.	Bidder to comply with RFP terms and conditions.
229	165	SIEM	Technical Specifications of each SOC Solutions	The proposed solution shall be capable of dual forwarding/ streaming/ replication from DC to DRC and vice versa at the events from collection and correlation layer. Storage must be arranged accordingly.	Seeking relaxation on dual forwarding on collector layer	Bidder to refer Corrigendum-2



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
230	23	Solution (NGSOC Solutions and other Security Solutions and Services) Uptime (Individual systems at DC/ DR)	Penalties/ Liquidated Damages	Penalty will not be applicable, if the down time is caused due to any Bank dependency or planned and approved downtime. However, the bidder shall work in tandem with Bank and its existing System Integrator (SI) to resolve such issues and make the solution up & running. Above LD is applicable for the following solutions SIEM, SOAR, UEBA, EDR, PIM, Anti-DDoS, Anti -APT and for other NG SOC solutions/services minimum uptime of 90 percent to be maintained, else flat 20% of monthly NGSOC operations charges will be levied	Seeking relaxation on penalty clause, to be capped at 10% of the monthly charges	Bidder to refer Corrigendum-2.
231	24	Manpower services	Penalties/ Liquidated Damages	However, total penalty under this will be limited to 20% of the total charges payable for Resource charges for the monthly payout.	Seeking relaxation on penalty clause, to be capped at 10% of the monthly charges	Bidder to refer Corrigendum-2.
232	73	Pre-Qualification Criteria	Qualification criteria - OEM	OEM should have provided on- prem SIEM solution should have been implemented at least 1,00,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids .	seeking relaxation to 70K ePS for both	Bidder to refer Corrigendum-2.
233	38	Section D - Bid Process	Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD	6.1.The bidder shall furnish Non interest earning Earnest Money Deposit (EMD) amount as mentioned in the Bid Schedule by way of Demand Draft drawn on any Scheduled Commercial Bank in India in favor of Canara Bank, payable at Bengaluru.	As per the RFP, EMD is exempted only for MSEs and start-ups. However, as per GeM, we are also exempted from EMD submission. Please confirm if GeM would supercede RFP clause or the bidder has to submit EMD as per RFP?	Bidder to comply with RFP terms and conditions
234	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.3	PO to Bidder	Will customer issue different POs for different services or a single PO for all services?	Single PO.
235	17	Penalties/ Liquidated Damages	6.19	All the above liquidated damages are independent of each other and are applicable separately and concurrently	Request to cap overall liquidated damages to 5% of the PO value	Bidder to comply with RFP terms and conditions.
236	21	Penalties/ Liquidated Damages	6.4.Penalty on Service levels during Operations phase		Request to cap overall project penalties to 10% of the quarterly payout	Bidder to comply with RFP terms and conditions.
237	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.3 Project Timeline	1.3.Bidders are requested to keep the following timelines (module wise) in regard to the implementation of solutions. T denotes the date of acceptance of the PO to the bidder, for example: T+ No. of weeks represents that the solution needs to be implemented within No of weeks from the date of acceptance of the PO.	As this is migration project from existing CSOC to NGSOC environment & many devices will not have dual forwarding and also there should not be any impact on existing environment, we request to extend the timeline from T+37 weeks to T+54 weeks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
238	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.3 Project Timeline	PIM & All other solutions	As its migration from existing solution T+24 weeks timeline is less. Request to make it T+36 weeks minimum.	Bidder to comply with RFP terms and conditions.
239	130	TIF	Threat Intelligence Platform (TIP)	The Bidder will be responsible for onboard internal and external threat intelligence feeds such as open-source, commercial, government, etc. Bank shall provide the commercial TI feed API to consume.	Please clarify if there is a requirement for any new commercials feed or we can use the current commercial feed from the bank	Bidder to comply with RFP terms and conditions.
240	24	6.9	6.9.Penalties/Liquidated damages on failure to resolve incidents like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents)	Resolution time Within 480 minutes 480 to < 540 minutes 540 to < 600 minutes	Please clarify if Resolution SLA will be part of all SOC security incident, request to change the resolution SLA clause for spcific service not for all the SOC security incidents.	Bidder to comply with RFP terms and conditions.
241	15	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.3 Project Timeline	Hardware Delivery Timeline	Request you to increase Hardware delivery timeline from T+8 weeks to T+12 weeks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
242	33	17. Right to Audit	17. Right to Audit	17.1The selected bidder has to get itself annually audited by internal/ external empanelled Auditors appointed by the Bank/inspecting official from the Reserve Bank of India or any regulatory authority, covering the risk parameters finalized by the Bank /such auditors in the areas of products (IT hardware/software) and services etc., provided to the Bank and the selected bidder is required to submit such certification by such Auditors to the Bank. The selected bidder and or his/their outsourced agents/subcontractors (if allowed by the Bank) shall facilitate the same. The Bank can make its expert assessment on the efficiency and effectiveness of the security, control, risk management, governance system and process created by the selected bidder. The selected bidder shall, whenever required by the Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the Bank. 17.2Where any deficiency has been observed during audit of the selected bidder on the risk parameters finalized by the Bank or in the certification submitted by the Auditors, the selected bidder shall correct/resolve the same at the earliest and shall provide all necessary documents related to resolution thereof and the auditor shall further certify in respect of resolution of the deficiencies. The resolution provided by the selected bidder shall require to be certified by the Auditors covering the respective risk parameters against which such deficiencies have been observed. 17.3The selected bidder shall, whenever required by the	Bidder's suggestion - Frequency of audit shall be once per year upon giving a thirty (30) days prior written notice to the Bidder.All partner/vendor-initiated audit costs to be borne by partner/vendor. Bidder does not allow it partner/vendor to execute tools or run scripts in its infrastructure.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
243	49	Part E - 12. Order Cancellation/Termination of Contract	12. Order Cancellation/Termination of Contract	12.1.The Bank reserves its right to cancel the entire / unexecuted part of the Purchase Order at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions: 12.1.1.Delay in delivery beyond the specified period for delivery. 12.1.2.Serious discrepancies noted in the items delivered. 12.1.3.Breaches in the terms and conditions of the Order. 12.1.4.Non submission of acceptance of order within 7 days of order. 12.1.5.Excessive delay in execution of order placed by the Bank. 12.1.6.The Vendor/Service Provider commits a breach of any of the terms and conditions of the bid. 12.1.7.The Vendor/Service Provider goes in to liquidation voluntarily or otherwise. 12.1.8.An attachment is levied or continues to be levied for a period of 7 days upon the effects of the bid. 12.1.9.The progress made by the Vendor/Service Provider is found to be unsatisfactory. 12.1.10.If deductions on account of liquidated Damages exceeds more than 10% of the total contract price. 12.1.11.If found blacklisted by any Govt. Department / PSU / other Banks / CERT-In, during the course of contracted	Request to cap the total liability to previous 12 months of billing or 10% of the PO value	Bidder to comply with RFP terms and conditions.
244	53	Section G: General Terms and conditions 6. Inspection of Records		Bank at its discretion may verify the accounts and records or appoint third party for verification including an auditor for audit of accounts and records including Hardware, Software & other items provided to the Bank under this RFP and the selected bidder shall extend all cooperation in this regard.	The bidder can audit the transactions related to this contract subject to 2 weeks prior notice before the commencement of audit and also we can support for audit 1 year from the end of the contract.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
245	54	Section G: General Terms and conditions 12. Intellectual Property Rights	12. Intellectual Property Rights	12.1.Bidder warrants that the inputs provided shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. Bidder warrants that the deliverables shall not infringe upon any third party intellectual property rights, including copyrights, patents and other intellectual property rights of any nature whatsoever. The bidder should ensure that the Hardware and Software supplied to the Bank shall not infringe the third party intellectual property rights, if any. The bidder has to ensure that third party rights are not infringed even in case of equipment /software supplied on behalf of consortium as bidder. 12.2.In the event that the Deliverables become the subject of claim of violation or infringement of a third party's intellectual property rights, bidder shall at its choice and expense: [a] procure for Bank the right to continue to use such deliverables; [b] replace or modify such deliverables to make them non-infringing, provided that the same function is performed by the replacement or modified deliverables as the infringing deliverables; or [c] if the rights to use cannot be procured or the deliverables cannot be replaced or modified, accept the return of the deliverables and reimburse bank for any amounts paid to bidder for such deliverables, along with the replacement costs incurred by Bank for procuring an equivalent equipment in addition to	NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR (A) ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR (B) ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, LOSS OF DATA, INTERFERENCE WITH BUSINESS OR COST OF PURCHASING REPLACEMENT SERVICES, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE CUSTOMER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

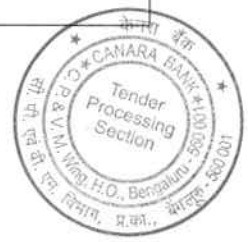
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
246	58	Section G: General Terms and conditions 22 - Indemnity	22 - Indemnity	22.1.The BIDDER/VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of: 22.1.1.The breach, default or non-performance of undertakings, warranties, covenants or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER; 22.1.2.Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements by the BIDDER/VENDOR/ SERVICE PROVIDER; 22.1.3.Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER. 22.2.The BIDDER/VENDOR/ SERVICE PROVIDER shall indemnify, protect and save the Bank against all claims, losses, costs, damages, expenses, action, suits and other proceedings, resulting from infringement of any law pertaining to patent, trademarks, copyrights etc. or such other statutory infringements in respect of service provided by them. 22.3.All Employees engaged by the BIDDER/VENDOR/ SERVICE PROVIDER shall be in sole employment of the	NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR (A) ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR (B) ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, LOSS OF DATA, INTERFERENCE WITH BUSINESS OR COST OF PURCHASING REPLACEMENT SERVICES, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE CUSTOMER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY.	Bidder to comply with RFP terms and conditions.
247	60	25.Force Majeure	25.Force Majeure	23.3.In the event of any such intervening Force Majeure, the selected bidder shall notify the Bank in writing of such circumstances and the cause thereof immediately within five calendar days. Unless otherwise directed by the Bank, the selected bidder shall continue to perform / render / discharge other obligations as far as they can reasonably be attended / fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure. 23.4.In such a case, the time for performance shall be extended by a period (s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the Bank and the selected bidder shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding above, the decision of the Bank shall be final and binding on the selected bidder	Bidder's suggestion: Force Majeure to be a mutual right for both Parties. In case any event of Force Majeure continbues for a period of three (03) months, either party shall have the right to terminate the agreement upon notice to the other party without any obligations to each other, except for the payment obligations of the customer / Bank for the work done till the date of such termination.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
248	64	33.Resolution of Disputes	33.Resolution of Disputes	All disputes and differences of any kind whatsoever, arising out of or in connection with this Contract or in the discharge of any obligation arising under this Contract (whether during the course of execution of the order or after completion and whether beyond or after termination, abandonment or breach of the Agreement) shall be resolved amicably. In case of failure to resolve the disputes and differences amicably the matter may be referred to a sole arbitrator mutually agreed upon after issue of at least 30 days' notice in writing to the other party clearly setting out there-in the specific disputes. In the event of parties failing to consent upon a single arbitrator than BOTH PARTIES shall approach Court of Law for the appointment of sole arbitrator as provided under the Arbitration and Conciliation Act 1996.Place of Arbitration shall be Bengaluru, INDIA which will be governed by Indian Arbitration and Conciliation Act 1996. Proceedings of Arbitration shall be conducted in English language only	We propose the place of arbitration to be either Delhi or Mumbai	Bidder to comply with RFP terms and conditions.
249	64	34.Legal Disputes and Jurisdiction of the court	34.Legal Disputes and Jurisdiction of the court	34.1.The Bank Clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain bidder/prospective bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages. 34.2.All disputes and controversies between Bank and bidder shall be subject to the exclusive jurisdiction of the courts in Bengaluru and the parties agree to submit themselves to the jurisdiction of such court as this RFP/Contract agreement shall be governed by the laws of India	We propose the place of jurisdiction of courts to be either Delhi or Mumbai	Bidder to comply with RFP terms and conditions.
250	GeM GTC 4.0 V 1.14	15		Extension of Delivery Period and Liquidated Damages	iv. Force Majeure Conditions - We propose extension of the force majeure condition period from 10 days to 60 days before terminating the contract by either parties	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
251	GeM GTC 4.0 V 1.14	18		Limitation of Liability	We propose the following clause to replace the current clause "NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR (A) ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR (B) ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, LOSS OF DATA, INTERFERENCE WITH BUSINESS OR COST OF PURCHASING REPLACEMENT SERVICES, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE CUSTOMER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY. "	Bidder to comply with RFP terms and conditions.
252	GeM GTC 4.0 V 1.14	19		Termination for Default	Customer may terminate only in case of material breach by the Bidder and in case Bidder fails to rectify the breach within 60 days of written notice from the Customer. Further, Bidder proposes to have mutual right for terminating the contract for material breach or default of Customer such as non-payment as per the contract terms etc.	Bidder to comply with RFP terms and conditions.
253	110	7	The Bidder is responsible to close all the Audit, VAPT and assessment observations of NG SOC solutions conducted by Bank in timely manner.	Scope of Work for Bidder/ System Integrator (SI)	Audit points will be closed only for new NGSOC setup and not being carried forward from existing solution	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
254	252	Commercial Format	Minimum resources 42 with L1-14, L2-16, L3 -11 and PM-1	Details of Manpower asked in Commercial Format	The Count of resources mentioned is not matching with Clause 6 of RFP Page 95 Manpower details. 1. As per this table Resource Needed at DC and DR locations but during calculation it is taken only for DC site. 2. If we calculate the ask in table total resource comes as minimum 58 with L1- 28, L2-17, L3-12, PM-1 3. Missing resource as per Scope of RFP is overall Structure are: a. SOC infra managmenta nd monitoring b. Threat Intel c. PCAP d. ITSM Requesting to relook the resources asked in RFP vs. Scope defined and provide clear Breakup of resource needed at DC and DR Locations with all technologies covered.	Bidder to refer Corrigendum-2.
255	NA	Genral	RFP looking forward 6 days working resources across Towers	NA	All Corporates follow 5 working days. Request to provide resource count based on 5 days working concept insteadf 6 days working atleast for L2, L3 and PM. Above mentioned resource count will change accordingly.	Bidder to comply with RFP terms and conditions.
256	165	SIEM	SIEM 8	Technical Specification	SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and Cloud). Kindly let us know expected number of custom parser to be planned.	Bidder/OEM needs to provide custom parser in case of non-availability of out-of-box Cloud integrations.
257	120	12.Scope of Work for Proposed Solutions	I.Security Information & Event Management (SIEM)	•Bidder should develop parsers for all log sources without any cost to the Bank. •Bidder should develop parsers for non-standard logs in the ongoing operations phase, Bidder team deputed onsite will be expected to develop parsers for non-standard logs required during the ongoing operations phase without any cost to the Bank.	If the parser is not available the bidder/ OEM should developed the parsers without any extra cost to bank.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
258	174	SIEM Packet Capture	Packet Capture #135	The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.	The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation.	Bidder to comply with RFP terms and conditions.
259	174	SIEM Packet Capture	Packet Capture #135	The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.	The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract. Should we be procuring 20 Gbps hardware from day one	Yes
260	94	Platform Management		Manpower Requirement	Platform management - Manpower requirement : SIEM, SOAR, & UEBA Engineer (L3 OEM) - Reuest you to change "Bidder/OEM Engineer"	Bidder to comply with RFP terms and conditions.
261	175	SOAR	General Requirement	Technical Specification	All the hardware/software required for the solution shall be provisioned by the OEM - Request to change "All the hardware/software required for the solution shall be provisioned by the Bidder"	Bidder to refer Corrigendum-2.
262	84	2. Scope of work	i. under Scope of work	Managing reporting and logging of security alerts /incidents through ticketing tools and closing the same as per the agreed SLA.	Any existing ticket tool to be used or new ticketing tool to factor?	Bidder to refer Corrigendum-2.
263	85	2. Scope of work	n. under Scope of work	Provide immediate forensic support in case of any security / cyber incident.	is forensic sservice requested here is on-demand service requirements with additional commercials or it needs to include as part of deliverable. If this is not on-demand, what is the maximum forensic efforts hour to consider.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
264	112	7. Scope of Work for Bidder/ System Integrator (SI)	7. Scope of Work for Bidder/ System Integrator (SI)	Wherever Bank has provided VMs/physical servers/storage for installation of OS/DB/middleware/application component for proposed SOC solutions, it is the responsibility of the Bidder to perform end to end maintenance, support, upgrade etc. in line with the comprehensive scope.	Hope the bare metal, VM level will be taken care by bank and only application level to be taken care by bidder. please confirm.	Bidder to comply with RFP terms and conditions.
265	190	EDR	16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Considering SIEM will collect the alert/threat data from EDR as well as UEBA, requesting bank to read the point as "The proposed EDR should integrate with SIEMv solution for better co-relation among different security controls."	Clause stands deleted. Bidder to refer Corrigendum-2.
266	192	EDR	39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Every OEM has their own nomenclature to define threat categories. Requesting bank to generalise the threat categories to the below general definition: 1) Ransomware 2) Cryptominer 3) Trojans 4) PUA 5) Infostealer 6) Rootkit 7) Spyware 8) Virus 9) Hacktools 10) Exploits 11) Backdoor 12) Adware 13) Malware 14) Malicious Macro	Bidder to comply with RFP terms and conditions.
267	197	EDR	88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Once a rogue device is discovered by the EDR platform it is recommended for an administrator to validate the asset and then deploy the OS specific agent (windows,macOS & linux). Requesting the bank to read the point as "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them"	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
268	198	EDR	121	The solution should support Endpoint Security Solution infrastructure i.e., management and administration console of Endpoint Security Solution on Virtual environment of Bank or alternatively vendor should provide scalable hardware/ infrastructure supplied for implementation of overall ESS Solution within the overall cost for the entire contract period.	Bank has requested for a SaaS solution and no management component of SaaS solution is required to be installed on-premises.	Clause stands deleted. Bidder to refer Corrigendum-2
269	200	EDR	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	The average file size sent to sandbox for analysis is typically between 5MB and 30MB and these are mostly executable files like".exe", ".dll" or documents such as ".pdf", ".docx". For files of size 1GB the sandbox analysis takes much longer time and can be prone to timeouts leading to missed detections. The extended tme required to analyse large fles can delay incident response and could slow down decision-making process and remediation efforts and potentially miss sophisticated threats. Also having mandated a 1Gb File size Sandbox is specific to an individual OEM , restricting participation of Pure Play best in class EDR / XDR solutions and thus request the Bank below. The point should be read as " The proposed sandboxing component should have the capability to scan the file size upto 50MB".	Bidder to refer Corrigendum-2
270	198	EDR	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Most of the EDR vendors do not support IBM AIX and Solaris operating systems. The point should be read as "The solution should protect all servers, endpoints, physical, virtual, having Windows/Non Windows systems (Windows 10 and above, Windows Server 2000 and above, RHEL, Oracle Linux, Ubuntu, CentOS, Suse Linux etc.). The solution should protect all latest and upcoming/upgraded OS in Bank's IT ecosystem during the contract period.	Bidder to refer Corrigendum-2
271	163	Section 18	Project Implementation Team	OEMs shall also provide on-site resources at each deployment location for their respective solutions during the implementation phase. The OEM officials will be responsible for: •Validation of solution design and architecture •Continuous monitoring of implementation at each location •Provide Subject Matter Expertise support to working teams. •Ensure customization is in line with bank's requirements.	Please confirm if bidder is allowed to implement infrastructure solution using Bidder staff (or) is OEM resources is mandatory. Also please confirm if infrastructure services can be implemented from Bidder office through remote connection or deployment from bank premises is mandatory.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
272	165	Section 1	Technical Specification of each solution - Security Incident and Event Management (SIEM)	The proposed solution must support the data replication /dual forwarding without relying on other third-party replication technologies on the operating system or storage level with near zero RPO & RTO. It should also admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	In this section it is stated DR should always be active. However in Section 5.3 (Page 19-Uptime) it is specified Active Passive setup (DC active and DR Passive). Please confirm if DC DR should be active-active or Active Passive setup.	Bidder to note that for SIEM , DC-DR is Active-Active Setup.
273	NA	Generic	N/A	N/A	Will Bank provide necessary equipment Racks with adequate power within their on-premise Primary and DR Data Centers. Or should bidder propose the Racks and Bank will provide only the space to place the rack and the power supply for the racks. Please confirm.	Bank will provide adequate racks and power for Server Stacking.
274	NA	Generic	N/A	N/A	Should bidder consider the necessary network links between DC and DR for replication traffic (or) should bidder leverage existing network links between these sites. If later is the approach to be followed please share the type of link and link bandwidth available between DC and DR Sites.	Bank will provide Network Links
275	16	Section C	Project Timelines	Delivery of all the equipment as quoted in the bill of materials for EDR Solution. T+4 weeks	Delivery of equipments T+4 Weeks can this be extended to 8 weeks	Bidder to comply with RFP terms and conditions.
276	22	Section 6.4	Penalty on Service Levels during Operations phase	Response of the incidents is depicted as per the Bank's SLA defined below: Severity Response Turnaround Time (TAT) Critical 10 mins High20 mins Medium60 mins Low180 mins	Incident response Service Level expections provided in this section, does it apply to Infrastructure Day2 management as well. If not please share the Service Level requirements to be complied for Infrastructure Day2 management for various levels (P1, P2, P3)	Bidder to note that it is applicable for NGSOC Security incidents.
277	95	Section 5	Manpower requirement		This section does not call out any resource roles specific to Infrastructure management. Is it correct to assume that bidder can propose their resource head count for infra management.	Yes, Bidder to comply with RFP terms and conditions.
278	96	Section 4	Responsibility Matrix		This section does not call out any activities with respect to Infrastructure Implementation or Infra Day2 Management. Is it correct to assume that Bidder will be responsible for the entire Infrastructure Day1 Implementation activities and Day2 activities	Yes, Bidder to comply with RFP terms and conditions.
279	253	12	Annexure-10 Technical Evaluation Criteria	SOAR - 5 certified OEM resource	Request for relaxation on separate SOAR certification for OEM Resource	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
280	202	9	III User Entity Behavioral Analysis (UEBA):	The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage custom data models if necessary	Request to relaxation on Artificial Intelligence in UEBA model	Bidder to refer Corrigendum-2
281	195	17	Security Orchestration and Automation (SOAR):	AI Capabilities:a. Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc.	Request to relaxation on Artificial Intelligence in SOAR model	Bidder to refer Corrigendum-2
282	26	7	Payment Terms for Hardware	HW Cost: Delivery (30%) + Installation (40%) +Training (20%) + Post warranty (10%)	Request to amend as below: HW Cost: Delivery (70%) + Installation (25%) +Training (5%) + Post warranty (0%)	Bidder to comply with RFP terms and conditions
283	26	7	Payment Terms for Hardware	One time implementation: UAT (30%)+ DC DR Go Live (55%) +DR Drill (10%) + NG SOC Implementation (5%)	Request to amend as: UAT (70%)+ DC DR Go Live (25%) +DR Drill (5%) + NG SOC Implementation (5%)	Bidder to comply with RFP terms and conditions.
284	26	7	Payment Terms for Hardware	AMC/ATS Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	Request to amend the payment term as Annual in advance for AMC/ ATS	Bidder to comply with RFP terms and conditions
285	27	7	Payment Terms for Services	NGSOC: Payment shall be released quarterly in arrears after completion of implementation of the SOC Services mentioned in the RFP and acceptance of the same by the Bank Officials for the respective Assignment.	Request to change the payment term to monthly arrears	Bidder to comply with RFP terms and conditions
286	53	7	Negligence	Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions
287	279	10.1	ORDER CANCELLATION/TERMINATION OF CONTRACT	Bank shall serve the notice of termination to the Vendor/Service Provider at least 30 days prior, of its intention to terminate services	Request to change the notice period of termination to 180 days	Bidder to comply with RFP terms and conditions.
288	279	10.2	ORDER CANCELLATION/TERMINATION OF CONTRACT	10.2.The Bank reserves its right to cancel the entire / unexecuted part of CONTRACT at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions	Request to grant cure period of 180 days	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
289	279	10.3	ORDER CANCELLATION/TERMINATION OF CONTRACT	10.3.In case the Vendor/Service Provider fails to deliver the quantity as stipulated in the delivery schedule, the Bank reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility of the Vendor/Service Provider by giving 7 days' prior notice to the Vendor/Service Provider.	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions.
290	279	10.4	ORDER CANCELLATION/TERMINATION OF CONTRACT	10.4.After the award of the contract, if the Vendor/Service Provider does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one months' notice for the same	Request to grant cure period of 180 days	Bidder to comply with RFP terms and conditions.
291	280	10.7	ORDER CANCELLATION/TERMINATION OF CONTRACT	Notwithstanding anything contained hereinabove, the Bank may terminate this contract by giving a 30 day's notice without assigning any cause.	Request to change the notice period of termination to 180 days	Bidder to comply with RFP terms and conditions.
292	25	6.14	Penalties/ Liquidated Damages	6.14.If any act or failure by the selected bidder under the agreement results in failure or inoperability of systems and if the Bank has to take corrective actions, to ensure functionality of its property, the Bank reserves the right to impose penalty, which may be equal to the cost it incurs or the loss it suffers for such failures.	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions
293	25	6.15	Penalties/ Liquidated Damages	6.15.If the selected bidder fails to complete the due performance of the contract in accordance with the specification and conditions of the offer document, the Bank reserves the right either to cancel the order or to recover a suitable amount as deemed reasonable as Penalty/ Liquidated Damage for non-performance.	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions
294	25	6.16	Penalties/ Liquidated Damages	6.16.Any financial loss to the Bank on account of fraud taking place due to selected bidder, its employee or their services provider's negligence shall be recoverable from the selected bidder along with damages if any with regard to the Bank's reputation and goodwill.	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions
295	20	6.17	Penalties/ Liquidated Damages	6.17.Bank may impose penalty to the extent of damage to its any equipment, if the damage was due to the actions attributable to the staff of the selected bidder	Request to cap all liabilities to previous 12 months billing or 10% of the PO value	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
296	71	Annexure-2	Pre-Qualification Criteria	Additional query	We request the bank to ask for atleast one reference on SaaS EDR implementation along with sign off since last 5 years in one PSU BFSI in India. Or atleast One reference of OEM with 85K nodes in a PSU bank in India. This will help canara bank to get such OEM who have a track record of performing and protecting a bank of canara bank size. This clause will ensure Quality OEM will participate in the RFP.	Bidder to comply with RFP terms and conditions.
297		Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5.End point is a complext project to deploy, its even more complex in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder allignment who have demonstrated a smooth deployment and sustance in such large environment in BFSI in India. This will make the bidder to allign with such OEM's who have a track record of protecting such large environment. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an oppertunity to evalute Bidder capability or allow bidder to allign with such bidders who have great track record in BFSI in India. hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5.	Bidder to comply with RFP terms and conditions.
298	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
299	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-2.
300	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-2.
301	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

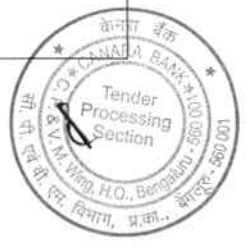
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
302	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-2.
303	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-2.
304	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
305	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2.
306	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-2.
307	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-2.
308	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2.
309	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
310	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
311	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
312	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
313		Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
314	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2.
315	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
316	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-2.
317	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

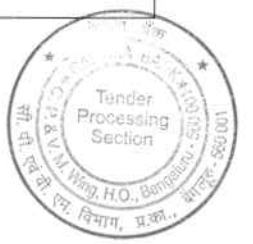
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
318	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
319	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
320	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
321	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
322	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2.
323	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-2.
324	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2.
325	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-2.
326	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
327	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
328	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-2.
329	24	6.9.	Penalties/Liquidated damages on failure to resolve incidents like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents)	The selected bidder should resolve the incidents reported. The selected bidder shall be -liable to pay Liquidated damages at the rates specified below subject to a cap of 20% of quarterly payment of in scope service. Resolution time Penalty Amount Within 480 minutes No Penalty 480 to < 540 minutes 3.00% on Basic invoice value of Quarterly payment 540 to < 600 minutes 5.00% on Basic invoice value of Quarterly payment	We request removal of this clause as resolution may involve takedown or assistance from Bank's internal teams to validate/isolate/patch issues that are identified. This SLA is unreasonable given dependencies.	Bidder to comply with RFP terms and conditions.
330	24	6.10.	Penalties/Liquidated damages of delay in Takedown of phishing sites specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.50 per takedown More than 48 hours, but less than 72 hours Rs.100 per takedown More than 72 hours Rs. 150 per takedown	We request modification of the same as - More than 48 hours, but less than 72 hours Rs.50 per takedown More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours Rs. 150 per takedown	Bidder to comply with RFP terms and conditions.
331	25	6.11.	Penalties/Liquidated damages of delay in Takedown of fraudulent mobile/Web apps specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.100 per takedown More than 48 hours, but less than 72 hours Rs.500 per takedown More than 72 hours Rs. 1000 per takedown	We request modification of the same as - More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours, but less than 168 hours Rs.500 per takedown More than 168 hours Rs. 1000 per takedown	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
332	25	6.12.	Penalties/Liquidated damages of failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	A genuine act of defacement on Bank's websites should be detected within 15 minutes of the incident. Penalty at the rate of 10% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 15 minutes but less than 1 hour. In case of response time more than 1 hour the penalty at the rate of 20% of quarterly payment of website scanning services will be charged. If the response time is more than 24 hrs, penalty at the rate of 100% of quarterly payment of website scanning services will be charged.	We request modification as - A genuine act of defacement on Bank's websites should be detected within 4 hours of the incident. Penalty at the rate of 1% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 4 hours but less than 6 hours. In case of response time more than 6 hours the penalty at the rate of 2% of quarterly payment of website scanning services will be charged. If the detection time is more than 24 hrs, penalty at the rate of 5% of quarterly payment of website scanning services will be charged. The Total Penalty levied cannot exceed 10% of the Quarterly Payment (Pro-Rata) for the tool.	Bidder to refer Corrigendum-2.
333	28	7.2.2.	Payment Terms for Services	Payment shall be released quarterly in arrears after completion of implementation of the SOC Services mentioned in the RFP and acceptance of the same by the Bank Officials for the respective Assignment.	We request modification to - Payment shall be released yearly in advance after completion of implementation of the Tool. Additionally, the subscription Date starting from the date of implementation and acceptance by the Bank).	Bidder to comply with RFP terms and conditions
334	146	(i)	Early Phishing Detection	Monitoring spam traps to detect phishing mails.	This is a email security tool capability. Canara Bank would be have subscribed to a dedicated e-mail security solution that covers Spam Traps use case. Today, there are several techniques used by spammer/defrauders that evade Spam Traps like using Spam Trap detection services (ex. www.zerobounce.net). We request this clause to be removed as it is an ineffective method to detect phishing campaigns. Monitoring Typo-squatted domain reginstrations, Monitoring Social Media platforms/Darkweb discussions, IRCs (Telegram/Discord) for any targetted phishing campaigns and blocking indicators associated with phishing infrastructure is a much effective way to defend phishing campaigns.	Clause stands deleted. Bidder to refer Corrigendum-2.
335	148	(m)	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:	Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	There is no legally obliged entity hosting forums and content on the dark web. Owing to this, there is no takedown possible of Dark Web Mentions or data leaks. We request the bank to remove this clause.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
336	149	(c)	Brand Protection and Monitoring:	Search engines (like Google, Yahoo, Bing etc.) and Generative AI (like chat GPT, Open AI, Gemini etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including but not limited to Truecaller and JustDial.	Kindly elaborate Generative AI monitoring scope. As Generative AI LLMs are trained on specific datasets and are susceptible to poisoning as well. The technology is still in the early days and each Generative AI platform provides unique answers. We request this to be removed from the scope as there isn't a reliable method to monitor GenAI platforms. Tracking of Branch Addresses when the Bank has over 9,000+ branches is not technically feasible and Google Maps enables any user to place a location marker and register a business. Post merger with Syndicate Bank, there are thousands of Canara Bank's Nitya Nidhi Deposit (NND) Scheme Collection agents who would have registered their business. An army of manual analysts would be needed to verify and takedown these addresses. This use case is challenging to address and beyond automation or AI capabilities to monitor.	Bidder to comply with RFP terms and conditions.
337	150	(c)	Attack Surface Monitoring:	The proposed solution shall identify potentially orphaned applications, and services.	We seek clarity from the Bank if "Orphaned applications" refers to shadow IT or dangling DNS records.	Bidder to comply with RFP terms and conditions.
338	151	(q)	Attack Surface Monitoring:	The proposed solution shall be able to validate the Current IP attribution is using DNS, Netblock, and Keywords to improve accuracy.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
339	151	(t)	Attack Surface Monitoring:	The proposed solution shall be able to do Active Banner Grabbing and advanced search based on banners to detect any vulnerable version and provide reports as mentioned earlier.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
340	151	(w)	Attack Surface Monitoring:	The proposed solution shall be able to perform Network-level Risk scanning to identify misconfigured servers, services, and devices.	We request the Bank to define "devices".	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
341	153	c)	Other Services & Requirements:	The solution shall provide correlation capability and actionable intelligence with respect to historical reference to threats.	We request the Bank to elaborate the use case.	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
342	154	b)	Service Level Agreements	Alert within 20 minutes of attack/compromise/down/not reachable.	This is a WAF/IPS/IDS/SIEM/Application Monitoring/EDR/MDR/NAC use case. We request the same to be removed from the scope.	Bidder to comply with RFP terms and conditions.
343	154	d)	Service Level Agreements	Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident and fraudulent mobile apps within 24 hours.	We request this to be modified to - Take down of Phishing Site within 48 hours of detection and fraudulent mobile apps within 72 hours.	Bidder to refer Corrigendum-2
344	154	f)	Service Level Agreements	Resolution of Trojan incidents with 24 hrs of detection.	This scope is beyond the scope of Threat Intelligence Services. We can alert of any Trojan Incident leading to data leak and it being available on the Dark Web or Freemium/Premium portals/marketplaces.	Clause stands deleted. Bidder to refer Corrigendum-2
345	143		Propose Addition of Clause		As a Best Practice - we suggest the Threat Intelligence Platform and Threat Intelligence Services to be subscribed from different OEMs/Vendors. Several Indian Government entities/PSUs have adopted this approach for better coverage.	Bidder to comply with RFP terms and conditions.
346	263		DDoS Drill	Number of test cases: 10 minimum	Please clarify if the test cases will be defined by the bank or can we consider the best test cases as per the trend by the service provider.	Bidder to suggest and the same will be defined based on Mutual aggrement.
347	142	14. SoW for Proposed Services - Threat Inteligence Services - Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage		Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Bidder to comply with RFP terms and conditions.
348	145	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/ tools/ exchange knowledge for banks brand		Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
349	146	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank: - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.		Kindly elaborate the scope.	Bidder to refer Corrigendum-2
350	174	PCAP / Technical Specification	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	The current technical specifications appear to reference the ingestion of logs, which is not directly relevant to packet capture (PCAP) solutions. For PCAP systems, only packet data and metadata related to ingested packets are applicable. We respectfully request that the specification be revised as follows to better reflect the requirements of a PCAP system: "The proposed Packet capture solution shall have capabilities to integrate with the proposed SIEM solution in both DC and DR. The OEM shall have the capacity to capture traffic at 10 Gbps and retain packet-like data and associated metadata for 7 days. Adequate storage shall be provisioned accordingly. The PCAP solution should also support both automated and manual mechanisms for selectively discarding, masking, or filtering packets based on their security relevance (e.g., customer PII, SPDI, or other classified information as per the Bank or Regulatory guidelines), to optimize storage.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
351	174	PCAP / Technical Specification	The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance with minimum 4 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 2*1/10G management port.	The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance with minimum 4 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 2*1/10G management port.	We propose the use of a Network Packet Broker to ingest traffic from multiple vantage points with various port configurations. To better reflect this approach, we respectfully request revising the clause as follows: "The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/outflow of data in the DC. The proposed solution should be a dedicated hardware with 4 X 10 Gig SFP+ and 2 X 1/10G management ports. For environments requiring traffic capture from more than four vantage points, a dedicated Network Packet Broker should be proposed." This revision allows for more flexibility in network design and ensures effective capture across multiple vantage points without compromising performance or expandability.	Bidder to refer Corrigendum-2.
352	174	PCAP / Technical Specification	The proposed packet capture solution should be a dedicated Hardware appliance, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports	The proposed packet capture solution should be a dedicated Hardware appliance, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports	Kindly consider the suggested points to secure enough storage on the proposed hardware: "The proposed packet capture solution should be a dedicated Hardware, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the dedicated hardware and the storage should utilize Self-Encrypting Drives (SED). Should have required OEM approved storage to scale upto 20Gbps throughput without the need to integrate with other storage solutions".	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
353	175	PCAP / Technical Specification	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should be a native feature of SIEM for sharing of network data (Packet + Meta data) in real time .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should be a native feature of SIEM for sharing of network data (Packet + Meta data) in real time .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	Given the critical need to protect customer privacy, particularly with respect to Personally Identifiable Information (PII), Sensitive Personal Data or Information (SPDI), and other classified information, we recommend limiting payload data capture to only suspicious and malicious traffic. This approach ensures that sensitive data is not unnecessarily captured and stored, aligning with privacy regulations and best practices. We respectfully request revising the clause as follows: "The proposed packet capture solution should be able to perform real-time monitoring and network traffic analysis to identify threats. The solution should feature Deep Packet Inspection (DPI) to provide visibility into all layers of the OSI stack (L2 to L7), including application payload data, but only for suspicious and malicious traffic. The solution should create indexes for payload objects as required and not just rely on header information." Additionally, the solution should provide network traffic insights by: a. Classifying protocols and applications b. Performing deep-packet inspection c. Supporting cross-correlation for analysis and aggregation d. Reconstructing sessions and analyzing artifacts e. Previewing artifacts and malicious attachments	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
354	175	PCAP / Technical Specification	Solution should provide meaningful artefacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files from Deep packet Inspection. Post reconstruction, solution should be able to do object extractions from sessions like pcaps, zip files, office documents, media, embedded malicious attachments etc.	Solution should provide meaningful artefacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files from Deep packet Inspection. Post reconstruction, solution should be able to do object extractions from sessions like pcaps, zip files, office documents, media, embedded malicious attachments etc.	In consideration of maintaining customer privacy and safeguarding Personally Identifiable Information (PII), Sensitive Personal Data Information (SPDI), and any classified information, we propose a modification to the specifications regarding payload data capture. We request that the requirement for comprehensive payload data capture for all traffic be adjusted to only include the storage of payloads associated with suspicious or malicious traffic for further analysis. We recommend rephrasing the specification as follows: "The solution should provide meaningful artifacts such as FTP data files, JavaScript, and .Net files derived from Deep Packet Inspection. After reconstruction, the solution should be capable of performing object extractions from sessions, including PCAPs, zip files, office documents, media files, and embedded malicious attachments." This amendment will help ensure compliance with privacy regulations while still delivering the necessary analytical capabilities.	Bidder to comply as per GeM Bid/ RFP terms and conditions.
355	175	PCAP / Technical Specification	The solution should have the capability to extract data/ files from the captured network packets	The solution should have the capability to extract data/ files from the captured network packets	We propose the following modification to enhance the specification: "The solution should possess the capability to extract data / malicious files from the captured network packets. Additionally, the solution should include the functionality for comprehensive host investigations, as well as session and packet analysis on the captured packets and any generated alerts." This revision ensures that the solution not only extracts relevant data but also provides crucial investigative capabilities that are essential for effective threat analysis.	Bidder to refer Corrigendum-2
356	175	PCAP / Technical Specification	The solution should have the functionality to reconstruct and replay the network packets which will help to identify the entire transaction	The solution should have the functionality to reconstruct and replay the network packets which will help to identify the entire transaction	We recommend the following modification to the specification: "The solution should have the functionality to reconstruct or complete packet analysis or replay the network packets which will help to identify the entire transaction." This adjustment underscores the importance of all three capabilities for a thorough understanding of network interactions and transaction integrity.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
357	124		PCAP	Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload &header as well (like TLS 1.3) etc.	We recommend the following modification to the specification: "Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload & header as well".	Bidder to refer Corrigendum-2
358	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		We strongly recommend that the bank insists on a dedicated solution that fully delivers all PCAP specifications and use cases outlined above. It is crucial to note that PCAP is inherently resource-intensive, requiring significant processing power, storage, and management capabilities. By integrating PCAP functionality as a subset of a Security Information and Event Management (SIEM) system or any other solution, the bank risks diluting the effectiveness and performance of both systems. Advantages of a Dedicated PCAP Solution: 1. Optimal Performance: A dedicated PCAP solution ensures that the capture, storage, and analysis of packet data occur without interference from other applications, leading to more reliable performance. 2. Comprehensive Coverage: Focusing exclusively on PCAP capabilities allows for a more thorough and targeted approach to data capture and incident investigation, enhancing security monitoring. 3. Scalability: Separating the PCAP solution facilitates better scalability, enabling the bank to adapt to growing data needs without compromising the functionality of a combined system. 4. Simplified Management: A dedicated solution streamlines management and maintenance, reducing complexity and	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
359	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		The PCAP solution must be capable of capturing and recording all network packets in full (both header and payload). Additionally, the solution should provide the flexibility to selectively save packet data based on specific applications, protocols, time durations, or a combination of these criteria. This customization is essential for efficiently capturing and analyzing data related to specific events or incidents within the Canara Bank network. For each application traffic flow, the solution should support the following capture options: - Full Packet Capture: Capture the entire packet, including both header and payload information. - Packet Truncation: Capture only a specified portion of the packet, reducing storage requirements while preserving essential data. - Packet Exclusion: Exclude specific packets based on defined criteria, such as application, protocol, or source/destination addresses. - Header-Only Capture: Capture only the packet headers, providing basic information without the full payload.	Bidder to comply with RFP terms and conditions.
360	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		The PCAP solution should be capable of capturing network traffic and flexibility to use tools to read / extract pcap files on the device itself rather than downloading it to local machine. This will ensure that the pcap file irrespective of its size can be opened directly on the device which otherwise requires the file to be downloaded and opened using tools. If the file size is large than 1GB, then the local machine / workstation struggles to open the file. Thus it is essential for the pcap to be opened on solution itself without having to download it for quick forensic investigations, security analysis, and integration with other network-based security tools. The solution should support manual export of captured packets or the ability to forward them to external security systems for further analysis.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
361	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		Given the criticality of real-time threat detection and the need for deep packet analysis, we suggest bank to consider the following requirement: - Zero-Day Threat Detection: The solution must be capable of identifying and mitigating zero-day threats as they emerge, ensuring proactive protection against emerging cyberattacks. - Retrospective Analysis: The system should allow for in-depth examination of captured packets, enabling the extraction of valuable metadata for subsequent analysis by an analytics engine. - Packet Storage and Analysis: The solution must have robust capabilities for storing, extracting, and analyzing packets, providing essential insights for incident response and threat intelligence.	Bidder to comply with RFP terms and conditions.
362	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		Considering the criticality and agility for precise packet retrieval, we request bank to consider the following: - Efficient Indexing and Searching: The solution must have robust indexing and searching capabilities to allow for quick and easy location of specific packets based on a wide range of criteria. - Comprehensive Search Support: The system should support search functionality not only at the network layer (Layer 3 and Layer 4) but also at the application layer (Layer 7), including protocols such as HTTP, DNS, DB, LDAP, and others. - Search Criteria: The solution should support searching based on various criteria, such as time, links, IP addresses, port applications, protocols, and any other relevant attributes.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
363	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		Proposed PCAP tool should have capability to ingest packets from all type of application footprint, On Premise, Public Cloud or Private Cloud, so we request to add this clause. "The PCAP solution should support for capturing and storing data from (but not limited to) multiple network segments, VLANs, network locations, etc. The solution must be capable of supporting Public or Private Cloud infrastructure deployment using industry standard ecosystems. The solution should support deployment into Public Cloud platforms like Amazon Web Services (AWS), Microsoft Azure environments, Google Cloud, etc. The solution should be capable of capturing traffic on Private Cloud, Containers, Dockers & other virtual Infrastructure without the need of third party components. > Microsoft Hyper-V > VMware's ESX, NSX-V & NSX-T > OpenStack > Ubuntu/KVM"	Clause added. Bidder to refer Corrigendum-2.
364	125	PCAP / Technical Specification	Additional Points to Consider for PCAP Solution		We recommend that the requirement for an advanced PCAP solution with real-time threat detection capabilities be included as part of this RFP. The solution should be able to detect and analyze the following incident categories (but not limited to): - Suspicious communication over non-standard ports - Data exfiltration attempts - Command and Control (C2) communications - The use of The Onion Router (TOR) - SSH communication with monitored countries - Privacy VPN usage detection - Reconnaissance activities - Detection of unknown Domain Generation Algorithm (DGA) attacks These capabilities are crucial for ensuring proactive security and effective threat mitigation. We believe incorporating this into the solution requirement will significantly enhance your ability to detect and respond to advanced threats in real-time.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
365	210	VI.Threat Intelligence Platform (TIP)	VI.Threat Intelligence Platform (TIP): - #25	The proposed solution must include a browser extension that can scrape all threat-relevant content from a source web page, including IOCs, actor names, malware names and relevant vulnerabilities, and generate a threat report with all content automatically parsed and included	Request Bank to remove this clause for browser extension.	Clause stands deleted. Bidder to refer Corrigendum-2
366	110	7. Scope of Work for Bidder/ System Integrator (SI)	28	Maintain the existing SOC solutions for 6 months.	Please share the inventory for exiting SOC and Scope for Manage existing SOC	Bidder to refer Corrigendum-2
367	111	7. Scope of Work for Bidder/ System Integrator (SI)	29	The Bidder shall prepare a project plan, obtain approval from the Bank, and then implement the project in accordance with the timelines specified in the RFP.	There is any specific timeline mentioned in RFP, Can you please help with defined Timeline for each solution	Bidder to comply with RFP terms and conditions.
368	114	8.Design and Implementation of NGSOC and other security solutions	32	Bidder shall provide the required Hardware including (Compute / Storage) for NGSOC and Other Solutions being implemented. The sizing and architecture required for this project should be endorsed by the OEM in writing and proof of this will have to be submitted.	Can Bank provide the required Hardware including (Compute / Storage) for NGSOC and Other Solutions being implemented?	Bidder to comply with RFP terms and conditions.
369	120	13.Solutions under tech refresh	51	Bank intends to continue following existing solution as part of NGSOC and bidder are required supply, implement, manage, and migrate these solutions by resizing and upgrading the hardware and license as per Bank's requirement.	Instead of tech refresh can we proposed new solution against the same technology	Bidder to comply with RFP terms and conditions.
370	110	2. Scope of Work		Managing reporting and logging of security alerts /incidents through ticketing tools	We have to consider Ticketing tool as well for implementation or Bank is having any existing tickting tool	NO, Bidder should leverage SOAR solution or integrate to existing ITSM Service now.
371	125	PCAP	43	Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools	Only DC DR need to consider for Log ingestion in PCAP or anyother Remote location/Brnaches also there	Bidder to comply with RFP terms and conditions.
372	233-236	Annexure-10	1	*BFSI must be an organization having minimum of 1000 branches or 1 Lakh crore Business in India.	Can you please Delete this ask	Bidder to comply with RFP terms and conditions.
373	233-236	Annexure-10	2	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India.	Can you please add Private entities option as well	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
374	233-236	Annexure-10	3	The Bidder should have the experience in implementing or managing SIEM Solution in Organization(s) in India 1 lakh EPS with 2 clients - Score of 5 1 lakh EPS with 1 client - Score of 2	Can you please change it 50-60K	Bidder to comply with RFP terms and conditions.
375	233-236	Annexure-10	4	The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions SIEM - 10 certified OEM resource PIM - 5 certified OEM resource SOAR - 5 certified OEM resource EDR - 5 certified OEM resource Note: All respective certified resources must be on direct payroll of Bidder.	Can you change it to any OEM solution instead of the proposed OEM?	Bidder to comply with RFP terms and conditions.
376	184	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, I. Security Incident and Event Management (SIEM), Log Storage	30. SAN storage Systems should support Native Storage virtualization of 3rd party storage system for centralized management and SAN Storage systems should support 100 % Data Availability guarantee. 31. SAN Storages must Scale-Up & Scale out with support for intermix of different type of drives (NVMe SSDs, NL SAS, SAS). Data tiering (Auto sub-LUN tiering) should be supported. 32. No single point of failure, The SAN system should deliver Industry leading Performance of up to 2M+ IOPS 33. End to End SAN Infra monitoring from a single management suite. 34. SAN system should support native remote replication both synch & Asynch replication for backup/DR purposes. The storage system should support Zero RTO natively. 35. SAN system should allow intelligent compression & de-duplication per workload and can be disabled on non-compressible workloads. 36. The NAS system should be symmetric active-active architecture and should have unified capability i.e., should	SAN/NAS for the storage of data in a SIEM can negatively affect performance due to increased latency, reduced data retrieval speeds, and potential bottlenecks in data processing. This can lead to slower query response times, delayed detection of security incidents, and overall reduced efficiency in monitoring and threat management operations. Kindly clarify whether the storage can also be proposed as an alternative storage within the server.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
377	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	41. The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Kestral is a universal threat hunting language that is proprietary in nature. This mode of specific language eliminates other qualified OEMs who are achieving the requested functionalities via other methods. To keep the participation not limiting to a certain OEM. We request to either remove the clause or amend the clause as : " The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel or via any other methods. Attaching the link for reference: https://www.ibm.com/docs/en/cloud-paks/cp-security/1.10?topic=explorer-threat-hunt	Clause stands deleted. Bidder to refer Corrigendum-2.
378	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	51. The solution must include a in-product script editor with run buttons to facilitates debug and perform tests on scripts.	The requested functionalities can be achieved through other methods such as GUI driven test labs which will ease the analysts to debug easily without depending on any custom scripts. Hence we request not to limit achieving this requested functionality only via scripts and accept the Test Lab debugging and automation workflows.	Bidder to comply with RFP terms and conditions.
379	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	50. The solution must include a in-product script editor with autocomplete and syntax highlighting, to support automation of incident response workflow.	The requested functionalities can be achieved through other methods such as through system UI, with a playbook editor canvas. Hence we request not to limit achieving this requested functionality only via scripts and accept the GUI driven automation workflows.	Bidder to comply with RFP terms and conditions.
380	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	127. The platform should allow user to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts	This technical requirements is of proprietary nature to an OEM, Hence we request you to kindly remove the same. Reference : https://exchange.xforce.ibmcloud.com/hub/extension/f4a537a424977e155105d8aa9f5283c3	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
381	NA	NA	General	General	We request Canara Bank to kindly consider and add the following clause: "In case of corporate restructuring involving Business Transfer, all the Qualifying Criteria / Technical Scoring Criteria / Financial Criteria (or any other criteria pertaining to bidder's credentials) can be met by the bidding entity itself, or by the bidding entity's parent company (if the bidding entity is 100% owned subsidiary of the parent company) or by fellow subsidiary company (which is 100% owned by the parent company). Supporting documents of the parent company's / fellow subsidiary company's credentials shall also be acceptable for all the Eligibility Criteria/Technical Scoring / Financial criteria and any other criteria requiring bidder's credentials to qualify."	Bidder to comply with RFP terms and conditions
382	12	5. Requirement Details	The term of contract will be for a period of five (05) years	NA	Please confirm if the total contract duration is 5 years inclusive of implementation timeline or 5 years will start from the date of Go Live /Final User Acceptance	5 Years will start from date of Sign off by the Bank on production.
383	15	1. Project Timelines	A. SIEM, SOAR, UEBA	NA	We request that the project timeline for each respective activities be modified as:	Bidder to comply with RFP terms and conditions.
384	15-17	1. Project Timelines	Acceptance of Purchase Order by successful bidder.		T = 2 weeks from issuance of the Purchase Order	Bidder to comply with RFP terms and conditions.
385	15-17	1. Project Timelines	Delivery of all the equipment (software and hardware) as quoted in the bill of materials for SIEM, SOAR, UEBA and PCAP. Date of delivery of last item shall be taken as date of delivery for all items.		T+ 16 weeks	Bidder to comply with RFP terms and conditions.
386	15-17	1. Project Timelines	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform		T+ 32 weeks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
387	15-17	1. Project Timelines	Phase 2: Implementation of SOAR and integrate the following solutions, 1) SIEM 2) TIP 3) Proxy 4) Firewall 5) Active Directory 6) CMDB 7) Threat Intelligence 8) Vulnerability Management 9) ITSM (Service Now) 10) Bank's existing Antivirus & proposed EDR Solutions		T+36 weeks	Bidder to comply with RFP terms and conditions.
388	15-17	1. Project Timelines	Phase 3: SOAR Automation Playbooks for top 10 Incidents		T+40 weeks	Bidder to comply with RFP terms and conditions.
389	15-17	1. Project Timelines	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go-Live Certificate from the Bank.		T+42 weeks	Bidder to comply with RFP terms and conditions.
390	15-17	1. Project Timelines	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.		T+45 weeks	Bidder to comply with RFP terms and conditions.
391	15-17	1. Project Timelines	B. PIM			Bidder to comply with RFP terms and conditions.
392	15-17	1. Project Timelines	Acceptance of Purchase Order by successful bidder.		T = 2 weeks from issuance of the Purchase Order	Bidder to comply with RFP terms and conditions.
393	15-17	1. Project Timelines	Delivery of all the equipment as quoted in the bill of materials for PAM Solution. Date of delivery of last item shall be taken as date of delivery for all items.		T+ 16 weeks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
394	15-17	1. Project Timelines	Implementation of PIM and onboard in scope (from existing PAM solution) servers, applications and privilege accounts.		T+28 weeks	Bidder to comply with RFP terms and conditions.
395	15-17	1. Project Timelines	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go Live Certificate from the Bank.		T+30 weeks	Bidder to comply with RFP terms and conditions.
396	15-17	1. Project Timelines	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.		T+32 weeks	Bidder to comply with RFP terms and conditions.
397	15-17	1. Project Timelines	C. EDR			Bidder to comply with RFP terms and conditions.
398	15-17	1. Project Timelines	Acceptance of Purchase Order by successful bidder.		T = 2 weeks from issuance of the Purchase Order	Bidder to comply with RFP terms and conditions.
399	15-17	1. Project Timelines	Delivery of all the equipment as quoted in the bill of materials for EDR Solution. Date of delivery of last item shall be taken as date of delivery for all items.		T+ 16 weeks	Bidder to comply with RFP terms and conditions.
400	15-17	1. Project Timelines	Design and implementation of all the EDR components except the agents		T+14 weeks	Bidder to comply with RFP terms and conditions.
401	15-17	1. Project Timelines	Policy configuration		T+18 weeks	Bidder to comply with RFP terms and conditions.
402	15-17	1. Project Timelines	Installation of agents on Endpoints and servers (Agent can be pushed through Bank's SCCM tool)		T+30 weeks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
403	15-17	1. Project Timelines	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go Live Certificate from the Bank.		T+32 weeks	Bidder to comply with RFP terms and conditions.
404	15-17	1. Project Timelines	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.		T+36 weeks	Bidder to comply with RFP terms and conditions.
405	15-17	1. Project Timelines	D. All Other Solutions			Bidder to comply with RFP terms and conditions.
406	15-17	1. Project Timelines	Acceptance of Purchase Order by successful bidder.		T = 2 weeks from issuance of the Purchase Order	Bidder to comply with RFP terms and conditions.
407	15-17	1. Project Timelines	Delivery of all the equipment as quoted in the bill of materials. Date of delivery of last item shall be taken as date of delivery for all items.		T+ 16 weeks	Bidder to comply with RFP terms and conditions.
408	15-17	1. Project Timelines	Implementation and configuration of all the solutions		T+28 weeks	Bidder to comply with RFP terms and conditions.
409	15-17	1. Project Timelines	Successful Final Acceptance Test of all in-scope solutions/ services and Issue of Go Live Certificate from the Bank.		T+30 weeks	Bidder to comply with RFP terms and conditions.
410	15-17	1. Project Timelines	Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.		T+32 weeks	Bidder to comply with RFP terms and conditions.
411	15-17	1. Project Timelines	E. All Other Services			Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

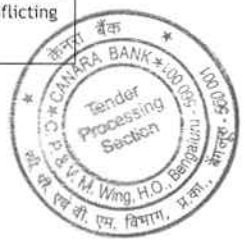
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
412	15-17	1. Project Timelines	Acceptance of Purchase Order by successful bidder.		T = 2 weeks from issuance of the Purchase Order	Bidder to comply with RFP terms and conditions.
413	15-17	1. Project Timelines	Implementation and configuration of all the services		T+10 weeks	Bidder to comply with RFP terms and conditions.
414	15-17	1. Project Timelines	Successful Final Acceptance Test of all in-scope services and Issue of Go Live Certificate from the Bank.		T+11 weeks	Bidder to comply with RFP terms and conditions.
415			Production Rollout. Completion of entire IT infra integration & security operations and commencement of advanced security operations.			Bidder to comply with RFP terms and conditions.
416	21	6. Penalties/ Liquidated Damages	The maximum penalty levied shall not be more than the 100% of the monthly charges payable to NG SOC services operations.	6.1.2.	The penalty capping is very stringent and we request to modify the oenalty clause as: The maximum penalty levied shall not be more than the 10% of the monthly charges payable to NG SOC services operations. Further all applicable penalties will be calculated concurrently.	Bidder to refer Corrigendum-2
417	24	6. Penalties/ Liquidated Damages	However, the total Penalty/LD to be recovered under above clause 6.6.1, shall be restricted to 10% of the total value mentioned in TCO of Annexure-17.	6.6.2.	The penalty capping is very stringent and we request to modify the oenalty clause as: However, the total Penalty/LD to be recovered under above clause 6.6.1, shall be restricted to 10% of the implementation value of respective component mentioned in TCO of Annexure-17.	Bidder to comply as per GeM Bid/ RFP terms and conditions.
418	26	7.Payment Terms:	Hardware cost (including OS & associated Softwares)	7.1.	We request to modify the payment terms as	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
419	26	7.Payment Terms:	After complete delivery of all hardware and its related software. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed.		0.6	Bidder to comply with RFP terms and conditions
420	26	7.Payment Terms:	After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.		0.2	Bidder to comply with RFP terms and conditions
421	26	7.Payment Terms:	After completion of training and on submission invoices duly acknowledge by the Bank's Officials i.e., 3 months post sign off.		0.2	Bidder to comply with RFP terms and conditions
422	26	7.Payment Terms:	After completion of Warranty period and submission of Bank Guarantee of equivalent amount.		We understand the actual clause is After completion of Warranty period OR submission of Bank Guarantee of equivalent amount. Pleae confirm. Further, we request for deletion of this payment milestone. Bidder is already submitting PBG as per RFP conditions which covers warranty period for all components hence no payment should be withheld.	Bidder to comply with RFP terms and conditions
423	27	7.Payment Terms:	One time implementation cost			Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
424	27	7.Payment Terms:	On successful implementation in UAT and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents.		0.5	Bidder to comply with RFP terms and conditions
425	27	7.Payment Terms:	On successful implementation in DC, DR and go-live and on submission of Invoice and Acceptance/ Sign off by the Bank on production of relevant documents.		0.3	Bidder to comply with RFP terms and conditions
426	27	7.Payment Terms:	On successful completion of DR Drill and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents.		0.1	Bidder to comply with RFP terms and conditions
427	27	7.Payment Terms:	On successful implementation of NG SOC solution and on submission of Invoice and Acceptance/ Sign off by the Bank on production of relevant documents.		0.1	Bidder to comply with RFP terms and conditions
428	27	7.Payment Terms:	AMC/ ATS - Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	7.1.	Please clarify ATS is being refered to which softwares as payment terms mentions 100% payment of license cost post delivery.	Bidder to comply as per GeM Bid/ RFP terms and conditions.
429	38	6. Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD	6. Earnest Money Deposit (EMD)/Bank Guarantee in lieu of EMD	6	As per GeM criteria / clause, bidder is exempted from paying any EMD / Bid security. Please clarify if GeM exemption supercedes RFP conditions or bidder has to submit EMD as per RFP.	The Terms and Conditions stipulated in ATC & SLA will supersede those in GTC and Terms and Conditions stipulated in ATC will supersede those in GTC and STC in case of any conflicting provisions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
430	74	Annexure-2 Pre-Qualification Criteria	The proposed SOAR solution should have been implemented satisfactorily in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids	Point 15	We understand this criteria needs to be met bt the OEM. Please confirm	Bidder to refer Corrigendum-1
431	74	Annexure-2 Pre-Qualification Criteria	The proposed UEBA solution should have been implemented in two Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	Point 16	We understand this criteria needs to be met bt the OEM. Please confirm	Bidder to refer Corrigendum-2
432	232	Annexure-10 Technical Evaluation Criteria	The Bidder's Annual turnover in the last 3 years • >500 crore <=1000 crore - Score of 2 • >1000 crore <=1500 crore - Score of 5 • >1500 crore - Score of 10	Point 2	We request Canara Bank to kindly consider and add the following clause: "In case of corporate restructuring involving Business Transfer, all the Qualifying Criteria / Technical Scoring Criteria / Financial Criteria (or any other criteria pertaining to bidder's credentials) can be met by the bidding entity itself, or by the bidding entity's parent company (if the bidding entity is 100% owned subsidiary of the parent company) or by fellow subsidiary company (which is 100% owned by the parent company). Supporting documents of the parent company's / fellow subsidiary company's credentials shall also be acceptable for all the Eligibility Criteria/Technical Scoring / Financial criteria and any other criteria requiring bidder's credentials to qualify."	"Clause stands deleted. Bidder to refer Corrigendum-1."
433	233	Annexure-10 Technical Evaluation Criteria	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India.	Point 7	We request to modify the clause as: The Bidder must have implemented ON-Premn / SaaS EDR solution in BFSI/ PSU/ Government entities in India.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
434	233	Annexure-10 Technical Evaluation Criteria	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience • For 5 or more clients - 5 marks • For 2 clients - 3 marks	Point 7	We request the scoring criteria to be modified as: Implementation Experience • For 5 or more clients - 5 marks For 3 clients - 4 marks • For 2 clients - 3 marks	Bidder to comply with RFP terms and conditions.
435	234	Annexure-10 Technical Evaluation Criteria	The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India	Point 9	PIM solution implementation is based on number of devices. Count asked for privledged user is very high. We request to amend the coause as: The Bidder should have implemented or managed PIM Solution with minimum of 500 devices in Organization(s) in India	Bidder to comply with RFP terms and conditions.
436	234	Annexure-10 Technical Evaluation Criteria	Resources: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 5 Note: For CEH maximum 5 number of certified resources will be considered	Point 11	In current scoring criteria, only selected bidders will be able to meet the scoring requirement. We request to amend the clause as: Resources: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 7 (c) >25 and < 50 - 5 marks (d) < 25 - 3 marks Note: For CEH maximum 10 number of certified resources will be considered	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

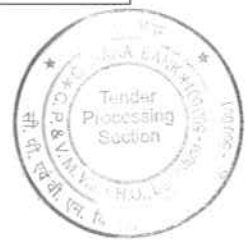
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
437	234	Annexure-10 Technical Evaluation Criteria	Resources: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH	Point 11	We request to cosider additional certificates and amend the clause as: Resources: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH / CC from ISC2	Bidder to comply with RFP terms and conditions.
438	84	2. Scope of Work	f. Bidder to do proactive Security Threat Hunting across Bank's environment and implement adequate information security controls to protect Bank IT assets from breach.		How many proactive threat hunting use case will be tested in each hunting exercise?	Bidder has to submit Threat Hunting plan of the month alongwith the details hypothesis.
439	84	2. Scope of Work	f. Bidder to do proactive Security Threat Hunting across Bank's environment and implement adequate information security controls to protect Bank IT assets from breach.		What would be frequency expected for Threat hunting exercise: once in a quarter or once in six month?	Monthly.
440	84	2. Scope of Work	c. Supply all required infrastructure and manpower for operations of NGSOC and other security solutions as per the detailed scope mentioned in this RFP.		Can bidder also need to consider LAN switches /Top of rack switch for connecting Security solutions appliance /server in DC/DR network?	No
441	84	2. Scope of Work	i. Managing reporting and logging of security alerts /incidents through ticketing tools and closing the same as per the agreed SLA.		Do you provide access of Canara Bank existing ITSM tool-ServiceNow to bidder onsite resources for managing incident tickets ?	Yes
442	85	2. Scope of Work	m. Perform Vulnerability Management for various IT assets such as devices / servers / applications as per the requirement of the Bank and at regular interval defined by the Bank.		What is frequency of performing vulnerability scanning of below devices: 1. Infra and network devices 2. applications	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
443	85	2. Scope of Work	n. Provide immediate forensic support in case of any security / cyber incident.		We understand forensic support is limited to providing evidences from inscope security solutions and support on investigation. Please confirm.	Bidder to refer Corrigendum-2.
444	85	2. Scope of Work	q. The proposed solutions implemented by the Bidder should adopt evolving threats and technological advancements, including quantum computing.		Please elaborate on requirement of Quantum computing?	Bidder to comply with RFP terms and conditions.
445	88	4. Responsibility Matrix: 1. SOC Governance & Program Management	Compliance Management: Conduct regular compliance audits and assessments		Bidder is responsible for performing sample based internal compliance review done by onsite SOC managing team. There is no external audit require by 3rd party. Please confirm	Yes, no external/ 3rd party audit is in bidder's scope.
446	89	8. Platform Management-SIEM, UEBA	14. Creation of parser for unknown log sources OEM: R SI: R,A		Any custom parser development during operational support which require OEM support to develop will come with additional cost. This will be cover by raising change request. Hope you agreed on this, please confirm.	Bidder to comply with RFP terms and conditions.
447	101	17. Migration of existing CSOC to proposed NGSOC and security solutions	4. The above requirements and approach need to be followed for all NGSOC solutions like NBAD, Deception, VA, PIM, Anti - DDOS and other security solutions wherever applicable as proposed by the Bidder.		Please mention: 1. Is Deception solution exist today in bank environment? If not, does bidder need to include in scope of this RFP? 2. If Deception solution exist today in network, please mention which deception solution it is? 3. Please mention how many licenses of deception is deployed or required ?	1. Yes 2, 3. - Details will shared with selected bidder.
448	108	6. Manpower Roles and Responsibilities	Vulnerability Management & DAST Specialist	Deployed resource shall ensure regular remote backups with retention capabilities, ensuring data restoration for at least the past 3 years	Does Canara bank provide storage or back or bidder needs to consider for 3 year retention?	Bidder has to provision.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
449	110	7. Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months.		We understand your existing SOC team will provide complete Knowledge transfer during handover of existing SOC services to bidder, please confirm?	Yes, Bidder shall provide comprehensive transition plan which shall be discussed and agreed with the bank and with incumbant partner.
450	110	7. Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months.		We understand your existing SOC will continue provide manage SOC services until bidder resources on boarded for existing SOC operational support, please confirm?	Bidder to comply with RFP terms and conditions.
451	110	7. Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months.		How many resources require to manage existing SOC, please share count of resources -L1,L2 and L3 ?	Bidder to refer Corrigendum-2
452	110	7. Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months.		If require bidder can extend operation support of existing SOC more than 6 months ?	Bidder to refer Corrigendum-2



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
453	111	7. Scope of Work for Bidder/ System Integrator (SI)	The complete NGSOC infrastructure, including but not limited to hardware, software, storage, services, licenses would be provided by the bidder. The Bank will provide facilities to host the devices for the personnel and workstations (Desktop/Laptop).		Does bidder need to provide laptop/desktop for operational resources who will sits in Bank location which can be hardened as per bank image or bank will provide laptop/desktop to bidder onsite resources?	The requirement is self explainatory.
454	111	7. Scope of Work for Bidder/ System Integrator (SI)	The bidder shall supply and install network ports with a minimum capacity of 10 Gigabit(10Gig).		Do you want bidder to supply network switches of min. port 10G ? If yes , how many switches require with how many port capacity?	Bidder to refer Corrigendum-2.
455	111	7. Scope of Work for Bidder/ System Integrator (SI)	The bidder shall supply and install network ports with a minimum capacity of 10 Gigabit(10Gig).		Does these switches require to connect proposed SOC and other security solutions in existing LAN Setup of Canara bank?	Bidder to refer Corrigendum-2.
456	111	7. Scope of Work for Bidder/ System Integrator (SI)	The bidder shall supply and install network ports with a minimum capacity of 10 Gigabit(10Gig).		Can bidder also need to consider network switches require in their design?	No
457	111	7. Scope of Work for Bidder/ System Integrator (SI)	NGSOC should deliver and implement the solutions/services to Bank in compliance with International Standards such as ISO 27001:2013 /2022, ISO 31000:2018, ISO 27017:2019, ISO 27701:2019, ISO 22301:2019, PCI-DSS and advisories issued from regulatory and statutory authorities from time to time.		We understand Canara Banka has already security controls defined and you will share with bidder teams to apply during implementation , please confirm?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
458	111	7. Scope of Work for Bidder/ System Integrator (SI)	• The Bidder should ensure the proposed solutions should be compatible with or able to integrate with quantum-resistant technologies and encryption methods.		Please elaborate on requirement of quantum-resistant technologies here?	Bidder to comply with RFP terms and conditions.
459	114	7. Scope of Work for Bidder/ System Integrator (SI)	Bidder shall provide required load balancers for the NGSOC.		Please elaborate purpose of Load balancer require in NGSOC?	As mentioned in Technical Specifications of SIEM & PIM Solution.
460	114	7. Scope of Work for Bidder/ System Integrator (SI)	- Bidder should ensure that the configured correlation alerts and live dashboards of NGSOC and other solutions should be displayed on bank's existing LED/Display board.		1. Please confirm that bank will provide connectivity and connection to the existing LED/Dashboard to integrate SIEM dashboard ? 2. Do you want to integrate all security solutions dash board with LED/Display board or only SIEM/SOAR ?	Bidder to comply with RFP terms and conditions.
461	114	7. Scope of Work for Bidder/ System Integrator (SI)	• The Bidder shall maintain comprehensive backup and Disaster recovery plan, including		Can bidder levreage Canara bank existing Backup solution to take back of security devices ?	Yes
462	114	7. Scope of Work for Bidder/ System Integrator (SI)	• Bidder shall provide the required Hardware including (Compute / Storage) for NGSOC and Other Solutions being implemented. The sizing and architecture required for this project should be endorsed by the OEM in writing and proof of this will have to be submitted.		Is this endorsement from OEM require during submission of bid proposal or before implementation time?	During implementation time.
463	115	9. NGSOC Operations	• Bidder shall provide technical/functional/operational training for all services of NGSOC and in scope solutions, monitoring of incidents and logs, raising alerts, designing, and customizing reports.		We understand this training (to bank officials) would be one time activity pre and post implementation? Please confirm.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
464	116	9. NGSOC Operations	• Bidder should provide consolidated security status reports through live, integrated, centralized, and automated dashboards. The service will include. ▫ Develop security reporting across all systems, services, and projects. ▫ Provide a centralized security dashboard with integrated reporting of all systems and services.		1. Security reports will be generated through respective solution tools which will further consolidate by SOC resource. Centralize dashboard would be hard to achieve in case of multiple technologies . Please confirm that manual consolidated report will suffice bank reporting requirement?	Bidder to comply with RFP terms and conditions.
465	116	9. NGSOC Operations	• Bidder shall provide integrated dashboard with customized views depending on role of the user and provide an online secured portal (web-based dashboard) for viewing real-time incidents/events, alerts, status of actions taken, etc. The views required by Bank are as follows:		We assume this is only require for SIEM dashboard?	Bidder to comply with RFP terms and conditions.
466	117	9. NGSOC Operations	• Bidder should develop custom plug-ins/ connectors/ agents for business application monitoring.		We assume that each business application is capable of sending audit or require logs to collector for security monitoring . Please confirm Please share count of business application for customer parser development?	Yes. The count of business application will be shared with selected bidder.
467	116	9. NGSOC Operations	• Bidder must ensure the BCP test of NG SOC Solutions are performed quarterly. Comprehensive report with RTO & RPO achieved along with lessons learnt to be submitted to the bank.		Please confirm what would be scope of quarterly frequency testing, does it require to test each security solution at individual level OR all security solution will be testing in single downtime window?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
468	117	9. NGSOC Operations	• The Bidder should implement required solutions for local log retention supported by log analysis tool for offline monitoring and reporting.		Do you want bidder to implement separate log management solution apart from what comes with SIEM platform?	Bidder to comply with RFP terms and conditions.
469	117	10. Security Device Management and Administration	• Bidder shall provide 24x7x365 on-site management & monitoring of security devices which includes proposed NGSOC solutions, other security solutions and Bank's existing security solutions. It is to be noted that the Bidder shall have separate teams for monitoring, maintenance, and management of NGSOC.		1. Please confirm what includes in 'other security solution' ? 2. Please elaborate on separate team for monitoring, maintenance, and management of NGSOC requirement .	Bidder to comply with RFP terms and conditions.
470	117	10. Security Device Management and Administration	• The Bidder is expected to maintain and track the AMC/ATS/License renewal etc. for all components (hardware, software, LEDs/ Display board, appliances, tools, or any other components) proposed in this RFP and escalate to Bank team in case of any lapses.		we understand LED/display board is available with bank which is maintained and manage by BANK Resources. Please confirm.	Bidder to comply with RFP terms and conditions.
471	119	11. Incidents and Problem Management	• Bidder should integrate the Incident Management tool with ITSM procured by the Bank in future without any additional cost to Bank. Bidder should also move and migrate data of incidents from existing solution to any future procured by the Bank.		Does bidder need to bring new Incident Management tool which will integrate with bank existing ITSM tool?	Incident Management has to be performed using proposed SOAR solution which shall be integrated with banks ITSM solution (Service Now).

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
472	118	11. Incidents and Problem Management	• The Bidder must provide incident management solution and integrate it with the existing ticketing tool to generate automated tickets for the alerts or any security events generated by security solutions and devices such as log monitoring tool, Network Intrusion Prevention/Detection Systems, Firewall/ SIEM/ DAM/ PIM/ DLP/ WAF/ DRM/ FIM/ GRC and in scope NGSOC solutions including other proposed security solutions.		Does all new in-scope solution needs to be integrate with bank existing ITSM tool ?	Yes, Primarily with proposed SOAR and for ticketing integration to be done with banks Service Now ITSM solution.
473	120	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• The bidder should configure/ migrate the use-cases deployed in the current SIEM to the newly procured SIEM.	Does all rules needs to migrate or bidder can optimize rule set based on Canara bank business requirement? How many rules are configured in current SIEM?	Primarily all rules to be migrated, details will be shared with selected Bidder. In case of optimization of rule sets bidder can propose same to bank during implementation phase.
474	120	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• The offered solution shall include toolkits/modules/utilities for integrating all required devices supported by the SIEM equipment without any additional cost implication to Bank.	Please share list of all required devices that needs to be integrate with SIEM ?	The details will be shared with selected Bidder
475	120	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• In case of separate logger and collector, If connectivity between log collection agents and logger is down, then the Log collector agents should retain the logs until connectivity is restored and send them once connectivity is re-established.	For collector sizing kindly confirm how many days logs can collector store in case of connectivity break between collector and logger?	Bidder to comply with RFP terms and conditions.
476	121	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• Bidders should integrate the proposed SIEM with a ticketing tool for automated ticket generation.	Does bidder needs to integrate SIEM with bank existing ticketing tool BMC ? We hope bank team will do require configuration changes at tool end to integrate it with SIEM platform ?	Bidder need to integrate with SOAR Incident Management or ITSM.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
477	122	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• Logs from all devices / appliances / servers / applications / databases located at the geographically dispersed location should be collected. Bidder should develop the baseline for the level of logs to be enabled from different components of IT infrastructure assets.	Please share details of all locations where log sources are distributed and collector needs to be deployed?	The details will be shared with selected Bidder.
478	123	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM) • Integration with in-scope monitored devices and interoperability.	• The SIEM should be compatible with Data Lakes or any other central database system so that the same can be used as a centralized repository aimed at maintaining and managing all log or other data sources.	Do you have any existing Data Lake solution , if yes please share name of solution to check SIEM compatibility?	No
479	126	12. Scope of Work for Proposed Solutions	III. Security Orchestration, Automation and Response (SOAR)	The bidder shall develop custom integration as necessary within the defined timeline.	Please elaborate on expectation of integration , what all needs to be integrate?	The details will be shared with selected Bidder.
480	176	Annexure-9:Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions II. Security Orchestration and Automation (SOAR):	The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank	Please mention all multi cloud environment details where SOAR needs to be implement ?	Bidder to comply with RFP terms and conditions.
481	127	12. Scope of Work for Proposed Solutions	V. Endpoint Detection & Response (EDR)	• Supply, installation, commissioning, and implementation of Endpoint Security Solution across the Bank, including its administration, support, upgradation with no additional cost during the entire contract period of 5 years.	Please elaborate on expectation of upgrade of EDR as EDR solution is SaaS based ?	Although it is SaaS based Installation, administration, support and upgradation is applicable.
482	203	Annexure-9:Functional and Technical Requirements	V. Privileged Identity Management (PIM)	The solution shall have feature to manage system and application-level privilege accounts. OEM to support application integration	Please share list of applications that needs to be integrate with PIM solution	Bidder to comply with RFP terms and conditions.
483	128	12. Scope of Work for Proposed Solutions	VI. Privileged Identity Management (PIM)	• The successful bidder will migrate, upgrade, and maintain the solution to the full satisfaction of the Bank with all the required functionalities. The system should be in HA architecture at DC as well as HA in DR. The Bidder would be responsible for installation, upgradation, migration to VM, testing, commissioning, configuring, maintenance of the existing solution.	Please explain on migration part of PIM Solution, does it mean bidder need to migrate PIM solution from existing vensor to new proposed vendor? Please share name of your existing PIM solution vendor name ? IS it SaaS based on on-prem hosted ?	The details will be shared with selected Bidder.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
484	128	12. Scope of Work for Proposed Solutions	VI. Privileged Identity Management (PIM)	• The Bidder would install the solution in test environment, train the Bank's personnel for independent operation, creation of policies/rules, generation of reports, analysis of the reports, correlation with other relevant security related applications/events, familiarization of features and functionalities.	We understand solution can be tested in Test envirnement whereas deployment will be happen in productoion setup. Please confirm	Bidder to comply with RFP terms and conditions.
485	128	12. Scope of Work for Proposed Solutions	VI. Privileged Identity Management (PIM)	• The successful bidder will migrate, upgrade, and maintain the solution to the full satisfaction of the Bank with all the required functionalities. The system should be in HA architecture at DC as well as HA in DR. The Bidder would be responsible for installation, upgradation, migration to VM, testing, commissioning, configuring, maintenance of the existing solution.	Does all the multi-layers (DB and application) of solution require in HA in both -DC and DR ?	Yes
486	129	12. Scope of Work for Proposed Solutions	VII. Threat Intelligence Platform (TIP)	Bank is procuring Centralized Cyber Threat Intelligence Platform solution for which Bidder has to provide the services which includes but not limited to the following:	Is this solution exist and bidder is only provide services, please confirm. IF yes, kindly share solution name (Make and model)	No, Threat Intelligent Platform Solution to be provided by the Bidder.
487	209	12. Scope of Work for Proposed Solutions	VI. Threat Intelligence Platform (TIP):	The proposed solution shall be deployed at on-premises components that permits the organization to store IOCs and investigations confidentially on their physical premises in local HA in DC & DR.	Does solution needs to deployed in HA in DC and seprate HA in DR, please confirm?	Yes
488	131	12. Scope of Work for Proposed Solutions	VIII. Dynamic Application Security Testing (DAST)	• The Bidder will be responsible for providing weekly updates on the testing progress, any critical findings, and potential blockers.	What is frequency of DAST testing on per appliactaion ?	Bidder to comply with RFP terms and conditions.
489	NA	12. Scope of Work for Proposed Solutions	Generic	Generic	What is frequency of scanning 600 application ?	Bidder to comply with RFP terms and conditions.
490	NA	12. Scope of Work for Proposed Solutions	Generic	Generic	Please elaborate on type of application consists of 600 number- COTS/home grown/open source/legacy/industry specefic?	Bidder to comply with RFP terms and conditions.
491	191	Annexure-9:Functional and Technical Requirements	IV. Endpoint Detection and Response (EDR):	The proposed OEM should have a comprehensive XDR approach with correlation across multiple layers like endpoint security, email security, server security, network security and mobile security.	Do you need XDR solution along with EDR?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
492	191	Annexure-9:Functional and Technical Requirements	IV. Endpoint Detection and Response (EDR):	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Please clarify this ask, does this mean EDR OEM must have product offering of hybrid cloud, endpoint, email and network security solutions geared towards layered security approach but these are not part of proposed solution ?	Bidder to comply with RFP terms and conditions.
493	191	Annexure-9:Functional and Technical Requirements	IV. Endpoint Detection and Response (EDR):	The proposed solution should have capabilities to distribute the local threat intelligence to all the endpoints immediately after the local threat intelligence ingested by the existing sandbox.	As it mentioned existing sandbox , so do you have sandbox existing on-prem which bidder can also leverage with proposed EDR solution ?	Bidder to note that it is from the Sandbox solution which is proposed as a part of EDR.
494	132	12. Scope of Work for Proposed Solutions	IX. Anti-APT and Sandboxing	• The proposed solution should support currently available operating systems to perform inception for malware, zero day and stealth attacks etc.	Please mention all Operating systems deployed in your environment on server and enduser machines?	Bidder to comply with RFP terms and conditions.
495	216	Annexure-9:Functional and Technical Requirements	VIII. Anti - APT:	Each of the bidders proposed solution would be evaluated thoroughly against functional as well as technical requirements. The proposed solution should be from a single OEM (for all components) to ensure the integrated platform requirements and capabilities are utilized and desired security objectives are achieved. The solution expected to import multiple TLS/ SSL certificates.	Please elaborate on all componenets that is require from single vendor of Anti-APT? does this mean Anti-APT and sandboxing solution from same vendor? Please explain what do you mean by single vendor here ?	Bidder to comply with RFP terms and conditions.
496		Annexure-9:Functional and Technical Requirements	VIII. Anti - APT:	Proposed appliance should have below hardware requirements: Network Traffic Analysis appliances should be supplied with minimum below port requirements with a separate dedicated management and IPMI port with 10/100/1000GBASE-T 4 X 1G/10G RJ45 4 X 1G/10G SFP+ (With Bypass) 8 X 10G SFP+	Is this port specification given for Netwok Traffic Analyzer or Anti-APT?	Bidder to refer Corrigendum-2
497	123	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	• Development of connectors/parsers for customized applications/devices It is the responsibility of the Bidder to develop connector applications for all devices.	Could you please share list of your custom applications and log source list to analyze where custom parsers needs to be develop?	The details will be shared with the successful bidder.
498	166	Annexure-9:Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):	SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and Cloud). If the parser is not available the bidder/ OEM should developed the parsers without any extra cost to bank	Please specify which cloud platform will integrate with SIEM solution?	All cloud platforms

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
499	142	12. Scope of Work for Proposed services	a) Threat Intel Services	Generic	Following services Functional and Non-functional requirement are missing under Annexture 9, please add if there is any specific requirment you have regarding these 3 services: Threat Intel Service DDOS Drill Cyber Range	Bidder to comply with RFP terms and conditions.
500	142	12. Scope of Work for Proposed services	a) Threat Intel Services	Additional requirement: Bank is looking for the following services in addition to the services provided by M/s Izoologic.	Please clarify that bank is only looking for below additional services to be provided by bidder (not include services which is provided by Izologic today): • Attack Surface Monitoring • IP reputation check • Hash check • Whois check • IP Geo Location • OU Details • File or URL Sandboxing	As mentioned in the RFP it is "in addition to that"
501	87	Annexure-8 Scope of Work	3. Sizing & Scalability Requirements Cyber Range	Partcipants:5/batch Hours: 40 hours per year	How many batch require to run per year?	Bidder to refer Corrigendum-2.
502	134	Annexure-9:Functional and Technical Requirements	13. Solutions under tech refresh- Scope for Anti - DDOS:	• Data Migration: Transfer relevant data from the old to the new system.	what is the data size for data transfer ?	Bidder to comply with RFP terms and conditions.
503	165-232	Annexure-9:Functional and Technical Requirements		DR Drill Frequency : quaterly	Drill consider each security solution separate, individually or DR will be done for whole secruity solution in once Frequency : quaterly	As per Bank requirement , It may be individual or consolidate, but the frequency is Quarterly.
504	141	Annexure-8 Scope of Work	13. Solutions under tech refresh d. Vulnerability Assessment (VA)	• Bank is procuring 5000 licenses which will be upgraded in upcoming 5 years with asset licenses along with the hardware changes, The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract,	Please clarify that bank procure 5000 license from Day 1 of contract or current count 2300 will increase upto 5000 in 5 years ?	5000 licenses from day one.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
505	141	Annexure-8 Scope of Work	13. Solutions under tech refresh d. Vulnerability Assessment (VA)	• Bank is procuring 5000 licenses which will be upgraded in upcoming 5 years with asset licenses along with the hardware changes, The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract,	1. Does bank want to change hardware as per 5 year capacity fom Day 1 or can we er upgarde hardware as per requirment of bank time to time? 2. Does bidder need to propose new hardware completely or can upgrade in existing hardware of bank?	Bidder to propose new hardware with 5 years capacity from day one.
506	160	b) Training	1. Scope of work for OEMs		can bidder provide training from 3rd party trainers specilized on inscope given technology solutions?	Bidder to comply with RFP terms and conditions.
507	160	Annexure-8 Scope of Work	15. Scope of work for OEMs b) Training	(e) Bidder shall extend 2 to 3 days of training on Information/Cyber security awareness and best practices to selected Bank officials (two batches of up to 50 officers) at Mumbai and Bengaluru locations of the Bank, thrice during the project period. All out of pocket expenses related to the Trainer for such training sessions shall be borne by the Bidder.	Does it mean one batch in Mumbai and one batch in Banaglore of upto 50 people?	Bidder to comply with RFP terms and conditions.
508	160	Annexure-8 Scope of Work	15. Scope of work for OEMs b) Training	(e) Bidder shall extend 2 to 3 days of training on Information/Cyber security awareness and best practices to selected Bank officials (two batches of up to 50 officers) at Mumbai and Bengaluru locations of the Bank, thrice during the project period. All out of pocket expenses related to the Trainer for such training sessions shall be borne by the Bidder.	We undertsand security awareness training require thrice in 5 year contract. Please confirm?	Yes
509	160	Annexure-8 Scope of Work	15. Scope of work for OEMs b) Training	(a) The selected bidder will be responsible for training the Bank's employees in the areas of implementation, operations, management, monitoring, error handling, system administration etc. Training will be given both pre-implementation and post-implementation for the proposed solution.	Please consider training on remote sessions also or mix of onsite and remote?	Onsite training to be considered.
510	160	Annexure-8 Scope of Work	15. Scope of work for OEMs b) Training	(a) The selected bidder will be responsible for training the Bank's employees in the areas of implementation, operations, management, monitoring, error handling, system administration etc. Training will be given both pre-implementation and post-implementation for the proposed solution.	Is this training be conduted at bank premise ?	Bidder to comply with RFP terms and conditions.
511	161	Annexure-8 Scope of Work	15. Scope of work for OEMs c) Reporting and Security Dashboard	D. As part of Deliverables, bidder must provide integrated dashboard covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. leveraging SOAR	SIEM shows consolidated view of multiple security controls logs , does this suffice your requirment?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
512	162	Annexure-8 Scope of Work	15. Scope of work for OEMs c) Reporting and Security Dashboard	D. As part of Deliverables, bidder must provide integrated dashboard covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. leveraging SOAR	Bidder consider that SIEM has visibility of all integarted security appliances logs and events generated so SIEM dashbaord can provide required view of different dashbords as per requirment. Please confirm if this SIEM dashboard can suffice your requirment?	Bidder to comply with RFP terms and conditions.
513	161	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines A. SIEM, SOAR, UEBA	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	Please share construct of 4500 log sources ,type of logsource and quantity of each type log sources	The details will be shared with selected Bidder.
514	15-17	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines A. SIEM, SOAR, UEBA	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/ Migrate current use cases/policies to new platform	Please confirm how many total application needs to integarte with SIEM during implementation time?	The details will be shared with selected Bidder.
515	161	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines A. SIEM, SOAR, UEBA	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	We understand configuration changes at logsource end would be done by bank IT team to push logs on new SIEM Collector, please confirm?	Bidder to comply with RFP terms and conditions.
516	161	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1. Project Timelines A. SIEM, SOAR, UEBA	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	Any delay in doing required configuration changes at log source end will stop implementaion SLA clock of bidder, please confirm?	Bidder to comply with RFP terms and conditions.
517	19	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5. Uptime	5.3. The selected bidder should consider high-availability (active-passive) at DC & DR with RPO of 15 minutes and RTO of 120 minutes.	Can bidder leverage bank existing network connectivty between DC and DR for data replication between security solution components of DC/DR?	Yes
518	19	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5. Uptime	5.3. The selected bidder should consider high-availability (active-passive) at DC & DR with RPO of 15 minutes and RTO of 120 minutes.	We assume RPO of 15 minutes and RTO of 120 minutes is applicable in case of even failover of any one security solution component in DR, please confirm?	Bidder to refer Corrigendum-2.
519	19	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	5. Uptime	5.3. The selected bidder should consider high-availability (active-passive) at DC & DR with RPO of 15 minutes and RTO of 120 minutes.	Does bidder need to consider any calculation or procurement of nay network bandwidth in their scope?	No

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
520	163	Annexure-8 Scope of Work	17. Migration of existing CSOC to proposed NGSOC and security solutions	1. Migration of all existing solutions (Existing SOC and security solutions to proposed NGSOC and other security solutions)	Existing solutions that needs data migration to new proposed or upgarded solution are: 1. SOC corelation rules 2. DLP 3. Anti DDOS 4. NBA 5. PIM 6. VA Data migration is not required apart from above mentioned solutions, please confirm?	Bidder to comply with RFP terms and conditions.
521	163	Annexure-8 Scope of Work	17. Migration of existing CSOC to proposed NGSOC and security solutions	1. Migration of all existing solutions (Existing SOC and security solutions to proposed NGSOC and other security solutions)	We undertsand existing SIEM data migartion includes only rules/corelation rules migration from existing to new , not existing logs migration on new tool , please confirm?	Yes
522	163	Annexure-8 Scope of Work	17. Migration of existing CSOC to proposed NGSOC and security solutions	1. Migration of all existing solutions (Existing SOC and security solutions to proposed NGSOC and other security solutions)	We assume existing SOC logs will not migrate on new SIEM solution , please confirm?	Yes
523	163	Annexure-8 Scope of Work	17. Migration of existing CSOC to proposed NGSOC and security solutions	3. The Bidder has to continue the use of existing SIEM till all the log sources gets migrated and the existing SIEM is decommissioned as per the need.	Please mention timeperiod for managing existing SIEM aetup by bidder to arrange resources accordingly ?	Clause stands deleted. Bidder to refer Corrigendum-2.
524	163	Annexure-8 Scope of Work	17. Migration of existing CSOC to proposed NGSOC and security solutions	3. The Bidder has to continue the use of existing SIEM till all the log sources gets migrated and the existing SIEM is decommissioned as per the need.	We understand resources require for managing existing SOC is additional to Manpower (total 42) ask in RFP , please confirm?	For Manpower Requirement Bidder has to refer Corrigendum-1 to the GeM Bid.
525	101	4. Responsibility Matrix:	Endpoint Security Specialist Deception		Does bidder needs to propose deception solution along with EDR for endpoint security ?	Bidder to manage the existing bank's Deception Solution which will be shared to the selected Bidder

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
526	84	2. Scope of Work	a. Ensure all the commissioning, Integration, migration, relocation, updates, Upgrades, Patching, de-commissioning, Enhancements, Troubleshooting, Analysis, Health Checks, Backups, Audits, Documentation, SOP's, Creation of Knowledge Articles at Onsite for proposed NGSOC.		Please confirm that bidder can leverage existing SOP's where its is available for any technology and ceate only new SOP where require ?	No
527	84	2. Scope of Work	a. Ensure all the commissioning, Integration, migration, relocation, updates, Upgrades, Patching, de-commissioning, Enhancements, Troubleshooting, Analysis, Health Checks, Backups, Audits, Documentation, SOP's, Creation of Knowledge Articles at Onsite for proposed NGSOC.		Please elaborate what is expected to be include in Knowledge articles ?	Bidder to comply with RFP terms and conditions.
528	13	8. Scope of Work	8.2. Bank reserves the right to modify the scope due to change in regulatory instructions, market scenario and internal requirement within the overall objective of End to End implementation of NGSOC solutions for 5 (five) years.		Please change in clause that any change in SOW will be mutualy agreed between both parties G109 considering cost implication	Bidder to comply with RFP terms and conditions.
529	136	13. Solutions under tech refresh	b. DLP		Our understanding is that Data Classification is not in the scope of this RFP. Are you using any data classification tool, if yes please share name of solution ?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
530	85	3. Sizing & Scalability Requirements	10. VA, existing license 2300 and procuring 5000		Please confirm that total 5000K licenses require on Day 1 which includes 2300 existing licences nd 1700 new licneses ?	Yes
531	87	3. Sizing & Scalability Requirements	15. Cyber Range Partcipants:5/batch Hours: 40 hours per year		Please confirm on sizing of Cyber range 1. How many total batches of 5 persons need to consider ? 2. Do you need 40hrs /year for each batch or per participant?	Bidder to refer Corrigendum-2.
532	17	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	1.4 Implementation Phase: The System Integrator is required to deploy personnel as per the expected organization structure for the SOC implementation phase. The SI is required to provide team details (as per Manpower Requirements mentioned in Scope of Work (Annexure-8) in line with the roles and responsibilities). The SI shall ensure that 100% of the resources deployed at the Bank shall be on the payroll of the primary SI.		Request you to consider OEM certified partner/resources for implementation of inscope security controls	Bidder to comply with RFP terms and conditions.
533	138	13. Solutions under tech refresh	c. NBA Scope of Work for NBA: • Implementing NBAD with Management console, 3-node data store cluster, telemetry brokers, Flow Collectors, ISE PIC for managing both DC,DR of NBAD solution.		Does ISE PIC is also part of this RFP Scope?	Bidder to comply with RFP terms and conditions.
534	261	Annexure-17(C) :Sizing of Hardware of Retained Solutions	NBAD (Network Behavioral Analysis Detection) ISE PIC software (VM based)		Please share under lying hardware sizing for implementing ISE PIC solution ? OR Is ISE PIC node is already deployed and we need to install only license on it?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
535	NA	Generic	Generic	Generic	Do you extend your existing TrendMicro antivirus and NAC solution for the endpoint security control of proposed security solution underlying server and network devices?	Bidder to comply with RFP terms and conditions.
536	94	5. Manpower Requirement	PIM Specialist and SIEM, SOAR & UEBA Engineer OEM (L3)		Please consider OEM(L3) support remotely ?	Bidder to comply with RFP terms and conditions.
537	94	5. Manpower Requirement	PIM Specialist and SIEM, SOAR & UEBA Engineer OEM (L3)		Can bidder place OEM certified resource on premise for L3 support for this ask?	No
538		Training			Can bidder conduct training sessions for bank officials G121online remotly?	Bidder to comply with RFP terms and conditions.
539	57	17. Business Continuity Plan:	17.2. The service provider/vendor/ Bidder shall periodically test the Business Continuity and Management of Disaster Recovery Plan. The Bank may consider joint testing and recovery exercise with the Service provider/vendor.		Bidder expect that Bank has already defined BCP /DR plans which will be leverage by bidder fo rtheir proposed solution, please confirm?	Bidder to comply with RFP terms and conditions.
540	84	2. Scope of Work	b. Design, validate & review the NGSOC architecture along with in scope solutions at least once in year from OEM review of respective security solutions with concurrence of the Bank.		Please consider yearly review with OEM/OEM Certified partner ?	Bidder to comply with RFP terms and conditions.
541	86	DLP	Upgrade the licenses to 90k for Endpoint and Network DLP Licenses along with new hardware		Please confirm new required hardware can be a virtual machine or appliance or we can choose as per our solution?	Bidder can choose the hardware according to the solution sizing for all the in scope solutions , Accordingly it can be physical/virtual

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
542	114	7. Scope of Work for Bidder/ System Integrator (SI)	• Bidder needs to ensure that the NGSOC solution can integrate with other IT Systems using standard methods/ protocols/ message formats without affecting the existing functionality of the Bank.		Please mention what are other IT solutions of bank, which needs to be integrate with SOC solution, to check compatability?	The details will be shared with selected Bidder
543	259	Annexure-17(C) :Sizing of Hardware of Retained Solutions	Anti-DDOS E-081AX-HWBAA Qty:2		As per Scope vendor needs to upgrade only one Arbor device which is in DR (APS 2600 to AED 8100) but in BOQ it show quantity as 2 , so could you please clarify that given BOQ is given for manage service perspective to bidder only ? Please clarify	1 in DC and 1 in DR (total 2)
544	174	Annexure-9 Functional and Technical Requirements	Packet Capture, Point 133	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	SIEM, PCAP, and UEBA from the same OEM ensures seamless integration, leading to better data correlation and faster threat detection. A unified platform provides consistent data formats, reduces integration complexity, and eliminates gaps in security coverage. This allows for more accurate analysis of network traffic, user behaviour, and security events along with reduced operational costs, improved efficiency through a centralized dashboard. With PCAP and UEBA from same OEM, it will give additional network models which will augment the network detection capability. Request to consider PCAP also from the same OEM along with SIEM and UEBA Kindly change this to "The proposed Packet capture solution should be from the same OEM which offers SIEM and UEBA to ensure seamless integration between all detection layers with native capabilities to integrate with proposed SIEM and UEBA solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same"	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
545	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 9	The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage custom data models if necessary	Machine learning models are delivered through UEBA which are preconfigured and managed by OEM only as they are complex in nature and requires high skill set. Custom data models can be a security concern as it exposes the Data Models to be manipulated. Please Change this point to allow more reputed OEM's to participate. Kindly modify the line as "The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage inbuilt non customised data models for ML OR custom data models if necessary"	Bidder to refer Corrigendum-2
546	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 15	The solution shall use unsupervised and supervised machine learning algorithms for anomaly detection mentioned below (a) Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency. (b) Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time. (c) Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly. (d) Usage deviates from peer group such as User pattern of activity starts deviating from the peer group. (e) Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems. (f) Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing. (g) Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data (h) Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data (i) Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users	Supervised learning demands a large volume of labelled data and ongoing supervision from data scientists, increasing the complexity and effort. Unsupervised ML methods thus offer scalability and adaptability in dynamic environments with less human intervention. This complexity is better owned by product owners than operations teams i.e. OEMs only. Hence request you to change the clause to "The solution shall use unsupervised/supervised machine learning algorithms for anomaly detection mentioned below"	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
547	176	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 9	The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	This requirement is proprietary to single OEM and highly restrictive for fair participation Kindly change this to "The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost."	Bidder to refer Corrigendum-2
548	178	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 29	Bank shall have 15 user licenses and 2 read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	With fewer admin users, organizations reduce the risk of misconfigurations, unauthorized changes, and potential security breaches. Admins can oversee critical tasks like setting up automation workflows and managing incident responses, while read-only users can monitor, analyse, and collaborate without altering configurations. This approach improves accountability, as key decision-makers maintain control, while enabling broader visibility across teams. It balances security with transparency, allowing stakeholders to stay informed without compromising the integrity of the SOAR environment. Hence, we recommend unlimited read only users for better monitoring and visibility throughout across management of Bank. Kindly modify the clause to "Bank shall have 15 user licenses and unlimited read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract"	Bidder to comply with RFP terms and conditions.
549	179	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Custom Threat hunting is not a native SOAR functionality and is supported through SIEM Platform. Kindly remove this requirement.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
550	175	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 1	The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank	Gartner research highlights the benefits of integrating SOAR and TIP (from the same OEM to enhance security efficiency and reduce complexity. A unified platform streamlines data sharing, automates threat intelligence enrichment, and improves response times by eliminating the need for custom integrations. According to Gartner, consolidating these tools minimizes operational overhead and improves incident response capabilities, as they work in sync to detect and mitigate threats more effectively. By leveraging a single vendor, organizations can ensure better interoperability, reduce management challenges, and strengthen their overall security posture through automated, cohesive workflows. Hence we suggest, SOAR and TIP should be from same OEM Kindly modify this clause to "The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank. Proposed SOAR and TIP solutions should be from the same OEM"	Bidder to comply with RFP terms and conditions.
551	210	Annexure-9 Functional and Technical Requirements	VI. Threat Intelligence Platform (TIP) :, Point 20	The proposed solution offers more than 130 open-sourced intelligence and also provide Free Feeds' content as well	Kindly change the clause to "The proposed solution offers more than 50+ open-sourced intelligence and also provide Free Feeds' content as well"	Bidder to refer Corrigendum-2.
552	177	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 19	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	This is typical case management usecases and is OEM specific Kindly remove this requirement to ensure fair participation	Bidder to comply with RFP terms and conditions.
553	183	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 2	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Given that,SIEM and UEBA are required to be from the same OEM. Our understanding is that the functionalities mentioned in the SIEM,UEBA technical specifications can be achieved through either of the solutions. Please confirm if our understanding is correct.	No, UEBA Technical specifications has to be achived through UEBA solution only.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
554	165	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM): , Point 2	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	a) As per our understanding, solution needs to be sized for 1,00,000 sustained EPS with peak handling capacity of 1,50,000 EPS for both DC and DR respectively. Kindly confirm on the sustained and peak EPS values for both DC and DR respectively. b) To ensure there are no assumptions done by the OEM for solution sizing on log sizing and licensing. Kindly consider modifying this clause as below "The solution shall be sized for 1,00,000 EPS as sustained EPS or 6.5 TB log capture per day (average log size as 800 Bytes) and 150,000 as peak EPS for both for DC & DR respectively during contract period. Solution should have same license across all layers i.e. collection, correlation and management layer to ensure no dropping or queuing of logs on any proposed SIEM components as per bank requirement. There should not be any limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Solution should support unlimited device integrations."	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
555	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 43	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system with critical fields like server IP, Server hostname, OS Name, OS Version, Criticality, Date of discovery etc. to be populated automatically	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.
556	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 44	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
557	166	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 18	Proposed solution should support both automatic and manually escalation of incidents to proposed SOAR and should allow the proposed SOAR to query data from the SIEM	SIEM and SOAR can be from different OEMs as per the RFP. This clause is restrictive as it favours a single OEM which offers both SIEM and SOAR. Please change the clause to "Proposed solution should support export of incidents to proposed SOAR and should allow the proposed SOAR to query incident data from the SIEM"	Bidder to comply with RFP terms and conditions.
558	71	Annexure-2 Pre-Qualification Criteria	Eligibility Criteria	Considering the complexity of the Banking environment, the SIEM, PCAP, UEBA, SOAR and TIP solutions should be from the Proven & Reputed OEMs.	Request you to kindly incorporate below criteria - The SIEM OEM should be incorporated in India under the Companies Act 1956 for at least 10 years . - Minimum Average Annual Turnover (MAAT) for last three years out of last five financial years of the SIEM OEM should not be less than INR Five Hundred (500) Crore. SIEM OEM must have positive net worth.	Bidder to comply with RFP terms and conditions.
559	246	Annexure-17 Bill of Material - Table 3	Price for NGSOC Tech Refresher	As Bank wants to have tech refresh of the existing solutions(Anti DDoS, NBA, DLP, VA), the particular OEM.s associated with these solutions will have an advantage of price negotiation with bidder and not allowing bidder to have freehand in deciding the prices to be quoted for newly asked solutions .	Request Bank to remove these items from this RFP, for all the bidders/OEMs to have fair chance to bid in this RFP.	Bidder to comply with RFP terms and conditions.
560	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	127. The platform should allow user to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts	This technical requirements is of proprietary nature to an OEM, Hence we request you to kindly remove the same. Reference : https://exchange.xforce.ibmcloud.com/hub/extension/f4a537a424977e155105d8aa9f5283c3	Bidder to refer Corrigendum-2
561	166	1.Technical Specifications of each SOC Solutions	I. Security Incident and Event Management (SIEM): Log Storage	Point no 29 to 40	Online storage shall be provided by the SIEM vendor on the server in-built/HCI storage with necessary uptime with failover & performance.SAN appears to be an overhead for the solution.	Bidder to comply with RFP terms and conditions.
562	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	5. The solution should auto replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data	Replication of rules/playbook requirs minimum manual intervention / process between DC & DR with minimum configuration changes required as the assets/IP/User Creds may be different in DC & DR. Kindly modify clause as following "The solution should auto/manual replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data"	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
563	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	9. The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Different OEM's have different count of OOB integrations available. putting such a high number will make it a very limited OEM participation(might be only one) in the bid. We request the bank to modify the clause as The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Bidder to refer Corrigendum-2
564	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	10. Solution should include 100+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank	Different OEM's have different count of OOB playbooks. putting such a high number will make it a very limited OEM participation(might be only one/two oem) in the bid. We request the bank to modify the clause as "Solution should include 50+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank"	Bidder to comply with RFP terms and conditions.
565	177	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	18. The solution should suggest contextual between incidents using machine learning.	We request the bank to modify the clause as "The solution should enrich alert/incident with contextual information using machine learning platform.	Bidder to refer Corrigendum-2
566	178	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	36. Bidder should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc.	We request the bank to modify the clause as "Bidder/OEM should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc."	Bidder to refer Corrigendum-2
567	NA	Generic	Generic	Generic	2. We would like to understand if Bank would like to have training and certification on DLP directly from OEM at Administration or System Engineer level. Bank may include specific requirements on the same like number of trainees and if training is required every year as Bank team changes every few years.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
568	200	V.Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% Yo-Yo Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.
569	Na	Generic	Generic	Generic	Please help us with number of service accounts managed by the current PAM Solution. This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder
570	204	V.Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be trated as 1 application)
571	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
572	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
573	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-2.
574	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
575	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-2
576	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-2.
577	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
578	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-2
579	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-2
580	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-2
581	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2
582	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
583	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
584	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
585	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
586	165-232	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
587	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2
588	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2
589	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-2
590	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
591	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
592	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
593	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2.
594	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
595	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2
596	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-2
597	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2
598	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-2
599	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2
600	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
601	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-2.
602	189	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	7	The solution shall sized to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud	Request you to please amend the clause as "to change data retention period for incidents and alerts on the cloud to 90 days" Beyond this, the solution should be capable of sending events to a SIEM to ensure compliance with Bank regulations.	Bidder to comply with RFP terms and conditions.
603	190	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Given that EDR is deployed on endpoints, the Tap mode is not applicable. Request you to please amend the clause as "to either remove this clause from the requirement or provide further clarification on its intended purpose"	Clause stands deleted. Bidder to refer Corrigendum-2.
604	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	27	The solution should support incident response automation.	Incident Response will be triggered by an admin, and the solution will ensure that these triggers are executed without manual intervention. Kindly confirm if our understanding on this point is the same.	Bidder to comply with RFP terms and conditions.
605	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	34	The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features	Vulnerability assessment is a core component of a vulnerability management solution. Therefore, we request the Bank to remove this clause.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
606	193	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Request you to please amend the clause to modify below points:- Capability of running a coordinated command (such as CMD interface) as capability to execute command or script Request Bank to modify as below function should be available or there should be feasibility to execute command from EDR console to manage Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Bidder to refer Corrigendum-2.
607	198	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Request you to please amend the clause to change supported platform as below:- Windows 10 and above Windows server 2008 and above Kindly request Bank to remove below operating system support IBM AIX, Solaris	Bidder to refer Corrigendum-2.
608	200	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	Request you to please amend the clause as " proposed ssolution to include static scanning up to 1GB and dynamic scanning up to 100MB."	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
609	215	Section 8 , Anti - APT, Annexure 9	2	Each of the bidders proposed solution would be evaluated thoroughly against functional as well as technical requirements. The proposed solution should be from a single OEM (for all components) to ensure the integrated platform requirements and capabilities are utilized and desired security objectives are achieved. The solution expected to import multiple TLS/ SSL certificates.	Request you to please amend the clause as "the proposed SSL Offloader can be from a different OEM than the primary solution provider as long as the solution/requirement meets the functional purpose"	Bidder to comply with RFP terms and conditions.
610	216	Section 8 , Anti - APT, Annexure 9	13	Proposed appliance should have below hardware requirements: Network Traffic Analysis appliances should be supplied with minimum below port requirements with a separate dedicated management and IPMI port with 10/100/1000GBASE-T 4 X 1G/10G RJ45 4 X 1G/10G SFP+ (With Bypass) 8 X 10G SFP+	We request the Bank to let us know if below ports will be ok 2 X 40G QSFP+ 4 X 10G SFP+ 2 X 1G/10G SFP+ 4 X 1G/10G RJ45 bypass 2 X 100G QSFP28	Bidder to refer Corrigendum-2.
611	219	Section 8 , Anti - APT, Annexure 9	35	The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, TAXII and OpenIOC feeds with automated investigation and analysis search function.	Request you to please amend the clause as mentioned below:- The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence using STIX or TAXII or OpenIOC feeds with automated investigation and analysis search function.	Bidder to refer Corrigendum-2.
612	220	Section 8 , Anti - APT, Annexure 9	40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Request you to please amend the clause as the supported operating system as Windows,Linux and MAC	Bidder to refer Corrigendum-2.
613	220	Section 8 , Anti - APT, Annexure 9	42	The solution should have SSL Decryption capabilities available out of the box	Request you to please amend the clause as below If SSL decryption is not feasible on the appliance then bidder should provide SSL decryption	If SSL decryption is not feasible on same appliance. The Bidder has to provide separate SSL decryptor.
614	220	Section 8 , Anti - APT, Annexure 9	47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Given the variability in vendor practices, Request you to please amend the clause as "the proposed solution to either provide the operating system with all necessary licenses or allow the customer to upload their own licenses"	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
615	221	Section 8 , Anti - APT, Annexure 9	53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	Request you to please amend the clause as per below: The solution should support integration with proposed EDR/XDR platform	Bidder to comply with RFP terms and conditions.
616	142	14. SoW for Proposed Services - Threat Inteligence Services - Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage		Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Bidder to comply with RFP terms and conditions.
617	145	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/tools/exchange knowledge for banks brand		Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.
618	146	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank: - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.		Kindly elaborate the scope.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
619	24	6.9.	Penalties/Liquidated damages on failure to resolve incidents like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents)	The selected bidder should resolve the incidents reported. The selected bidder shall be -liable to pay Liquidated damages at the rates specified below subject to a cap of 20% of quarterly payment of in scope service. Resolution time Penalty Amount Within 480 minutes No Penalty 480 to < 540 minutes 3.00% on Basic invoice value of Quarterly payment 540 to < 600 minutes 5.00% on Basic invoice value of Quarterly payment	We request removal of this clause as resolution may involve takedown or assistance from Bank's internal teams to validate/isolate/patch issues that are identified. This SLA is unreasonable given dependencies.	Bidder to comply with RFP terms and conditions.
620	24	6.10.	Penalties/Liquidated damages of delay in Takedown of phishing sites specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.50 per takedown More than 48 hours, but less than 72 hours Rs.100 per takedown More than 72 hours Rs. 150 per takedown	We request modification of the same as - More than 48 hours, but less than 72 hours Rs.50 per takedown More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours Rs. 150 per takedown	Bidder to comply with RFP terms and conditions.
621	25	6.11.	Penalties/Liquidated damages of delay in Takedown of fraudulent mobile/Web apps specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Resolution time Penalty amount More than 24 hours, but less than 48 hours Rs.100 per takedown More than 48 hours, but less than 72 hours Rs.500 per takedown More than 72 hours Rs. 1000 per takedown	We request modification of the same as - More than 72 hours, but less than 120 hours Rs.100 per takedown More than 120 hours, but less than 168 hours Rs.500 per takedown More than 168 hours Rs. 1000 per takedown	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
622	25	6.12.	Penalties/Liquidated damages of failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	A genuine act of defacement on Bank's websites should be detected within 15 minutes of the incident. Penalty at the rate of 10% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 15 minutes but less than 1 hour. In case of response time more than 1 hour the penalty at the rate of 20% of quarterly payment of website scanning services will be charged. If the response time is more than 24 hrs, penalty at the rate of 100% of quarterly payment of website scanning services will be charged.	We request modification as - A genuine act of defacement on Bank's websites should be detected within 4 hours of the incident. Penalty at the rate of 1% of quarterly payment for Website scanning services will be charged for delay in detection of defacement for more than 4 hours but less than 6 hours. In case of response time more than 6 hours the penalty at the rate of 2% of quarterly payment of website scanning services will be charged. If the detection time is more than 24 hrs, penalty at the rate of 5% of quarterly payment of website scanning services will be charged. The Total Penalty levied cannot exceed 10% of the Quarterly Payment (Pro-Rata) for the tool.	Bidder to refer Corrigendum-2
623	28	7.2.2.	Payment Terms for Services	Payment shall be released quarterly in arrears after completion of implementation of the SOC Services mentioned in the RFP and acceptance of the same by the Bank Officials for the respective Assignment.	We request modification to - Payment shall be released yearly in advance after completion of implementation of the Tool. Additionally, the subscription Date starting from the date of implementation and acceptance by the Bank).	Bidder to comply with RFP terms and conditions
624	146	(i)	Early Phishing Detection	Monitoring spam traps to detect phishing mails.	This is a email security tool capability. Canara Bank would be have subscribed to a dedicated e-mail security solution that covers Spam Traps use case. Today, there are several techniques used by spammer/defrauders that evade Spam Traps like using Spam Trap detection services (ex. www.zerobounce.net). We request this clause to be removed as it is an ineffective method to detect phishing campaigns. Monitoring Typo-squatted domain reginstrations, Monitoring Social Media platforms/Darkweb discussions, IRCs (Telegram/Discord) for any targetted phishing campaigns and blocking indicators associated with phishing infrastructure is a much effective way to defend phishing campaigns.	Clause stands deleted. Bidder to refer Corrigendum-2
625	148	(m)	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:	Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	There is no legally obliged entity hosting forums and content on the dark web. Owing to this, there is no takedown possible of Dark Web Mentions or data leaks. We request the bank to remove this clause.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
626	149	(c)	Brand Protection and Monitoring:	Search engines (like Google, Yahoo, Bing etc.) and Generative AI (like chat GPT, Open AI, Gemini etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including but not limited to Truecaller and JustDial.	Kindly elaborate Generative AI monitoring scope. As Generative AI LLMs are trained on specific datasets and are susceptible to poisoning as well. The technology is still in the early days and each Generative AI platform provides unique answers. We request this to be removed from the scope as there isn't a reliable method to monitor GenAI platforms. Tracking of Branch Addresses when the Bank has over 9,000+ branches is not technically feasible and Google Maps enables any user to place a location marker and register a business. Post merger with Syndicate Bank, there are thousands of Canara Bank's Nitya Nidhi Deposit (NND) Scheme Collection agents who would have registered their business. An army of manual analysts would be needed to verify and takedown these addresses. This use case is challenging to address and beyond automation or AI capabilities to monitor.	Bidder to comply with RFP terms and conditions.
627	150	(c)	Attack Surface Monitoring:	The proposed solution shall identify potentially orphaned applications, and services.	We seek clarity from the Bank if "Orphaned applications" refers to shadow IT or dangling DNS records.	Bidder to comply with RFP terms and conditions.
628	151	(q)	Attack Surface Monitoring:	The proposed solution shall be able to validate the Current IP attribution is using DNS, Netblock, and Keywords to improve accuracy.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
629	151	(t)	Attack Surface Monitoring:	The proposed solution shall be able to do Active Banner Grabbing and advanced search based on banners to detect any vulnerable version and provide reports as mentioned earlier.	We request the Bank to elaborate the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
630	151	(w)	Attack Surface Monitoring:	The proposed solution shall be able to perform Network-level Risk scanning to identify misconfigured servers, services, and devices.	We request the Bank to define "devices".	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
631	153	c)	Other Services & Requirements:	The solution shall provide correlation capability and actionable intelligence with respect to historical reference to threats.	We request the Bank to elaborate the use case.	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
632	154	b)	Service Level Agreements	Alert within 20 minutes of attack/compromise/down/not reachable.	This is a WAF/IPS/IDS/SIEM/Application Monitoring/EDR/MDR/NAC use case. We request the same to be removed from the scope.	Bidder to comply with RFP terms and conditions.
633	154	d)	Service Level Agreements	Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident and fraudulent mobile apps within 24 hours.	We request this to be modified to - Take down of Phishing Site within 48 hours of detection and fraudulent mobile apps within 72 hours.	Bidder to refer Corrigendum-2.
634	154	f)	Service Level Agreements	Resolution of Trojan incidents with 24 hrs of detection.	This scope is beyond the scope of Threat Intelligence Services. We can alert of any Trojan Incident leading to data leak and it being available on the Dark Web or Freemium/Premium portals/marketplaces.	Clause stands deleted. Bidder to refer Corrigendum-1.
635			Propose Addition of Clause		As a Best Practice - we suggest the Threat Intelligence Platform and Threat Intelligence Services to be subscribed from different OEMs/Vendors. Several Indian Government entities/PSUs have adopted this approach for better coverage.	Bidder to comply with RFP terms and conditions.
636	125	III. Security Orchestration, Automation and Response (SOAR)	The solution should ensure that time between MTTD and MTTR should be improved gradually. Further, the vulnerability window should be within the tolerable time limit of the Bank.		What is tolerable limit? We understand there is a tolerable limit for vulnerability, Please elaborate what is the expectaion in relation to Vulnerability in SOAR and what is the tolerable limit in terms of timeline?	As per the defined SLA for updates/upgrades documented in the RFP
637	125	III. Security Orchestration, Automation and Response (SOAR)	The bidder shall develop custom integration as necessary within the defined timeline.		The expectation is to build custom integration in SOAR within defined timeline, please clarify what is the timeline? What type of custom integration are expected? How many custom integration are expected?	Bidder to comply with RFP terms and conditions.
638	125	III. Security Orchestration, Automation and Response (SOAR)	· Bidder to perform periodic backup and store in a secure storage. · Bidder to fix the gaps identified by OEM or Auditor as part of the assessment · Bidder to build incident and alert layout.		The expectation is to perform periodic backup and storage, Please clarify whether you want to have backup of alerts or raw logs? Please clarify for what timeline is the storage required?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
639	130	VII. Threat Intelligence Platform (TIP)	Bank is procuring Centralized Cyber Threat Intelligence Platform solution for which Bidder has to provide the services which includes but not limited to the following:		Please clarify whether the requirements mentioned below are in relation to Threat Intel Management as a platform or as a service?	Threat Intelligence Platform (TIP)
640	130	VII. Threat Intelligence Platform (TIP)	· Perform periodic validation of integration, data flow, and automation configurations.		Please clarify what is the frequency of periodic validation?Who will do validation? Bidder?	Bidder to comply with RFP terms and conditions.
641	130	VII. Threat Intelligence Platform (TIP)	· Train security analysts and relevant personnel on TIP operations, use cases, and best practices.		Please clarify who is expected to train security analyst and personnel, is it expected from Bidder? Who will train analyst? Bidder?	Bidder to comply with RFP terms and conditions.
642	87	Sizing & Scalability Requirements	Anti-APT - 20 Gig Hardware Capacity with 10Gig on day one TLS Inspection Throughput at DC, DR		Does the bank need 20 Gbps throughput with TLS decryption ? Or does the RFP state that the bank needs 20Gbps threat prevention with support for TLS decryption.	Yes , bank needs 20Gbps throughput with TLS decryption.
643	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	Are you seeking a cybersecurity solution that offers internal attack path analysis and continual testing functionality across Microsoft Azure, AWS, and on-premise environments?	Yes, but not limited to any specific cloud providers
644	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	Do you require the ability to simulate real attacker activities continuously, leveraging misconfigurations, user behaviors, and vulnerabilities within your infrastructure?	Yes
645	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	Is real-time discovery of new security issues impacting critical assets a critical requirement for your organization?	Yes
646	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	Would you like the platform to enable the creation of an unlimited number of attack scenarios to assess and improve your security defenses continuously?	Bidder to comply with RFP terms and conditions.
647	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	Are you interested in a cybersecurity solution that provides a wide range of recommended, 'out of the box' attack scenarios for comprehensive security testing?	Bidder to comply with RFP terms and conditions.
648	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	What is the total number of servers in your environment?	The details will be shared with selected Bidder

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
649	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	How many desktops do you have within your organization?	The details will be shared with selected Bidder
650	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	What is the total number of public cloud instances across AWS, Azure, and GCP, including VMs, DB PaaS services, workstations, workloads, cloud databases, servers, and Kubernetes clusters?	The details will be shared with selected Bidder
651	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	How many external IPs or domains does your organization need to monitor and protect against potential threats?	The details will be shared with selected Bidder
652	142	14. Scope of Work for Proposed services	b) Breach Attack Simulation (BAS)	Generic	What is the total number of technologies (e.g. Firewall, EDR etc....)	The details will be shared with selected Bidder
653	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should have MFA capabilities of SMS, Email or Application based authenticator (TOTP). If the solution does not have in-built feature, then the OEM should provide additional tool to meet the objective without any additional cost. It should have an inbuilt authentication for Biometrics and must integrate with Bank's existing biometric solution	Kindly provide details on Bank's existig biometrics solution ? is it FIDO compliant and which is the OEM ?	Bidder to refer Corrigendum-2
654	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.	Kindly provide list of applications and application platform for which this capability is required ? Also request to clarify the number of application for BOQ.	The list of applications will be provided to selected Bidder, however the number of applications is 50
655	204	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution should be able to provide rotation capabilities at scale (across technologies)	Kindly provide the ist of technologies for which require credentials rotation capabilities	Bidder to comply with RFP terms and conditions.
656	206	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution must enforce auto- rotation for each password/ key before the default expiry of custom expiry date of the keys/ certificate.	Kindly mention the type of keys/certificates. Kindly clarify the count of such certificates to arrive at BOQ .	Bidder to refer Corrigendum-2
657	202	Annexure-9	Technical Specifications of each SOC Solutions: PIM	The solution shall have feature to manage system and application-level privilege accounts. OEM to support application integration	Kindly provide list of applications for integrationg to PAM	Bank will provide the details to the selected Bidder
658	243	Annexure 17	Bill of Material	User Licenses Cost	For PIM Solution which is subscription based, how do we represent costing in the table	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
659	251	Annexure 17		Table 5) AMC/ATS Cost for items mentioned in Table- 1 and Table- 2	For PIM solution which is subscription based, it will be spread across all the 5 years and there is no separate licenses and AMC costing how do we represent the 4th and 5th year costing in this table?	Bidder to refer Corrigendum-2
660	255	Annexure 17A	Optional Cost	Optional cost for PIM Solution - Cost per Additional 100 IDs (in bundles)	The cost for additional 100 IDs meaning cost for additional users? Also is this licenses cost per year?	Yes, the cost for 100 IDs meaning cost for additional users
661	27	Payment terms	License cost	100% After complete delivery of license and on production of relevant documents like delivery signoff and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment	Kindly consider license cost from date of delivery as the start of the term of contract period	Bidder to comply with RFP terms and conditions.
662	27	Payment terms	License cost	100% After complete delivery of license and on production of relevant documents like delivery signoff and invoice with product serial number of the items supplied duly approved by the Bank Officials while claiming the payment	Kindly consder US $ fluctuation variation factor for yearly annual invoicing	Bidder to comply with RFP terms and conditions.
663	86	Annexure 8 - SOW	3. Sizing and scalability requirement	12. PIM - 1500 users licenses requirement	Pls share the profiles of these 1500 users - are they all Bank's internal employees, or vendor resources, What other profiling details can you share of these 1500 users - Networki team, DB team, App team, admins, super admins, approvers, etc	Bidder to comply with RFP terms and conditions.
664	201	Annexure-9	Technical Specifications of each SOC Solutions: (V) PIM	The solution shall have redundancy to failover in DC and DR both in HA in case the primary solution goes down. All the required hardware, software, OS, storage and required licenses shall be provided by the bidder.	Kindly provide the maximum concurrent sessions required in order to recommend appropriate hardware requirement.	Bidder to comply with RFP terms and conditions.
665	156	14. Scope of Work for Proposed services	c) Cyber Range	Generic	Our understanding is that a total of 40 Hours per year of Range access along with trainer as applicable has to be provided to the Bank. This will be done for a batch of 5 people. Please clarify if this is correct. Also kindly let us know for how many years should this be quoted?	Bidder to refer Corrigendum-2
666	156	14. Scope of Work for Proposed services	c) Cyber Range	Generic	Our understanding is that the bidder has to own the preparatory hours for training to be done on Cyber Range. Ideally this is outside the 40 hours mentioned for the Cyber range SAAS platform. Please clarify if our understanding is correct.	Bidder to refer Corrigendum-2
667	166	1.Technical Specifications of each SOC Solutions	I. Security Incident and Event Management (SIEM): Log Storage	Point no 29 to 40	Online storage shall be provided by the SIEM vendor on the server in-built/HCI storage with necessary uptime with failover & performance.SAN appears to be an overhead for the solution.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
668	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	5. The solution should auto replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data	Replication of rules/playbook requirs minimum manual intervention / process between DC & DR with minimum configuration changes required as the assets/IP/User Creds may be different in DC & DR. Kindly modify clause as following "The solution should auto/manual replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data"	Bidder to comply with RFP terms and conditions.
669	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	9. The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Different OEM's have different count of OOB integrations available. putting such a high number will make it a very limited OEM participation(might be only one) in the bid. We request the bank to modify the clause as The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Bidder to refer Corrigendum-2
670	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	10. Solution should include 100+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank	Different OEM's have different count of OOB playbooks. putting such a high number will make it a very limited OEM participation(might be only one/two oem) in the bid. We request the bank to modify the clause as "Solution should include 50+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank"	Bidder to comply with RFP terms and conditions.
671	177	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	18. The solution should suggest contextual between incidents using machine learning.	We request the bank to modify the clause as "The solution should enrich alert/incident with contextual information using machine learning platform.	Bidder to refer Corrigendum-2
672	178	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	36. Bidder should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc.	We request the bank to modify the clause as "Bidder/OEM should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc."	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
673	2	Annexure 10 , Point no.6	The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. 10 Marks		This gives undue advantage to one specific technology OEM (PIM Vendor). For all other technologies, the highest scoring is capped at 5 marks, However in case of PIM, the marking is very high. We highly recommend to reduce from 10 to 5 marks & provision the remaining 5 marks for other technologies which bank intends to procure.(Example: DAST/TIP)	Bidder to comply with RFP terms and conditions.
674	2	Annexure 10 , Point no.10	Evaluation Criteria	Presentation by the Bidder:	Since this is a QCBS RFP & minimun marks required to qualify under technical evaluation is set at 70 marks, allocating 25 marks only for the bidder presentation can make it to difficult for bidders to qualify.	Bidder to comply with RFP terms and conditions.
675	222	Annexure-9 Functional and Technical Requirements	IX.Breach Attack Simulation (BAS):		1.Can you provide an overview of your organization's structure and size? oNumber of servers oNumber of Desktops oNumber of Public Cloud Instances (AWS, Azure & GCP) - for example number of VMs and DB PaaS Services - (i) Workstations; (ii) Workloads (Virtual Machines such as EC2s, VMs, Compute Engines) + Cloud Database + Servers + K8 clusters	The details will be shared with selected Bidder
676	222	Annexure-9 Functional and Technical Requirements	IX.Breach Attack Simulation (BAS):		Number of External IP or Domains	The details will be shared with selected Bidder
677	2	Annexure - 8	Scope of Work	d. Deploy qualified personnel in Bank's premises at Bengaluru and Mumbai for configuration, monitoring and management of in scope NGSOC solutions.	Is the bank expecting resources to be located at Bangalore only or Mumbai aswell. In which case, can the bank give the split of resoruces required in Bangalore and Mumbai. Also, request bank to allow the bidder to place resources with the mix of both the locations for the SOC operations	This will be shared to succcessful bidder
678	2	Annexure - 8	Scope of Work	f. Bidder to do proactive Security Threat Hunting across Bank's environment and implement adequate information security controls to protect Bank IT assets from breach.	Request bank to clarify if they are expecting a dedicated resource for threat hunting. Considering the volume, request bank to include a threat hunter as a dedicated resource under manpower	Bidder to comply with RFP terms and conditions.
679	3	Annexure - 8	Scope of Work	n. Provide immediate forensic support in case of any security / cyber incident.	Is this additional services expected and how many hours of forensic services expected	Bidder to refer Corrigendum-1
680	4	Annexure - 8	Sizing & Scalability Requirements	10. 5000 licenses along with the new hardware	Is the overall quantity expected is 2300+5000 or its combined to 5000 only	Combined 5000

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
681	28	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months.	Is bank expecting the the OEM PS to be used only for the migration of the existing 4 solutions which is retained or the overall solution stack	Bidder to refer Corrigendum-2.
682	29	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	The complete NGSOC infrastructure, including but not limited to hardware, software, storage, services, licenses would be provided by the bidder. The Bank will provide facilities to host the devices for the personnel and workstations (Desktop/Laptop).	Is is presumed that bank will provision the required rack space, power and cooling. Also, will the bank provide the required Network and SAN switches or is this expected from the bidders.	SAN/ NAS Switches to be provisioned by the Bidder.
683	29	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	The Bidder should ensure the proposed solutions should be compatible with or able to integrate with quantum-resistant technologies and encryption methods.	Can bank provide more details on the required integrations based on the quantum-resitant solutions.	Bidder to comply with RFP terms and conditions.
684	30	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	All phases of installation, configuration, and integration of all solutions shall be done by the bidder in coordination with the OEM till sign-off. For designing and deployment validation, sign-off would be jointly done by both OEM and Bidder's engineers. It will be the Bidder's responsibility to liaison with the OEM to provide full technical support to the satisfaction of the Bank for the complete tenure of the agreement i.e., the project.	Under the point 2 of the same section, it is mentioned that bidder should involve OEM PS. Can bank clarify if the implemenation needs to be carried out by the bidder or OEM PS or any of bidder partners?	Bidder to comply with RFP terms and conditions.
685	30	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	Wherever Bank has provided VMs/physical servers/storage for installation of OS/DB/middleware/application component for proposed SOC solutions, it is the responsibility of the Bidder to perform end to end maintenance, support, upgrade etc. in line with the comprehensive scope.	This point is contradictory as the bank has mentioned that the bidders to provide the required Hardware and Software. Can bank clarify under what circumstances this point will be applicable.	Bidder to comply with RFP terms and conditions.
686	30	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	NGSOC and other solutions should be scalable and user configurable to cater to the future requirement of the Bank with a projection for next 5 years.	We presume the overall the specifications shared is based on the scalability in consideration for the next 5 years and also bank metioned 10% YoY growth for DLP & VA only. Can bank also clarify the YoY growth for the rest of the solutions.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
687	31	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	The period of support coverage for NGSOC and in scope solutions would be for 5 years from the date on which last sign-off / project closure document covering all NGSOC, and other solutions covered under this RFP is provided to the Bidder from the Bank, or the extended contract period, if any.	This point is contradictory as the bank has already mentioned in one of the earlier point as mentioned below, that the support start will be from the sign-off for each solution/group and not the entire NGSOC solutions. Kindly confirm when the support start period to be considered whether from the signoff of respective solutions or the overall project. (Reference to the page number 30, point 1 "The bidder should ensure that NGSOC and other solutions have a comprehensive onsite warranty of 3 years and 2 Years of AMC / ATS. The warranty shall commence from the acceptance / sign-off date from Bank for each solution / group of solutions.")	Bidder to comply with RFP terms and conditions.
688	31	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	The period of support coverage for NGSOC and in scope solutions would be for 5 years from the date on which last sign-off / project closure document covering all NGSOC, and other solutions covered under this RFP is provided to the Bidder from the Bank, or the extended contract period, if any.	Kindly clarify when the warranty start period to be considered whether from the signoff of respective solutions or the overall project.	Yes, Warranty will start from the Sign off respective Solution/Service.
689	32	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	Bidder needs to ensure that the NGSOC solution can integrate with other IT Systems using standard methods/ protocols/ message formats without affecting the existing functionality of the Bank.	Can bank provide details about the other IT Systems present at the bank.	Bidder to comply with RFP terms and conditions.
690	32	Annexure - 8	Scope of Work for Bidder/ System Integrator (SI)	Bidder shall provide required load balancers for the NGSOC.	The Load Balancers mentioned are only in the SIEM architecture mentioned in the RFP. Can bank provide the sizing details.	Bidder to note that it is as per SIEM & PIM Solution sizing
691	34	Annexure - 8	NGSOC Operations	Bidder should develop custom plug-ins/connectors/agents for business application monitoring.	Can bank proivde details and number of the custom plug-ins required to be built during the implementation phase	Bidder to comply with RFP terms and conditions.
692	37	Annexure - 8	Incidents and Problem Management	Bidder should document or develop playbooks complying with Bank's Crisis Management Plan based on various threat scenarios. These playbooks should be tested on quarterly basis in coordination with various stakeholders in Bank/Other relevant service providers. These playbooks should be reviewed on an annual basis and should be modified as and when required.	Please mention the number of playbooks required to be delivered during the implementaiton phase	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
693	37	Annexure - 8	Incidents and Problem Management	Bidder should document or develop playbooks complying with Bank's Crisis Management Plan based on various threat scenarios. These playbooks should be tested on quarterly basis in coordination with various stakeholders in Bank/Other relevant service providers. These playbooks should be reviewed on an annual basis and should be modified as and when required.	Is the expectation to develop these playbooks withing the implementation phase or during the operation phase In case during the implemenation phase, request bank to kinldy mention the number of playbooks to be created.	Bidder to comply with RFP terms and conditions.
694	38	Annexure - 8	Scope of Work for Proposed Solutions	Bidder should develop parsers for all log sources without any cost to the Bank.	How many parsers to be developed during the implementation phase and the operation phase	Bidder to comply with RFP terms and conditions.
695	39	Annexure - 8	Scope of Work for Proposed Solutions	Bidders should integrate the proposed SIEM with a ticketing tool for automated ticket generation.	What is the existing Ticketing tool available with bank or is the bidder expected to provide the tool	Existing ITSM Solution is Service Now.
696	42	Annexure - 8	SIEM Use case Management	1,00,000 EPS for each site with Hardware Scalable up to 1,50,000 EPS (i.e At each site Hardware should support for min. 3 Lakh EPS)	The understanding is bank is expecting the hardware & Storage to support 3lakh EPS at each location (DC and DR)	Yes
697	42	Annexure - 8	SIEM Use case Management	1,00,000 EPS for each site with Hardware Scalable up to 1,50,000 EPS (i.e At each site Hardware should support for min. 3 Lakh EPS)	Centrain vendors provides licenses based on GB's per day (Capcity based) instead of EPS. Request bank to clarify what should be the GB's needed	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
698	42	Annexure - 8	SIEM Use case Management	1,00,000 EPS for each site with Hardware Scalable up to 1,50,000 EPS (i.e At each site Hardware should support for min. 3 Lakh EPS)	Request bank to clarify the event size for the EPS to size the storage accordingly	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
699	119	RFP	Scope of Work for Proposed Solutions	Security Information & Event Management (SIEM)	As bank asked for SaaS platform for EDR, request bank to clarify whether if they would need a separate log collector at the DMZ for the log ingession from the outside to inside.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
700	44	Annexure - 8	Security Orchestration, Automation and Response (SOAR)	The bidder shall develop custom integration as necessary within the defined timeline.	Can bank provide some insights into the number of integrations required	Bidder to comply with RFP terms and conditions.
701	48	Annexure - 8	Threat Intelligence Platform (TIP)	The Bidder will be responsible for onboard internal and external threat intelligence feeds such as open-source, commercial, government, etc. Bank shall provide the commercial TI feed API to consume.	Some of the government threat feeds are provided in CSV format and this can only be updated manually, we presume bank is in agreement on this as there is no automation possible in such cases.	Bidder to comply with RFP terms and conditions.
702	50	Annexure - 8	Anti-APT and Sandboxing	Bidder should install and configure an Anti-APT solution to protect against web and email attacks.	Request bank to clarify if they are expecting solution to be integrated with their O365 cloud to protect against email attacks	Bidder to note that the requires ANTI-APT Solution is to protect Web traffic alone.
703	13	RFP	Scope of Work	During the course of the project, there might be related areas which Bank would like the selected Bidder to undertake which may not have envisaged earlier.	Can bank be more specific in this ask. Is is related to a new solution deployment?	Bidder to comply with RFP terms and conditions.
704	14	RFP	Project Timelines	Delivery of all the equipment (software and hardware) as quoted in the bill of materials for SIEM, SOAR, UEBA and PCAP. Date of delivery of last item shall be taken as date of delivery for all items.	Request bank to extend the delivery to 12 weeks considering the fact that the required infrastructure components like hardware, software and storage needs to be delivered as well	Bidder to comply with RFP terms and conditions.
705	14	RFP	Project Timelines	Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	Considering the scale of the deployment, request bank to extend this 24 weeks without considering the 8 weeks of delivery.	Bidder to refer Corrigendum-2
706	21	RFP	Penalties/ Liquidated Damages	The maximum penalty levied shall not be more than the 100% of the monthly charges payable to NG SOC services operations	Requet bank to change the overall penalty on the SI/MSP which shall not exceed 20% of the quarterly payment	Bidder to refer Corrigendum-2
707	23	RFP	Manpower Services	Onsite personnel resources (L1/L2/L3)	Can bank provide the below. 1. Location wise breakup for the L1 and L2 deployment 2. Can hybrid working be allowed to attract more talents	Bidder to comply with RFP terms and conditions.
708	85	RFP	Sizing & Scalability Requirements	Threat intelligence management platform	Request bank to also consider cloud service (Hybrid model)	Bidder to comply with RFP terms and conditions.
709	86	RFP	Sizing & Scalability Requirements	DAST	Request bank to also consider cloud service (Hybrid model)	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
710	87	RFP	Sizing & Scalability Requirements	Anti-APT	Do we need a separate SSL Offloader, if so bank has to provide the sizing for the same.	If SSL offloader is not feasible on same appliance. The Bidder has to provide separate SSL offloader.
711	234	RFP	Annexure-10	The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 5 Note: For CEH maximum 5 number of certified resources will be considered	Certifications mentioned in this point such as CISSP and other are more focused on the governance and architecture roles. Whereas the CEH is predominantly will be on the handson for threat hunting, forensic analysis and etc. Hence, request bank not to restrict CEH certifiation or increase the cerfication count.	Bidder to refer Corrigendum-2
712	1	Payment Terms	1	Product (HW+SW) Delivery - 30% Install - 40% After 3 Months - 20% After warranty - 10% License Delivery - 100% Installation UAT - 30% On Install - 55% DR Drill - 10% NGSoc - 5% AMC/ATS Quarterly in Arrears Additional requirement On Install - 100% FMS Monthly in Arrears	Request Canara Bank to modify the clause as per below Product (HW+SW) Delivery - 80% Install - 10% After 3 Months - 10% License Delivery - 100% Installation UAT - 30% On Install - 55% DR Drill - 10% NGSoc - 5% AMC/ATS Quarterly in Arrears Additional requirement On Install - 100% FMS Monthly in Arrears	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
713	31	Generl T&C	15	iii. Liquidated Damages: If the Seller/Service Provider fails to deliver any or all of the Goods/Services within the original/re-fixed delivery period(s) specified in the contract, the Buyer will be entitled to deduct/recover the Liquidated Damages for the delay, unless covered under Force Majeure conditions aforesaid, @ 0.5% of the contract value of delayed quantity per week or part of the week of delayed period as pre-estimated damages not exceeding 10% of the contract value of delayed quantity without any controversy/dispute of any sort whatsoever.	Request Bank to modify the clause as per below. iii. Liquidated Damages: If the Seller/Service Provider fails to deliver any or all of the Goods/Services within the original/re-fixed delivery period(s) specified in the contract, the Buyer will be entitled to deduct/recover the Liquidated Damages for the delay, unless covered under Force Majeure conditions aforesaid, @ 0.5% of the contract value of delayed quantity per week or part of the week of delayed period as pre-estimated damages not exceeding 5% of the contract value of delayed quantity without any controversy/dispute of any sort whatsoever.	Bidder to comply with RFP terms and conditions.
714	233	RFP	Annexure-10, point 7	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience •For 5 or more clients - 5 marks •For 2 clients - 3 marks	Considering the availability & updation of the solution which resides with the OEM, request bank to change this to OEM or Bidder/OEM as the criteria.	Bidder to refer Corrigendum-2.
715	253	RFP	Table 7	Cost for any additional requirements /additional customization/ enhancement	Request Bank to confirm charges would be only for for per man days and not for any additional Hardware.	Bidder to comply with RFP terms and conditions.
716	248	RFP	Table 3) Price for NGSOC Tech Refresher	In future if any additional Hardwares/ Softwares are required for the smooth functioning of the solution the same has to be provided by the bidder at no extra cost to the Bank.	Request Bank to change the clause as per below. For any future Hardware/ Software requirement, bidder shall charge the Bank at a mutually agreed price for the respective Hardware and Software.	Bidder to refer Corrigendum-2.
717	49	RFP	12.2	12.2.Bank shall serve the notice of termination to the bidder at least 30 days prior, of its intention to terminate services without assigning any reasons.	Request Bank to terminate only for cause. Customer shall, apart from paying NTT for Products/ Licenses already delivered, shall also pay NTT for orders already placed with OEMs/ Software Licensors, which Orders cannot be cancelled with the OEMs/ Software Licensors, cancellation costs, if any, levied by the OEMs/ Software Licensors, and logistical and administrative expenses, if any, incurred by NTT on account of such cancellations, which expenses shall be billed on actuals.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
718	20	RFP	6	Above LD is applicable for the following solutions SIEM, SOAR, UEBA, EDR, PIM, Anti-DDoS, Anti -APT and for other NG SOC solutions/services minimum uptime of 90 percent to be maintained, else flat 20% of monthly NGSOC operations charges will be levied.	Request Bank to modify the clause as per below. Above LD is applicable for the following solutions SIEM, SOAR, UEBA, EDR, PIM, Anti-DDoS, Anti -APT and for other NG SOC solutions/ services minimum uptime of 90 percent to be maintained, else flat 10% of monthly NGSOC operations charges will be levied.	Bidder to refer Corrigendum-2
719	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	Log Storage (Clause Nos. 30 -40)	The technical specifications for Log Storage in the RFP appear to be favourable towards a particular vendor. In the spirit of open participation, we would request Canara Bank to kindly make the specifications for storage more generic which would enable bidders to choose from among multiple leading storage technology OEMs and be more competitive.	Bidder to comply with RFP terms and conditions.
720	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	30. SAN storage Systems should support Native Storage virtualization of 3rd party storage system for centralized management and SAN Storage systems should support 100 % Data Availability guarantee	Considering that bidders will be proposing a new storage array, we do not see the relevance of the functionality of native storage virtualization of 3rd party storage systems. This functionality also appears to be favouring a partcular vendor. So, in the spirit of open participation, we would request Canara Bank to kindly remove this clause.	Bidder to comply with RFP terms and conditions.
721	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	32. No single point of failure, The SAN system should deliver Industry leading Performance of up to 2M+ IOPS	Since the storage to be offered would need to be sized in line with the performance requirements of the SIEM solution to be proposed, we would request Canara Bank to kindly remove this clause and mention that the offered storage should be able to deliver the required performance in line with the SIEM solution requirements.	Bidder to comply with RFP terms and conditions.
722	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	33. End to End SAN Infra monitoring from a single management suite.	Please clarify what functionality is required and what needs to be monitored.	Bidder to comply with RFP terms and conditions.
723	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	34. SAN system should support native remote replication both synch & Asynch replication for backup/DR purposes. The storage system should support Zero RTO natively.	Since the requirement is for the SIEM Application to provide the functionality of dual forwarding / streaming / replication without relying on other 3rd party replication technologies on the OS or storage level, kindly confirm that the functionality of storage based replication is not relevant as part of the proposed storage systems. Moreover, Zero RPO/RTO solutions would typically entail active-active storage solution across sync/metro distances only, and not across larger distances, so that would also not be relevant under the current circumstances. We would request Canara Bank to kindly delete this clause.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
724	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	36. The NAS system should be symmetric active-active architecture and should have unified capability i.e., should support block and file access with host connectivity for FC, iSCSI, CIFA and NFS. If external appliance required, it should be proposed with necessary licenses.	Please clarify what is meant by symmetric active-active functionality and what is expected as part of this functionality in NAS. This functionality also appears to be favouring a partcular vendor. So, in the spirit of open participation, we would request Canara Bank to kindly remove this clause.	Bidder to comply with RFP terms and conditions.
725	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	38. Proposed NAS system should have purpose built hardware acceleration through specialized hardware such as FPGA for superior performance.	Please clarify why FPGA is required, since different OEMs/technology vendors have their own methods of achieving performance. Kindly confirm if it would be adequate to offer the required performance for log storage as per the sizing of the SIEM solution. This functionality also appears to be favouring a particular vendor. So, in the spirit of open participation, we would request Canara Bank to kindly remove this clause.	Bidder to comply with RFP terms and conditions.
726	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	39. The system must be dedicated appliance with specifically optimized OS to provide both flash and NAS functionalities. The architecture should allow modular upgrades of hardware and software. The system should be suitably configured for achieving enhanced performance and throughput	Flash drives can be offered in both SAN and NAS. Please clarify whether we need to offer NAS functionality for Archival on Flash, as Archival storage is not normally considered on Flash disks. Also kindly confirm if the storage needs to be Unified or if it is acceptable to offer SAN and NAS separately.	Bidder to comply with RFP terms and conditions.
727	166	RFP	Annexure-9, I.Security Incident and Event Management (SIEM):	41. At any time during contract period technological advances w.r.to solution (Application/ Software/ Hardware etc.) introduced by the OEM/ Bidder for information technologies originally offered by the supplier in its bid, the bidder and OEM shall be obliged to offer to bank the latest version of the available technologies having equal or better performance or functionality throughout the contract period without any extra cost to bank. During performance of the Contract, the bidder shall offer to bank all new versions, releases and updates of standard software/ hardware/ application etc, as well as related technical support within 30 days of their availability from the OEM.	OS/firmware upgrades for storage can be offered while the storage is under active support. However, that would not be applicable to technological advances regarding hardware refresh. So we would request Canara Bank to kindly remove references to Hardware in this clause.	Bidder to comply with RFP terms and conditions.
728	125	Security Orchestration, Automation and Response (SOAR)	RFP	The solution should ensure that time between MTTD and MTTR should be improved gradually. Further, the vulnerability window should be within the tolerable time limit of the Bank.	We understand there is a tolerable limit for vulnerability, Please elaborate what is the expectaion in relation to Vulnerability in SOAR and what is the tolerable limit in terms of timeline?	As per the defined SLA for updates/ upgrades documented in the RFP.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
729	125	Security Orchestration, Automation and Response (SOAR)	RFP	The bidder shall develop custom integration as necessary within the defined timeline.	The expectation is to build custom integration in SOAR within defined timeline, please clarify what is the timeline? What type of custom integration are expected? How many custom integration are expected?	Bidder to comply with RFP terms and conditions.
730	125	Security Orchestration, Automation and Response (SOAR)	RFP	Bidder to perform periodic backup and store in a secure storage. · Bidder to fix the gaps identified by OEM or Auditor as part of the assessment · Bidder to build incident and alert layout.	The expectation is to perform periodic backup and storage, Please clarify whether you want to have backup of alerts or raw logs? Please clarify for what timeline is the storage required?	Bidder to comply with RFP terms and conditions.
731	130	Threat Intelligence Platform (TIP)	RFP	Bank is procuring Centralized Cyber Threat Intelligence Platform solution for which Bidder has to provide the services which includes but not limited to the following:	Please clarify whether the requirements mentioned below are in relation to Threat Intel Management as a platform or as a service?	Threat Intelligence Platform (TIP).
732	130	Threat Intelligence Platform (TIP)	RFP	Perform periodic validation of integration, data flow, and automation configurations	Please clarify what is the frequency of periodic validation?	Bidder to comply with RFP terms and conditions.
733	130	Threat Intelligence Platform (TIP)	RFP	Train security analysts and relevant personnel on TIP operations, use cases, and best practices.	Please clarify who is expected to train security analyst and personnel, is it expected from Bidder?	Bidder to comply with RFP terms and conditions.
734	216	Anti-APT	RFP	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Does the bank need 20 Gbps throughput with TLS decryption ? Or does the RFP state that the bank needs 20Gbps threat prevention with support for TLS decryption.	Yes, bank needs 20 Gbps throughput with TLS decryption.
735	165	SIEM	Technical Specification	SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and Cloud). If the parser is not available the bidder/ OEM should developed the parsers without any extra cost to bank	Kindly let us know expected number of custom parser to be planned.	Bidder to comply with RFP terms and conditions.
736	174	SIEM Packet Capture	Technical Specification	The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation.	Should we be procuring 20 Gbps hardware from day one	Yes

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
737				The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.		Bidder to comply with RFP terms and conditions.
738	94	Platform Management	Manpower Requirement	Platform management - Manpower requirement : SIEM, SOAR, & UEBA Engineer (L3 OEM)	Reuest you to change "Bidder/OEM Engineer"	Bidder to comply with RFP terms and conditions.
739	175	SOAR	Technical Specification	All the hardware/software required for the solution shall be provisioned by the OEM	Request to change "All the hardware/software required for the solution shall be provisioned by the Bidder"	Bidder to refer Corrigendum-2
740	200	EDR	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	The average file size sent to sandbox for analysis is typically between 5MB and 30MB and these are mostly executable files like".exe", ".dll" or documents such as ".pdf", ".docx". For files of size 1GB the sandbox analysis takes much longer time and can be prone to timeouts leading to missed detections. The extended tme required to analyse large fles can delay incident response and could slow down decision-making process and remediation efforts and potentially miss sophisticated threats. Also having mandated a 1Gb File size Sandbox is specific to an individual OEM , restricting participation of Pure Play best in class EDR / XDR solutions and thus request the Bank below. The point should be read as " The proposed sandboxing component should have the capability to scan the file size upto 50MB".	Bidder to refer Corrigendum-2
741	191	EDR	23	The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files, data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).	Data Exfiltration use cases are handled by the DLP solutions installed on the endpoints/systems and bank is exploring DLP solution as part of this RFP. Requesting bank to remove data exfiltration capability from EDR requirements.	Bidder to refer Corrigendum-2
742					The point should be read as "The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files."	Bidder to refer Corrigendum-2
743	195	EDR	71	Should have outbreak prevention feature that allows to configure port blocking, block shared folder, and deny writes to files and folders manually.	This is vendor specific and restricts large and prominent EDR players to participate. This exact point is outlined in https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/outbreak_prevention_policy.html.and explains the technique/approach used to handle outbreak prevention.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
744					The point should be read as "Should have outbreak prevention capabilities."	Bidder to comply with RFP terms and conditions.
745					SentinelOne's approach to outbreak prevention is as outlined below:	Bidder to comply with RFP terms and conditions.
746	200	V.Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% Yo-Yo Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.
747		General	General	General	Please help us with number of service accounts to be managed by PIM This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder.
748	200	V.Privileged Identity Management (PIM)	Architecture & General	5. The solution shall have redundancy to failover in DC and DR both in HA in case the primary solution goes down. All the required hardware, software, OS, storage and required licenses shall be provided by the bidder.	Please help us with DC and DR locations.	This will be shared to succcessful bidder.
749	204	V.Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be trated as 1 application)
750	189	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	7	The solution shall sized to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud	Request you to please amend the clause as "to change data retention period for incidents and alerts on the cloud to 90 days" Beyond this, the solution should be capable of sending events to a SIEM to ensure compliance with Bank regulations.	Bidder to comply with RFP terms and conditions.
751	190	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Given that EDR is deployed on endpoints, the Tap mode is not applicable. Request you to please amend the clause as "to either remove this clause from the requirement or provide further clarification on its intended purpose"	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
752	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	27	The solution should support incident response automation.	Incident Response will be triggered by an admin, and the solution will ensure that these triggers are executed without manual intervention. Kindly confirm if our understanding on this point is the same.	Bidder to comply with RFP terms and conditions.
753	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	34	The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features	Vulnerability assessment is a core component of a vulnerability management solution. Therefore, we request the Bank to remove this clause.	Bidder to comply with RFP terms and conditions.
754	193	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Request you to please amend the clause to modify below points:- Capability of running a coordinated command (such as CMD interface) as capability to execute command or script Request Bank to modify as below function should be available or there should be feasibility to execute command from EDR console to manage Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
755	198	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Request you to please amend the clause to change supported platform as below:- Windows 10 and above Windows server 2008 and above Kindly request Bank to remove below operating system support IBM AIX, Solaris	Bidder to refer Corrigendum-2
756	200	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	Request you to please amend the clause as " proposed ssolution to include static scanning up to 1GB and dynamic scanning up to 100MB."	Bidder to refer Corrigendum-2
757	215	Section 8 , Anti - APT, Annexure 9	2	Each of the bidders proposed solution would be evaluated thoroughly against functional as well as technical requirements. The proposed solution should be from a single OEM (for all components) to ensure the integrated platform requirements and capabilities are utilized and desired security objectives are achieved. The solution expected to import multiple TLS/ SSL certificates.	Request you to please amend the clause as "the proposed SSL Offloader can be from a different OEM than the primary solution provider as long as the solution/requirement meets the functional purpose"	Bidder to comply with RFP terms and conditions.
758	216	Section 8 , Anti - APT, Annexure 9	13	Proposed appliance should have below hardware requirements: Network Traffic Analysis appliances should be supplied with minimum below port requirements with a separate dedicated management and IPMI port with 10/100/1000GBASE-T 4 X 1G/10G RJ45 4 X 1G/10G SFP+ (With Bypass) 8 X 10G SFP+	We request the Bank to let us know if below ports will be ok 2 X 40G QSFP+ 4 X 10G SFP+ 2 X 1G/10G SFP+ 4 X 1G/10G RJ45 bypass 2 X 100G QSFP28	Bidder to refer Corrigendum-2
759	219	Section 8 , Anti - APT, Annexure 9	35	The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, TAXII and OpenIOC feeds with automated Investigation and analysis search function.	Request you to please amend the clause as mentioned below:- The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence using STIX or TAXII or OpenIOC feeds with automated Investigation and analysis search function.	Bidder to refer Corrigendum-2
760	220	Section 8 , Anti - APT, Annexure 9	40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Request you to please amend the clause as the supported operating system as Windows,Linux and MAC	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
761	220	Section 8 , Anti - APT, Annexure 9	42	The solution should have SSL Decryption capabilities available out of the box	Request you to please amend the clause as below If SSL decryption is not feasible on the appliance then bidder should provide SSL decryption	If SSL decryption is not feasible on same appliance. The Bidder has to provide separate SSL decryptor.
762	220	Section 8 , Anti - APT, Annexure 9	47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Given the variability in vendor practices, Request you to please amend the clause as "the proposed solution to either provide the operating system with all necessary licenses or allow the customer to upload their own licenses"	Clause stands deleted. Bidder to refer Corrigendum-2.
763	221	Section 8 , Anti - APT, Annexure 9	53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	Request you to please amend the clause as per below: The solution should support integration with proposed EDR/XDR platform	Bidder to comply with RFP terms and conditions.
764	11	SOW / 5 - Manpower Requirement		General	1. What is the shift work timings (start & End time including the time to provide handover of the shift tasks to the next shift resources) for Morning, General, Afternoon and Night? 2. Will Bank be providing Seating, Laptop, Internet Connectivity, Phone, Mail & Access to the tools and systems to required resources deployed to execute scope management? 3. Location wise split of resources required for each of the solution. 4. Resources deployed will be eligible for leave as per the law of the country, if any of the manpower requirement given under a shift consists of only 1 resource and if such a resource is availing leave; will there be a penalty applicable or the penalty is applicable only for absentism beyond the leaves authorized as per law of the country.	Bidder to comply with RFP terms and conditions.
765	13	SOW / 6- Manpower Roles & Responsibilities		5 resources per shift for Morning and Afternoon and 2 resources in night shift. SOC Location: The resources shall be deployed at both Primary and DR SOC situated in Bengaluru and Mumbai respectively	1. Which is the location address for Mumbai & Bangalore where the manpower is to be placed as there is a dependency on the transportation availability due to night shift involved.	The details will be shared with successful bidder.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
766	14	SOW / 6- Manpower Roles & Responsibilities - L2 Incident Responder		2 Resources per shifts	Kindly update the statement of 2 resources per Shifts as there are more than 2 resources currently mentioned within the Manpower Requirement Table: General Shift with 2 resources each in: Use case Engineering & Automation, Endpoint Security, Network Security, PIM Specialist and SIEM_SOAR_&_UEBA Engineer. General Shift with 1 Resource in: Vulnerability Management_BAS_ASM_DAST Threat Management has 2 resource in Morning, 2 resource in afternoon and 1 resource in night shift.	Bidder to comply with RFP terms and conditions.
767	37	SOW / 11.Incidents and Problem Management		Bidder should integrate the Incident Management tool with ITSM procured by the Bank in future without any additional cost to Bank. Bidder should also move and migrate data of incidents from existing solution to any future procured by the Bank	What is Bank's existing ITSM tool? Can the resources deployed use existing ITSM tool from the Bank and integrate tickets within the Queue of existing ITSM tool?	Service Now -ITSM.
768	74	Annexure-2 Pre-Qualification Criteria		OEM for any technology / security solution/ solution for NGSOC and other security solutions should have support center in India with availability of 24x7 onsite, telephonic, and remote support (Preferably in Mumbai, Bengaluru)	Request to exclude SaaS solution such as Threat Intel Services from this eligibility.	Bidder to comply with RFP terms and conditions.
769	144	14. Scope of Work for Proposed services	Domain & Social Media for Impersonation Monitoring:	Monitor banks official handles of Social media sites like Twitter, Facebook, LinkedIn, Instagram, YouTube, Pinterest, Threads etc. for indicator of compromise, unauthorized changes to official information, alert in case of any changes etc.	Please provide the count of different social media handles	The details will be shared with successful bidder.
770	145	14. Scope of Work for Proposed services	Rogue Mobile Application Protection:	a) The solution should identify rogue/fake mobile applications (Web/Mobile)/ APKs on play store, Apple store and other similar third-party application stores/ suspicious websites that targeting Bank's customers/ to capture their credential hosted and take all the necessary steps for their takedown.	Please provide total count of all official mobile apps	The details will be shared with successful bidder.
771	146	14. Scope of Work for Proposed services	Brand Protection and Monitoring:	Bidder must have capability for monitoring of look-alike domain name registrations and alerting the Bank in case of detection.	Please provide list and count of all official domains that require monitoring.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
772	148	14. Scope of Work for Proposed services	Attack Surface Monitoring:	k) The solution should provide the rescan report within 24hours for any observation upon requested.	Request to change the clause as - k) The solution should provide the rescan report within 24-72 hours for any observation upon requested.	Bidder to comply with RFP terms and conditions.
773	149	14. Scope of Work for Proposed services	Attack Surface Monitoring:	z) Any query/ticket should be resolve within 24 Hours and a Single Point of contact should be available for faster response/escalation.	Request to change the timeline to based on severity and not for all type of query or issues.	Bidder to comply with RFP terms and conditions.
774	150	14. Scope of Work for Proposed services	Attack Surface Monitoring:	(mm)The solution should support scanning of static and dynamic links and also specify how the suspicious hidden web links/ pages will be detected.	Request to provide moreclarity on this requirement for dertecting Hidden web links with an example	Bidder to comply with RFP terms and conditions.
775	150	14. Scope of Work for Proposed services	Other Services & Requirements:	The solution shall provide end users to collaborate on the platform by posting comments on threats, tagging other users to comment, and maintaining activity log	This is an OEM specific clause hence request you to remove it.	Bidder to refer Corrigendum-2
776	151	14. Scope of Work for Proposed services	Mobile Applications Malware Scanning The solution should provide a malware scan report of Bank's mobile applications hosted in Play store, Appstore. The Bidder is expected to provide monthly mobile malware scan report and as and when a version change is found. The malware scanning shall include but not limited to:	Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident and fraudulent mobile apps within 24 hours.	Request to update the takedown SLAs as - Take down of Phishing Site, fraudulent mobile apps within 24 hours of incident and fraudulent mobile apps within 3 to 5 working days.	Bidder to refer Corrigendum-1
777	218	22		Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations with all licenses and dependencies included in the solution.	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
778	220	40		The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2
779	221	53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.		EDR/XDR are supposed to use Cloud Sandbox and for Network Anti-APT solution on prem Sandbox is specified. This will give a much wider detection matrix to the customer. But with Anti-APT integration with EDR/XDR, the End User may loose the critical factor of two systems identifying threats at different levels. This will also rule out any additional advantage to any specific vendor	Bidder to comply with RFP terms and conditions.
780	74	Annexure-2 Pre-Qualification Criteria	OEM for any technology / security solution/ solution for NGSOC and other security solutions should have support center in India with availability of 24x7 onsite, telephonic, and remote support (Preferably in Mumbai, Bengaluru)		Request to exclude SaaS solution such as Threat Intel Services from this eligibility.	Bidder to comply with RFP terms and conditions.
781	144	14. Scope of Work for Proposed services	Domain & Social Media for Impersonation Monitoring:	Monitor banks official handles of Social media sites like Twitter, Facebook, LinkedIn, Instagram, YouTube, Pinterest, Threads etc. for indicator of compromise, unauthorized changes to official information, alert in case of any changes etc.	Please provide the count of different social media handles	The details will be shared with successful bidder.
782	145	14. Scope of Work for Proposed services	Rogue Mobile Application Protection:	a) The solution should identify rogue/fake mobile applications (Web/Mobile)/ APKs on play store, Apple store and other similar third-party application stores/ suspicious websites that targeting Bank's customers/ to capture their credential hosted and take all the necessary steps for their takedown.	Please provide total count of all official mobile apps	The details will be shared with successful bidder.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
783	146	14. Scope of Work for Proposed services	Brand Protection and Monitoring:	Bidder must have capability for monitoring of look-alike domain name registrations and alerting the Bank in case of detection.	Please provide list and count of all official domains that require monitoring.	Bidder to comply with RFP terms and conditions.
784	148	14. Scope of Work for Proposed services	Attack Surface Monitoring:	k) The solution should provide the rescan report within 24hours for any observation upon requested.	Request to change the clause as - k) The solution should provide the rescan report within 24-72 hours for any observation upon requested.	Bidder to comply with RFP terms and conditions.
785	149	14. Scope of Work for Proposed services	Attack Surface Monitoring:	z) Any query/ticket should be resolve within 24 Hours and a Single Point of contact should be available for faster response/escalation.	Request to change the timeline to based on severity and not for all type of query or issues.	Bidder to comply with RFP terms and conditions.
786	150	14. Scope of Work for Proposed services	Attack Surface Monitoring:	(mm)The solution should support scanning of static and dynamic links and also specify how the suspicious hidden web links/ pages will be detected.	Request to provide moreclarity on this requirement for dertecting Hidden web links with an example	Bidder to comply with RFP terms and conditions.
787	150	14. Scope of Work for Proposed services	Other Services & Requirements:	The solution shall provide end users to collaborate on the platform by posting comments on threats, tagging other users to comment, and maintaining activity log	This is an OEM specific clause hence request you to remove it.	Bidder to comply with RFP terms and conditions.
788	151	14. Scope of Work for Proposed services	Mobile Applications Malware Scanning The solution should provide a malware scan report of Bank's mobile applications hosted in Play store, Appstore. The Bidder is expected to provide monthly mobile malware scan report and as and when a version change is found. The malware scanning shall include but not limited to:	Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident and fraudulent mobile apps within 24 hours.	Request to update the takedown SLAs as - Take down of Phishing Site, fraudulent mobile apps within 24 hours of incident and fraudulent mobile apps within 3 to 5 working days.	Bidder to refer Corrigendum-2
789	218	22		Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations with all licenses and dependencies included in the solution.	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
790	220	40		The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-1
791	221	53		The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	EDR/XDR are supposed to use Cloud Sandbox and for Network Anti-APT solution on prem Sandbox is specified. This will give a much wider detection matrix to the customer. But with Anti-APT integration with EDR/XDR, the End User may loose the critical factor of two systems identifying threats at different levels. This will also rule out any additional advantage to any specific vendor	Bidder to comply with RFP terms and conditions.
792	12	5.2	Term of Contract	The term of contract will be for a period of five (05) years	The total contract term is mentioned as 5 Years, which includes the deployment/build period, which varies from solution to solution between 24 and 34 weeks. Kindly suggest How much will be the Operations period post Go-live.	Bidder to comply with RFP terms and conditions.
793	20	6.1	Uptime Penalty	20% of monthly NGSOC operations charges	Bidder request to cap the maximum penalty to 10%	Bidder to refer Corrigendum-1
794	21	6.2	Penalty	Penalties for delay in replacement of devices	Bidder request bank to allow 24 hours to replace the faulty device post OEM diagnosis	Bidder to comply with RFP terms and conditions.
795	23	6.4	Penalty on EOS	End of sale/ end of support/ end of life of any component	Bidder suggest to limit this penalty to end of support only, as End of Sale and End of life will not impact the solution	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
796	29	8.3	Warranty	The hardware deployed for this project shall be under Comprehensive Onsite Replacement Warranty covering update of software, maintenance or support for its proper operation, performance and output as specified in the tender technical specifications for a period of Three years from the date of go live of the Solution.	Bidder wants to understand if Bank is looking for upfront Warranty covering update of software, maintenance or support for all the supplied material for 3 years? If yes, kindly share the Payment term for same. Also the suggest the payment term for Subscription & Warranty utilized during 6 -9 months of Deployment phase. Bidder also needs to understand the Bank's planning to procure Warranty and AMC support for supplied material, as without OEM support bidder will not be able to deliver their services and maintain SLAs.	Bidder has to factor accordingly for the deployment phase.
797	30	9.4	AMC / ATS	The Bank will pay AMC/ATS charges for Solution (including Hardware, Operating System, and associated software Items) after the end of warranty period. Such payment shall be released quarterly in arrears after satisfactory completion of service during the period and submission of reports and invoices	Bidder requests Bank to change the payment term to Yearly in advance for Hardware, Software & OEM Services like AMC/Subscription charges.	Bidder to comply with RFP terms and conditions
798	165	SIEM	SIEM 8	Technical Specification: SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and Cloud). If the parser is not available the bidder/ OEM should developed the parsers without any extra cost to bank.	Kindly let us know expected number of custom parser to be factored by bidder.	Bidder to comply with RFP terms and conditions.
799	174	SIEM Packet Capture	Packet Capture 135	Technical Specification The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.	Does bidder need to factor 20 Gbps hardware from day one, kindly confirm	Yes
800	94	Platform Management	Manpower Requirement	Platform management - Manpower requirement : SIEM, SOAR, & UEBA Engineer (L3 OEM)	Request you to either change "Bidder/OEM Engineer" or OEM certified Engineer	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
801	175	SOAR	General Requirement	Technical Specification All the hardware/software required for the solution shall be provisioned by the OEM	Request to change "All the hardware/software required for the solution shall be provisioned by the Bidder"	Bidder to refer Corrigendum-2.
802	200	V.Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% YoY Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.
803		V.Privileged Identity Management (PIM)			Please help us with number of service accounts managed by the current PAM Solution. This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder
804	200	V.Privileged Identity Management (PIM)	Architecture & General	5. The solution shall have redundancy to failover in DC and DR both in HA in case the primary solution goes down. All the required hardware, software, OS, storage and required licenses shall be provided by the bidder.	Please help us with DC and DR locations.	Bidder to comply with RFP terms and conditions.
805	204	V.Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be treated as 1 application)
806	125	SOAR	III.Security Orchestration, Automation and Response (SOAR)	The solution should ensure that time between MTTD and MTTR should be improved gradually. Further, the vulnerability window should be within the tolerable time limit of the Bank.	Bidder understands there is a tolerable limit for vulnerability, Please elaborate what is the expectaion in relation to Vulnerability in SOAR and what is the tolerable limit in terms of timeline?	As per the defined SLA for updates/ upgrades documented in the RFP.
807	125	SOAR	III.Security Orchestration, Automation and Response (SOAR)	The bidder shall develop custom integration as necessary within the defined timeline.	The expectation is to build custom integration in SOAR within defined timeline, please clarify what is the timeline? What type of custom integration are expected? How many custom integration are expected?	Bidder to comply with RFP terms and conditions.
808	125	SOAR	III.Security Orchestration, Automation and Response (SOAR)	Bidder to perform periodic backup and store in a secure storage. Bidder to fix the gaps identified by OEM or Auditor as part of the assessment · Bidder to build incident and alert layout.	The expectation is to perform periodic backup and storage, Please clarify whether you want to have backup of alerts or raw logs? Please clarify for what timeline is the storage required?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
809	130	TIP	VII.Threat Intelligence Platform (TIP)	Bank is procuring Centralized Cyber Threat Intelligence Platform solution for which Bidder has to provide the services which includes but not limited to the following	Please clarify whether the requirements mentioned below are in relation to Threat Intel Management as a platform or as a service?	Threat Intelligence Platform (TIP).
810	130	TIP	VII.Threat Intelligence Platform (TIP)	Perform periodic validation of integration, data flow, and automation configurations.	Please clarify what is the frequency of periodic validation?	Bidder to comply with RFP terms and conditions.
811	130	TIP	VII.Threat Intelligence Platform (TIP)	Train security analysts and relevant personnel on TIP operations, use cases, and best practices.	Please clarify who is expected to train security analyst and personnel, is it expected from Bidder?	Bidder to comply with RFP terms and conditions.
812	74	Annexure-2	Pre-Qualification Criteria	Additional query	we request the bank to ask for atleast one reference on SaaS EDR implementation along with sign off letter or email since last 5 years in one PSU BFSI in India. Or atleast One reference of OEM with 85K nodes in a bank in India. This will help canara bank to get such OEM who have a track record of performing and protecting a bank of canara bank size.	Bidder to comply with RFP terms and conditions.
813	233	Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5. End point is a complext project in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder who have demonstrated a smooth deployment and sustenance in such large environment in BFSI in India. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an opportunity to evalute Bidder capability or allow bidder to allign with such OEM'S who have great track record in BFSI in India. Hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5. <u>Suggested Modified Clause:</u> The OEM/Bidder must have PO reference of 50000 users and above SaaS EDR solution in last 5 years in BFSI/ PSU/ Government entities in India. •For 5 or more clients - 10 marks •For 4 clients - 5 marks •For 2 clients - 3 marks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
814	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
815	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-2
816	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
817	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.
818	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

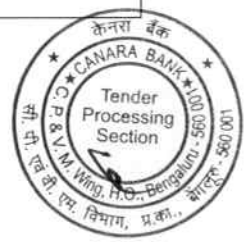
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
819	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-1
820	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2
821	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-2
822	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-1
823	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
824	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2
825	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-2
826	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
827	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
828	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
829	165-232	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.
830	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2
831	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2

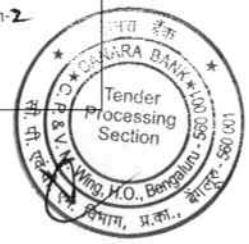


Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
832	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-2
833	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
834	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
835	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
836	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1
837	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-1
838	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1
839	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-1
840	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
841	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-1
842	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-1
843	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-1
844	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-1
845	211	Threat Intelligence Management	36	The proposed solution can create a snapshot of threat intelligence data based on a search filter and can integrate to third party services for consumption.	Bidder's understanding is, the solution should support putting specific filters on keyword combinations, sources, event types based on a specific timeframe and export that to be used for third party services for consumption	Bidder to comply with RFP terms and conditions.
846	211	Threat Intelligence Management	37	The proposed solution must provide a Threat Management incident handling capability with the ability to create incidents and/or tickets depending on organizational workflow	Bidder's understanding is, Ticket/Incident handeling is being carried on ITSM Platform hence requesting bank to move this to relevant section	Bidder to comply with RFP terms and conditions.
847	211	Integration & Dissemination	42	The proposed solution must support automated dissemination of IOCs to security controls including as a minimum, SIEM, Firewalls, Web Proxies, SOAR, Anti - APT, Antivirus and EDR, out of the box	Bidder understanding is, the Threat Intelligence Feed will integrated with TIP, SIEM & SOAR Solutions directly and rest of the solutions like Firewalls, Web Proxies, SOAR, Anti - APT, Antivirus and EDR will integrate with TIP and SOAR to get the Feeds and bring automation.	Yes
848	148	Attack Surface Monitoring	i	The proposed solution shall identify and create an inventory of all exposed Web applications, Websites, Domain, APIs, Mobile applications and IP addresses exposed.	Generally Mobile Application Monitoring are covered under Brand Monitoring hence it is requested to move this specification to the relevant one.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
849	149	Attack Surface Monitoring	t	The proposed solution shall be able to do Active Banner Grabbing and advanced search based on banners to detect any vulnerable version and provide reports as mentioned earlier.	Bidder's understanding is, the solution should discover active banners with login admin pages and identify the vulnerable version of applications behind it, kindly confirm.	Requirement is Self - Explanatory, Bidder to comply with RFP terms and conditions.
850	149	Attack Surface Monitoring	dd	The solution shall be able to access to Triage Centre to get access to critical ports and services within 24 hours of creation.	Bidder's understanding is, Triage Centre is the security operations cerntre being run at customer premises by bidder, kindly confirm.	Bidder to comply with RFP terms and conditions.
851	150	Attack Surface Monitoring	ll	The solution should monitor compromised servers for forensic information related to the Bank till the primary incident is closed.	Bidder's understanding is, while the incident is being managed by the analyst, all the parameters that are to be monitored by passive monitoring for that asset will be taken care by Attack Surface Monitoring tool, kindly confirm.	Bidder to comply with RFP terms and conditions.
852	150	Attack Surface Monitoring	mm	The solution should support scanning of static and dynamic links and also specify how the suspicious hidden web links/ pages will be detected.	Please elaborate the term dynamic links also the bider's understanding here with respect to suspicious hidden web link is to identify all the registered sub-domains and also get the DNS details for the same.	Bidder to comply with RFP terms and conditions.
853	26	Payment Terms	7.1	10% will be released After completion of Warranty period and submission of Bank Guarantee of equivalent amount.	What is the meaning of warranty period ? Please clarify. Request to release the payment post delivery and against submission of BG.	Bidder to comply with RFP terms and conditions
854	101	Endpoint Security Specialist	Under the header of Endpoint Security Specialist, Deception Points 1-5.	Deception - All the points 1-5.	Kindly provide specifications of the Deception solution to be deployed as part of the SecOps	Bidder to note to maintain the existing Bank's Deception solution. Specifications will be shared to the selected Bidder.
855	110	7.Scope of Work for Bidder/ System Integrator (SI)	7.7	The bidder shall supply and install network ports with a minimum capacity of 10 Gigabit(10Gig).	Kindly confirm if Network switches with 10 G ports also needs to be proposed or only network interfaces on proposed servers/appliances are to be 10G	Bidder has to provide all the SOC solutions with capacity of 10 Gig port interfaces.
856	119	12. Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	Integration of log sources from various devices/servers/network devices/ security devices/applications/APIs with SIEM as part of the implementation	Kindly provide the list of log sources and their locations to be integrated so that appropriate sizing of log collection and storage can be done.	The details will be shared with successful bidder.
857	121	Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	Bidders should integrate the proposed SIEM with a ticketing tool for automated ticket generation.	Kindly provide us with details of existing Ticketing tool for integration or provide instructions for supply of a new ticketing tool for this project.	Existing ITSM Solution is Service Now

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
858	122	Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	Log Archival The solution will be able to retain six months logs online and 1 year Archival (Six months - 12 months). The online storage shall be stored in SAN and NAS can be considered for Archival	Kindly confirm if we can utilize capacity on existing SAN and NAS for log retention or do we need to provide the required SAN and NAS system. Kindly confirm if the existing backup solution in the bank can be used for configuration backup etc. of the critical SIEM components	Bidder to propose SAN and NAS Storage as part of RFP.
859	123	Scope of Work for Proposed Solutions	I. Security Information & Event Management (SIEM)	The bidder shall ensure all the current SIEM use cases are transferred to the Next Gen SIEM solutions.	Kindly confirm that only use cases/co-relation rules are to be migrated to new SIEM. Migration of logs stored on existing SIEM is not in scope.	Bidder has to comply with RFP terms (Migration of logs is not required)
860	124	Scope of Work for Proposed Solutions	II.PCAP	The proposed PCAP solution should capture the network traffic and support replay functionality.	Kindly provide details of the network segments to be integrated into the PCAP solution In terms of current network utilization so that required PCAP solution can be sized appropriately . Also kindly provide the estimation of the SSL/TLS traffic to be inspected and captured. Kindly provide the retention period for captured packet data.	Bidder to comply with RFP terms and conditions.
861	73	Annexure 2 Pre Qualification Criteria	14	OEM should have provided on- prem SIEM solution should have been implemented at least 1,00,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	OEM should have provided on- prem SIEM solution should have been implemented at least 10,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids or SIEM solution implemented with 75,000 EPS in single entity of any industry vertical in the last 5 years or SIEM solution implemented with 100,000 EPS in single entity anywhere in the globe in the last 5 years.	Bidder to refer Corrigendum-2
862	74	Annexure 2 Pre Qualification Criteria	21	OEM for any technology / security solution/ solution for NGSOC and other security solutions should have support center in India with availability of 24x7 onsite, telephonic, and remote support (Preferably in Mumbai, Bengaluru)	We have 24*7 support center in Bangalore, however have follow the sun model to make sure we support round the clock. Hope this is agreeable.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
863	176	II.Security Orchestration and Automation (SOAR):	15	Workflow and playbook capabilities: a. The solution should auto assign playbooks for each alert along with recommendation to a particular analyst. b. The solution should provide simulation environment to test playbooks without any dependency on real environment. c. The solution should repeat workflow until all assigned tasks are completed and the solution should be able to raise alert in case of failure. d. The solution should provide exception report, detailed analysis of failure and corrective steps. e. The solution should have a versioning mechanism to save and maintain multiple versions for the playbooks. f. The solution should allow for viewing version history for all or selected playbook and provide option for restoring to an older version.	Kindly remove auto assign playbook clause (Point a). Rest if fine.	Bidder to comply with RFP terms and conditions.
864	179	II.Security Orchestration and Automation (SOAR):	41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Kindly remove the clause. It seems to be OEM specific.	Clause stands deleted. Bidder to refer Corrigendum-5
865	183	II.Security Orchestration and Automation (SOAR):	106	The solution should offer any auto-casing / auto-population based on the incident type or other relevant incident attributes	Can you pl share the use cases here for more clarity on the requirement.	This will be shared to succcessful bidder
866	94	Annexure 9	5.Manpower Requirement	SIEM, SOAR & UEBA Engineer (OEM (L3)) - 1 (SOAR) General Shift	Are there a clear, Roles and Responsobilities defined for this role. Kindly clarify.	Bidder to comply with RFP terms and conditions.
867	146	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:	m	Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	Can you define the maximum takedowns or average takedowns (per month for example) that will be required for the contract term	Bidder to refer Corrigendum-1
868	146	Brand Protection and Monitoring:	a	The bidder shall provide the Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti- Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown for the tenure of the Contract	Can you define the maximum takedowns or average takedowns (per month for example) that will be required for the contract term	The clause is self explantory (unlimited incidents and takedown for the tenure of the contract)

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
869	24	6.4. Penalty on Service levels during Operations phase	6.10.	Penalties/Liquidated damages of delay in Takedown of phishing sites specifically targeting Canara Bank (Standalone attacks) (To be calculated on incident basis)	Takedown request will be taken and sent within 24 hours, can we have more time for the takedown to happen as it also depends on vendor and service provider	Bidder to refer Corrigendum-२.
870	126	IV. User and Entity Behaviour		UEBA should provide complete case management with quick, accurate, efficient, and complete replay of attack / kill chain life cycle on the console and reports right from reconnaissance, external penetration, gaining a foothold, deliver payload, appropriating privileges, lateral movement, internal reconnaissance, data collection, maintain presence & exfiltration of data, information, logs, self-destruct, wipe out forensic proof etc.	Not a UEBA use case but can be done using SIEM Mitre mapping - please remove this point	Bidder to comply with RFP terms and conditions.
871	184	III. User Entity Behavioral Analysis (UEBA):	15. (i)	Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users	Why rules need to be adjusted we can adjust user and assets risk score - please remove or modify the point	Bidder to comply with RFP terms and conditions.
872	184	III. User Entity Behavioral Analysis (UEBA):	16	UEBA should activate a rules for a set of users until a specified condition or specified time window.	They are UEBA based on machine learning so will not be applicable - so point to be removed	Bidder to comply with RFP terms and conditions.
873	185	III. User Entity Behavioral Analysis (UEBA):	20	Data Exfiltration by Removable Media	Does it mean data exfiltration to removable media	Bidder to comply with RFP terms and conditions.
874	185	III. User Entity Behavioral Analysis (UEBA):	21	Browsing behavior:	UEBA will not perform this action as it's a privacy concern. We can collect logs from firewalls for this purpose or this can be achieved by the firewall itself - please have the point removed	Bidder to comply with RFP terms and conditions.
875	185	III. User Entity Behavioral Analysis (UEBA):	22	Network Traffic and Attacks	This will be network activity usecase and will not be done by UEBA but we can check as long as we have integration with ddos or relevant tools and can also be achieved by these tools- Please have the point removed	Bidder to comply with RFP terms and conditions.
876	185	III. User Entity Behavioral Analysis (UEBA):	23	DNS Analysis	This is not a UEBA usecase but we can check as long as we have relevant tools integration or can be achieved by the tools dorectly - Please have the point removed	Bidder to comply with RFP terms and conditions.
877	185	III. User Entity Behavioral Analysis (UEBA):	25	Solution must have network forensic analysis solution as integrated part of offering	What is meant by forensic analysis. Is it network or logs or traffic based. Can you please delete this point as most of the SIEM do not support this point.	Clause stands deleted. Bidder to refer Corrigendum-२.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
878	186	III. User Entity Behavioral Analysis (UEBA):	26	Abnormal P2P Usage detected on Critical Bank Servers	How do we get the critical bank servers, will we be provided with the list	Bidder to comply with RFP terms and conditions.
879	186	III. User Entity Behavioral Analysis (UEBA):	27	Critical Commands execution on SWIFT Servers - success/ failed	Will we be provided with the details of the swift servers	Bidder to comply with RFP terms and conditions.
880	187	III. User Entity Behavioral Analysis (UEBA):	42	PIM Bypass	Will we able able to get relevant telemetry data from PIM to detect the below PIM usecases	Bidder to comply with RFP terms and conditions.
881	187	III. User Entity Behavioral Analysis (UEBA):	44	Rare Malicious PowerShell Scripts Downloads on Critical Servers	We will need to have EDR logs	Bidder to comply with RFP terms and conditions.
882	188	III. User Entity Behavioral Analysis (UEBA):	75	The solution should provide analytical capabilities pertaining to ML models such as Outliers, Peer- Group Analytics, Time-Series Analytics, Predictive Analytics, Geo-location & ISP Analytics, Pattern Match Analysis etc.	Can we remove pattern match, Geo location and ISP anayltics since is not based on any ML based algorthms	Bidder to comply with RFP terms and conditions.
883	189	III. User Entity Behavioral Analysis (UEBA):	77	The solution should have inbuilt platform support for automation of routine L1/L2 activities.	This can be done with integration with SOAR	Clause stands deleted. Bidder to refer Corrigendum-2
884	189	III. User Entity Behavioral Analysis (UEBA):	78	The solution should detect slow attacks, advance persistent threats, and file less attacks, zero-day attacks, in-memory attacks, leveraging in-built self-learning and analytics leveraging AI / ML	This is not a UEBA usecase and this can be achieved via EDR	Bidder to comply with RFP terms and conditions.
885	167	I. Security Incident and Event Management (SIEM):	29	The SIEM solution OEM shall provision hardware to retain six months events online and 1 year Archival (Six months + 12 months). The online storage shall be stored in SAN and NAS can be considered for Archival.	The hardware will be providioned by the bidder	Bidder to refer Corrigendum-1
886	4	GeM Bid Doc Buyer Added Bid Specific Terms and Conditions:	1. Generic	OPTION CLAUSE: The buyer can increase or decrease the contract quantity or contract duration up to 25 percent at the time of issue of the contract. However, once the contract is issued, contract quantity or contract duration can only be increased up to 25 percent. Bidders are bound to accept the revised quantity or duration	Bidder requests that the clause be amended as follows: OPTION CLAUSE: The buyer can increase or decrease the contract quantity up to 25 percent at the time of issue of the contract. However, once the contract is issued, contract quantity or contract duration cannot be increased, unless mutually agreed upon.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
887	12	SECTION B - INTRODUCTION	5.Requirement Details	5.2.The term of contract will be for a period of five (05) years. However, Bank reserves the right to have an annual review on completion of 12 months the date of acceptance of purchase order. If the services are found to be unsatisfactory Bank reserves the right to discontinue the Services.	Bidder requests to amend the clause as below: "The term of contract will be for a period of five (05) years. However, Bank reserves the right to have an annual review on completion of 12 months the date of acceptance of purchase order. If the services are found to be unsatisfactory Bank reserves the right to discontinue the Services. In case of any extension beyond 5 years, the same will be based on mutually discussed price and conditions."	Bidder to comply with RFP terms and conditions.
888	15	1. Project Timelines	A. 3	Phase 1: Implementation of SIEM, UEBA and PCAP and integrate all the required log sources (4500 Log sources and 64 crown jewel Applications), configure/Migrate current use cases/policies to new platform	Since the scope of implementation and migration of log sources, migration of use cases are involved. Bidder request to extend the timelines to 32 Weeks.	Bidder to refer Corrigendum-2
889	15	1. Project Timelines	A. 3	Phase 2: Implementation of SOAR and integrate the following solutions, 1) SIEM 2) TIP 3) Proxy 4) Firewall 5) Active Directory 6) CMDB 7) Threat Intelligence 8) Vulnerability Management 9) ITSM (Service Now) 10) Bank's existing Antivirus & proposed EDR Solutions	SOAR integration with proposed solution and also with existing solutions are involved, this will require some time to implement, test and start integrating the solutions with SOAR. Bidder request to extend the timelines to 42 weeks.	Bidder to comply with RFP terms and conditions.
890	15	1.Project Timelines	C. 5	Installation of agents on Endpoints and servers (Agent can be pushed through Bank's SCCM tool)	EDR rollout to all the endpoints in branches require additional time to install and configure. Bidder request to extend the timelines to 32 weeks.	Bidder to comply with RFP terms and conditions.
891	23-25	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	6.5-6.12 Penalties/ Liquidated Damages		Bidder request that the overall penalty/LD be capped at 10% of the affected/ delayed value.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
892	26	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	7.1.Payment Terms for Solutions and Hardware:	1. Hardware cost (including OS & associated Softwares) 30%: After complete delivery of all hardware and its related software. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. 40%: After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. 20%: After completion of training and on submission invoices duly acknowledge by the Bank's Officials i.e., 3 months post sign off. 10%: After completion of Warranty period and submission of Bank Guarantee of equivalent amount	Bidder requests change as follows: 7.1.1 Hardware Cost (including OS & associated Software) 60% - After complete delivery of all hardware and its related software. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed. 10% - After successful installation, configuration & commissioning of all Hardware & Software items supplied as per Scope of Work. The Bidder has to submit installation reports duly signed by the Bank officials of the respective Branch/ offices, while claiming payment. The invoice and installation report should contain the product serial number of the items supplied. 20% - After completion of training and on submission invoices duly acknowledge by the Bank's Officials i.e., 3 months post sign off. 10% - After Completion of warranty period Or On submission of a bank guarantee of equivalent amount.	Bidder to comply with RFP terms and conditions
893	27	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	7.1.Payment Terms for Solutions and Hardware:	3.One time implementation cost 30%: On successful implementation in UAT and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents. 55%: On successful implementation in DC, DR and go-live and on submission of Invoice and Acceptance/ Sign off by the Bank on production of relevant documents. 10%: On successful completion of DR Drill and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents. 5%: On successful implementation of NG SOC solution and on submission of Invoice and Acceptance/ Sign off by the Bank on production of elevant documents.	Bidder requests the following: 3.One time implementation cost 50%: On successful implementation in UAT and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents. 30%: On successful implementation in DC, DR and go-live and on submission of Invoice and Acceptance/ Sign off by the Bank on production of relevant documents. 15%: On successful completion of DR Drill and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents. 5%: On successful implementation of NG SOC solution and on submission of Invoice and Acceptance/ Sign off by the Bank on production of elevant documents.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
894	27	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	7.1.Payment Terms for Solutions and Hardware:	4. AMC/ATS Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	Bidder requests that payment be made yearly in advance for the AMC/ATS	Bidder to comply with RFP terms and conditions
895	31	10.Scope involved during Contract period	10.7	10.7.The selected bidder shall provide centralized complaint booking/lodging facility to the bank and the dash board shall be provided to the Bank. The method of booking complaints shall be E-mail, Toll-free no, on line portal, web, etc.	Request Bank to confirm wheather bank wants bidder to use Bank's in-house ticketing tool or to propose bidder's ticketing tool? We recommend using the bank's ticketing tool for centralized complaint tracking. This will serve as a single platform where we can integrate the proposed security tools like SIEM, SOAR, NDR, etc.	Bidder can use either SOAR incident reponse capability or Bank's existing ITSM ticketing tool
896	33	Section C - Deliverable And Service Level Agreements	16. Subcontracting	16.1 Principle bidder only can participate, and bidder should not sub-contract to any other company/ firm/ trust/ Proprietorship/ partnership. After Selection process of the bidder and order placement, resources deployed should be employed with the selected bidder and they should be on the payroll of the selected bidder.	With role-wise minimum qualifications, experience and cost already called out, mandatory bidder payroll condition may not be needed. Also, clause 16.4 clearly states that "Even if the selected bidder gets into subcontracting, accountability and responsibility of the resource provided shall lie with selected bidder only". Hence, bidder requests modification of this clause as below: All resources must be bidder/ OEM/ OEM Authorized Partner resources and must have the required qualifications and experience for the role. Key resources like SOC Manager/ Project Manager (1 no.) and L3 Engineer for SIEM, SOAR and UEBA (2 nos.) must mandatorily be on the payroll of the selected bidder.	Bidder to comply with RFP terms and conditions.
897	33	SECTION C - DELIVERABLE AND SERVICE LEVEL AGREEMENTS	17. Right to Audit		We would request that this right be exercised post a notice period of 14 days being provided to the Bidder. Request bank to clarify that do bidder need to arrange the mentioned audits? Or bidder is expected to support the audit team which bank will appoint as and when required?	Bidder to support/ coordinate to support the bank appointed audit team.
898	38	Section D - BID PROCESS	6.7	The EMD may be forfeited/ Bank Guarantee may be invoked: 6.7.1.If the bidder withdraws or amends the bid during the period of bid validity specified in this document. 6.7.2.If the selected bidder fails to accept the purchase order within 7 days or fails to sign the contract or fails to furnish performance guarantee in accordance with the terms of the RFP.	We request that the EMD be forfeited only on the grounds of fraudulent activites.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
899	46	Section F - OWNERSHIP & AWARDING OF CONTRACT	1. Bid Validity Period	The Offer submitted and the prices quoted therein shall be valid for 180 days from the date of opening of Commercial Bid. Bid valid for any shorter period shall be rejected by the Bank.	We would request that this be shortened to 90 days as it becomes difficult to account for any and all variations that may occur outside of the Bidder's control.	Bidder to comply with RFP terms and conditions
900	49	Section F - OWNERSHIP & AWARDING OF CONTRACT	12.1	Events leading to termination	We would request that points 12.1.1-12.1.6 and 12.1.9 be amnded to reflect only material breaches and not for any breaches, as we would wish to continue our services with you and not terminate these unless they are significant deviations.	Bidder to comply with RFP terms and conditions
901	49	Section F - OWNERSHIP & AWARDING OF CONTRACT	12.Order Cancellation/Termination of Contract	12.4.After the award of the contract, if the selected bidder does not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one-month notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within reasonable limits & at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled.	Bidder requests that such additional liability be limited to 10% of the differential.	Bidder to comply with RFP terms and conditions.
902	51	Section G - GENERAL CONDITIONS	3.2	The Bank will call for Audited Balance Sheet of the selected bidder at any point of time during contract period and the selected bidder shall provide the same.	We would request that this be with a notice period of 7 days.	Bidder to comply with RFP terms and conditions.
903	53	Section G - GENERAL CONDITIONS	7. Negligence	In connection with the work or contravenes the provisions of General Terms, if the selected bidder neglects to execute the work with due diligence or expedition or refuses or neglects to comply with any reasonable order given to him in writing by the Bank, in such eventuality, the Bank may after giving notice in writing to the selected bidder calling upon him to make good the failure, neglect or contravention complained of, within such times as may be deemed reasonable and in default of the said notice, the Bank shall have the right to cancel the Contract holding the selected bidder liable for the damages that the Bank may sustain in this behalf. Thereafter, the Bank may make good the failure at the risk and cost of the selected bidder.	Would these damages be over and beyond the LOL / indemnity / penalties?	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
904	55	Section G - GENERAL CONDITIONS	13. Confidentiality and Non-Disclosure	13.1 The bidder shall take all necessary precautions to ensure that all confidential information is treated as confidential and not disclosed or used other than for the purpose of project execution. Bidder shall suitably defend, indemnify Bank for any loss/damage suffered by Bank on account of and to the extent of any disclosure of the confidential information. The bidder shall furnish an undertaking as given in Annexure-11.	We would request that this be limited to wilful disclosure of confidential information, which has been specifically called out / marked as confidential.	Bidder to comply with RFP terms and conditions.
905	57	Section G - GENERAL CONDITIONS	20. Protection of Data	20.1 The BIDDER/VENDOR/ SERVICE PROVIDER warrants that at all times, when delivering the Deliverables and providing the Services, use appropriate procedures and care to avoid loss or corruption of data. However, in the event that any loss or damage to Bank data occurs as a result of Bidder/Vendor/Service provider failure to perform its responsibilities in the RFP, Bidder/ Vendor/Service Provider will at Bank's request correct or cause to be corrected any loss or damage to Bank data. Further, the cost of the any corrective action in relation to data loss of any nature will be borne by Bidder/Vendor/Service Provider, if such loss or damage was caused by any act or omission of Bidder/Vendor/Service provider or its officers, employees, contractors or agents or other persons under Bidder/ Vendor/Service provider control.	We would request that this be limited to wilful disclosure of confidential information.	Bidder to comply with RFP terms and conditions.
906	57	Section G - GENERAL CONDITIONS	20. Protection of Data	20.3 The BIDDER/VENDOR/ SERVICE PROVIDER is required to adhere to RBI guidelines for storage of data in India as per regulatory requirements, also to provide complete details of data captured, processed and stored, maintain confidentiality of the bank's and its customer's data and report same to the bank, Bidder/Vendor/Service provider will be liable to bank for any event for security breach and leakage of data/information	Could we please have clarity as to which specific guidelines are to be complied with? As an IT/ITeS SP, we comply with the applicable laws for such services, however, not being a financial institute, we may not be aware of these leading to inadvertent noncompliance.	Bidder to comply with RFP terms and conditions.
907	58	Section G - GENERAL CONDITIONS	22. Indemnity	Indemnity	We would request that all indemnity claims only be for third party claims and party to party claims would be addressed under liabilities.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

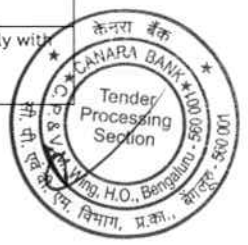
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
908	58	Section G - GENERAL CONDITIONS	22. Indemnity	22.1 The BIDDER/VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of: 22.1.1. The breach, default or non-performance of undertakings, warranties, covenants or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER. 22.1.2. Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements by the BIDDER/VENDOR/ SERVICE PROVIDER. 22.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER.	We would request that the clause be amended as follows, as indemnities are only for unforeseen special losses: "The BIDDER/VENDOR/ SERVICE PROVIDER shall keep and hold the Bank indemnified and harmless from time to time and at all times against all third party actions, proceedings, claims, suits, liabilities (including statutory liability), penalties, demands, charges, costs (including legal costs) and expenses, damages, losses and any other expenses which may be caused to or suffered by or made or taken against the Bank arising out of: ~~22.1.1. The breach, default or non-performance of undertakings, warranties, covenants or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER.~~ 22.1.2. Any contravention or Non-compliance with any applicable laws, regulations, rules, statutory or legal requirements as applicable to an IT/ITeS service provider, by the BIDDER/VENDOR/ SERVICE PROVIDER. ~~22.1.3. Fines, penalties, or punitive damages levied on Bank resulting from supervisory actions due to breach, default or non-performance of undertakings, warranties, covenants, or obligations by the BIDDER/VENDOR/ SERVICE PROVIDER.~~"	Bidder to comply with RFP terms and conditions.
909	58	Section G - GENERAL CONDITIONS	22. Indemnity	22.3 All Employees engaged by the BIDDER/VENDOR/ SERVICE PROVIDER shall be in sole employment of the BIDDER/VENDOR/ SERVICE PROVIDER and the BIDDER/VENDOR/ SERVICE PROVIDER shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall the Bank be liable for any payment or claim or compensation (including but not limited to compensation on account of injury / death / termination) of any nature to the employees and personnel of the BIDDER/VENDOR/ SERVICE PROVIDER.	We would request clarity as to why the Bank would exclude any actions of gross negligence or willful misconduct on its part that leads to injury or death of personnel.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
910	58	Section G - GENERAL CONDITIONS	22. Indemnity	22.6 The limits specified in above clauses shall not apply to claims made by the Bank/third parties in case of infringement of Intellectual property rights or loss caused due to breach of confidential obligations or applicable data protection laws or commission of any fraud by the bidder or its employees or agents or for claims relating to the loss or damage to real property and tangible personal property and for bodily injury or death and in these cases the liability will be unlimited.	We would request that this be limited to wilful disclosure of confidential information.	Bidder to comply with RFP terms and conditions.
911		Section G - GENERAL CONDITIONS	22. Indemnity	Insertion of new clause under indemnity	We would request that the following language be included in the RFP as well under indemnity: "Neither party will be liable to other party in respect of any loss of profits, business, custom, revenue, anticipated savings, goodwill, data or contracts or any type of special, indirect, economic, punitive or consequential loss (including loss or damage suffered as a result of any claims brought by a third party) even if such loss was reasonably foreseeable or the party had been advised of the possibility of the other party incurring the same."	Bidder to comply with RFP terms and conditions.
912	60	Section G - GENERAL CONDITIONS	25. Force Majeure	Insertion of new clause under Force Majeure	We would request that the additional clause be added: "For clarity, a force majeure event does not exempt the Bank from making good the due payments."	Bidder to comply with RFP terms and conditions.
913	71	Annexure-2 Pre-Qualification Criteria	Pre-Qualification Criteria	Additional query	we request the bank to ask for atleast one reference on SaaS EDR implementation along with sign off letter or email since last 5 years in one PSU BFSI in India. Or atleast One reference of OEM with 85K nodes in a bank in India. This will help canara bank to get such OEM who have a track record of performing and protecting a bank of canara bank size.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
914	73	Annexure-2	Pre-Qualification Criteria	12. The bidder should have its own/ Captive New Generation SOC Setup in India (technology and customer logs should be stored in Indian jurisdiction only) providing SOC as a service/ managed SOC services including remote log monitoring, correlation and analysis and security incident management services, etc.	Bank is already asking for 100+ certified onroll professionals as a separate pre-qualification criterion and 50+ certified cyber security resources as a minimum technical evaluation criterion. Asking for a separate captive SOC setup may not serve any additional purpose. RFP ask is for the implementation of captive SOC where all the technologies and resources are to be deployed on-premises at Bank's DC and DR. Additionally, bidders should reference the qualifications outlined in pre-qualification clauses #8 and #13 to demonstrate the capabilities and experience required for System Integrators (SI's). Hence requesting to remove this clause.	Bidder to refer Corrigendum-1
915	73	Annexure-2	Pre-Qualification Criteria	14. OEM should have provided on- prem SIEM solution should have been implemented at least 1,00,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids. Provide copies of completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/invoices.	Bidder requests deletion of need to provide purchase order/ contract agreement/ work order/ engagement letter/ invoices since these could be between any of the other SI's & customer and OEM might not have access to the same. While this is a OEM qualification clause, effectively it becomes a qualification clause for bidder-OEM qualification. This is favoring certain bidders. Hence, bidder requests to modify the clause as below: Provide copies of completion certificate/ reference letter email from client/ purchase order/ contract agreement/ work order/ engagement letter/ invoices.	Bidder to refer Corrigendum-1
916	94	Annexure-8	Scope of Work	5. Manpower Requirement PIM Specialist OEM L3 - 1	Since the primary ownership of operations and SLA management is with the bidder, request bank to consider "Bidder/OEM Engineer/OEM Authorized Partner"	Bidder to comply with RFP terms and conditions.
917	94	Annexure-8	Scope of Work	5. Manpower Requirement SIEM, SOAR & UEBA Engineer OEM L3 - 1 (SOAR)	Since the primary ownership of operations and SLA management is with the bidder, request bank to consider "Bidder/OEM Engineer/OEM Authorized Partner"	Bidder to comply with RFP terms and conditions.
918	148	Attack Surface Monitoring	i	The proposed solution shall identify and create an inventory of all exposed Web applications, Websites, Domain, APIs, Mobile applications and IP addresses exposed.	Please dilute Mobile Applications from the list. This is a Brand Monitoring use case and can be achieved by the Brand monitoring soltuion.	Bidder to comply with RFP terms and conditions.
919	149	Attack Surface Monitoring	s	The proposed solution shall be able to perform Network Vulnerability Assessment to validate passive risks and remove false positives.	Please elaborate more on the use case	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
920	149	Attack Surface Monitoring	t	The proposed solution shall be able to do Active Banner Grabbing and advanced search based on banners to detect any vulnerable version and provide reports as mentioned earlier.	Please elaborate more on the use case	Requirement is Self - Explanatory , Bidder to comply with RFP terms and conditions.
921	149	Attack Surface Monitoring	dd	The solution shall be able to access to Triage Centre to get access to critical ports and services within 24 hours of creation.	Please elaborate more on the use case and Triage Center	Bidder to comply with RFP terms and conditions.
922	150	Attack Surface Monitoring	ll	The solution should monitor compromised servers for forensic information related to the Bank till the primary incident is closed.	Please elaborate more on the use case	Bidder to comply with RFP terms and conditions.
923	150	Attack Surface Monitoring	mm	The solution should support scanning of static and dynamic links and also specify how the suspicious hidden web links/ pages will be detected.	Please elaborate more on the use case	Bidder to comply with RFP terms and conditions.
924	165	SIEM	SIEM 8	Technical Specification: SIEM should provide out of box Cloud integrations to retain full visibility into cloud security stack and support hybrid integration (On prem and Cloud). If the parser is not available the bidder/ OEM should developed the parsers without any extra cost to bank	Kindly let us know expected number of custom parser to be planned.	Bidder to comply with RFP terms and conditions.
925	174	SIEM Packet Capture	Packet Capture 134	Technical Specification: The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance with minimum 4 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 2*1/10G management port.	Since SIEM solution as asked in the RFP is hardware or software based, request bank to modify the clause to software-based packet capture where bidder will take the responsibility of sizing the required hardware as per RFP. Modified clause as below "The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance or software with required hardware which should have minimum 4 X 1G/10G RJ45 and 2*1/10G management port.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
926	174	SIEM Packet Capture	Packet Capture 135	Technical Specification: The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.	Since SIEM solution as asked in the RFP is hardware or software based, request bank to modify the clause to software-based packet capture where bidder will take the responsibility of sizing the required hardware as per RFP. Modified clause as below "The proposed packet capture solution should be proposed with 10 Gbps of license from Day-1 and should support future expansion of up to 20 Gbps using same hardware or by adding additional nodes in cluster and adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.	Bidder to comply with RFP terms and conditions.
927	174	SIEM Packet Capture	Packet Capture 136	Technical Specification: The proposed packet capture solution should be a dedicated Hardware appliance, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports	Since SIEM solution as asked in the RFP is hardware or software based, request bank to modify the clause to software-based packet capture where bidder will take the responsibility of sizing the required hardware as per RFP. Modified clause as below "The proposed packet capture solution should be a dedicated Hardware appliance or software with required hardware, all Core Appliances or hardware for different layers should have hardened OS to provide optimal performance. All disks of the appliance or hardware and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN/NAS storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports"	Bidder to refer Corrigendum-2
928	175	SOAR	General Requirement	Technical Specification All the hardware/software required for the solution shall be provisioned by the OEM	Since SOAR is a software solution which will be installed on Bidder supplied OEM servers, Request bank to change "All the hardware/software required for the solution shall be provisioned by the Bidder"	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
929	178	II. Security Orchestration and Automation (SOAR):	36	Bidder should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc.	Bank is procuring the Threat Intelligence Feed as part of this RFP, Hence request this clause to be deleted. This clause will favor a bidder who is providing their own Threat Intel Feeds. (or) the clause can be modified as - "Bidder should integrate the proposed threat intelligence feeds with SOAR to check threat score, reputation etc."	Bidder to refer Corrigendum-1.
930	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
931	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-1.
932	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
933	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.
934	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-2

केनरा बैंक CANARA BANK Tender Processing Section C.P.& V.M. Wing, H.O., Bengaluru - 560 001 सी. पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
935	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-2
936	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-2
937	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-2
938	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-2
939	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
940	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2.
941	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-2.
942	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
943	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
944	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
945	165-232	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.
946	200	V.Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% Yo-Yo Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.
947		General			Please help us with number of service accounts managed by the current PAM Solution. This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder
948	200	V.Privileged Identity Management (PIM)	Architecture & General	5. The solution shall have redundancy to failover in DC and DR both in HA in case the primary solution goes down. All the required hardware, software, OS, storage and required licenses shall be provided by the bidder.	Please help us with DC and DR locations.	Bidder to comply with RFP terms and conditions.
949	204	V.Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be trated as 1 application)

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
950	208	VI. Threat Intelligence Platform (TIP):	1	The proposed solution shall be deployed at on-premises components that permits the organization to store IOCs and investigations confidentially on their physical premises in local HA in DC & DR	TIP is consider as non-critical component in SOC so HA is not required. In case of failure back-up restore option available.	Bidder to comply with RFP terms and conditions.
951	211	Threat Intelligence Management	37	The proposed solution must provide a Threat Management incident handling capability with the ability to create incidents and/or tickets depending on organizational workflow	Please move this clause to SOAR section. SOAR/ITSM will be the single pane of glass for monitoring the events centrally.	Bidder to comply with RFP terms and conditions.
952	211	Integration & Dissemination	42	The proposed solution must support automated dissemination of IOCs to security controls including as a minimum, SIEM, Firewalls, Web Proxies, SOAR, Anti - APT, Antivirus and EDR, out of the box	The security control lole Firewall, Web Proxy, EDR etc will be integrated with SOAR and dissemination is always recommended via SOAR which can help filter relevbant intel based on internal Workdflow to the Security controls. Please modify the point to "The proposed solution must support automated dissemination of IOCs to security controls including as a minimum, SIEM, Firewalls, Web Proxies, SOAR, Anti - APT, Antivirus and EDR, out of the box / via SOAR.	Bidder to comply with RFP terms and conditions.
953	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2.
954	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
955	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-2
956	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
957	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
958	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
959	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-2
960	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-2
961	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2
962	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-2
963	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
964	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-1
965	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-1
966	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-1
967	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
968	233	Annexure-10	Technical Evaluation Criteria	7. The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience • For 5 or more clients - 5 marks • For 2 clients - 3 marks	On-premises EDR solution and SaaS EDR are fundamentally similar technology, with the primary difference being that telemetry data is sent to OEM cloud in the latter. Bank's EDR sizing is for 85,000 Endpoint licenses & 5,000 Server licenses, thus instead of asking for count, bidder suggests scale of proposed EDR deployment with minimum number of endpoints to demonstrate necessary experience and expertise of the bidder with the proposed EDR solution at sufficient scale of rollout. Hence, bidder requests to modify the clause as below: The Bidder must have implemented proposed EDR solution in BFSI/ PSU/ Government entities in India for a minimum endpoint count of: • Greater than or equal to 15,000 endpoints -> 5 Marks • Greater than or equal to 10,000 endpoints -> 3 Marks • Greater than or equal to 5,000 endpoints -> 2 Marks	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
969	233	Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5. End point is a complext project in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder who have demonstrated a smooth deployment and sustenance in such large environment in BFSI in India. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an opportunity to evalute Bidder capability or allow bidder to allign with such OEM'S who have great track record in BFSI in India. Hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5. Suggested Modified Clause: The OEM/Bidder must have PO reference of 50000 users and above SaaS EDR solution in last 5 years in BFSI/ PSU/ Government entities in India. •For 5 or more clients - 10 marks •For 4 clients - 5 marks •For 2 clients - 3 marks	Bidder to comply with RFP terms and conditions.
970	234	Annexure-10	Technical Evaluation Criteria	9. The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in India 500 privileged users with more than 5 clients - Score of 5 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	Request Bank to change from PIM to PIM/ PAM solution as these terminologies are interchangeably used across OEM's. This is inline with the PIM/ PAM qualification criterion in PQ clause #8. Bank's present PIM sizing is for 750 privileged users, with estimated future sizing of 1,500 privileged users, thus quantity of privileged users deployed by bidder ensure the capability and expertise of implementing and managing the PIM/ PAM solution. Hence, bidder requests to modify the clause as below: The Bidder should have implemented or managed PIM/ PAM Solution with minimum of 500 privileged users in Organization (s) in India • 1,000 privileged users and above - Score of 5 • 500 to 999 privileged users - Score of 2	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
971	236	RFP; Annexure 11		Insertion of additional language	We would request that the following language be included in the NDA: "Confidential Information excludes any information which:(i) was in Bidder's possession prior to receipt from Discloser (ii) is publicly known or readily ascertainable by proper means, (iii) is rightfully received by Bidder from a third party without a duty of confidentiality, (iv) is disclosed by Bank to a third party without a duty of confidentiality on the third party, (v) is independently developed or learned by the Bidder, or (vi) is disclosed by Bidder with the Bank's prior written approval. This NDA will be valid for the contract term or for 8 years, whichever is longer."	Bidder to comply with RFP terms and conditions
972	242-254	RFP: Annexure-17	Table 1 & Table 3 of Commercial template		Bidders understanding is that Table 1 & Table 3 of the commercial template are for 3 years and the remaining 2 years are covered under Table 5 in AMC/ATS	Yes
973	242-254	RFP: Annexure-17	Table 5 of Commercial template	Heading: Table 5) AMC/ATS Cost for items mentioned in Table- 1 and Table- 2	Bidders understanding is that Table 5 of the commercial template is for AMC/ATS for the line items in Table 1 & Table 2	Yes
974	266	RFP; Appendix D		Bank Guarantee Format for Earnest Money Deposit	We would request that similar amendments be made for the grounds of forfeiture of EMD as under point 7.	Bidder to comply with RFP terms and conditions
975	267	RFP; Appendix E		Proforma of Bank Guarantee for Contract Performance	We would request that the Bank Guarantee be restricted to material breaches and post a notice period of 30 days being provided prior to invoking the same. We would also request that any amendments to the contract be only for those amendments which have been mutually agreed upon.	Bidder to comply with RFP terms and conditions
976	273	Appendix-F Pre-integrity pact	6.3	In the case of successful BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER, a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provisions of Sanctions for violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.	We would kindly request that the forfeiture, if any, be by assigning reason for such forfeiture.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
977	273	Pre-integrity pact	7.1	SANCTIONS FOR VIOLATIONS	We would request that the actions be restricted to clauses I, ii, iii, iv (sums without interest), vi and vii as otherwise it provides multiple recourse for the customer that is punitive in nature.	Bidder to comply with RFP terms and conditions.
978	274	Pre-integrity pact	8	FALL CLAUSE The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems/services at a price lower than that offered in the present bid to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law and if it is found at any stage that similar product/systems or sub systems/services was supplied by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to any other Bank or PSU or Government Department or to any other organization/entity whether or not constituted under any law, at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER to the BUYER, if the contract has already been concluded.	We request deletion of this clause since the solution provided under this RFP is completely different from the solution provided under other contracts and should not be considered for the purpose of evaluation of bid prices.	Bidder to comply with RFP terms and conditions.
979	275	Pre-integrity pact	9.6	The BIDDER(s) accepts that the Monitors have the right to access without restriction to all Project /Procurement documentation of the BUYER including that provided by the BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. The BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER will also grant the Monitors, upon their request and demonstration of a valid interest, unrestricted and unconditional access to his documentation pertaining to the project for which the RFP/Tender is being /has been submitted by BIDDER/SELLER/CONTRACTOR/SERVICE PROVIDER. The same is applicable to Subcontractors. The Monitors shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractors () with confidentiality.	We would request that the clause be amended to include a notice period as well.	Bidder to comply with RFP terms and conditions.
980	277	RFP; Appendix G		DRAFT CONTRACT AGREEMENT	We would request that draft contract remain consistent with the terms as under the RFP and the clauses above, such as for indemnity, termination, etc.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
981	279	RFP; Appendix G	10.1	Bank shall serve the notice of termination to the Vendor/Service Provider at least 30 days prior, of its intention to terminate services.	We would request that a termination for convenience be with a notice period of 90 days.	Bidder to comply with RFP terms and conditions
982				The Bidder will be responsible to deploy the proposed VM solution in both (DC) and (DR) sites in an active/passive configuration to ensure high availability and ensure the implementation of the solution in a manner that does not impact the bank's network and assets.	It can be achieved by resyncing the files/directories to a backup server and when the main goes down run the rpm for SC and re-activate the license. https://community.tenable.com/s/article/Tenable-sc-Formerly-SecurityCenter-Disaster-Recovery-Options?language=en_US	Bidder to comply with RFP terms and conditions.
983	234	Annexure 10	Technical Evaluation Criteria	The OEM must have supplied on-prem SOAR solution in BFSI/ PSU/ Government entities in India. Supply Experience •For 3 or more clients - 5 marks •For 2 clients - 2 marks	We kindly request if there is a possibility to adjust or relax this criterion to allow for a score of 5 marks based on additional relevant factors. These factors could include certifications, successful large deployments, and overall project performance, which demonstrate our capability and reliability in delivering on-prem SOAR solutions.	Bidder to refer Corrigendum-2
984	NA	Generic	Generic	New Proposed clause - Marking system on Make in India preference	While the current marking system rightly emphasizes previous successful deployments, it inadvertently disadvantages "Make in India" vendors. These vendors, despite having superior technical capabilities, may lack the scale or precedence of larger global OEMs, thus causing bidders to favor non-Indian vendors to avoid losing points. To address this, we request the bank to revise its evaluation criteria by awarding higher marks to bidders who propose "Make in India" vendors or OEMs. By doing so, the bank can encourage bidders to align more closely with the "Make in India" initiative. Without such provisions, the current format heavily favors non-Indian OEMs, leaving Indian-origin companies at a significant disadvantage and ultimately defeating the purpose of the initiative.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
985	234	Annexure 10	Technical Evaluation Criteria	The OEM must have supplied on-prem SOAR solution in BFSI/ PSU/ Government entities in India. Supply Experience •For 3 or more clients - 5 marks •For 2 clients - 2 marks	To ensure a more comprehensive evaluation of supply experience, we request the bank to consider including large managed services deployments as part of the criteria, alongside BFSI, PSU, and Government entities. Expanding the criteria to recognize successful deployments in managed services will reflect the broader capabilities of vendors and provide a more balanced assessment. This adjustment will also help to account for the extensive expertise in handling large-scale SOAR implementations outside the BFSI/PSU/Govt sectors, ensuring fair competition.	Bidder to refer Corrigendum-2
986	71	Annexure - 2	Pre- Qualification Criteria	The Bidder (including OEM and OSD/OSO, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020.	With utmost respect for the bank's commitment to the 'Make in India' initiative, we kindly seek clarification regarding the RFP's alignment with the mandate that at least 60% of the security solution should be Indian-origin, with IP registered in India. While we fully support the bank's efforts in promoting this national objective, we've noticed that the RFP appears to permit substantial participation from foreign OEMs. We would be grateful if the bank could help us understand how this is reconciled with the 'Make in India' mandate, as we strive to align our efforts with the bank's vision. Your guidance on this matter would be deeply appreciated.	Bidder to comply with RFP terms and conditions
987	NA	Generic	Generic	Make in India Clause	With the utmost respect for the bank's adherence to government guidelines, we kindly seek your valuable guidance regarding the provision allowing non-'Make in India' Security vendors/OEM's for RFPs exceeding ₹200 crore, which seems to apply in this case. While we understand the necessity of such a provision, we are concerned about ensuring that it is not inadvertently used in a way that bypasses the broader intent of promoting Indian-origin solutions. Could you please help us understand how the bank ensures that this threshold is not misused, especially in cases where the bid exceeds ₹200 crore? Your insights would be deeply appreciated, as we remain fully committed to supporting the bank's vision of fostering local innovation	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
988	NA	Generic	Generic	Make in India Clause	With sincere respect for the bank's efforts to uphold both fairness and the government's 'Make in India' initiative, we kindly seek your guidance on an important concern. Indian OEMs, despite offering proven solutions, often face challenges in meeting the scale and eligibility criteria set in the RFP, putting them at a disadvantage compared to global MNCs. Given the government's emphasis on promoting Indian-origin solutions, we would be deeply grateful to understand how the bank plans to address this imbalance in the eligibility criteria. We trust that the bank shares our commitment to creating a level playing field for local innovation, and your insights on this matter would be invaluable.	Bidder to comply with RFP terms and conditions
989	NA	Generic	Generic	Make in India Clause	With the utmost respect for the bank's commitment to supporting national objectives, we humbly seek clarity on an important concern. Indian OEMs, despite offering proven solutions, often find themselves at a disadvantage due to the scale and eligibility criteria set in RFPs, which tend to favor larger global MNCs. This seems to limit their ability to compete, even though the government's 'Make in India' initiative emphasizes the promotion of Indian-origin solutions. Could you kindly help us understand how the bank plans to address this imbalance in the eligibility criteria, so that Indian OEMs can have a fair opportunity to participate? We deeply value the bank's efforts and would greatly appreciate any insights on how local innovation can be better supported	Bidder to comply with RFP terms and conditions
990	NA	Generic	Generic	Make in India Clause	With great respect for the bank's adherence to 'Make in India' guidelines, we kindly seek your understanding on a matter of concern. While the bank may technically comply with the guidelines, the current approach appears to allow foreign OEMs to dominate the process, which could be perceived as bypassing the essence of the policy intended to promote Indian-origin solutions. We humbly ask if the bank acknowledges this potential concern and what steps might be taken to more genuinely support Indian OEMs in line with the spirit of the 'Make in India' initiative. Your guidance and insights would be immensely appreciated, as we share the same vision of fostering local innovation and growth.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
991	NA	Generic	Generic	Make in India Clause	With the utmost respect for the bank's efforts to support the 'Make in India' initiative, we humbly seek your guidance on a concern regarding the current RFP structure. As it stands, the broad clubbing of multiple solutions under one tender seems to unintentionally favor non-Indian OEMs, potentially working against the initiative's core intent. In light of this, we kindly ask if the bank might consider revising the RFP terms to ensure a more balanced and fair evaluation of Indian-origin solutions. We deeply value the bank's commitment to fostering local innovation, and your guidance on this matter would be greatly appreciated.	Bidder to comply with RFP terms and conditions
992	NA	Generic	Generic	Make in India Clause	With deep respect for the bank's commitment to compliance and national directives, we humbly seek clarity on a matter of concern. The current RFP seems to overlook the mandatory preference for Indian-developed cybersecurity products, as encouraged by the government order. We kindly ask how the bank plans to reconcile this decision, which may be seen as diverging from the government's directive to prioritize Indian solutions. We sincerely value the bank's dedication to fostering local innovation and would greatly appreciate your guidance on how this mandate might be upheld in the RFP process.	Bidder to comply with RFP terms and conditions
993	NA	Generic	Generic	Make in India Clause	With the utmost respect for the bank's commitment to securing information and networks in alignment with government mandates, we humbly seek clarification on an important matter.as per Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products A Cyber Security Product is defined as any product, appliance, or software developed to protect information and networks. Given the significant inclusion of foreign OEMs in the RFP, we kindly request guidance on how the bank ensures that the products align with this government-mandated definition. We deeply appreciate the bank's efforts in maintaining compliance and fostering secure solutions, and any insights you could provide would be sincerely valued.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
994	NA	Generic	Generic	Make in India Clause	With deep respect for the bank's commitment to the 'Make in India' initiative, we kindly seek your guidance on a point of concern. as per Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products A 'local supplier' is defined as an Indian company deriving revenue from products with at least 60% local content and IP ownership. Given that many global OEMs participating in the RFP may not meet these criteria, we humbly request your insights on how the bank plans to address this in alignment with the mandate. We truly appreciate the bank's efforts in supporting local industry and would be grateful for any guidance you could provide on this matter	Bidder to comply with RFP terms and conditions
995	NA	Generic	Generic	Make in India Clause	With the utmost respect for the bank's dedication to the 'Make in India' initiative, we humbly seek clarification regarding the IP ownership requirements stipulated within this framework. as per Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products The initiative mandates that local suppliers own the IP rights, including commercialization and modification, without third-party consent. Given that many global OEMs participating in the RFP may not fulfill this important stipulation, we kindly ask how the bank ensures compliance with this requirement. Your insights on this matter would be immensely valuable, as we all share a commitment to supporting local innovation and adhering to government mandates	Bidder to comply with RFP terms and conditions
996	NA	Generic	Generic	Make in India Clause	With deep respect for the bank's commitment to fairness and compliance with the government's directives, we humbly seek clarification on an important matter. reference to as per Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products the order excludes resellers, distributors, and service agencies with limited IP rights from benefiting, we kindly ask what measures the bank is taking to ensure that such entities do not gain an unfair advantage in the RFP process. Your insights on this issue would be greatly appreciated, as we all share the goal of fostering a level playing field and supporting genuine innovation.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
997	NA	Generic	Generic	Make in India Clause	With great respect for the bank's diligence in adhering to procurement guidelines, we would like to humbly seek clarification on an important aspect of the process. reference to as per Public_Procurement_(Preference_to_make_in_India)_order_2019_for_Cyber_Security_Products For procurements exceeding ₹10 crore, it is required that companies provide a statutory auditor's certificate verifying compliance with the local supplier definition. We kindly ask how the bank intends to enforce this requirement, especially in instances where non-Indian OEMs are participating in the bid. Your guidance on this matter would be invaluable, as we all strive to ensure compliance and support local suppliers in alignment with government initiatives.	Bidder to comply with RFP terms and conditions
998	NA	Generic	Generic	Tech Solutions Refresh	With deep respect for the bank's strategic decision-making process, we would like to humbly seek clarification on a matter of significance. We understand that some previously deployed solutions have been retained while others are being considered for new purchases. Could you kindly share what objective criteria or metrics the bank has used to determine which solutions should be retained and which should undergo fresh procurement? Your insights on this matter would be greatly appreciated, as we all share a commitment to ensuring the effectiveness and efficiency of our resources.	Bidder to comply with RFP terms and conditions.
999	NA	Generic	Generic	Procurement	With great respect for the bank's commitment to fostering innovation and ensuring fairness in the procurement process, we would like to humbly seek clarification on a matter that has raised some concern. In the past, the bank has emphasized the importance of procuring new solutions rather than renewing existing ones, citing procurement policies to give new OEMs a chance. However, we are curious about how the bank justifies the decision to retain certain previously deployed solutions while applying fresh procurement processes for others. Could you kindly share your perspective on this approach, especially considering the potential implications for other Indian-origin OEMs who could offer equivalent or superior solutions? Your insights would be immensely valuable and appreciated as we navigate this process together	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1000	NA	Generic	Generic	Make in India Clause	While the current marking system rightly emphasizes previous successful deployments, it inadvertently disadvantages "Make in India" vendors. These vendors, despite having superior technical capabilities, may lack the scale or precedence of larger global OEMs, thus causing bidders to favor non-Indian vendors to avoid losing points. To address this, we request the bank to revise its evaluation criteria by awarding higher marks to bidders who propose "Make in India" vendors or OEMs. By doing so, the bank can encourage bidders to align more closely with the "Make in India" initiative. Without such provisions, the current format heavily favors non-Indian OEMs, leaving Indian-origin companies at a significant disadvantage and ultimately defeating the purpose of the initiative.	Bidder to comply with RFP terms and conditions
1001	74	Annexure 2 - Pre-Qualification Criteria	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	We request the bank to reconsider this point inline with Annexure-10 Technical Evaluation Criteria (234) and consider OEM references instead of bidder implemented references. This will ensure support requirements for next 5 years and also provide expertise of new age PIM products implemented elsewhere by us or OEM directly in India.	Bidder to comply with RFP terms and conditions.
1002	234	Annexure-10 Technical Evaluation Criteria	9) The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India - 500 privileged users with more than 5 clients - Score of 5 - 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	9) The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India - 500 privileged users with more than 5 clients - Score of 5 - 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	Request the Bank to relax this clause and reduce the minimum number to 200. Suggested clause: The Bidder should have implemented or managed PIM Solution with minimum of 200 privileged users in Organization(s) in Organization(s) in India - 200 privileged users with more than 5 clients - Score of 5 - 200 privileged users with more than 2 clients and up to and including 5 clients - Score of 2	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1003		Privileged Identity Management (PIM)	The Solution should have Indian Common Criteria Certificate (IC3S) issued by MeitY, Govt of India OR The Solution should certified with Common Criteria Evaluation Certificate with a minimum assurance level of EAL 2.	The Solution should have Indian Common Criteria Certificate (IC3S) issued by MeitY, Govt of India OR The Solution should certified with Common Criteria Evaluation Certificate with a minimum assurance level of EAL 2.	Common Criteria certification is recognized as Testing certificate for specific version of the product. Future product version need to be tested again for achieve such certifications. Reference: https://www.commoncriteriaportal.org/pps/collaborativePP.cfm?cpp=1 Several international common criteria certifying association bodies including United States now provides recommended protection profiles and doesn't consider Assurance Level like EALs for testing assurance. As per publicly available information in Common Criteria portal, It is also to be noted that common criteria with assurance level of EAL 2+ may be restricted to a specific OEM in Privileged Access Management. Such clause may indicate only a certain vendor can participate in the bid. We understand that Bank would like high security assurance from supplied products during the term of the contract. We humbly request to consider assurance considerations across all products viz certifications like ISO 27001 and Safe to Host Certificates / Penetration Testing Certificates for all supplied & future upgraded version supplied to the bank.	Bidder to comply with RFP terms and conditions.
1004		Annexure 2 - Pre-Qualification Criteria	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	We are Make in India OEM and have reasonable reference in India to support banks minimum reference requirements. We request bank to consider OEM references for the bidder. This will allow bidder with expertise elsewhere to provide fair options to the bank.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1005		Annexure 2 - Pre-Qualification Criteria	OEM should have provided on prem PIM solution with minimum 1500 privileged users licenses or 10000 servers licenses in two Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date of submission of Bids.	OEM should have provided on prem PIM solution with minimum 1500 privileged users licenses or 10000 servers licenses in two Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date of submission of Bids.	We understand that bank requirements for sizable reference in Indian Context. We are Make in India OEM of PAM technology and have reasonable referenceable customer inline with requirement of the bank. Also basis the nature of technology, adoption patterns and government technology refresh cycles in India, we humbly request the bank to consider 500 users or 5000 servers as minimum reference.	Bidder to comply with RFP terms and conditions.
1006	233-236	Annexure-10 Technical Evaluation Criteria	6) The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. Supply Experience - For 3 or more clients - 10 marks - For 2 clients - 5 marks	6) The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. Supply Experience - For 3 or more clients - 10 marks - For 2 clients - 5 marks	Considering eligibility criteria and minimum requirements for technical scoring for other products evaluated in the bid, we request the bank to re-consider references across industry verticals i.e. Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI instead of only banking references.	Bidder to comply with RFP terms and conditions.
1007	233-236	Annexure-10 Technical Evaluation Criteria	6) The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. Supply Experience - For 3 or more clients - 10 marks - For 2 clients - 5 marks	6) The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. Supply Experience - For 3 or more clients - 10 marks - For 2 clients - 5 marks	We also humbly request bank to consider references of 500 users or 5000 servers in Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India.	Bidder to comply with RFP terms and conditions.
1008	I. Security Incident and Event Management (SIEM)	168	7	Solution should contain Generative AI based automatic/ custom use case rules builder based on Analyst prompt.	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-1
1009	173		76	The proposed solution must allow access to the rules written in Sigma/Generic SIEM and EDR/XDR query languages. It supports common data schemas of SIEM along with the integration with content service to directly deploy rules from threat detection marketplace.	Request you to kindly elaborate the appropriate use case for the proposed clause. Also request this clause to be removed as it does not make relevance with regards to the SIEM requirements	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1010	174		85	The platform should Query-less search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values	Request to modify the clause as "The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values"	Bidder to refer Corrigendum-1
1011	177		125	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, offense, and the generic APIs.	Offense is a vendor-specific terminology. Request you to remove this clause	Bidder to refer Corrigendum-1
1012					The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.	Bidder to comply with RFP terms and conditions.
1013					Machine learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Bidder to comply with RFP terms and conditions.
1014					The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re-ingesting security analyst would	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1015					The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	Bidder to comply with RFP terms and conditions.
1016					The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.	Bidder to comply with RFP terms and conditions.
1017	II. Security Orchestration and Automation (SOAR):	179	9	The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Request to kindly modify this to "The solution shall have 400+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost"	Bidder to refer Corrigendum-1
1018	180		17	AI Capabilities: a. Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc.	Request you to modify this to "Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department etc." This is specific to a single vendor	Bidder to refer Corrigendum-1
1019	180		18	The solution should suggest contextual between incidents using machine learning.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-1
1020	180		19	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	Request this clause to be removed as it is specific to a single vendor	Bidder to comply with RFP terms and conditions.
1021	181		30	The platform shall have threat visibility and investigation depth, speed and consistency with AI based automated analysis of EDR, NDR and SIEM telemetry sources	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1022	182		38	The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console as in when required.	Request you to modify this to "The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console/cli as in when required."	Bidder to refer Corrigendum-1
1023	182		41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Request this clause to be removed as it is specific to a single vendor	Bidder to comply with RFP terms and conditions.
1024	182		49	The solution must provide a visual workflow editor that is based on BPMN-Business Process Model and Notation to enforce sequencing of incident response activities	Reqest to modify the clause as "The solution must provide a visual workflow editor to enforce sequencing of incident response activities" since this is specific to a single vendor	Bidder to refer Corrigendum-1
1025	185		92	The solution must maintain a database of incidents. The user must be able to search this database using the embedded Elasticsearch. Please describe how your solution meets this requirement.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-1
1026	187		2	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Request the bank to confirm that the UEBA solution in the RFP should perform both user and entity behavior analytics since it is not explicitly mentioned	Yes, UEBA solution in the RFP should perform both user and entity behavior analytics.
1027	187		7	The solution shall have native integration available with leading SIEM, SOAR and ITSM solutions such as IBM, Palo Alto, ServiceNow, BMC Remedy etc.	This contradicts #2. Request to remove this clause	Bidder to refer Corrigendum-1
1028	188		16	UEBA should activate a rules for a set of users until a specified condition or specified time window.	Request you to kindly clarify the use case for this as this does not makes sense for UEBA Solution	Bidder to comply with RFP terms and conditions.
1029	189		22	D/DoS Attack Detected	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-1
1030				Honeytoken Activity		Clause stands deleted. Bidder to refer Corrigendum-1
1031				Capture, Monitoring and Analysis Program Usage		Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1032	189		25	Solution must have network forensic analysis solution as integrated part of offering.	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-1.
1033	190		27	Critical Commands execution on SWIFT Servers - success/ failed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Bidder to comply with RFP terms and conditions.
1034				Critical Password Retrievals From Unauthorized Accounts		Clause stands deleted. Bidder to refer Corrigendum-1.
1035				Critical Server Rooms/Locations Access Attempts By Non-Admin Users		Clause stands deleted. Bidder to refer Corrigendum-1.
1036	190		29	Defense Evasion - T1070 - Indicator Removal on Host - Unauthorized audit logs modification	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1037	190		30	Defense Evasion - T1484 - Group Policy Modification - Account created and deleted in short interval of time	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1038	190		31	Defense Evasion, Persistence - T1108 - Redundant Access - Potential Account Misuse: Disabled Account	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1039	190		32	Direct RDP access of Windows server	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1040	190		37	Interactive Login Detected From Service Accounts on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1041	190		38	Intranet/Internet Activity Via Rare /unauthorized User Agents	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1042	190		39	IOC Compromise Activity Followed By Security risk found-in End point	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1043	190		40	Malware / Ransomware Activity Detected - External Facing Hosts	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1044	190		42	PAM Bypass Activity Detection and Direct Critical infrastructure logins	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1045				Password Dumper Activity on LSASS	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1046				Password sharing - Access to Critical Servers Via multiple locations in very short period of time	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1047				PIM - PAM bypass on Critical servers	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1048				PIM Monitoring PAM - High Volume Login Activity from Multiple Hosts	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1049				Potential Account Compromise - Activity From Rare Country Followed By Rare Application Accessed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1050				Potential Flight Risk: Unusual Visits to Job Sites	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1051				Potential Multi-Channel Data Ex filtration Attempt: DLP Egress and Upload to Webmail Detected	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1052				Potential PIM Monitoring ByPass Activity Detected - Successful RDP Event Without PAM Request	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

CANARA BANK Tender Processing Section C.P.C., I.V.M. Wing, H.O., Bengaluru

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1053				Potential PIM Monitoring ByPass Activity Detected - Successful SSH Login Event Without PAM Request	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1054				Potential Webex Data Transfer/Control	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1055				Privilege Actions / Servers Accessed By Unauthorized Group Members	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1056				Privileged Access Misuse - Audit Log Deletion	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1057	191		43	Ransomware behavior on Critical servers via botnets	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1058	191		44	Rare Malicious PowerShell Scripts Downloads on Critical Servers	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1059	191		45	SMB Traffic / Sessions on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1060	191		47	Suspicious Activity Detected From Non-Compliant Device / Host	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1061	191		48	Suspicious Kerberos RC4 Ticket Encryption	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1062	191		49	Terminated User Activity on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1063	191		50	Testing-Defense Evasion - T1484 - Group Policy Modification - Unauthorized self-privilege escalation - User Context	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1064	191		55	VIP Accounts Monitoring - Watchlists	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1065	191		56	Web Access-Potential Person of Concern	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1066	191		57	Web Access-Potentially Unwanted Software Accessed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1067	191		59	Web Traffic / EDR Alert - Malicious File Download Followed by High Severity EDR Virus Alert	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1068	191		60	Windows - scheduled task created by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1069	191		61	Windows logon-Terminated User Activity	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1070	191		62	Windows- registry value was modified by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1071	191		63	Potential Flight Risk: Unusual Visits to Job Sites	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1072	192		71	The solution should provide Identity Access Analytics use cases along with Access Outliers, Access Clean-up, Dormant Access, Orphan Account Analysis & Terminated Account Access monitoring. The Remediation should happen via Risk Based certifications from the UEBA tool itself.	Request to remove the clause since SOAR is already a part of this RFP	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1073	193		80	The solution should have inbuilt platform support for automation of routine L1/L2 activities.	Request to remove the clause since SOAR is already a part of this RFP	Clause stands deleted. Bidder to refer Corrigendum-1.
1074	19		5.3	Uptime	Request the bank to modify this too active- active high availability with zero RPO and RTO. This is to make sure that there are no challenges with the bank during DC and DR drills and audits as performed by RBI	Bidder to refer Corrigendum-1.
1075	N/A		N/A	Additional points to be included	The UEBA solution should not require internet access to upade any machine learning models	Bidder to comply with RFP terms and conditions.
1076	N/A		N/A	Additional points to be included	The UEBA solution should not need a seperate data lake and should be able to fetch data from SIEM	Bidder to comply with RFP terms and conditions.
1077	216		9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	20 Gbps from Day 1, scale upto 40 Gbps with active-active cluster. We request to consider 20 Gbps from Day 1 and 40 Gbps using Cluster solution.	Bidder to refer Corrigendum-1.
1078	216		12	The proposed solution must be deployed in span mode on day one and also should support inline blocking mode with automatically block inbound exploits, malware, and outbound multi-protocol callbacks.	Is inline mode required from Day 1 or this is a future requirement. Kindly clarify	Solution should support Inline-Monitoring mode and Out of Band (Span) mode from day one.
1079	218		22	Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations with all licenses and dependencies included in the solution.	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-1.
1080	220		40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1081	221		53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	EDR/XDR are supposed to use Cloud Sandbox and for Network Anti-APT solution on prem Sandbox is specified. This will give a much wider detection matrix to the customer. But with Anti-APT integration with EDR/XDR, the End User may loose the critical factor of two systems identifying threats at different levels. This will also rule out any additional advantage to any specific vendor	Bidder to comply with RFP terms and conditions.
1082				Additional points to be included	The Sandbox solution should support at-least 5000 File submissions per day and should be upgradable to higher file submissions in future with additional licenses.	Bidder to comply with RFP terms and conditions.
1083				Additional points to be included	The Sandbox solution must Support of analysis of file size of up to 200MB. Justification: Today the files accessed by uses on a daily basis have increases considerably in terms of file size. A typical PPT can be easily of 15-20MB, a small exe/msi file is of 50-70MB thus in order to be able to detect these large files it is important that the sandbox should be able to scan files upto of 200MB	Bidder to comply with RFP terms and conditions.
1084				Additional points to be included	The proposed sandbox solution should be able to track for network I/O to raw disks and any modification to MBR made by the samples during the dynamic analysis. Justification: MBR is the most critical part of the windows system as it stores the information on where the OS is there on disk and to be loaded. Modifications to this can corrupt the entire system thus it is very important for sandbox to check for this.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1085				Additional points to be included	The proposed sandbox solution should allow user to manually interact with the sample within the analysis environment while the analysis is taking place. Justification: Manualy interaction by admin on malware sample in analysis environment facilitate them with simulating real user scernarios and help in inverstigating the malware with various behvaioural indicators and develop the response strategries without infecting the end user machine	Bidder to comply with RFP terms and conditions.
1086				Additional points to be included	A video recording of the malware analysis should be made and be able to have playback and download capability for further analysis. curity expertise to interpret reports. Justification: Video Playback of sample execution helps the admins to better visualise the analysis and triggers leading upto the file being flagged.and gaining valuable insight into the behaiour of file. It also serves as a great evidence to be submiited to other teams for their consumption for reporting purposes	Bidder to comply with RFP terms and conditions.
1087				Additional points to be included	The sandbox solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed. Justification: Allowing admin's/incident responders to have the capability to interact with the malware sample execution helps them to understand the every samples behvaiour and its impact on the system	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1088				Additional points to be included	The sandbox must have capability to Analyze more than 800+ highly accurate and actionable advanced behavioral indicators. Justification: A detonation engine works on by detecting a behvaiour and matching it against the baseline behvaiour data that the sytem has in order to determine whether it is clean or bad. Thus a sandbox which is a behvaioural detection engine working on by detonating files in controlled environment. thus the higher number of behvaioural indicators ensures the higher catch rate and efficay of sandbox	Bidder to comply with RFP terms and conditions.
1089					AntiAPT solution must have static and dynamic analysis capabilities. Dynamic Analysis solution should have a file processing capability of 50K files per day in case solution scans all the files or 5K file per day if solution scans only unknown/zero-day files.	Bidder to comply with RFP terms and conditions.
1090	225	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	51. The tool should be able to customize the risk categorization. The report generated should highlight the attacks detected along with the category of the same and risk associated with them.	Please clarify the meaning of "risk categorization" in this context and specify the required customization options for risk categorization.	Bidder to comply with RFP terms and conditions.
1091	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	126. The report should contain granular details, which include timestamps, payload information, risk, type of attack, target, description, mitigation, IOC or IOB, etc.	Proposing modification to this point: The report should contain granular details, including timestamps, payload information, risk, type of attack, target, description, mitigation, IOC or IOB (such as File Download, File Write, Registry Modification and Creation, Process Execution, WMI Query, Service Modification and Creation, Web Request performed, etc.) The modification is suggested to provide a more comprehensive list of IOCs and IOBs that are critical for analyzing malicious behavior. Including these specific indicators will enhance the report's value by offering deeper insights into potential threats and enabling more effective response and mitigation strategies.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1092	228	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	90. Solution should have capability to test SIEM rules by simulating a multi- vector attack	The current requirement specifies that the solution should have the capability to test SIEM rules by simulating a multi-vector attack. It is recommended to enhance this point to state that the proposed solution must provide multi-stage attack chains with capabilities involving different execution mechanisms to emulate the realistic nature of the adversaries, like performing DLL Hijack, Process Injection, PPID Spoofing, and Command-line Spoofing for executing malicious payloads or progressing to further stages. This modification is crucial to comprehensively evaluate SIEM rules against threats, ultimately improving detection and response capabilities. We propose enhancing this point: Solution should have capability to test SIEM rules by simulating a multi- vector attack . The solution should provide multi-stage attack chains with capabilities including but not limited to DLL Hijack, Process Injection, PPID Spoofing, and Command-line Spoofing to execute malicious payloads or further stages to simulate realistic testing of SIEM rules.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1093	225	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	47. The solution should be able to simulate Real attacks and provide malware artefacts (capability to simulate real exploits and latest malware)	To enhance the effectiveness of attack simulations, the solution must not only simulate real attacks and provide malware artefacts but also dynamically generate unique payloads for each attack simulation. This addition will create a realistic and varied testing environment, bypassing static signature checks, improving the assessment of security controls and providing deeper insights into the impact of different attack vectors. We propose modifying this point: The solution should be able to simulate real attacks and provide malware artefacts (the capability to simulate real exploits and the latest malware). Additionally, the proposed solution should dynamically generate unique payloads for each attack simulation execution, which the agent shall execute as separate processes with the required privileges. The generated payloads shall be of different types, including, but not limited to, DLL, EXE, and Service.	Bidder to comply with RFP terms and conditions.
1094	227	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	86. Solution should have Ability to simulate breach methods based on attacker profile (APT) and data assets to be protected	To enhance the simulation of breach methods, the solution must focus on the attacker profile and data assets and incorporate testing for advanced techniques like kernel attacks. This addition will provide a more comprehensive assessment of the security posture against advanced threats. We propose modifying this point: The solution should be able to simulate breach methods based on the attacker profile (APT) and data assets to be protected. The proposed solution should also support testing advanced techniques like kernel attacks such as malicious drivers and rootkits. The simulations should utilise and interact with the driver to perform adversarial behaviours, such as killing EDR or other endpoint security solutions on the target asset.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1095	165	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	Suggested Additions	Recommendation for Addition: To enhance the effectiveness of the security solution, it is vital to include various attacker collection techniques in the simulations. This will enable organisations to better understand how attackers can gather sensitive information and improve their defensive measures accordingly. Proposed Point: The proposed solution must provide different attacker collection techniques, such as screenshots, clipboards, keyloggers, audio captures, and more. These simulations must have evasive capabilities, such as using Windows APIs instead of commands and scripts.	Bidder to comply with RFP terms and conditions.
1096	227	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	77. Solution should support Extracting credentials from memory (Endpoint privilege escalation test)	To ensure comprehensive endpoint privilege escalation testing, it is essential for the solution not only to support extracting credentials from memory but also to incorporate evasive mechanisms. This will enhance the effectiveness of the tests by simulating more sophisticated attack techniques. We propose modifying this point: The solution should support extracting credentials from memory (Endpoint privilege escalation test). Additionally, it should provide evasive mechanisms to perform privilege escalation via Reflective DLL Injection, Process Injection, MSHTA shortcuts, ISO files, and Process Hollowing to launch dynamic payloads.	Bidder to comply with RFP terms and conditions.
1097	3	Annexure 8	Sizing & Scalability Requirements	Mentioned Requirements: Breach and Attack Simulation: SaaS with 99.90% uptime	Please provide clarification on the following: 1. The number of agents required for the 5-year SaaS annual subscription. 2. Aside from the two designated manpower, the total number of end users expected to use the platform. 3. The number of users to be targeted for the integrated email phishing simulation module.	Bidder to comply with RFP terms and conditions.
1098	225	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	53. The solution should be capable of importing data from various sources like CMDB to do prioritization.	Request for clarification for this point, please clarify the data sources and formats required for CMDB integration.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1099	229	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	106. The solution should have the ability to import, extract malicious content and weaponize PCAP attack files or malicious traffic.	Request for clarification for this point, please clarify the process for importing, extracting, and weaponizing PCAP attack files or malicious traffic, and any specific formats or protocols to be supported.	Clause stands deleted. Bidder to refer Corrigendum-1
1100	229	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	113. The solution must provide a dashboard that shows a negative deviation from baseline security controls.	Request for clarification for this point, please clarify the baseline definition for security controls and how the negative deviation is expected to be displayed on the dashboard.	Bidder to comply with RFP terms and conditions.
1101	229	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	114. The solution must allow custom dashboard creation directly from the platform. Custom dashboards should give the option to select historical data, comparisons between results, trends, graphs, charts, etc.	Request for clarification for this point, please clarify the specific customization options available for dashboard creation, including the types of historical data, comparisons, and visual elements that can be incorporated.	Bidder to comply with RFP terms and conditions.
1102	229	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	115. The solution must allow selecting datasets from existing data results to create customized dashboards.	Request for clarification for this point, please clarify the types of datasets that can be selected from existing data results for creating customized dashboards.	Clause stands deleted. Bidder to refer Corrigendum-1
1103	229	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	116. The solution must allow cloning and editing of customized dashboards as and when required.	Request for clarification for this point, please clarify the process and limitations regarding the cloning and editing of customized dashboards.	Bidder to comply with RFP terms and conditions.
1104	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	117. The solution must provide benchmarking and comparison results for organizations in the same industry.	Request for clarification for this point, please clarify how benchmarking and comparison results will be generated and which industry data will be used for these comparisons.	Bidder to comply with RFP terms and conditions.
1105	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	123. The report must have previous comparisons to show changes in current control, i.e., improved or deteriorated.	Request for clarification for this point, please clarify how previous comparisons will be incorporated into the report to show whether current controls have improved or deteriorated.	Bidder to comply with RFP terms and conditions.
1106	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	127. The solution must allow custom report creation directly from the platform. A custom report should give the option to select historical data, comparisons between results, trends, graphs, charts, etc.	Request for clarification for this point, please clarify the specific customization options available for report creation, including the types of historical data, comparisons, and visual elements that can be included.	Bidder to comply with RFP terms and conditions.
1107	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	128. The solution must provide industry-standard reporting templates, e.g., remediation guides, prevention and detection reports, overall security posture, and security control performance.	Request for clarification for this point, please clarify the specific industry-standard reporting templates that will be provided and any customization options available for these templates.	Bidder to comply with RFP terms and conditions.
1108	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	130. The solution must allow cloning and editing of customized reports as and when required.	Request for clarification for this point, please clarify the process and any limitations regarding the cloning and editing of customized reports.	Bidder to comply with RFP terms and conditions.
1109	230	Annexure 9	Functional and Technical Requirements: Breach and Attack Simulation	133. The solution must provide comparative reporting, allowing the end-user to compare the results of an agent or group of agents mapped to the MITRE ATT&CK TTPs.	Request for clarification for this point, please clarify how comparative reporting will be implemented, particularly regarding the mapping of agent results to the MITRE ATT&CK TTPs.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1110	3	Annexure 8	Scope of Work Document: Sizing & Scalability Requirements	Breach and Attack Simulation: SaaS model supporting 99.90 percent uptime	Request for clarification for this point, please clarify the number of agents required for the 5-year SaaS annual subscription, the total number of end users expected to use the platform aside from the two fixed manpower, and the number of users targeted for the integrated email phishing simulation module.	Bidder to comply with RFP terms and conditions.
1111	279	Cl.10	Termination of contract	Addition of new clause	We propose to add Contractor's termination rights in the event of breach by UPPCL/Discom as per below: In the event Bank materially breaches the Contract, which breach is not cured within thirty (30) days after written notice specifying the breach is given to Bank, the Contractor may terminate the Contract or any portion thereof or by giving written notice to Bank.	Bidder to comply with RFP terms and conditions
1112	283	Cl.14	Indemnity	Addition of new clause (14.7)	NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY DAMAGES FOR LOST PROFITS, LOST REVENUES, LOSS OF GOODWILL, LOSS OF ANTICIPATED SAVINGS, LOSS OF CUSTOMERS, OR LOSS OF DATA, OR INTERFERENCE WITH BUSINESS, ARISING OUT OF THE PERFORMANCE OR FAILURE TO PERFORM UNDER THIS AGREEMENT, WHETHER OR NOT CAUSED BY THE ACTS OR OMISSIONS OR NEGLIGENCE (INCLUDING GROSS NEGLIGENCE OR WILLFUL MISCONDUCT) OF ITS EMPLOYEES OR AGENTS, AND REGARDLESS OF WHETHER SUCH PARTY HAS BEEN INFORMED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1113	287	Cl.21	Hiring of Bank staff or Ex staff	The VENDOR/ SERVICE PROVIDER or subcontractor(s) shall not hire any of the existing/ ex/retired employees of the Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory guidelines/HR policies of the Bank	We propose to modify the below clause such that: During the term of the Contract and for a period of one year thereafter, neither Party ~~The VENDOR/ SERVICE PROVIDER or subcontractor(s)~~ shall ~~not~~ hire any of the existing~~/ ex/retired~~ employees of the other party or aid any third person to do so, without the specific written consent of the other party. This provision shall however not apply to any solicitation conducted through general advertisement of employment opportunities through placement agencies, public advertisement or otherwise which do not specifically target such employees. The above restriction also applies to each party's affiliates, agents, vendors, contractors, and any third parties with whom such party has a relationship (collectively, "Representatives"). Representatives are also prohibited from soliciting or inducing any employee, consultant, or independent contractor of other party to leave their employment or engagement with such other party."~~Bank during the contract period or after the closure/termination of contract even if existing/ ex/retired employee actively seek employment from the VENDOR/ SERVICE PROVIDER or sub-contractor(s). The period /duration after the date of resignation/ retirement/ termination after which the existing/ex/retired employee shall be eligible for taking up such employment shall be governed by regulatory~~	Bidder to comply with RFP terms and conditions
1114	20	Cl.6	Penalties/ Liquidated Damages	Penalties/Liquidated damages for delay in Delivery and Installation	We request the bank to consider to limit the maximum penalty for delivery/installation to 5% of the value of undelivered portion of Delivery/Installation	Bidder to comply with RFP terms and conditions.
1115	22	Cl.6	Penalties/ Liquidated Damages	Penalty on Service levels during Operations phase	We request the bank to consider to limit the maximum penalty for SLA, Uptime and Manpower services to 10% of the value of monthly/quarterly charges payable	Bidder to comply with RFP terms and conditions.
1116	232	Cl.2	Annexure-10 Technical Evaluation Criteria	The Bidder's Annual turnover in the last 3 years •>500 crore <=1000 crore - Score of 2 •>1000 crore <=1500 crore - Score of 5 •>1500 crore - Score of 10	We request the bank to kindly exclude Annual turnover from the Technica Evaluation Criteria. As the same is not a technical scoring or technical capability measure of an organisation. Usually annual turnover is considered as part of the Pre Qualification Criteria which is already included in the current RFP.	Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1117	233	Cl.7	Annexure-10 Technical Evaluation Criteria	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience •For 5 or more clients - 5 marks •For 2 clients - 3 marks	The SaaS based EDR is a relatively a new technology adopted by very few BFSI/PSU/Government organisations. Majority of the deployments are onprem. Hence we kindly request bank to consider the onprem implementation also for this criteria. We kindlyrequest the amend the clause as below The Bidder must have implemented any EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience •For 3 or more clients - 5 marks •For 2 clients - 3 marks	Bidder to refer Corrigendum-1.
1118	235	Cl.12	Annexure-10 Technical Evaluation Criteria	The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions SIEM - 10 certified OEM resource PIM - 5 certified OEM resource SOAR - 5 certified OEM resource EDR - 5 certified OEM resource Note: All respective certified resources must be on direct payroll of Bidder.	We request the bank to remove "Proposed OEM certifications" as having the combination of all the mentioned OEM Certification is practically not feasible. Hence we request the bank to consider any major OEM certifications for the mentioned technologies/Solutions.	Bidder to comply with RFP terms and conditions.
1119	96	Cl.7	L2 Incident Responder	The L2 Incident responder shall have minimum 5 years of experience in Incident response, possess at least one of the following certifications, a) Security+ b) ECSA c) GCFA d) GCFE e) CISPP f) Any SIEM Certification	We kindly request to include CISM/CISA certification as well which is a sandard industry practice	Bidder to comply with RFP terms and conditions.
1120	98	Cl.8	L3 Incident Investigator	The L3 Incident investigator shall have minimum7 years of experience in Incident response, possess at least one of the following certifications, 1) CHFI 2) GCFA 3) GCFE 4) CISSP	We kindly request to include CISM/CISA certification and Any SIEM certification as well which is a sandard industry practice	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1121	23	Cl.4	Manpower services	Penalty of Rs.5000 per resource per day for absence of L1 and Penalty of Rs.10000 per resource per day for absence of L2 SOC Analyst (of monthly payout). Penalty of Rs.15000 per resource per day for L3/ Project Manager of monthly payout. However, total penalty under this will be limited to 20% of the total charges payable for Resource charges for the monthly payout.	We request to limit the penalty to 10% of the total charges payable for Resource charges for the monthly payout.	Bidder to comply with RFP terms and conditions.
1122	26	Clause 7	Payment Terms -Hardware cost (including OS & associated Softwares	30% - After complete delivery of all hardware and its related software. Please note that Originals of invoices (plus One Copy) reflecting Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/ office should be submitted while claiming payment in respect of orders placed.	We request the bank to consider the payment terms on hardware cost as 70% payment on delivery, which will improve the Cashflow for the SI	Bidder to comply with RFP terms and conditions
1123	27	Clause 7	Payment Terms - AMC/ ATS	Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.	As all the OEM provide only yearly advance payment terms, hence we request the bank to consider the payment as Yearly in Advance	Bidder to comply with RFP terms and conditions
1124	246	Annexure-17 Bill of Material	Table 3	Price for NGSOC Tech Refresher	As the Tech Refresher table is with named OEM solutions, we request the bank to exclude the table 3 from the total TCO. The bank may obtain the commercials in a closed cover from these OEMs and add same commercials commonly to all the technical qualified bidders to avoid these OEMs taking any biased stand. Alos, this will prevent the named OEMs quoting non competitative rates or inflated commercials to the bidders.	Bidder to comply with RFP terms and conditions.
1125	29	Clause 8	Warranty 8.2	8.2 The selected bidder has to provide comprehensive On-site warranty for the period of Three (3) years from the date of go live for the proposed Solution.	Request Bank to consider upfront warranty of 5 years which will benefit the total TCO	Bidder to comply with RFP terms and conditions.
1126	167	Annuexure 9	Technical specification	34. SAN system should support native remote replication both synch & Asynch replication for backup/DR purposes. The storage system should support Zero RTO natively.	Sync or Zero RTO can be achieved only if the distance is within the range, hence request Bank to change the clause	Bidder to comply with RFP terms and conditions.
1127	114	7	Scope of Work for Bidder/ System Integrator (SI)	•The Bidder shall maintain comprehensive backup and Disaster recovery plan, including (a) regular backups of all data configurations software's etc. (b) regular testing of backups and DR failures	Request Bank to confirm if the backup of the complete solution taken should be placed in the Tape library or D2D stoarge	Bidder to comply with RFP terms and conditions.
1128	85	2.n	Scope of Work- Forensic Support	Provide immediate forensic support in case of any security / cyber incident.	Please confirm if the Bank is looking for a Forensic Retainer (example: predefined block of 50 or 100 hours) or a dedicated service	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1129	85	2.n	Scope of Work- Forensic Support	Provide immediate forensic support in case of any security / cyber incident.	Please confirm if the Forensic Services can be delivered remotely from Inspira's office/SOC or you need onsite support as well. If osnite support is needed, how many locations will be in scope ?	Bidder to refer Corrigendum-1
1130	85	2.n	Scope of Work- Forensic Support	Provide immediate forensic support in case of any security / cyber incident.	Request you to provide the SLAs applicable for Forensic Analysis	Bidder to refer Corrigendum-1
1131	71	Annexure-2	Pre-Qualification Criteria	Additional query	we request the bank to ask for atleast one reference on SaaS EDR implementation along with sign off since last 5 years in one PSU BFSI in India. Or atleast One reference of OEM with 85K nodes in a PSU bank in India. This will help canara bank to get such OEM who have a track record of performing and protecting a bank of canara bank size. This clause will ensure Quality OEM will participate in the RFP.	Bidder to comply with RFP terms and conditions.
1132	233-236	Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5.End point is a complext project to deploy, its even more complex in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder allignment who have demonstrated a smooth deployment and sustance in such large environment in BFSI in India. This will make the bidder to allign with such OEM's who have a track record of protecting such large environment. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an oppertunity to evalute Bidder capability or allow bidder to allign with such bidders who have great track record in BFSI in India. hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1133	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
1134	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-1.
1135	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1136	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.
1137	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1138	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-1
1139	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-1
1140	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-1
1141	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-1
1142	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1143	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-1
1144	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-1
1145	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
1146	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1147	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
1148	165	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.
1149	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2
1150	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1151	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-1.
1152	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1.
1153	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1.
1154	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1155	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1.
1156	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-1.
1157	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1.
1158	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-1.
1159	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1160	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-2.
1161	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
1162	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-2.
1163	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-2.
1164	222	IX. Breach Attack Simulation (BAS):	BAS, Point 18	For the proposed Solution, The Simulation agent should be compatible on Windows, Linux, UNIX (All flavors including but not limited to Ubuntu, RHEL, Cent OS, MAC OS, IBM AIX and Solaris) etc.	No/major solutions don't support Unix like AIX, Solaris etc. Please remove the Unix support clause	Bidder to refer Corrigendum-2.
1165	223	IX. Breach Attack Simulation (BAS):	BAS, Point 20	The Solution agent component must be installable as a software package (Publishing it through group policy) and can be included in Golden image.	BAS agent is not required to be deployed organisation-wide like any other endpoint agents. This is deployed on selected VMs/Desktops/Laptops where simulation will be run. Please remove the clause.	Bidder to comply with RFP terms and conditions.
1166	224	IX. Breach Attack Simulation (BAS):	BAS, Point 43	The solution should be able to source latest threats in the industry and should be able to provide simulations immediately, not later than 1 day of discovery of any new threat.	Different threat has different SLAs. Please change to 'Critical threats should be enabled by 24hrs/1 day'.	Bidder to refer Corrigendum-2.
1167	226	IX. Breach Attack Simulation (BAS):	BAS, Point 58	The solution should have the capability to execute attacks over multiple layers including attack through tunnelling.	Please explain the 'tunnelling' meaning in the context of attack execution	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1168	227	IX. Breach Attack Simulation (BAS):	BAS, Point 81	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g., Gdrive, OneDrive, Dropbox, slack etc.)	The exfiltration to cloud drives use 'https' as protocol. There is no significant outcome to have these as separate requirements. Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1.
1169	228	IX. Breach Attack Simulation (BAS):	BAS, Point 101	Solution should have integrated Email phishing simulation module with the capability of accessing the responses.	This is a phishing campaign requirement. Request is to keep phishing separate and remove this clause or allow third-party phishing solution to be part of this	Bidder to comply with RFP terms and conditions.
1170	229	IX. Breach Attack Simulation (BAS):	BAS, Point 105	The solution should have the capability to Execute a custom data exfiltration action through email, pen-drive, SFTP etc. attempting to physically remove data from customer infrastructure.	Most of the organisations stopped the USB using AD group policies, so there is no point in opening this and simulating exfiltration. By default pen-drive will be disabled. Please remove this clause No organisation opens SFTP port (22) from inside-out. Just for simulating opening TCP port 22 doesnt make any sense. We request you to remove this clause	Bidder to comply with RFP terms and conditions.
1171	229	IX. Breach Attack Simulation (BAS):	BAS, Point 106	The solution should have the ability to import, extract malicious content and weaponize PCAP attack files or malicious traffic.	Anything which is not tested properly in lab should not be done in live environment. Simulating PCAP file can have adverse effects. We request you to remove this clause	Clause stands deleted. Bidder to refer Corrigendum-1.
1172	87	3.Sizing & Scalability Requirements	Point 15	Cyber Range: Partcipants:5/batch, Hours: 40 hours per year	Our understanding is that a total of 40 Hours per year of Range access along with trainer as applicable has to be provided to the Bank. This will be done for a batch of 5 people. Please clarify if this is correct. Also kindly let us know for how many years should this be quoted?	Bidder to refer Corrigendum-1.
1173	87	3.Sizing & Scalability Requirements	Point 15	Cyber Range: Partcipants:5/batch, Hours: 40 hours per year	Our understanding is that the bidder has to own the preparatory hours for training to be done on Cyber Range. Ideally this is outside the 40 hours mentioned for the Cyber range SAAS platform. Please clarify if our understanding is correct.	Bidder to refer Corrigendum-1.
1174	142	14. SoW for Proposed Services	Threat Inteligence Services - Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage	Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Bidder to comply with RFP terms and conditions.
1175	145	14. SoW for Proposed Services	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/tools/exchange knowledge for banks brand	Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1176	146	14. SoW for Proposed Services	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank: - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	Kindly elaborate the scope.	Bidder to refer Corrigendum-2.
1177	174	Annexure-9 Functional and Technical Requirements	Packet Capture, Point 133	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	SIEM, PCAP, and UEBA from the same OEM ensures seamless integration, leading to better data correlation and faster threat detection. A unified platform provides consistent data formats, reduces integration complexity, and eliminates gaps in security coverage. This allows for more accurate analysis of network traffic, user behaviour, and security events along with reduced operational costs, improved efficiency through a centralized dashboard. With PCAP and UEBA from same OEM, it will give additional network models which will augment the network detection capability. Request to consider PCAP also from the same OEM along with SIEM and UEBA Kindly change this to "The proposed Packet capture solution should be from the same OEM which offers SIEM and UEBA to ensure seamless integration between all detection layers with native capabilities to integrate with proposed SIEM and UEBA solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same"	Bidder to refer Corrigendum-2.
1178	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 9	The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage custom data models if necessary	Machine learning models are delivered through UEBA which are preconfigured and managed by OEM only as they are complex in nature and requires high skill set. Custom data models can be a security concern as it exposes the Data Models to be manipulated. Please Change this point to allow more reputed OEM's to participate. Kindly modify the line as "The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage inbuilt non customised data models for ML OR custom data models if necessary"	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1179	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 15	The solution shall use unsupervised and supervised machine learning algorithms for anomaly detection mentioned below (a) Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency. (b) Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time. (c) Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly. (d) Usage deviates from peer group such as User pattern of activity starts deviating from the peer group. (e) Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems. (f) Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing. (g) Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data (h) Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data (i) Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users	Supervised learning demands a large volume of labelled data and ongoing supervision from data scientists, increasing the complexity and effort. Unsupervised ML methods thus offer scalability and adaptability in dynamic environments with less human intervention. This complexity is better owned by product owners than operations teams i.e. OEMs only. Hence request you to change the clause to "The solution shall use unsupervised/supervised machine learning algorithms for anomaly detection mentioned below"	Bidder to refer Corrigendum-1.
1180	176	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 9	The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	This requirement is proprietary to single OEM and highly restrictive for fair participation Kindly change this to "The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost."	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1181	178	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 29	Bank shall have 15 user licenses and 2 read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	With fewer admin users, organizations reduce the risk of misconfigurations, unauthorized changes, and potential security breaches. Admins can oversee critical tasks like setting up automation workflows and managing incident responses, while read-only users can monitor, analyse, and collaborate without altering configurations. This approach improves accountability, as key decision-makers maintain control, while enabling broader visibility across teams. It balances security with transparency, allowing stakeholders to stay informed without compromising the integrity of the SOAR environment. Hence, we recommend unlimited read only users for better monitoring and visibility throughout across management of Bank. Kindly modify the clause to "Bank shall have 15 user licenses and unlimited read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract"	Bidder to comply with RFP terms and conditions.
1182	179	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Custom Threat hunting is not a native SOAR functionality and is supported through SIEM Platform. Kindly remove this requirement.	Clause stands deleted. Bidder to refer Corrigendum-1.

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Wing, H.O., Bengaluru - 560 001 सी. पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1183	175	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 1	The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank	Gartner research highlights the benefits of integrating SOAR and TIP (from the same OEM to enhance security efficiency and reduce complexity. A unified platform streamlines data sharing, automates threat intelligence enrichment, and improves response times by eliminating the need for custom integrations. According to Gartner, consolidating these tools minimizes operational overhead and improves incident response capabilities, as they work in sync to detect and mitigate threats more effectively. By leveraging a single vendor, organizations can ensure better interoperability, reduce management challenges, and strengthen their overall security posture through automated, cohesive workflows. Hence we suggest, SOAR and TIP should be from same OEM Kindly modify this clause to "The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank. Proposed SOAR and TIP solutions should be from the same OEM"	Bidder to comply with RFP terms and conditions.
1184	210	Annexure-9 Functional and Technical Requirements	VI. Threat Intelligence Platform (TIP) :, Point 20	The proposed solution offers more than 130 open-sourced intelligence and also provide Free Feeds' content as well	Kindly change the clause to "The proposed solution offers more than 50+ open-sourced intelligence and also provide Free Feeds' content as well"	Bidder to refer Corrigendum-2.
1185	177	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 19	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	This is typical case management usecases and is OEM specific Kindly remove this requirement to ensure fair participation	Bidder to comply with RFP terms and conditions.
1186	183	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 2	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Given that,SIEM and UEBA are required to be from the same OEM. Our understanding is that the functionalities mentioned in the SIEM,UEBA technical specifications can be achieved through either of the solutions. Please confirm if our understanding is correct.	No, UEBA Technical specifications has to be achived through UEBA solution only.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1187	165	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM): , Point 2	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	a) As per our understanding, solution needs to be sized for 1,00,000 sustained EPS with peak handling capacity of 1,50,000 EPS for both DC and DR respectively. Kindly confirm on the sustained and peak EPS values for both DC and DR respectively. b) To ensure there are no assumptions done by the OEM for solution sizing on log sizing and licensing. Kindly consider modifying this clause as below "The solution shall be sized for 1,00,000 EPS as sustained EPS or 6.5 TB log capture per day (average log size as 800 Bytes) and 150,000 as peak EPS for both for DC & DR respectively during contract period. Solution should have same license across all layers i.e. collection, correlation and management layer to ensure no dropping or queuing of logs on any proposed SIEM components as per bank requirement. There should not be any limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Solution should support unlimited device integrations."	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
1188	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 43	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system with critical fields like server IP, Server hostname, OS Name, OS Version, Criticality, Date of discovery etc. to be populated automatically	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.
1189	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 44	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1190	166	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 18	Proposed solution should support both automatic and manually escalation of incidents to proposed SOAR and should allow the proposed SOAR to query data from the SIEM	SIEM and SOAR can be from different OEMs as per the RFP. This clause is restrictive as it favours a single OEM which offers both SIEM and SOAR. Please change the clause to "Proposed solution should support export of incidents to proposed SOAR and should allow the proposed SOAR to query incident data from the SIEM"	Bidder to comply with RFP terms and conditions.
1191	71	Annexure-2 Pre-Qualification Criteria	Eligibility Criteria	Considering the complexity of the Banking environment, the SIEM, PCAP, UEBA, SOAR and TIP solutions should be from the Proven & Reputed OEMs.	Request you to kindly incorporate below criteria - The SIEM OEM should be incorporated in India under the Companies Act 1956 for at least 10 years . - Minimum Average Annual Turnover (MAAT) for last three years out of last five financial years of the SIEM OEM should not be less than INR Five Hundred (500) Crore. SIEM OEM must have positive net worth.	Bidder to comply with RFP terms and conditions.
1192	246	Annexure-17 Bill of Material - Table 3	Price for NGSOC Tech Refresher	As Bank wants to have tech refresh of the existing solutions(Anti DDoS, NBA, DLP, VA), the particular OEM.s associated with these solutions will have an advantage of price negotiation with bidder and not allowing bidder to have freehand in deciding the prices to be quoted for newly asked solutions .	Request Bank to remove these items from this RFP, for all the bidders/OEMs to have fair chance to bid in this RFP.	Bidder to comply with RFP terms and conditions.
1193	168	7	I. Security Incident and Event Management (SIEM)	Solution should contain Generative AI based automatic/ custom use case rules builder based on Analyst prompt.	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-1.
1194	173	76	I. Security Incident and Event Management (SIEM)	The proposed solution must allow access to the rules written in Sigma/Generic SIEM and EDR/XDR query languages. It supports common data schemas of SIEM along with the integration with content service to directly deploy rules from threat detection marketplace.	Request you to kindly elaborate the appropriate use case for the proposed clause. Also request this clause to be removed as it does not make relevance with regards to the SIEM requirements	Bidder to comply with RFP terms and conditions.
1195	174	85	I. Security Incident and Event Management (SIEM)	The platform should Query-less search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values	Request to modify the clause as "The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change condition, operator, time frame, column display, and values"	Bidder to refer Corrigendum-1.
1196	177	125	I. Security Incident and Event Management (SIEM)	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, offense, and the generic APIs.	Offense is a vendor-specific terminology. Request you to remove this clause	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1197			I. Security Incident and Event Management (SIEM)	Additional points to be included	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.	Bidder to comply with RFP terms and conditions.
1198			I. Security Incident and Event Management (SIEM)	Additional points to be included	Machine learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	Bidder to comply with RFP terms and conditions.
1199			I. Security Incident and Event Management (SIEM)	Additional points to be included	The solution must ensure that if data ingested is not parsed then with the new parser old data ingested should also be parsed without need to re-ingest data throughout the retention period. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re-ingesting security analyst would	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1200			I. Security Incident and Event Management (SIEM)	Additional points to be included	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre- defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.	Bidder to comply with RFP terms and conditions.
1201			I. Security Incident and Event Management (SIEM)	Additional points to be included	The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.	Bidder to comply with RFP terms and conditions.
1202	179	9	II. Security Orchestration and Automation (SOAR):	The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Request to kindly modify this to "The solution shall have 400+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost"	Bidder to refer Corrigendum-1.
1203	180	17	II. Security Orchestration and Automation (SOAR):	AI Capabilities: a. Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc.	Request you to modify this to "Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department etc." This is specific to a single vendor	Bidder to refer Corrigendum-1.
1204	180	18	II. Security Orchestration and Automation (SOAR):	The solution should suggest contextual between incidents using machine learning.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-1.
1205	180	19	II. Security Orchestration and Automation (SOAR):	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	Request this clause to be removed as it is specific to a single vendor	Bidder to comply with RFP terms and conditions.
1206	181	30	II. Security Orchestration and Automation (SOAR):	The platform shall have threat visibility and investigation depth, speed and consistency with AI based automated analysis of EDR, NDR and SIEM telemetry sources	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-1.
1207	182	38	II. Security Orchestration and Automation (SOAR):	The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console as in when required.	Request you to modify this to "The Platform must support Evidence retention, case notes, and attached artifacts should be retained retain six months events online and 1 year Archival (Six months + 12 months). The bidder shall size the hardware accordingly. There should be a mechanism for Bank to configure Data retention and archival settings through console/cli as in when required."	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

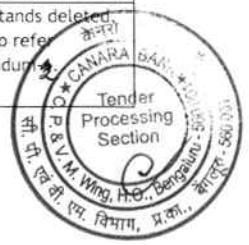
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1208	182	41	II. Security Orchestration and Automation (SOAR):	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Request this clause to be removed as it is specific to a single vendor	Clause stands deleted. Bidder to refer Corrigendum-1.
1209	182	49	II. Security Orchestration and Automation (SOAR):	The solution must provide a visual workflow editor that is based on BPMN-Business Process Model and Notation to enforce sequencing of incident response activities	Reqest to modify the clause as "The solution must provide a visual workflow editor to enforce sequencing of incident response activities" since this is specific to a single vendor	Bidder to refer Corrigendum-1.
1210	185	92	II. Security Orchestration and Automation (SOAR):	The solution must maintain a database of incidents. The user must be able to search this database using the embedded Elasticsearch. Please describe how your solution meets this requirement.	Request this clause to be removed as it is specific to a single vendor	Bidder to refer Corrigendum-1.
1211	187	2	III. User Entity Behavioral Analysis (UEBA)	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Request the bank to confirm that the UEBA solution in the RFP should perform both user and entity behavior analytics since it is not explicitly mentioned	Yes, UEBA solution in the RFP should perform both user and entity behavior analytics.
1212	187	7	III. User Entity Behavioral Analysis (UEBA)	The solution shall have native integration available with leading SIEM, SOAR and ITSM solutions such as IBM, Palo Alto, ServiceNow, BMC Remedy etc.	This contradicts #2. Request to remove this clause	Bidder to refer Corrigendum-1.
1213	188	16	III. User Entity Behavioral Analysis (UEBA)	UEBA should activate a rules for a set of users until a specified condition or specified time window.	Request you to kindly clarify the use case for this as this does not makes sense for UEBA Solution	Bidder to comply with RFP terms and conditions.
1214	189	22	III. User Entity Behavioral Analysis (UEBA)	22. Network Traffic and Attacks D/DoS Attack Detected Honeytoken Activity Capture, Monitoring and Analysis Program Usage	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-1.
1215	189	25	III. User Entity Behavioral Analysis (UEBA)	Solution must have network forensic analysis solution as integrated part of offering.	Request clarification on the use cases, as these are not aligned to UEBA	Clause stands deleted. Bidder to refer Corrigendum-1.
1216	190	27	III. User Entity Behavioral Analysis (UEBA)	27. Critical Applications Critical Commands execution on SWIFT Servers - success/ failed Critical Password Retrievals From Unauthorized Accounts Critical Server Rooms/Locations Access Attempts By Non-Admin Users	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA in this	Clause stands deleted. Bidder to refer Corrigendum-1.
1217	190	29	III. User Entity Behavioral Analysis (UEBA)	Defense Evasion - T1070 - Indicator Removal on Host - Unauthorized audit logs modification	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1218	190	30	III. User Entity Behavioral Analysis (UEBA)	Defense Evasion - T1484 - Group Policy Modification - Account created and deleted in short interval of time	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1219	190	31	III. User Entity Behavioral Analysis (UEBA)	Defense Evasion, Persistence - T1108 - Redundant Access - Potential Account Misuse: Disabled Account	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1220	190	32	III. User Entity Behavioral Analysis (UEBA)	Direct RDP access of Windows server	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1221	190	37	III. User Entity Behavioral Analysis (UEBA)	Interactive Login Detected From Service Accounts on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1222	190	38	III. User Entity Behavioral Analysis (UEBA)	Intranet/Internet Activity Via Rare /unauthorized User Agents	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1223	190	39	III. User Entity Behavioral Analysis (UEBA)	IOC Compromise Activity Followed By Security risk found-in End point	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1224	190	40	III. User Entity Behavioral Analysis (UEBA)	Malware / Ransomware Activity Detected - External Facing Hosts	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1225	190	42	III. User Entity Behavioral Analysis (UEBA)	PAM Bypass Activity Detection and Direct Critical infrastructure logins	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1226	190	42	III. User Entity Behavioral Analysis (UEBA)	Password Dumper Activity on LSASS	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1227	190	42	III. User Entity Behavioral Analysis (UEBA)	Password sharing - Access to Critical Servers Via multiple locations in very short period of time	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1228	190	42	III. User Entity Behavioral Analysis (UEBA)	PIM - PAM bypass on Critical servers	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1229	190	42	III. User Entity Behavioral Analysis (UEBA)	PIM Monitoring PAM - High Volume Login Activity from Multiple Hosts	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1230	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential Account Compromise - Activity From Rare Country Followed By Rare Application Accessed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1231	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential Flight Risk: Unusual Visits to Job Sites	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1232	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential Multi-Channel Data Ex filtration Attempt: DLP Egress and Upload to Webmail Detected	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1233	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential PIM Monitoring ByPass Activity Detected - Successful RDP Event Without PAM Request	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1234	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential PIM Monitoring ByPass Activity Detected - Successful SSH Login Event Without PAM Request	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1235	190	42	III. User Entity Behavioral Analysis (UEBA)	Potential Webex Data Transfer/Control	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1236	190	42	III. User Entity Behavioral Analysis (UEBA)	Privilege Actions / Servers Accessed By Unauthorized Group Members	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1237	190	42	III. User Entity Behavioral Analysis (UEBA)	Privileged Access Misuse - Audit Log Deletion	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

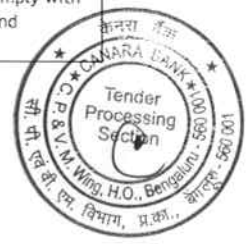


Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1238	191	43	III. User Entity Behavioral Analysis (UEBA)	Ransomware behavior on Critical servers via botnets	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1239	191	44	III. User Entity Behavioral Analysis (UEBA)	Rare Malicious PowerShell Scripts Downloads on Critical Servers	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1240	191	45	III. User Entity Behavioral Analysis (UEBA)	SMB Traffic / Sessions on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1241	191	47	III. User Entity Behavioral Analysis (UEBA)	Suspicious Activity Detected From Non-Compliant Device / Host	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1242	191	48	III. User Entity Behavioral Analysis (UEBA)	Suspicious Kerberos RC4 Ticket Encryption	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1243	191	49	III. User Entity Behavioral Analysis (UEBA)	Terminated User Activity on Critical Infrastructure	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1244	191	50	III. User Entity Behavioral Analysis (UEBA)	Testing-Defense Evasion - T1484 - Group Policy Modification - Unauthorized self-privilege escalation - User Context	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1245	191	55	III. User Entity Behavioral Analysis (UEBA)	VIP Accounts Monitoring - Watchlists	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1246	191	56	III. User Entity Behavioral Analysis (UEBA)	Web Access-Potential Person of Concern	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1247	191	57	III. User Entity Behavioral Analysis (UEBA)	Web Access-Potentially Unwanted Software Accessed	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.

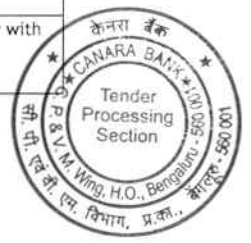
Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1248	191	59	III. User Entity Behavioral Analysis (UEBA)	Web Traffic / EDR Alert - Malicious File Download Followed by High Severity EDR Virus Alert	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1249	191	60	III. User Entity Behavioral Analysis (UEBA)	Windows - scheduled task created by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1250	191	61	III. User Entity Behavioral Analysis (UEBA)	Windows logon-Terminated User Activity	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1251	191	62	III. User Entity Behavioral Analysis (UEBA)	Windows- registry value was modified by unusual user	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1252	191	63	III. User Entity Behavioral Analysis (UEBA)	Potential Flight Risk: Unusual Visits to Job Sites	This use case can be achieved by SIEM, request the Bank to clarify the requirement of UEBA on this	Clause stands deleted. Bidder to refer Corrigendum-1.
1253	192	71	III. User Entity Behavioral Analysis (UEBA)	The solution should provide Identity Access Analytics use cases along with Access Outliers, Access Clean-up, Dormant Access, Orphan Account Analysis & Terminated Account Access monitoring. The Remediation should happen via Risk Based certifications from the UEBA tool itself.	Request to remove the clause since SOAR is already a part of this RFP	Clause stands deleted. Bidder to refer Corrigendum-1.
1254	193	80	III. User Entity Behavioral Analysis (UEBA)	The solution should have inbuilt platform support for automation of routine L1/L2 activities.	Request to remove the clause since SOAR is already a part of this RFP	Clause stands deleted. Bidder to refer Corrigendum-1.
1255	19	5.3	III. User Entity Behavioral Analysis (UEBA)	Uptime	Request the bank to modify this too active- active high availability with zero RPO and RTO. This is to make sure that there are no challenges with the bank during DC and DR drills and audits as performed by RBI	Bidder to refer Corrigendum-1.
1256	N/A	N/A	III. User Entity Behavioral Analysis (UEBA)	Additional points to be included	The UEBA solution should not require internet access to upade any machine learning models	Bidder to comply with RFP terms and conditions.
1257	N/A	N/A	III. User Entity Behavioral Analysis (UEBA)	Additional points to be included	The UEBA solution should not need a seperate data lake and should be able to fetch data from SIEM	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1258	216	9	VIII Anti APT	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	20 Gbps from Day 1, scale upto 40 Gbps with active-active cluster. We request to consider 20 Gbps from Day 1 and 40 Gbps using Cluster solution.	Bidder to refer Corrigendum-2.
1259	216	12	VIII Anti APT	The proposed solution must be deployed in span mode on day one and also should support Inline blocking mode with automatically block inbound exploits, malware, and outbound multi-protocol callbacks.	Is inline mode required from Day 1 or this is a future requirement. Kindly clarify	Solution should support Inline-Monitoring mode and Out of Band (Span) mode from day one.
1260	218	22	VIII Anti APT	Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as Execution of suspicious network traffic against thousands of operating system, service pack, IoT application type and application version combinations with all licenses and dependencies included in the solution.	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2.
1261	220	40	VIII Anti APT	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Most Sandboxes in the industry runs Windows VMs to identify the unknown file to be malicious or not. So, it is not necessary to run the execute the file in hardened systems like Macintosh or Linux. The intent is to define the file to be safe or unsafe and Windows OS allows such identification easily.	Bidder to refer Corrigendum-2.
1262	221	53	VIII Anti APT	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	EDR/XDR are supposed to use Cloud Sandbox and for Network Anti-APT solution on prem Sandbox is specified. This will give a much wider detection matrix to the customer. But with Anti-APT integration with EDR/XDR, the End User may loose the critical factor of two systems identifying threats at different levels. This will also rule out any additional advantage to any specific vendor	Bidder to comply with RFP terms and conditions.
1263	N/A	N/A	VIII Anti APT	Additional points to be included	The Sandbox solution should support at-least 5000 File submissions per day and should be upgradable to higher file submissions in future with additional licenses.	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1264	N/A	N/A	VIII Anti APT	Additional points to be included	The Sandbox solution must Support of analysis of file size of up to 200MB. Justification: Today the files accessed by uses on a daily basis have increases considerably in terms of file size. A typical PPT can be easily of 15-20MB, a small exe/msi file is of 50-70MB thus in order to be able to detect these large files it is important that the sandbox should be able to scan files upto of 200MB	Bidder to comply with RFP terms and conditions.
1265	N/A	N/A	VIII Anti APT	Additional points to be included	The proposed sandbox solution should be able to track for network I/O to raw disks and any modification to MBR made by the samples during the dynamic analysis. Justification: MBR is the most critical part of the windows system as it stores the information on where the OS is there on disk and to be loaded. Modifications to this can corrupt the entire system thus it is very important for sandbox to check for this.	Bidder to comply with RFP terms and conditions.
1266	N/A	N/A	VIII Anti APT	Additional points to be included	The proposed sandbox solution should allow user to manually interact with the sample within the analysis environment while the analysis is taking place. Justification: Manualy interaction by admin on malware sample in analysis environment facilitate them with simulating real user scernarios and help in inverstigating the malware with various behvaioural indicators and develop the response strategries without infecting the end user machine	Bidder to comply with RFP terms and conditions.
1267	N/A	N/A	VIII Anti APT	Additional points to be included	A video recording of the malware analysis should be made and be able to have playback and download capability for further analysis. curity expertise to interpret reports. Justification: Video Playback of sample execution helps the admins to better visualise the analysis and triggers leading upto the file being flagged.and gaining valuable insight into the behaiour of file. It also serves as a great evidence to be submiited to other teams for their consumption for reporting purposes	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1268	N/A	N/A	VIII Anti APT	Additional points to be included	The sandbox solution must have a user interaction tool that provides a safe environment to dissect malware without the risk of infecting your network. Built into the appliance, analysts are able to interact with the sample while it is being analyzed including opening applications, clicking through dialogue boxes, and even reboot the virtual machine if needed. Justification: Allowing admin's/incident responders to have the capability to interact with the malware sample execution helps them to understand the every samples behvaiour and its impact on the system	Bidder to comply with RFP terms and conditions.
1269	N/A	N/A	VIII Anti APT	Additional points to be included	The sandbox must have capability to Analyze more than 800+ highly accurate and actionable advanced behavioral indicators. Justification: A detonation engine works on by detecting a behvaiour and matching it against the baseline behvaiour data that the sytem has in order to determine whether it is clean or bad. Thus a sandbox which is a behvaioural detection engine working on by detonating files in controlled environment. thus the higher number of behvaioural indicators ensures the higher catch rate and efficay of sandbox	Bidder to comply with RFP terms and conditions.
1270	N/A	N/A	VIII Anti APT	Additional points to be included	AntiAPT solution must have static and dynamic analysis capabilities. Dynamic Analysis solution should have a file processing capability of 50K files per day in case solution scans all the files or 5K file per day if solution scans only unknown/zero-day files.	Bidder to comply with RFP terms and conditions.
1271	135		DLP	General	Our understanding is that Data Classification is not in the scope of this RFP, pls. clarify	Bidder to comply with RFP terms and conditions.
1272	135		DLP	General	We would like to understand if Bank would like to have training and certification on DLP directly from OEM at Administration or System Engineer level. Bank may include specific requirements on the same like number of trainees and if training is required every year as Bank team changes every few years.	Bidder to comply with RFP terms and conditions.
1273	135		DLP	General	We would like to understand if Bank wants to have Annual Health Check and review directly from OEM professional Services team for the DLP Solution.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1274	189	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	7	The solution shall sized to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud	Request you to please amend the clause as "to change data retention period for incidents and alerts on the cloud to 90 days" Beyond this, the solution should be capable of sending events to a SIEM to ensure compliance with Bank regulations.	Bidder to comply with RFP terms and conditions.
1275	190	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Given that EDR is deployed on endpoints, the Tap mode is not applicable. Request you to please amend the clause as "to either remove this clause from the requirement or provide further clarification on its intended purpose"	Clause stands deleted. Bidder to refer Corrigendum-2.
1276	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	27	The solution should support incident response automation.	Incident Response will be triggered by an admin, and the solution will ensure that these triggers are executed without manual intervention. Kindly confirm if our understanding on this point is the same.	Bidder to comply with RFP terms and conditions.
1277	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	34	The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features	Vulnerability assessment is a core component of a vulnerability management solution. Therefore, we request the Bank to remove this clause.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1278	193	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Request you to please amend the clause to modify below points:- Capability of running a coordinated command (such as CMD interface) as capability to execute command or script Request Bank to modify as below function should be available or there should be feasibility to execute command from EDR console to manage Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Bidder to refer Corrigendum-1.
1279	198	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Request you to please amend the clause to change supported platform as below:- Windows 10 and above Windows server 2008 and above Kindly request Bank to remove below operating system support IBM AIX, Solaris	Bidder to refer Corrigendum-1.
1280	200	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	Request you to please amend the clause as " proposed ssolution to include static scanning up to 1GB and dynamic scanning up to 100MB."	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1281	215	Section 8 , Anti - APT, Annexure 9	2	Each of the bidders proposed solution would be evaluated thoroughly against functional as well as technical requirements. The proposed solution should be from a single OEM (for all components) to ensure the integrated platform requirements and capabilities are utilized and desired security objectives are achieved. The solution expected to import multiple TLS/ SSL certificates.	Request you to please amend the clause as "the proposed SSL Offloader can be from a different OEM than the primary solution provider as long as the solution/requirement meets the functional purpose"	Bidder to comply with RFP terms and conditions.
1282	216	Section 8 , Anti - APT, Annexure 9	13	Proposed appliance should have below hardware requirements: Network Traffic Analysis appliances should be supplied with minimum below port requirements with a separate dedicated management and IPMI port with 10/100/1000GBASE-T 4 X 1G/10G RJ45 4 X 1G/10G SFP+ (With Bypass) 8 X 10G SFP+	We request the Bank to let us know if below ports will be ok 2 X 40G QSFP+ 4 X 10G SFP+ 2 X 1G/10G SFP+ 4 X 1G/10G RJ45 bypass 2 X 100G QSFP28	Bidder to refer Corrigendum-2.
1283	219	Section 8 , Anti - APT, Annexure 9	35	The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, TAXII and OpenIOC feeds with automated Investigation and analysis search function.	Request you to please amend the clause as mentioned below:- The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence using STIX or TAXII or OpenIOC feeds with automated Investigation and analysis search function.	Bidder to refer Corrigendum-2.
1284	220	Section 8 , Anti - APT, Annexure 9	40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Request you to please amend the clause as the supported operating system as Windows,Linux and MAC	Bidder to refer Corrigendum-2.
1285	220	Section 8 , Anti - APT, Annexure 9	42	The solution should have SSL Decryption capabilities available out of the box	Request you to please amend the clause as below If SSL decryption is not feasible on the appliance then bidder should provide SSL decryption	If SSL decryption is not feasible on same appliance. The Bidder has to provide separate SSL decryptor.
1286	220	Section 8 , Anti - APT, Annexure 9	47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Given the variability in vendor practices, Request you to please amend the clause as "the proposed solution to either provide the operating system with all necessary licenses or allow the customer to upload their own licenses"	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1287	221	Section 8 , Anti - APT, Annexure 9	53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	Request you to please amend the clause as per below: The solution should support integration with proposed EDR/XDR platform	Bidder to comply with RFP terms and conditions.
1288	184	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, I. Security Incident and Event Management (SIEM), Log Storage	30. SAN storage Systems should support Native Storage virtualization of 3rd party storage system for centralized management and SAN Storage systems should support 100 % Data Availability guarantee. 31. SAN Storages must Scale-Up & Scale out with support for intermix of different type of drives (NVMe SSDs, NL SAS, SAS). Data tiering (Auto sub-LUN tiering) should be supported. 32. No single point of failure, The SAN system should deliver Industry leading Performance of up to 2M+ IOPS 33. End to End SAN Infra monitoring from a single management suite. 34. SAN system should support native remote replication both synch & Asynch replication for backup/DR purposes. The storage system should support Zero RTO natively. 35. SAN system should allow intelligent compression & de-duplication per workload and can be disabled on non-compressible workloads. 36. The NAS system should be symmetric active-active architecture and should have unified capability i.e., should	SAN/NAS for the storage of data in a SIEM can negatively affect performance due to increased latency, reduced data retrieval speeds, and potential bottlenecks in data processing. This can lead to slower query response times, delayed detection of security incidents, and overall reduced efficiency in monitoring and threat management operations. Kindly clarify whether the storage can also be proposed as an alternative storage within the server.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1289	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	41. The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Kestral is a universal threat hunting language that is proprietary in nature. This mode of specific language eliminates other qualified OEMs who are achieving the requested functionalities via other methods. To keep the participation not limiting to a certain OEM. We request to either remove the clause or amend the clause as : " The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel or via any other methods. Attaching the link for reference: https://www.ibm.com/docs/en/cloud-paks/cp-security/1.10?topic=explorer-threat-hunt	Clause stands deleted. Bidder to refer Corrigendum-1.
1290	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	51. The solution must include a in-product script editor with run buttons to facilitates debug and perform tests on scripts.	The requested functionalities can be achieved through other methods such as GUI driven test labs which will ease the analysts to debug easily without depending on any custom scripts. Hence we request not to limit achieving this requested functionality only via scripts and accept the Test Lab debugging and automation workflows.	Bidder to comply with RFP terms and conditions.
1291	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	50. The solution must include a in-product script editor with autocomplete and syntax highlighting, to support automation of incident response workflow.	The requested functionalities can be achieved through other methods such as through system UI, with a playbook editor canvas. Hence we request not to limit achieving this requested functionality only via scripts and accept the GUI driven automation workflows.	Bidder to comply with RFP terms and conditions.
1292	197	Annexure-9, Functional and Technical Requirements	1. Technical Specifications of each SOC Solutions, II. Security Orchestration and Automation (SOAR), Analysis and Incident Management	127. The platform should allow user to Assign thresholds to Big Number, Time Series, Tabular, and Geographical charts	This technical requirements is of proprietary nature to an OEM, Hence we request you to kindly remove the same. Reference : https://exchange.xforce.ibmcloud.com/hub/extension/f4a537a424977e155105d8aa9f5283c3	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

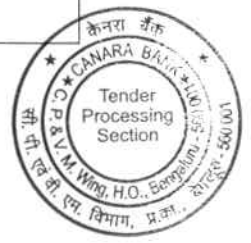
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1293	232	Annexure-10 Technical Evaluation Criteria		The Bidder must have successfully implemented or managed on-prem Security operation center (*SOC) during last 5 years in organizations like Government/ BFSI/ PSU/ RBI /NPCI/ NSE/ BSE/ SEBI. The SOC must be currently operational and running (a) 3 and above clients - Score of 10 Marks (b) more than 1 and below 3 clients - Score of 5 Marks Note: *BFSI must be an organization having minimum of 1000 branches or 1 Lakh crore Business in India. *SOC - Bidder must have provided any of the two solutions (SOAR, UEBA, EDR/XDR, PIM/PAM, NBA, DLP, Anti-DDOS, Anti-APT,WAF,DAM) along with SIEM.	The Bidder must have successfully implemented or managedany security solution during last 5 years in organizations like Government/ BFSI/ PSU/ RBI /NPCI/ NSE/ BSE/ SEBI/large corporates The support services currently operational and running (a) 3 and above clients - Score of 10 Marks (b) more than 1 and below 3 clients - Score of 5 Marks Note: *BFSI must be an organization having minimum of 1000 branches or 1 Lakh crore Business in India. *SOC - Bidder must have provided any of the two solutions (SOAR, UEBA, EDR/XDR, PIM/PAM, NBA, DLP, Anti-DDOS, Anti-APT,WAF,DAM,HSM) along with SIEM.	Bidder to comply with RFP terms and conditions.
1294	232			The Bidder's Annual turnover in the last 3 years • >500 crore <=1000 crore - Score of 2 • >1000 crore <=1500 crore - Score of 5 • >1500 crore - Score of 10	The Bidder's Annual turnover in the last 3 years • >100crore <=200 crore - Score of 2 • >201 crore <=300 crore - Score of 5 • >350 crore - Score of 10	Clause stands deleted. Bidder to refer Corrigendum-2.
1295	233			The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience • For 5 or more clients - 5 marks • For 2 clients - 3 marks	The Bidder / OEM must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience • For 5 or more clients - 5 marks • For 2 clients - 3 marks	Bidder to refer Corrigendum-2.
1296	234			The Bidder should have the experience in implementing or managing SIEM Solution in Organization(s) in India 1 lakh EPS with 2 clients - Score of 5 1 lakh EPS with 1 client - Score of 2	The Bidder /OEMshould have the experience in implementing or managing SIEM Solution in Organization(s) in India 1 lakh EPS with 2 clients - Score of 5 1 lakh EPS with 1 client - Score of 2	Bidder to comply with RFP terms and conditions.
1297	234			The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India 500 privileged users with more than 5 clients - Score of 5 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	The Bidder /OEMshould have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India 500 privileged users with more than 5 clients - Score of 5 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1298	234			The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 5 Note: For CEH maximum 5 number of certified resources will be considered	The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH/portal Certifications (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 5 Note: For CEH maximum 5 number of certified resources will be considered	Bidder to refer Corrigendum-2.
1299	235			The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions SIEM - 10 certified OEM resource PIM - 5 certified OEM resource SOAR - 5 certified OEM resource EDR - 5 certified OEM resource Note: All respective certified resources must be on direct payroll of Bidder.	The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions SIEM - 2 certified OEM resource PIM - 2 certified OEM resource SOAR - 2 certified OEM resource EDR - 5 certified OEM resource Note: All respective certified resources must be on direct payroll of Bidder.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1300	175	Annexure-9/ Functional and Technical Requirements	SIEM-Packet capture/137	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should be a native feature of SIEM for sharing of network data (Packet + Meta data) in real time .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	The requirement stated in the RFP under SIEM is asking for PCAP Solution, which is NOT a functionality of SIEM. SIEM and PCAP are two different solutions, combining these two gives undue advantage to particular OEM and does not provide a fair and level playing field to other OEM's. Request you to kindly refer to the RFPs for PCAP requirement of other Banks such as SBI, UBI, IDBI,PSB, IDFC etc. hence request you to keep the requirement for PCAP and SIEM separate. As per clause no. 3.Procurement through Local Suppliers (Make in India), page no. 67 RFP clearly states support for MAKE IN INDIA but it restricts participation from Indian OEMs by way of merging specifications of totally different solutions and thereby giving undue advantage to few OEM's. Hence kindly rephrase it to " The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should not be a native feature of SIEM or any other soltions .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web	Bidder to refer Corrigendum-2
1301	124	Scope of Work for Proposed Solutions	II. PCAP	Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload &header as well (like TLS 1.3) etc.	Since PCAP is a passive technology functioning out of band, decrypting TLS 1.3 communications requires inline/man-in-the middle deployment. Could you please confirm whether the bank will supply plaintext traffic to the PCAP solution from the existing SSL decryptor. Or please change the clause as " Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload &header as well (upto TLS 1.2) etc."	Bidder to refer Corrigendum-2



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1302	242	Table 1) Cost of Hardware, Software other items for implementation of NGSOC and Solutions	Solution	1. SIEM+PCAP	SIEM and PCAP are disparate tools used in SOC. These are not linked and both are available from multiple OEM's having specific expertise in these tools. Having a single tool for both the functionalities would restrict best of the breed players of SIEM and PCAP participate in this RFP. It will also reduce the options bank can explore for both the solution. Also as per clause no. 3.Procurement through Local Suppliers (Make in India), page no. 67 RFP clearly states support for MAKE IN INDIA but it restricts participation from Indian OEMs by way of merging specifications of totally different solutions and thereby giving undue advantage to few OEM's. Kindly request you to have dedicated PCAP solution as a separate technology rather than having as feature of SIEM.	Bidder to comply with RFP terms and conditions.
1303	249	Table 4) NGSOC Solutions One Time Implementation Charges	SOC solution	1. SIEM+PCAP	SIEM and PCAP are disparate tools used in SOC. These are not linked and both are available from multiple OEM's having specific expertise in these tools. Having a single tool for both the functionalities would restrict best of the breed players of SIEM and PCAP participate in this RFP. It will also reduce the options bank can explore for both the solution. Also as per clause no. 3.Procurement through Local Suppliers (Make in India), page no. 67 RFP clearly states support for MAKE IN INDIA but it restricts participation from Indian OEMs by way of merging specifications of totally different solutions and thereby giving undue advantage to few OEM's. Kindly request you to have dedicated PCAP solution as a separate technology rather than having as feature of SIEM.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1304	250	Table 5) AMC/ATS Cost for items mentioned in Table- 1 and Table- 2	Solution	1. SIEM+PCAP	SIEM and PCAP are disparate tools used in SOC. These are not linked and both are available from multiple OEM's having specific expertise in these tools. Having a single tool for both the functionalities would restrict best of the breed players of SIEM and PCAP participate in this RFP. It will also reduce the options bank can explore for both the solution. Also as per clause no. 3.Procurement through Local Suppliers (Make in India), page no. 67 RFP clearly states support for MAKE IN INDIA but it restricts participation from Indian OEMs by way of merging specifications of totally different solutions and thereby giving undue advantage to few OEM's. Kindly request you to have dedicated PCAP solution as a separate technology rather than having as feature of SIEM.	Bidder to comply with RFP terms and conditions.
1305	175	Annexure-9/ Functional and Technical Requirements	SIEM-Packet capture	Additional point	The solution must include a built-in, fully functional capability similar to Wireshark, allowing users to view and analyze event sequences using PCAP files without relying on any third-party tools.	Bidder to comply with RFP terms and conditions.
1306	189	EDR	2	The platform shall offer for 99.90% uptime	Given EDR management console is out of band and most modern EDR players such as CrowdStrike and SentinelOne are heavily reliant on public cloud infrastructure to provide SaaS based SLA's for their offerings, hence requesting the bank to read the point as "The platform shall offer 99.5% uptime".	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1307	189	EDR	7	The solution shall sized to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud	As per CERT-IN circular PFRDA/2022/14/I&CS02 dated 15th June 2022, page no: 3, sub-section: 4 "All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In." Thus, the logs for an EDR technology are the raw telemetry of the endpoint which are very critical specifically when performing forensics investigation. However the current bank request violates the CERT-IN guideline by only requesting 30 days of telemetry. We would thus recommend the bank to modify the point as below: "The solution must store all telemetry data (including applicable forensic data) for 180 days."	Bidder to comply with RFP terms and conditions.
1308	191	EDR	23	The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files, data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).	Data Exfiltration use cases are handled by the DLP solutions installed on the endpoints/systems and bank is exploring DLP solution as part of this RFP. Requesting bank to remove data exfiltration capability from EDR requirements. The point should be read as "The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files."	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1309	195	EDR	71	Should have outbreak prevention feature that allows to configure port blocking, block shared folder, and deny writes to files and folders manually.	This is vendor specific and restricts large and prominent EDR players to participate. This exact point is outlined in https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/outbreak_prevention_policy.html.and explains the technique/approach used to handle outbreak prevention. The point should be read as "Should have outbreak prevention capabilities against ransomware, cryptominers, infostealers, trojans and similar malware samples."	Bidder to refer Corrigendum-1.
1310	197	EDR	94	The solution shall have feature to route all the agent traffic via a proxy servers or broker. The proxy server/ broker shall be provided by the OEM.	A proxy/jump server is available with network security vendors such as Palo Alto and Trend Micro. Given the fact that bank has an existing proxy, requesting OEM of EDR to procure a proxy/jump server puts Palo Alto and Trend Micro into unfair advantage against best in class pure play EDR / XDR players such as CrowdStrike and SentinelOne. Thus request the point to be read as "The solution shall have feature to route all the agent traffic cia a proxy server or broker."	Bidder to comply with RFP terms and conditions.
1311	198	EDR	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Most of the EDR vendors do not support IBM AIX and Solaris operating systems. The point should be read as "The solution should protect all servers, endpoints, physical, virtual, having Windows/Non Windows systems (Windows 10 and above, Windows Server 2000 and above, RHEL, Oracle Linux, Ubuntu, CentOS, Suse Linux etc.). The solution should protect all latest and upcoming/upgraded OS in Bank's IT ecosystem during the contract period.	Bidder to refer Corrigendum-1.
1312	190	EDR	16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Considering SIEM will collect the alert/threat data from EDR as well as UEBA, requesting bank to read the point as "The proposed EDR should integrate with SIEMv solution for better co-relation among different security controls."	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1313	192	EDR	39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Every OEM has their own nomenclature to define threat categories. Requesting bank to generalise the threat categories to the below general definition: 1) Ransomware 2) Cryptominer 3) Trojans 4) PUA 5) Infostealer 6) Rootkit 7) Spyware 8) Virus 9) Hacktools 10) Exploits 11) Backdoor 12) Adware 13) Malware 14) Malicious Macro	Bidder to comply with RFP terms and conditions.
1314	200	EDR	88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Once a rogue device is discovered by the EDR platform it is recommended for an administrator to validate the asset and then deploy the OS specific agent (windows,macOS & linux). Requesting the bank to read the point as "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them"	Bidder to refer Corrigendum-2
1315	203	EDR	121	The solution should support Endpoint Security Solution infrastructure i.e., management and administration console of Endpoint Security Solution on Virtual environment of Bank or alternatively vendor should provide scalable hardware/ infrastructure supplied for implementation of overall ESS Solution within the overall cost for the entire contract period.	Bank has requested for a SaaS solution and no management component of SaaS solution is required to be installed on-premises.	Clause stands deleted. Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1316	200	EDR	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	The average file size sent to sandbox for analysis is typically between 5MB and 30MB and these are mostly executable files like".exe", ".dll" or documents such as ".pdf", ".docx". For files of size 1GB the sandbox analysis takes much longer time and can be prone to timeouts leading to missed detections. The extended tme required to analyse large fles can delay incident response and could slow down decision-making process and remediation efforts and potentially miss sophisticated threats. Also having mandated a 1Gb File size Sandbox is specific to an individual OEM , restricting participation of Pure Play best in class EDR / XDR solutions and thus request the Bank below. The point should be read as " The proposed sandboxing component should have the capability to scan the file size upto 50MB".	Bidder to refer Corrigendum-1.
1317	189	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	7	The solution shall sized to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud	Request you to please amend the clause as "to change data retention period for incidents and alerts on the cloud to 90 days" Beyond this, the solution should be capable of sending events to a SIEM to ensure compliance with Bank regulations.	Bidder to comply with RFP terms and conditions.
1318	190	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Given that EDR is deployed on endpoints, the Tap mode is not applicable. Request you to please amend the clause as "to either remove this clause from the requirement or provide further clarification on its intended purpose"	Clause stands deleted. Bidder to refer Corrigendum-1.
1319	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	27	The solution should support incident response automation.	Incident Response will be triggered by an admin, and the solution will ensure that these triggers are executed without manual intervention. Kindly confirm if our understanding on this point is the same.	Bidder to comply with RFP terms and conditions.
1320	191	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	34	The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features	Vulnerability assessment is a core component of a vulnerability management solution. Therefore, we request the Bank to remove this clause.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1321	193	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Request you to please amend the clause to modify below points:- Capability of running a coordinated command (such as CMD interface) as capability to execute command or script Request Bank to modify as below function should be available or there should be feasibility to execute command from EDR console to manage Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Bidder to refer Corrigendum-2.
1322	198	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Request you to please amend the clause to change supported platform as below:- Windows 10 and above Windows server 2008 and above Kindly request Bank to remove below operating system support IBM AIX, Solaris	Bidder to refer Corrigendum-2.
1323	200	Section 4 , Endpoint Detection and Response (EDR), Annexure 9	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	Request you to please amend the clause as " proposed ssolution to include static scanning up to 1GB and dynamic scanning up to 100MB."	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1324	215	Section 8 , Anti - APT, Annexure 9	2	Each of the bidders proposed solution would be evaluated thoroughly against functional as well as technical requirements. The proposed solution should be from a single OEM (for all components) to ensure the integrated platform requirements and capabilities are utilized and desired security objectives are achieved. The solution expected to import multiple TLS/ SSL certificates.	Request you to please amend the clause as "the proposed SSL Offloader can be from a different OEM than the primary solution provider as long as the solution/requirement meets the functional purpose"	Bidder to comply with RFP terms and conditions.
1325	216	Section 8 , Anti - APT, Annexure 9	13	Proposed appliance should have below hardware requirements: Network Traffic Analysis appliances should be supplied with minimum below port requirements with a separate dedicated management and IPMI port with 10/100/1000GBASE-T 4 X 1G/10G RJ45 4 X 1G/10G SFP+ (With Bypass) 8 X 10G SFP+	We request the Bank to let us know if below ports will be ok 2 X 40G QSFP+ 4 X 10G SFP+ 2 X 1G/10G SFP+ 4 X 1G/10G RJ45 bypass 2 X 100G QSFP28	Bidder to refer Corrigendum-1.
1326	219	Section 8 , Anti - APT, Annexure 9	35	The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX, TAXII and OpenIOC feeds with automated investigation and analysis search function.	Request you to please amend the clause as mentioned below:- The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence using STIX or TAXII or OpenIOC feeds with automated investigation and analysis search function.	Bidder to refer Corrigendum-1.
1327	220	Section 8 , Anti - APT, Annexure 9	40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Request you to please amend the clause as the supported operating system as Windows,Linux and MAC	Bidder to refer Corrigendum-1.
1328	220	Section 8 , Anti - APT, Annexure 9	42	The solution should have SSL Decryption capabilities available out of the box	Request you to please amend the clause as below If SSL decryption is not feasible on the appliance then bidder should provide SSL decryption	If SSL decryption is not feasible on same appliance. The Bidder has to provide separate SSL decryptor.
1329	220	Section 8 , Anti - APT, Annexure 9	47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Given the variability in vendor practices, Request you to please amend the clause as "the proposed solution to either provide the operating system with all necessary licenses or allow the customer to upload their own licenses"	Clause stands deleted. Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1330	221	Section 8 , Anti - APT, Annexure 9	53	The solution should support integration with proposed EDR/XDR platform to apply effective expert analytics and global threat intelligence using data collected across multiple vectors - endpoints, servers, networks, and email to meet future requirement.	Request you to please amend the clause as per below: The solution should support integration with proposed EDR/XDR platform	Bidder to comply with RFP terms and conditions.
1331	189	EDR	2	The platform shall offer for 99.90% uptime	Given EDR management console is out of band and most modern EDR players such as CrowdStrike and SentinelOne are heavily reliant on public cloud infrastructure to provide SaaS based SLA's for their offerings, hence requesting the bank to read the point as "The platform shall offer 99.5% uptime".	Bidder to comply with RFP terms and conditions.
1332	191	EDR	23	The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files, data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).	Data Exfiltration use cases are handled by the DLP solutions installed on the endpoints/systems and bank is exploring DLP solution as part of this RFP. Requesting bank to remove data exfiltration capability from EDR requirements.	Bidder to refer Corrigendum-1.
1333					The point should be read as "The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files."	Bidder to refer Corrigendum-1.
1334	195	EDR	71	Should have outbreak prevention feature that allows to configure port blocking, block shared folder, and deny writes to files and folders manually.	This is vendor specific and restricts large and prominent EDR players to participate. This exact point is outlined in https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/outbreak_prevention_policy.html.and explains the technique/approach used to handle outbreak prevention.	Bidder to refer Corrigendum-1.
1335					The point should be read as "Should have outbreak prevention capabilities against ransomware, cryptominers, infostealers, trojans and similar malware samples."	Bidder to refer Corrigendum-1.
1336	197	EDR	94	The solution shall have feature to route all the agent traffic via a proxy servers or broker. The proxy server/ broker shall be provided by the OEM.	A proxy/jump server is available with network security vendors such as Palo Alto and Trend Micro. Given the fact that bank has an existing proxy, requesting OEM of EDR to procure a proxy/jump server puts Palo Alto and Trend Micro into unfair advantage against best in class pure play EDR / XDR players such as CrowdStrike and SentinelOne. Thus request the point to be read as "The solution shall have feature to route all the agent traffic via a proxy server or broker."	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1337	198	EDR	115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Most of the EDR vendors do not support IBM AIX and Solaris operating systems. The point should be read as "The solution should protect all servers, endpoints, physical, virtual, having Windows/Non Windows systems (Windows 10 and above, Windows Server 2000 and above, RHEL, Oracle Linux, Ubuntu, CentOS, Suse Linux etc.). The solution should protect all latest and upcoming/upgraded OS in Bank's IT ecosystem during the contract period.	Bidder to refer Corrigendum-2.
1338					The point should be read as "The solution should protect all servers, endpoints, physical, virtual, having Windows/Non Windows systems (Windows 10 and above, Windows Server 2000 and above, RHEL, Oracle Linux, Ubuntu, CentOS, Suse Linux etc.). The solution should protect all latest and upcoming/upgraded OS in Bank's IT ecosystem during the contract period.	Bidder to refer Corrigendum-2.
1339	190	EDR	16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Considering SIEM will collect the alert/threat data from EDR as well as UEBA, requesting bank to read the point as "The proposed EDR should integrate with SIEMv solution for better co-relation among different security controls."	Clause stands deleted. Bidder to refer Corrigendum-2.
1340	192	EDR	39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Every OEM has their own nomenclature to define threat categories. Requesting bank to generalise the threat categories to the below general definition: 1) Ransomware 2) Cryptominer 3) Trojans 4) PUA 5) Infostealer 6) Rootkit 7) Spyware 8) Virus 9) Hacktools 10) Exploits 11) Backdoor 12) Adware 13) Malware 14) Malicious Macro	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1341	197	EDR	88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Once a rogue device is discovered by the EDR platform it is recommended for an administrator to validate the asset and then deploy the OS specific agent (windows,macOS & linux). Requesting the bank to read the point as "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them"	Bidder to refer Corrigendum-1.
1342	198	EDR	121	The solution should support Endpoint Security Solution infrastructure i.e., management and administration console of Endpoint Security Solution on Virtual environment of Bank or alternatively vendor should provide scalable hardware/ infrastructure supplied for implementation of overall ESS Solution within the overall cost for the entire contract period.	Bank has requested for a SaaS solution and no management component of SaaS solution is required to be installed on-premises.	Clause stands deleted. Bidder to refer Corrigendum-1.
1343	200	EDR	135	The proposed Sandboxing component should have the capability to scan the file size upto 1 GB.	The average file size sent to sandbox for analysis is typically between 5MB and 30MB and these are mostly executable files like".exe", ".dll" or documents such as ".pdf", ".docx". For files of size 1GB the sandbox analysis takes much longer time and can be prone to timeouts leading to missed detections. The extended tme required to analyse large fles can delay incident response and could slow down decision-making process and remediation efforts and potentially miss sophisticated threats. Also having mandated a 1Gb File size Sandbox is specific to an individual OEM , restricting participation of Pure Play best in class EDR / XDR solutions and thus request the Bank below.	Bidder to refer Corrigendum-1.
1344					The point should be read as " The proposed sandboxing component should have the capability to scan the file size upto 50MB".	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1345	174	PCAP / Technical Specification		The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	The current technical specifications appear to reference the ingestion of logs, which is not directly relevant to packet capture (PCAP) solutions. For PCAP systems, only packet data and metadata related to ingested packets are applicable. We respectfully request that the specification be revised as follows to better reflect the requirements of a PCAP system: "The proposed Packet capture solution shall have capabilities to integrate with the proposed SIEM solution in both DC and DR. The OEM shall have the capacity to capture traffic at 10 Gbps and retain packet-like data and associated metadata for 7 days. Adequate storage shall be provisioned accordingly. The PCAP solution should also support both automated and manual mechanisms for selectively discarding, masking, or filtering packets based on their security relevance (e.g., customer PII, SPDI, or other classified information as per the Bank or Regulatory guidelines), to optimize storage.	Bidder to refer Corrigendum-1.
1346	174	PCAP / Technical Specification		The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/ outflow of data in DC. Proposed solution should be a dedicated hardware appliance with minimum 4 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 2*1/10G management port.	We propose the use of a Network Packet Broker to ingest traffic from multiple vantage points with various port configurations. To better reflect this approach, we respectfully request revising the clause as follows: "The proposed packet capture solution should ensure lossless packet and payload capture with network inflow/outflow of data in the DC. The proposed solution should be a dedicated hardware with 4 X 10 Gig SFP+ and 2 X 1/10G management ports. For environments requiring traffic capture from more than four vantage points, a dedicated Network Packet Broker should be proposed." This revision allows for more flexibility in network design and ensures effective capture across multiple vantage points without compromising performance or expandability.	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1347	174	PCAP / Technical Specification		The proposed packet capture solution should be a dedicated Hardware appliance, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage and in case of Storage expansion solution should be compatible with the SAN storage to extract/forward to data archives using HBA/FC/SFP+ dedicated ports	Kindly consider the suggested points to secure enough storage on the proposed hardware: "The proposed packet capture solution should be a dedicated Hardware, all Core Appliances for different layers should have hardened OS to provide optimal performance. All disks of the dedicated hardware and the storage should utilize Self-Encrypting Drives (SED). Should have required OEM approved storage to scale upto 20Gbps throughput without the need to integrate with other storage solutions".	Bidder to refer Corrigendum-1.
1348	175	PCAP / Technical Specification	137	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and should be a native feature of SIEM for sharing of network data (Packet + Meta data) in real time .Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	Given the critical need to protect customer privacy, particularly with respect to Personally Identifiable Information (PII), Sensitive Personal Data or Information (SPDI), and other classified information, we recommend limiting payload data capture to only suspicious and malicious traffic. This approach ensures that sensitive data is not unnecessarily captured and stored, aligning with privacy regulations and best practices. We respectfully request revising the clause as follows: "The proposed packet capture solution should be able to perform real-time monitoring and network traffic analysis to identify threats. The solution should feature Deep Packet Inspection (DPI) to provide visibility into all layers of the OSI stack (L2 to L7), including application payload data, but only for suspicious and malicious traffic. The solution should create indexes for payload objects as required and not just rely on header information." Additionally, the solution should provide network traffic insights by: a. Classifying protocols and applications b. Performing deep-packet inspection c. Supporting cross-correlation for analysis and aggregation d. Reconstructing sessions and analyzing artifacts e. Previewing artifacts and malicious attachments	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

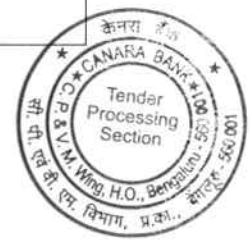
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1349	175	PCAP / Technical Specification	138	Solution should provide meaningful artefacts like email, FTP data files, VoIP conversations including PHP, JavaScript and .Net files from Deep packet Inspection. Post reconstruction, solution should be able to do object extractions from sessions like pcaps, zip files, office documents, media, embedded malicious attachments etc.	In consideration of maintaining customer privacy and safeguarding Personally Identifiable Information (PII), Sensitive Personal Data Information (SPDI), and any classified information, we propose a modification to the specifications regarding payload data capture. We request that the requirement for comprehensive payload data capture for all traffic be adjusted to only include the storage of payloads associated with suspicious or malicious traffic for further analysis. We recommend rephrasing the specification as follows: "The solution should provide meaningful artifacts such as FTP data files, JavaScript, and .Net files derived from Deep Packet Inspection. After reconstruction, the solution should be capable of performing object extractions from sessions, including PCAPs, zip files, office documents, media files, and embedded malicious attachments." This amendment will help ensure compliance with privacy regulations while still delivering the necessary analytical capabilities.	Bidder to comply as per GeM Bid/ RFP terms and conditions.
1350	175	PCAP / Technical Specification	139	The solution should have the capability to extract data/ files from the captured network packets	We propose the following modification to enhance the specification: "The solution should possess the capability to extract data / malicious files from the captured network packets. Additionally, the solution should include the functionality for comprehensive host investigations, as well as session and packet analysis on the captured packets and any generated alerts." This revision ensures that the solution not only extracts relevant data but also provides crucial investigative capabilities that are essential for effective threat analysis.	Bidder to refer Corrigendum-2.
1351	175	PCAP / Technical Specification	140	The solution should have the functionality to reconstruct and replay the network packets which will help to identify the entire transaction	We recommend the following modification to the specification: "The solution should have the functionality to reconstruct or complete packet analysis or replay the network packets which will help to identify the entire transaction." This adjustment underscores the importance of all three capabilities for a thorough understanding of network interactions and transaction integrity.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1352	124	PCAP	II	Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload &header as well (like TLS 1.3) etc.	We recommend the following modification to the specification: "Bidder to ensure selected PCAP tool to not only complement all other NGSOC solutions and security tools to help bank improve the time to detect, contain and respond to modern security threats but also to ensure it maintains its relevance when majority of traffic is encrypted including payload & header as well".	Bidder to refer Corrigendum-1.
1353	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	We strongly recommend that the bank insists on a dedicated solution that fully delivers all PCAP specifications and use cases outlined above. It is crucial to note that PCAP is inherently resource-intensive, requiring significant processing power, storage, and management capabilities. By integrating PCAP functionality as a subset of a Security Information and Event Management (SIEM) system or any other solution, the bank risks diluting the effectiveness and performance of both systems. Advantages of a Dedicated PCAP Solution: 1. Optimal Performance: A dedicated PCAP solution ensures that the capture, storage, and analysis of packet data occur without interference from other applications, leading to more reliable performance. 2. Comprehensive Coverage: Focusing exclusively on PCAP capabilities allows for a more thorough and targeted approach to data capture and incident investigation, enhancing security monitoring. 3. Scalability: Separating the PCAP solution facilitates better scalability, enabling the bank to adapt to growing data needs without compromising the functionality of a combined system. 4. Simplified Management: A dedicated solution streamlines management and maintenance, reducing complexity and	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1354	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	The PCAP solution must be capable of capturing and recording all network packets in full (both header and payload). Additionally, the solution should provide the flexibility to selectively save packet data based on specific applications, protocols, time durations, or a combination of these criteria. This customization is essential for efficiently capturing and analyzing data related to specific events or incidents within the Canara Bank network. For each application traffic flow, the solution should support the following capture options: - Full Packet Capture: Capture the entire packet, including both header and payload information. - Packet Truncation: Capture only a specified portion of the packet, reducing storage requirements while preserving essential data. - Packet Exclusion: Exclude specific packets based on defined criteria, such as application, protocol, or source/destination addresses. - Header-Only Capture: Capture only the packet headers, providing basic information without the full payload.	Bidder to comply with RFP terms and conditions.
1355		PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	The PCAP solution should be capable of capturing network traffic and flexibility to use tools to read / extract pcap files on the device itself rather than downloading it to local machine. This will ensure that the pcap file irrespective of its size can be opened directly on the device which otherwise requires the file to be downloaded and opened using tools. If the file size is large than 1GB, then the local machine / workstation struggles to open the file. Thus it is essential for the pcap to be opened on solution itself without having to download it for quick forensic investigations, security analysis, and integration with other network-based security tools. The solution should support manual export of captured packets or the ability to forward them to external security systems for further analysis.	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1356	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	Given the criticality of real-time threat detection and the need for deep packet analysis, we suggest bank to consider the following requirement: - Zero-Day Threat Detection: The solution must be capable of identifying and mitigating zero-day threats as they emerge, ensuring proactive protection against emerging cyberattacks. - Retrospective Analysis: The system should allow for in-depth examination of captured packets, enabling the extraction of valuable metadata for subsequent analysis by an analytics engine. - Packet Storage and Analysis: The solution must have robust capabilities for storing, extracting, and analyzing packets, providing essential insights for incident response and threat intelligence.	Bidder to comply with RFP terms and conditions.
1357	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	Considering the criticality and agility for precise packet retrieval, we request bank to consider the following: - Efficient Indexing and Searching: The solution must have robust indexing and searching capabilities to allow for quick and easy location of specific packets based on a wide range of criteria. - Comprehensive Search Support: The system should support search functionality not only at the network layer (Layer 3 and Layer 4) but also at the application layer (Layer 7), including protocols such as HTTP, DNS, DB, LDAP, and others. - Search Criteria: The solution should support searching based on various criteria, such as time, links, IP addresses, port applications, protocols, and any other relevant attributes.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1358	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	Proposed PCAP tool should have capability to ingest packets from all type of application footprint, On Premise, Public Cloud or Private Cloud, so we request to add this clause. "The PCAP solution should support for capturing and storing data from (but not limited to) multiple network segments, VLANs, network locations, etc. The solution must be capable of supporting Public or Private Cloud infrastructure deployment using industry standard ecosystems. The solution should support deployment into Public Cloud platforms like Amazon Web Services (AWS), Microsoft Azure environments, Google Cloud, etc. The solution should be capable of capturing traffic on Private Cloud, Containers, Dockers & other virtual Infrastructure without the need of third party components. > Microsoft Hyper-V > VMware's ESX, NSX-V & NSX-T > OpenStack > Ubuntu/KVM"	Clause added. Bidder to refer Corrigendum-1.
1359	165	PCAP / Technical Specification		Additional Points to Consider for PCAP Solution	We recommend that the requirement for an advanced PCAP solution with real-time threat detection capabilities be included as part of this RFP. The solution should be able to detect and analyze the following incident categories (but not limited to): - Suspicious communication over non-standard ports - Data exfiltration attempts - Command and Control (C2) communications - The use of The Onion Router (TOR) - SSH communication with monitored countries - Privacy VPN usage detection - Reconnaissance activities - Detection of unknown Domain Generation Algorithm (DGA) attacks These capabilities are crucial for ensuring proactive security and effective threat mitigation. We believe incorporating this into the solution requirement will significantly enhance your ability to detect and respond to advanced threats in real-time.	Bidder to comply with RFP terms and conditions.
1360	110	Scope of Work for Bidder/ System Integrator (SI)	_	The bidder shall supply and install network ports with a minimum capacity of 10 Gigabit(10Gig).	Kindly confirm if Network switches with 10 G ports also needs to be proposed or only network interfaces on proposed servers/appliances are to be 10G	Bidder has to provide all the SOC solutions with capacity of 10 G port interfaces.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1361	119	Scope of Work for Proposed Solutions	_	Integration of log sources from various devices/servers/network devices/ security devices/applications/APIs with SIEM as part of the implementation	Kindly provide the list of log sources and their locations to be integrated so that appropriate sizing of log collection and storage can be done.	The details will be shared with selected Bidder
1362	121	Scope of Work for Proposed Solutions	_	Bidders should integrate the proposed SIEM with a ticketing tool for automated ticket generation.	Kindly provide us with details of existing Ticketing tool for integration or provide instructions for supply of a new ticketing tool for this project.	Existing ITSM Solution is Service Now.
1363	122	Scope of Work for Proposed Solutions	_	Log Archival The solution will be able to retain six months logs online and 1 year Archival (Six months + 12 months). The online storage shall be stored in SAN and NAS can be considered for Archival	Kindly confirm if we can utilize capacity on existing SAN and NAS for log retention or do we need to provide the required SAN and NAS system. Kindly confirm if the existing backup solution in the bank can be used for configuration backup etc. of the critical SIEM components	(a) No (b) Yes
1364	123	Scope of Work for Proposed Solutions	_	The bidder shall ensure all the current SIEM use cases are transferred to the Next Gen SIEM solutions.	Kindly confirm that only use cases/co-relation rules are to be migrated to new SIEM. Migration of logs stored on existing SIEM is not in scope.	Bidder to comply with RFP terms and conditions. (Migration of logs is not required)
1365	179	Security Orchestration and Automation (SOAR):	41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Kindly remove the clause. It seems to be OEM specific.	Clause stands deleted. Bidder to refer Corrigendum-2
1366	183	Security Orchestration and Automation (SOAR):	106	The solution should offer any auto-casing / auto-population based on the incident type or other relevant incident attributes	Can you pl share the use cases here for more clarity on the requirement.	The details will be shared with selected Bidder
1367	94	Annexure 9 - 5.Manpower Requirement	_	1(SOAR) General Shift	Are there a clear, Roles and Responsobilities defined for this role. Kindly clarify.	Yes
1368	146	Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:	m)	m) Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.	Can you define the maximum takedowns or average takedowns (per month for example) that will be required for the contract term	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1369	146	Brand Protection and Monitoring:	a)	(a) The bidder shall provide the Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti- Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown for the tenure of the Contract	Can you define the maximum takedowns or average takedowns (per month for example) that will be required for the contract term	The clause is self explantory (unlimited incidents and takedown for the tenure of the contract)
1370	73	Annexure-2	Pre-Qualification Criteria		Will references from Non-Banking Financial Companies (NBFCs) be accepted as BFSI reference?	Bidder to comply with RFP terms and conditions
1371	73	Annexure-3	Pre-Qualification Criteria		Can customer references from global customers, supported from India, be considered valid?	No
1372	74	Annexure-2 Pre-Qualification Criteria	15	The proposed SOAR solution should have been implemented satisfactorily in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids	Could you please consider implementing SOAR in other verticals (Private Sector)as well?	Bidder to comply with RFP terms and conditions.
1373	73	Annexure-4	Pre-Qualification Criteria	The bidder should have experience in implementing/ managing SOC with On-prem SIEM with at least 50,000 EPS with at least one entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI or other equivalent government entities in India during last 5 years.	1.Can the EPS for the SoC be sourced from a SoC supporting global customers, operated from India? 2.Requesting to reduce the EPS requirement from 50000 to 30000	Bidder to comply with RFP terms and conditions.
1374	58	SECTION G	22		Bidder cannot accept the proposed interparty indemnity obligations because they are overly broad and potentially expose bidder to extensive liabilities, including penalties or damages incurred by the Bank, which may be outside of bidder's control. Bidder can accept only indemnity obligations for third party claims and not interparty.	Bidder to comply with RFP terms and conditions
1375	59	SECTION G	23		Bidder cannot accept conflict of interest language as it is overly broad and subjective. The clause imposes an absolute warranty that bidder has no current or potential interests that might conflict with its obligations, without clear definitions or boundaries for what constitutes a 'conflict.' Additionally, the right of the Bank to unilaterally terminate the agreement based on its own 'reasonable judgment' introduces uncertainty and significant risk to bidder. We propose narrowing the scope of the conflict-of-interest clause to define specific types of conflicts and include a collaborative resolution process before any termination can occur.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

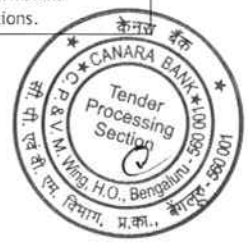
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1376	59		24.3		We notes that the referenced RBI guideline (RBI/2023-24/102DoS.CO.CSITEG/SEC.1/31.01.015/2023-24) may not be applicable to the present engagement. However, we assures compliance with all applicable laws and regulations relevant to this engagement and in line with its business operations.	Bidder to comply with RFP terms and conditions
1377	236	Annex-11		NDA	This is unilateral NDA and protects only Bank's confidential information. Bidder's confidential information must also be protected and hence cannot accept unilateral confidentiality obligations.	Bidder to comply with RFP terms and conditions
1378	263	Appendix-A		As per Annex-6 The list of Major clients to be shared with the Bank.	Bidder cannot share its list of customers due to confidentiality obligations and non-disclosure agreements in place with those clients. Sharing such information would violate their trust and potentially expose sensitive business relationships, which could harm bidder's reputation and legal standing	Bidder to comply with RFP terms and conditions
1379	35	General Terms and Conditions on GeM 4.0 (Version 1.18)	18		Bidder cannot accept the provision for unlimited liability as it imposes an excessive and unmanageable risk, particularly for events such as IP infringement. We propose to have the super cap for the exceptions mentioned under clause 18.	Bidder to comply with RFP terms and conditions
1380	35	General Terms and Conditions on GeM 4.0 (Version 1.18)	19		Bidder should also have the right to terminate the agreement to ensure balanced risk management and protection of its interests. Situations such as non-payment, material breach by the Bank, or changes in circumstances beyond bidder's control could make it unreasonable for bidder to continue the engagement. A mutual termination right ensures fairness and maintains a healthy, professional relationship between both parties.	Bidder to comply with RFP terms and conditions
1381	39	General Terms and Conditions on GeM 4.0 (Version 1.18)	23.2		As per this clause, there is an unlimited liability on bidder for the breach of contract, and third-party claims. Additionally, bidder must defend and indemnify the Buyer and third parties, including GeM, and cannot settle or admit liability without their written consent. This exposes bidder to significant financial risk, as it holds bidder fully accountable for an extensive range of potential liabilities without any mechanism to limit or manage the exposure. We propose it to be made limited to the claims brought by only third party and not otherwise.	Bidder to comply with RFP terms and conditions

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1382	6	Appendix-F	8		bidder cannot accept this language as it imposes an unreasonable pricing restriction that does not account for varying market conditions, volumes, or contractual terms that may differ between engagements. Prices may fluctuate based on factors such as order size, delivery timelines, or specific customer requirements. This clause could unfairly compel bidder to retroactively adjust prices, potentially resulting in financial loss.	Bidder to comply with RFP terms and conditions
1383	190	Annexure - 9/ Section IV/Sl No 16	Architecture & General Requirement	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Request to amend the existing clause as :- The solution should have advance advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats	Clause stands deleted. Bidder to refer Corrigendum-2
1384	191	Annexure - 9/ Section IV/Sl No 22	Threat Detection and Prevention	The solution should identify, and block credential theft attempts occurring in memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).	Request to amend the existing clause :-The solution should identify, and block credential theft attempts occurring in memory	Bidder to comply with RFP terms and conditions.
1385	191	Annexure - 9/ Section IV/Sl No 33	Threat Detection and Prevention	The solution should have Early Detection and Response capabilities with insightful investigative capabilities. Solution to have centralized visibility across the network by using an advanced EDR, strong SIEM integration, with open API integration features and threat intelligence sharing capabilities.	Request to amend the existing clause as:- The solution has Detection and Response capabilities with insightful investigative capabilities. Solution to have centralized visibility across the network by using an advanced EDR, SIEM integration and threat intelligence capabilities.	Bidder to comply with RFP terms and conditions.
1386	192	Annexure - 9/ Section IV/Sl No 38	Threat Detection and Prevention	The solution should have strong anti-evasion capabilities. It should also accurately identify evasion capabilities of malware such as evasion by detecting sandbox environment.	Request to amend the existing clause as:-The solution should have strong anti-evasion capabilities. It should also accurately identify evasion capabilities of malware by MITRE framework techniques.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1387	193	Annexure - 9/ Section IV/Sl No 43	Threat Detection and Prevention	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Request to amend the existing clause as:- The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as. • Running a live Query • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Bidder to refer Corrigendum-2.
1388	194	Annexure - 9/ Section IV/Sl No 54	Threat Detection and Prevention	The solution should be able to detect when system sleep functions are used by the malware to evade detection and accelerate the time to force the malware into execution	Request to amend the existing clause as:-The solution should be able to detect when system functions are used by the malware to evade detection and the malware into execution.	Bidder to comply with RFP terms and conditions.
1389	194	Annexure - 9/ Section IV/Sl No 57	Threat Detection and Prevention	The solution should have capability to analyze obfuscated and encrypted malware.	Request to amend the existing clause as:-The solution should have capability to analyze obfuscated and advanced Malwares attacks.	Bidder to comply with RFP terms and conditions.
1390	195	Annexure - 9/ Section IV/Sl No 71	Threat Detection and Prevention	Should have outbreak prevention feature that allows to configure port blocking, block shared folder, and deny writes to files and folders manually.	Request to amend the existing clause as:-Should have outbreak prevention feature that allows to send a notification to admin & also allows admin to manually configure port blocking & ip address in the firewall policy, run a scan on all systems, etc.	Bidder to refer Corrigendum-2.
1391	195	Annexure - 9/ Section IV/Sl No 76	Threat Detection and Prevention	The solution should show the assigned confidence/score in terms of Percentage/severity in the ML based detection logs.	Request to amend the existing clause as:-The solution should show the assigned confidence/score in terms of Percentage/severity level - high/low/medium	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1392	198	Annexure - 9/ Section IV/Sl No 115	Management Server, Agent and Reporting	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period	Request to amend the existing clause as:- The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, IBM, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period	Bidder to refer Corrigendum-1
1393	200	Annexure - 9/ Section IV/Sl No 137	Sandbox	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Request to amend the existing clause as:- The EDR should be able to overcome advanced malware evasion techniques.	Bidder to comply with RFP terms and conditions.
1394	200	Annexure - 9/ Section IV/Sl No 138	Sandbox	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Request to amend the existing clause as:- The proposed EDR solution should have sandboxing solution to support manual sample submission and IoC exchange to detect threats. Also, EDR solution should continuously analyze current and historical details and correlates these with related threat events into a single view for full visibility.	Bidder to comply with RFP terms and conditions.
1395	166	1.Technical Specifications of each SOC Solutions	I. Security Incident and Event Management (SIEM): Log Storage	Point no 29 to 40	Online storage shall be provided by the SIEM vendor on the server in-built/HCI storage with necessary uptime with failover & performance.SAN appears to be an overhead for the solution and we request the bank to remove the SAN specifications.	Bidder to comply with RFP terms and conditions.
1396	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	5. The solution should auto replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data	Replication of rules/playbook requirs minimum manual intervention / process between DC & DR with minimum configuration changes required as the assets/IP/User Creds may be different in DC & DR. Kindly modify clause as following "The solution should auto/manual replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data"	Bidder to comply with RFP terms and conditions.
1397	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	9. The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Different OEM's have different count of OOB integrations available. putting such a high number will make it a very limited OEM participation(might be only one) in the bid. We request the bank to modify the clause as The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1398	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	10. Solution should include 100+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank	Different OEM's have different count of OOB playbooks. putting such a high number will make it a very limited OEM participation(might be only one/two oem) in the bid. We request the bank to modify the clause as "Solution should include 50+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank"	Bidder to comply with RFP terms and conditions.
1399	177	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	18. The solution should suggest contextual between incidents using machine learning.	We request the bank to modify the clause as "The solution should enrich alert/incident with contextual information using machine learning platform.	Bidder to refer Corrigendum-2
1400	2	Annexure 10 , Point no.6	The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. 10 Marks		This gives undue advantage to one specific technology OEM (PIM Vendor). For all other technologies, the highest scoring is capped at 5 marks, However in case of PIM, the marking is very high. We highly recommend to reduce from 10 to 5 marks & provision the remaining 5 marks for other technologies which bank intends to procure.(Example: DAST/TIP)	Bidder to comply with RFP terms and conditions.
1401	74	Annexure-2 Pre-Qualification Criteria	Sr. No 15	The proposed SOAR solution should have been implemented satisfactorily in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids The bidder shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	Would request bank to ammend the sub clause to: The bidder/ OEM shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. OR Would request bank to ammend the sub clause to: The bidder should have been implemented SOAR solution satisfactorily in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1402	74	Annexure-2 Pre-Qualification Criteria	Sr. No 16	The proposed UEBA solution should have been implemented in two Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids. The bidder shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	Would request the bank to ammend sub clause to: The bidder/ OEM shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. OR Would request the bank to ammend RFP clause to: The bidder should have been implemented UEBA solution satisfactorily in two Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids. Justification for the request of change - We/bidder have worked with multiple UEBA solution OEMs in past and have experience in deploying and managing UEBA solution for clients; however, we do not want to restrict ourselves with only those OEMs with whom we have worked in the past; the OEM which we feel fits best for this RFP w.r.t solution and commercials, might be someone with whom we have not worked in past (please note all OEMs will be providing support for all 5 years); thus, would request that this clause not be restrictive for the bidder	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1403	233	Annexure-10 Technical Evaluation Criteria	Sr. No 2	The Bidder's Annual turnover in the last 3 years: • >500 crore <=1000 crore - Score of 2 • >1000 crore <=1500 crore - Score of 5 • >1500 crore - Score of 10 Bidder has to submit audited Balance Sheet copies for last 3 Years i.e., 2021-22, FY 2022-23, FY 2023-24 along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number. If Bidder is not able to submit audited balance sheet for 2023-24, they should provide provisional balance sheet signed by CA with UDIN	Would request the bank to re - formulate the scoring criteria to: The Bidder's Annual Turnover in the last 3 years: • >500 crore <=700 crore - Score of 2 • >700 crore <=900 crore - Score of 5 • >900 crore - Score of 10 Justification for the request of change - The range of Turnover provided per score is very large e.g. for >500 cr to <=1000 cr (almost 500 Cr in range); in addition, the turnover figure asked for each score is very high e.g. for >500 cr to <=1000 cr is just 2 marks; furthermore do not see turnover as a technical criteria in most of the other BFSI sector similar size SOC RFPs floated in last 2 years, other than few RFPs where none has such a huge turnover criteria for maximum marks; a company/bidder of turnover > INR 900 Cr can perform as well as a bidder of turnover >INR 1500 Cr based on the experience and scale criteria in prequalification & other TQs of this RFP	Clause stands deleted. Bidder to refer Corrigendum-1.
1404	234	Annexure-10 Technical Evaluation Criteria	Sr. No 7	If Bidder is not able to submit audited balance sheet for 2023-24, they should provide provisional balance sheet signed by CA with UDIN	Would request the bank to ammend RFP clause to: The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government Organziations/Private Sector entities in India. Justification for the request of change - We/bidder understand that Bank would like to technically evaluate bidders expereince w.r.t SaaS implementation as per this criteria; thus would request addition of private sector too; as implementation in private sector too is a valuable expereince; in addition, the prequalification criteria no. 17 already filters based on capability w.r.t EDR	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1405	234	Annexure-10 Technical Evaluation Criteria	Sr. No 7	The Bidder must have implemented SaaS EDR solution in BFSI/ PSU/ Government entities in India. Implementation Experience • For 5 or more clients - 5 marks • For 2 clients - 3 marks Bidder should provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	Would request the bank to ammend RFP clause to: The Bidder must have implemented EDR solution in BFSI/ PSU/ Government Organziations/entities in India. Justification for the request of change - There are number of large & prestigious government entities in India which have EDR deployed, however, there is no connetivity to cloud due to confidentiality and security reasons; however, the expereince gained from implementing and managing the EDR solution is very valuable, which will be benficial for the client	Bidder to refer Corrigendum-1
1406	235	Annexure-10 Technical Evaluation Criteria	Sr No 8	The Bidder should have the experience in implementing or managing SIEM Solution in Organization(s) in India • 1 lakh EPS with 2 clients - Score of 5 • 1 lakh EPS with 1 client - Score of 2 Bidder should provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	Would request the bank to ammend RFP clause to: The Bidder should have the experience in implementing or managing SIEM Solution in Organization(s) in India/Abroad And Would request bank to re - formulate the scoring criteria to: • >=70 Thousand to >=1 Lakh EPS with 2 clients - Score of 5 • >=70 Thousand to >=1 Lakh EPS with 1 client - Score of 2 Justification for the request of change - We/bidder understand that Bank would like to technically evaluate bidder's expereince and scalability w.r.t implementing or managing SIEM EPS solution as per this criteria; thus, would request Bank not to restrict experience only to organizations in India || Futhermore would request Bank to change the range in the marking critiera from 1 Lakh to >=70,000 to >= 1 Lakhs EPS, as an bidder which has experience and capability to manage between 70k to 1 Lakh EPS can also manage/scale 1 Lakh and above EPS; in addition, bidder which manages 70k to 1 Lakhs EPS would easily have observable and peak EPS > 1 Lakh; adding to the preceding justification, the EPS is also dependent on the devices whose make, model, year, update ,	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1407	235	Annexure-10 Technical Evaluation Criteria	Sr No 9	The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India • 500 privileged users with more than 5 clients - Score of 5 • 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2 Bidder should provide the completion certificate/reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/invoices.	Would request bank to ammend the RFP clause to: The Bidder/OEM should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India And Would request bank to ammend the sub clause to: The bidder/OEM shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices. OR Would request bank to re - formulate scoring criteria to: The Bidder should have implemented or managed PIM Solution with minimum of 100 privileged users in Organization(s) in India: • 100 privileged users with 5 clients - Score of 5 • 100 privileged users with >= 2 clients and upto and including 4 clients - Score of 2 OR Would request bank to re - formulate scoring criteria to: The Bidder should have implemented or managed PIM Solution	Bidder to refer Corrigendum-2.

केनरा बैंक CANARA BANK C.P.&V.M. Wing, H.O., Bangaluru - 560 001 Tender Processing Section सी.पी. एवं वी. एम. विभाग, प्र.का., बेंगलूरु - 560 001

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1408	235	Annexure-10 Technical Evaluation Criteria	Sr No 11 Resources:	The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) >=75 - Score of 10 (b) > 50 and <75 - Score of 5 Note: For CEH maximum 5 number of certified resources will be considered Undertaking on bidder letter head needs to be submitted	Would request bank to ammend RFP clause to: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH/ CCNA/CCNP/ ISO IEC 27001/ OEM Level Certifications And Would request bank to re - formulate scoring criteria to: a. > =50 - Score of 10 b. >30 and < 50 - Score of 5 Justification for the request of change - We/bidder understand that Bank would like to technically evaluate bidder w.r.t number of certificaions, resource availbility and foresight w.r.t Security and associated practices; thus, the bidder would like to recommend to add few more certifications such as CCNA, CCNP, ISO IEC 27001, OEM Level Certifications to the list of certifications mentioned which would showcase bidders intention and foresight w.r.t security (and associated practices) such as network, data, information, security governance etc., and not gravitate towards certification around few types of security certification only ii. Furthermore, have requested for re - formulation of scoring	Bidder to refer Corrigendum-2.
1409	233	Annexure-10 Technical Evaluation Criteria	Sr. No 2	The Bidder's Annual turnover in the last 3 years: • >500 crore <=1000 crore - Score of 2 • >1000 crore <=1500 crore - Score of 5 • >1500 crore - Score of 10 Bidder has to submit audited Balance Sheet copies for last 3 Years i.e., 2021-22, FY 2022-23, FY 2023-24 along with certificate from the Company's Chartered Accountant to this effect with Unique Document Identification Number. If Bidder is not able to submit audited balance sheet for 2023-24, they should provide provisional balance sheet signed by CA with UDIN	Would request the bank to ammend RFP clause to: The Bidder (100% subsidary)/Bidder Parent's (Indian Entity) Annual turnover in the last 3 years • >500 crore <=1000 crore - Score of 2 • >1000 crore <=1500 crore - Score of 5 • >1500 crore - Score of 10	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1410	73/74/233 /234/235	Pre-Qualification Criteria & Technical Evaluation Criteria	Pre- Qualification Criteria: Sr No 8, 13,15,16,17,19 Technical Evaluation Criteria: Sr No 1, 7, 8, 9,	The bidder shall provide the completion certificate/ reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/invoices.	We understand that the bank has asked the bidder to provider either completion certification or reference letter email from client along with copy of purchase order or contract agreement or work order or engagement letter invoices - Please confirm if our understanding is correct? AND Would request you to amend the sub clause to: Bidder should provide completion certificate/copy of purchase order/copy of purchase order with RFP document Scope of Work/ contract agreement/ work order/ engagement letter/ invoices. Justification for the request of change - 1) Extremely difficult to get reference letter email from client along with copy of PO in case the point of contact has changed from client's end specially in Govt Entities and Banks 2) Very difficult to get reference letter email from client along with copy of PO in case sometime has passed from date of completion of the project and there is no active project with that particular client 3) Client's may not revert back by submission of the bid 4) Many a times client gives a single PO order with 1 or 2 line items, which does not mention various products/services being provided to client, which was part of the scope of work as per the RFP e.g. PO may mention NGSOC services and NGSOC products but may not mention EDR, SIEM, SOAR, UEBA explicitly	Bidder to comply with RFP terms and conditions.
1411	28	SOW	Sr No. 7 : Scope of Work for Bidder/ System Integrator (SI)	Bidder should involve respective OEM/PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations and also maintain the existing SOC solutions for 6 months	Is Bidder has to manage existing SIEM/SOC solution with new SIEM solution for 6 Months? OR Existing SI will manage the existing SOC solution for 6 solution in concurrence/parallel to new SOC solution from New Bidder? Please clarify.	TBD Yes
1412	47	SOW	Sr No. VI: PIM	The proposed PIM solution should be seamlessly integrated with the Bank's SIEM solution, Network Access Control (NAC) solution, ITSM tools, IDAM, LDAP or any other existing or future solution, as required by the Bank	We need to do integrate with PIM and Bank's SIEM solution, Network Access Control (NAC) solution, ITSM tools, IDAM, LDAP or any other existing or future solution; Kindly let us know the OEM of NAC, ITSM, IDAM are currently being used to work on integration feasible.	Yes
1413	54	SOW	Sr No. b : DLP	Existing setup: • 80k endpoint DLP Licenses (managed by SOC) • 80k network DLP licenses inbuilt in Bank Proxy solution (managed by IT-NOC team)	Can you please share the existing Hardware details to check on upgrading the solution? OR you want Bidder to newly size the Hardware as per upgrade requirement?	The details shared with selected Bidder Yes

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1414	56	SOW	Sr No. c : NBA	Current setup: • 60k Flow Per Sec (FPS) at DC and DR • SMC Manager and flow collectors at DC and DR	Can you please share the existing Hardware details to check on upgrading the solution? OR you want Bidder to newly size the Hardware as per upgrade requirement?	The details shared with selected Bidder Yes
1415	59	SOW	Sr No. d : Vulnerability Assessment (VA)	Current setup: • 1 Nessus scanner server • 1 Tenable SC server • 2300 licenses available	Can you please share the existing Hardware details to check on upgrading the solution? OR you want Bidder to newly size the Hardware as per upgrade requirement?	The details shared with selected Bidder Yes
1416	60	SOW	Sr No. d : Vulnerability Assessment (VA) Scope of Work of VA	The Bidder will be responsible to integrate the proposed VM solution with Bank's ITSM tools (Service Now), PIM, SIEM, GRC solution, and other security solutions.	Please share the details of GRC solution tool for integration scope.	RSA Archer
1417	NA	General			Could you please confirm who will provide ITSM ticketing tool to the operation team, is it Canara Bank or Bidder?	Bank exisiting Servicenow ITSM tool
1418	61	SOW	Sr No. VII: Threat Intel Services	Since Bank is currently using Izoologic threat intelligence services, the Bidder shall provide Threat Intel services to Bank from other service provider. Detailed scope for the same is mentioned below	SOW says Bank has Threat Intel Services, which is to be managed by bidder by upgrading certain features, and it also says apart from Izoologic Threat Intel Services bidder has to provide different Threat Intel Services solution. Please clarify.	Bidder has to provide different Threat Intelligence services from another service provider
1419	71	Annexure-2	Pre-Qualification Criteria	Additional query	we request the bank to ask for atleast one reference on SaaS EDR implementation along with sign off since last 5 years in one PSU BFSI in India. Or atleast One reference of OEM with 85K nodes in a PSU bank in India. This will help canara bank to get such OEM who have a track record of performing and protecting a bank of canara bank size. This clause will ensure Quality OEM will participate in the RFP.	Bidder to comply with RFP terms and conditions.
1420	71	Annexure-2 Pre-Qualification Criteria	Eligibility Criteria	Considering the complexity of the Banking environment, the SIEM, PCAP, UEBA, SOAR and TIP solutions should be from the Proven & Reputed OEMs.	Request you to kindly incorporate below criteria - The SIEM OEM should be incorporated in India under the Companies Act 1956 for at least 10 years . - Minimum Average Annual Turnover (MAAT) for last three years out of last five financial years of the SIEM OEM should not be less than INR Five Hundred (500) Crore. SIEM OEM must have positive net worth.	Bidder to comply with RFP terms and conditions.
1421	84	2. Scope of Work	e. Inventory Management of all assets(hardware and software etc.) supplied as part of RFP		Is there any Asset Managament tool is used in canara bank or we need to procure in this RFP?	Bank has ITAM tool, Bidder has to maintain the NGSOC inventory

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1422	85	2. Scope of Work	n. Provide immediate forensic support in case of any security/cyber incident		Could you please eloborate the scope to consdier Forensic support; Also, let us know how many such incidents might be reported in a Month or Year.	Bidder to refer Corrigendum-2.
1423	95	ATC Main 6. Manpower Roles and Responsibilities	L1 Incident Responder -	Column: Resources/Shift SOC Location: The resources shall be deployed at both primary and DR SOC situated in Bengaluru and Mumbai respectively.	We would like to know: 1. Only L1 resources are required to seat in both DC & DR site in total 14? Because in clause it has mentioned specifically only for L1 Triage analyst requirement. 2. Rest L2, L3 & Project Manager to be seated in DC location i.e., Bangalore	Bidder to refer Corrigendum-1.
1424	96	ATC Main 6. Manpower Roles and Responsibilities	L1 Incident Responder -	Column: Resources/Shift 2 Resources per shifts	As per the clause, 2 resources/shift is requested, however in point no.5 Manpower Requirement Table, 2 resources are required for Morning and Afternoon Shift and 1 resource required at night. Please clarify.	Bidder to refer Corrigendum-1.
1425	109	ATC Main 6. Manpower Roles and Responsibilities	Endpoint Security specialist	Attack Surface Management & Breach Attack Simulation Specialist	Our understanding is that Attack surface Monitoring (ASM) and Breach Attack Simulation (BAS) is part of Threat Intel Services and it is not a standalone services. Do you require specialist resources for only this specific requirement (ASM & BAS Specialist); please confirm the same.	Yes
1426	110	7. scope of work for bidder/system integrator(SI)	The Bank will provide facilities to host the devices for the personnel and workstations(Desktop/Laptop)		Need clarification on this point: 1. "Host the devices for personnel" - Is there hardware devices for NGSOC OR Desktop/Laptop. 2. Workstations(Laptop/Desktop) will be provided by purchaser 3. LED front Screen TV to be suppled by bidder	(1 and 2) The laptops or desktop for SOC resources shall be provisioned by Bank, (3)LED screen are not part of the RFP scope
1427	112	7. Scope of Work for the bidder/System integrator(SI)		Wherever Bank has provided VMs/physical servers/storage for installation of OS/DB/middleware/application component for proposed SOC solutions, it is the responsibility of the Bidder to perform end to end maintenance, support, upgrade etc. in line with the comprehensive scope	Request you to clarify and share the hardware details like VMs/physical servers/storage to be used for SOC solutions.So that we shall consider in our SOC proposal.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1428	114	7. Scope of Work for the bidder/System integrator(SI)		The Bidder shall take over operations and management of the currently running CSOC setup till NGSOC implementation is completed	Conflict with Sr No. 7 : Scope of Work for Bidder/ System Integrator (SI) in SOW document that to clarify below. - Existing SI will manage the exisitng CSOC till 6 months parallel post deployment of new NGSOC by bidder OR - It states Bidder has manage the existing CSOC to run the operations untill the new NGSOC is in production. Please clarify.	Bidder to refer Corrigendum-1.
1429	142	14. SoW for Proposed Services - Threat Inteligence Services - Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage		Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Bidder to comply with RFP terms and conditions.
1430	145	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/tools/exchange knowledge for banks brand		Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.
1431	146	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank: - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.		Kindly elaborate the scope.	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

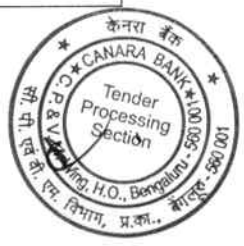
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1432	165	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM): , Point 2	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	a) As per our understanding, solution needs to be sized for 1,00,000 sustained EPS with peak handling capacity of 1,50,000 EPS for both DC and DR respectively. Kindly confirm on the sustained and peak EPS values for both DC and DR respectively. b) To ensure there are no assumptions done by the OEM for solution sizing on log sizing and licensing. Kindly consider modifying this clause as below "The solution shall be sized for 1,00,000 EPS as sustained EPS or 6.5 TB log capture per day (average log size as 800 Bytes) and 150,000 as peak EPS for both for DC & DR respectively during contract period. Solution should have same license across all layers i.e. collection, correlation and management layer to ensure no dropping or queuing of logs on any proposed SIEM components as per bank requirement. There should not be any limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Solution should support unlimited device integrations."	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
1433	166	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 18	Proposed solution should support both automatic and manually escalation of incidents to proposed SOAR and should allow the proposed SOAR to query data from the SIEM	SIEM and SOAR can be from different OEMs as per the RFP. This clause is restrictive as it favours a single OEM which offers both SIEM and SOAR. Please change the clause to "Proposed solution should support export of incidents to proposed SOAR and should allow the proposed SOAR to query incident data from the SIEM"	Bidder to comply with RFP terms and conditions.
1434	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 43	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system with critical fields like server IP, Server hostname, OS Name, OS Version, Criticality, Date of discovery etc. to be populated automatically	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1435	168	Annexure-9 Functional and Technical Requirements	I. Security Incident and Event Management (SIEM):, Point 44	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.	This requirement is OEM specific and restricts fair participation. Asset management is not a native SIEM requirement and is proprietary to particular OEM. Kindly remove this requirement to ensure level playing field.	Bidder to comply with RFP terms and conditions.
1436	174	Annexure-9 Functional and Technical Requirements	Packet Capture, Point 133	The proposed Packet capture solution shall have capabilities to integrate with proposed SIEM solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same	SIEM, PCAP, and UEBA from the same OEM ensures seamless integration, leading to better data correlation and faster threat detection. A unified platform provides consistent data formats, reduces integration complexity, and eliminates gaps in security coverage. This allows for more accurate analysis of network traffic, user behaviour, and security events along with reduced operational costs, improved efficiency through a centralized dashboard. With PCAP and UEBA from same OEM, it will give additional network models which will augment the network detection capability. Request to consider PCAP also from the same OEM along with SIEM and UEBA Kindly change this to "The proposed Packet capture solution should be from the same OEM which offers SIEM and UEBA to ensure seamless integration between all detection layers with native capabilities to integrate with proposed SIEM and UEBA solution in DC and DR. OEM shall have the capacity to capture 10 gbps and retain the packets and logs for 7 days. Adequate storage shall be factored for the same"	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1437	175	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 1	The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank	Gartner research highlights the benefits of integrating SOAR and TIP (from the same OEM to enhance security efficiency and reduce complexity. A unified platform streamlines data sharing, automates threat intelligence enrichment, and improves response times by eliminating the need for custom integrations. According to Gartner, consolidating these tools minimizes operational overhead and improves incident response capabilities, as they work in sync to detect and mitigate threats more effectively. By leveraging a single vendor, organizations can ensure better interoperability, reduce management challenges, and strengthen their overall security posture through automated, cohesive workflows. Hence we suggest, SOAR and TIP should be from same OEM Kindly modify this clause to "The proposed platform shall be hosted on-prem that integrates with all on-premises and hybrid, multi cloud architecture security components. The bidder shall provide all the required hardware which includes compute and storage to retain the data defined by the Bank. Proposed SOAR and TIP solutions should be from the same OEM"	Bidder to comply with RFP terms and conditions.
1438	176	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 9	The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	This requirement is proprietary to single OEM and highly restrictive for fair participation Kindly change this to "The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost."	Bidder to refer Corrigendum-1.
1439	177	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 19	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	This is typical case management usecases and is OEM specific Kindly remove this requirement to ensure fair participation	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1440	178	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 29	Bank shall have 15 user licenses and 2 read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	With fewer admin users, organizations reduce the risk of misconfigurations, unauthorized changes, and potential security breaches. Admins can oversee critical tasks like setting up automation workflows and managing incident responses, while read-only users can monitor, analyse, and collaborate without altering configurations. This approach improves accountability, as key decision-makers maintain control, while enabling broader visibility across teams. It balances security with transparency, allowing stakeholders to stay informed without compromising the integrity of the SOAR environment. Hence, we recommend unlimited read only users for better monitoring and visibility throughout across management of Bank. Kindly modify the clause to "Bank shall have 15 user licenses and unlimited read only licenses from day one. The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract"	Bidder to comply with RFP terms and conditions.
1441	179	Annexure-9 Functional and Technical Requirements	II. Security Orchestration and Automation (SOAR):, Point 41	The platform must have the ability to create custom hunting rules or hypotheses using Universal Threat Hunting Language like Kestrel.	Custom Threat hunting is not a native SOAR functionality and is supported through SIEM Platform. Kindly remove this requirement.	Clause stands deleted. Bidder to refer Corrigendum-1
1442	183	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 2	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Given that,SIEM and UEBA are required to be from the same OEM. Our understanding is that the functionalities mentioned in the SIEM,UEBA technical specifications can be achieved through either of the solutions. Please confirm if our understanding is correct.	No, UEBA Technical specifications has to be achived through UEBA solution only.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1443	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 9	The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage custom data models if necessary	Machine learning models are delivered through UEBA which are preconfigured and managed by OEM only as they are complex in nature and requires high skill set. Custom data models can be a security concern as it exposes the Data Models to be manipulated. Please Change this point to allow more reputed OEM's to participate. Kindly modify the line as "The solution should leverage Artificial Intelligence and machine learning for detecting anomalies. It should also enable bank to leverage inbuilt non customised data models for ML OR custom data models if necessary"	Bidder to refer Corrigendum-1.
1444	184	Annexure-9 Functional and Technical Requirements	III. User Entity Behavioural Analysis (UEBA):, Point 15	The solution shall use unsupervised and supervised machine learning algorithms for anomaly detection mentioned below (a) Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency. (b) Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time. (c) Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly. (d) Usage deviates from peer group such as User pattern of activity starts deviating from the peer group. (e) Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems. (f) Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing. (g) Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data (h) Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data (i) Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users	Supervised learning demands a large volume of labelled data and ongoing supervision from data scientists, increasing the complexity and effort. Unsupervised ML methods thus offer scalability and adaptability in dynamic environments with less human intervention. This complexity is better owned by product owners than operations teams i.e. OEMs only. Hence request you to change the clause to "The solution shall use unsupervised/supervised machine learning algorithms for anomaly detection mentioned below"	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1445	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 11	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach	Kindly modify the clause as below - "The proposed OEM offers comprehensive product lines from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach." Justification: With this bank will be getting a platform which will act as true XDR in future when the other sensors like email, network and clouds will be talking to the same platform. Bank will be to not only detect and monitor from the XDR platform but also can tale the actions. Having said that with normal integration, the logs will be coming to the platform but there will be no control in terms of taking action.	Bidder to comply with RFP terms and conditions.
1446	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 15	The proposed solution must have capacity to work in Monitoring/ Tap mode.	Kindly remove this clause as this is not applicable for Endpoint related solution. Justification: Monitoring/TAP mode is applicable for Network Security solutions which are running in TAP/SPAN/In-line blocking mode.	Clause stands deleted. Bidder to refer Corrigendum-1
1447	190	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 16	The solution should integrate with UEBA as part of solution, for applying advanced intelligence (AI) and machine learning (ML) to help the Bank to detect advanced threats.	Kindly modify the clause as below - "The proposed solution must have native AI/ML capability to help the Bank to detect advanced threats without depending on third party solution." Justification: The EDR platform itself has the capability to correlate between endpoint behaviour and User behaviour in case of any abnormal activity. Integrating with UEBA solution will not provide any additional intelligence.	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

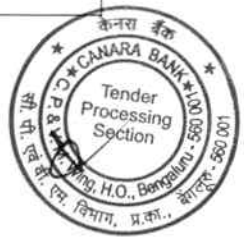
Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1448	192	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 39	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List	Kindly provide use cases and more details on the below mentioned categories: • Service Unavailable • Profiling	Bidder to comply with RFP terms and conditions.
1449	193	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 43	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Blocking communications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file.	Kindly remove the clause. Kindly modify the change as below: "Enable/Disable a local user account or a domain user."	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1450	194	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 62	The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals.	Requesting to modify the clause as follows: "The solution should be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS." Justification: There is no use case for Device control in Linux OS, hence requesting to modify the clause as specified above.	Bidder to refer Corrigendum-1.
1451	196	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 88	The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically discover newly added machines and have the agent installed on them without need of manual configuration.	Kindly modify the clause as below: "The solution should support automated distribution on endpoints/servers after the initial installation. Also, should automatically report newly deployed agent to management console with the agent's status."	Bidder to refer Corrigendum-1.
1452	197	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 105	The solution should have feature to uninstall and install agents from the console.	Pls modify the clause as below: "The solution should have feature to install/enable and uninstall/disable agents from the console."	Bidder to refer Corrigendum-1.
1453	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 111	The solution should provide functionality allowing a security analyst to remediate endpoints to a pre-infection state and should remove malicious files, roll back and repair other changes, or create Windows Microsoft Installer (MSI) files to be deployed by system management tools.	Kindly remove the point. This is vendor specific point. Or, Modify the point as below: The solution should provide functionality to automatically back up and restore files changed by the suspicious programs.	Bidder to refer Corrigendum-1.
1454	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 112	The solution should be capable of being rolled back with minimum time duration incase required on Endpoint Security Solution infrastructure as well as on end points.	Kindly remove the point. This is vendor specific point.	Clause stands deleted. Bidder to refer Corrigendum-1.

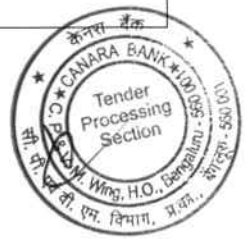
Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1455	198	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 115	The solution should protect all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2000 and above, RHEL, Oracle Linux, IBM AIX, Solaris, Ubuntu, Cent OS, Suse Linux etc.). The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period.	Kindly modify as below: "The solution should protect, detect and response for all Servers, Endpoints, Physical, Virtual, having Windows/Non Windows Operating Systems (Windows 10 and above, Windows server 2008 and above, RHEL, Oracle Linux, Ubuntu, Cent OS, Suse Linux etc.). The solution should only protect for the servers running with IBM AIX, Solaris server platforms. The solution should protect all latest and upcoming /upgraded OS in the Bank's IT ecosystem during the contract period."	Bidder to refer Corrigendum-2
1456	199	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 119	The solution should provide a means to see near real-time endpoint inventory, and online reports for system application, including versions of applications and the users that are running in real time and historically.	Kindly remove the point. This is vendor specific. Justification: The solution does provide endpoint inventory but getting application visibility is not the scope of EDR.	Clause stands deleted. Bidder to refer Corrigendum-1.
1457	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
1458	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 137	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.	Please modify the clause as below: "The sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks." Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat, it requires dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1459	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 138	The proposed sandboxing solution should have tight integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle.	Pls modify the clause as below: "The proposed sandboxing solution should have inbuilt integration with proposed EDR platform to support automated sample submission and IoC exchange to detect threats. Also, it should continuously analyze current and historical metadata and correlates these with related threat events into a single view for full visibility of the attack cycle."	Bidder to comply with RFP terms and conditions.
1460	200	V. Privileged Identity Management (PIM)	Architecture & General	3. The solution shall be sized for 10000 servers and 1500 privileged users from day one. The bidder shall plan for 10% YoY growth and size the hardware accordingly along with the bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	Can we consider approx. 2200 users and 15000 devices considering 10% Yo-Yo Growth during the contract period for 5 years.	Bidder to comply with RFP terms and conditions.
1461	200	Annexure-9/ Functional and Technical Requirements/ IV	Endpoint Detection and Response (EDR), Point 136	The solution should have the capability for sandbox /without sandbox /AI-ML model-based malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter.	Please modify the clause as below: The solution should have the capability for sandbox based zero day malware detection. The proposed sandbox can be deployed in either on cloud or in Bank's datacenter. Justification: AI/ML based techniques are static analysis technique to detect unknown threat but to detect zero-day threat we need dynamic analysis capability like sandbox.	Bidder to comply with RFP terms and conditions.
1462	NA	Generic	Generic	Generic	Please help us with number of service accounts to be managed by PIM This will help us in effort estimation to complete project within 24 weeks.	This will be shared to succcessful bidder
1463	204	V. Privileged Identity Management (PIM)	Secret Management	58. The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords The bidder shall provide unit price which can be leveraged by Bank to procure additional license as and when required during the tenure of the contract	How many number of applications to be considered for secrets management during the project duration ?	50 Applications (If a single application contains multiple password it should be trated as 1 application)



Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1464	234	Annexure-10	Sr. no. 7 Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5.End point is a complext project to deploy, its even more complex in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder allignment who have demonstrated a smooth deployment and sustance in such large environment in BFSI in India. This will make the bidder to allign with such OEM's who have a track record of protecting such large environment. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an oppertunity to evalute Bidder capability or allow bidder to allign with such bidders who have great track record in BFSI in India. hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5.	Bidder to comply with RFP terms and conditions.
1465	210	Annexure-9 Functional and Technical Requirements	VI. Threat Intelligence Platform (TIP) :, Point 20	The proposed solution offers more than 130 open-sourced intelligence and also provide Free Feeds' content as well	Kindly change the clause to "The proposed solution offers more than 50+ open-sourced intelligence and also provide Free Feeds' content as well"	Bidder to refer Corrigendum-2
1466	165-232	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT	Additional query	For Anti APT and SaaS EDR, we request the bank to allow OEM who have the option to use cloud based common sandboxing as well.(Currently these 2 technologies are asked to have on prem Sandboxing and Cloud based sandboxing respectively). Cloud based common sandboxing will ensure Architecture is simple and helps to share the threat intelligence between EDR, Deep Security and Anti-APT solutions. This will allow bank to have a better collaboration between above mentioned technologies in handling targetted attacks.	Bidder to comply with RFP terms and conditions.
1467	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 4	The bidders must propose a solution that must be hybrid in nature (Anti-APT and sandboxing should be deployed On-Prem, and any advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on cloud-based analysis platform.)	Please modify the clause as below: "The bidders must propose a solution that must be hybrid in nature. Anti-APT should be deployed On-Prem. Other technologies such as Sandboxing and advanced correlation technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or from cloud based analysis platform."	Bidder to refer Corrigendum-2

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1468	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 8	The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode with parallel VM execution capability on each appliance.	Please modify the clause as below: The bidders must propose APT solution for inline Web Traffic Analysis for a minimum 10 Gbps (TLS Inspection throughput) at DC & DR in high availability mode. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-1
1469	216	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 9	The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance.	Please modify the clause as below: "The proposed Anti-APT appliance must have built-in scalability where the appliance has TLS Inspection Throughput with all features enabled of 10 Gbps and TLS Concurrent connections of 5 Lakhs on day 1 and scalable to accommodate future requirements up to 20 Gbps on the Active - Active High Availability deployment of Anti-APT appliance."	Bidder to refer Corrigendum-1
1470	217	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 19	The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks.	Please modify the clause as below: "The bidders must ensure the proposed solution Analysis component is a secure purpose-built hypervisor/cloud sandboxing for the execution analysis of files, objects, flows, attachments, URL's and the environment should be able to unleash any hidden or targeted advance malware attacks. " Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1
1471	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 20	The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premise.	Please modify the clause as below: The bidders must ensure that each component has its own dedicated Analysis capability with all dependencies viz; additional licenses, customization or infrastructure to run exclusively on-premises/Cloud. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1472	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 21	The proposed hardware/appliance shall support minimum 100+ sandbox VMs. The bidder to size the hardware according to the throughput given above.	Please modify the clause as below: The proposed sandboxing platform shall support minimum 100+ sandbox VMs in On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above. Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1
1473	218	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 23	The solution should leverage a sandbox technology, featuring a custom hypervisor with built-in countermeasures. It must support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats.	Please modify the clause as below: "The proposed sandboxing technology should support multiple operating systems, service packs, and applications, and be capable of handling various file types. The solution should enable simultaneous executions and support multi-stage analysis to ensure thorough detection and mitigation of threats." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above	Bidder to refer Corrigendum-1
1474	219	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 29	The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on same appliance via SPAN port traffic integration	Please modify the clause as below: "The solution must have dedicated engines to support server-side detections, lateral movement detection and detection on post-exploitation traffic on the appliance via SPAN port traffic integration." Justification: To support the sizing requirements, asked in the RFP, there is a possibility to propose multiple devices. Hence, requesting to modify the clause as mentioned above	Clause stands deleted. Bidder to refer Corrigendum-1
1475	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 37	The solution must detect malicious TLS connections using a combination of JA3 blacklists and other logic/models designed to detect malicious activity based on TLS session attributes	Pls remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-1

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1476	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 40	The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, UNIX etc.)	Please remove Unix and modify the clause as below: "The proposed Anti - Apt solution should support operating system for sandboxing such as (Windows, Linux, Macintosh etc.)" In Point 22, Bank already mentioned about Windows, Macintosh & Linux environments.	Bidder to refer Corrigendum-2.
1477	220	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 47	The Proposed solution should support customer provided Microsoft OS and office license and environments for integrated Sandboxing. This requirement should be based on virtual execution and should not be external Hardware or chip-based function.	Please remove the clause.	Clause stands deleted. Bidder to refer Corrigendum-2.
1478	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 49	Sandboxing should provide detailed report and playback for malware.	Please modify the clause as below: "The solution should provide Sandboxing detailed report and playback for network analytics."	Bidder to refer Corrigendum-2.
1479	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 50	The proposed solution shall have on-prem sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation	Please modify the clause as below: "The proposed solution shall have on-prem/cloud sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation." Justification: The sandboxing capability can be on-prem or cloud. Hence, requesting to modify the clause as mentioned above.	Bidder to refer Corrigendum-2.
1480	221	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 51	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files	Please modify the clause as below: "The proposed solution should support YARA rules/STIX/OpenIoC and allow for editing and exporting/sharing of existing threat intelligence"	Clause stands deleted. Bidder to refer Corrigendum-2.
1481	222	Annexure-9/ Functional and Technical Requirements/ VIII	Anti - APT, Point 62	The solution must only be accessible via web UI and shall not require any plugins or thick client requirements for Admins or Analysts to access and manage.	Pls Modify the clause as below: The solution must be accessible via web UI/plugins/thick clients for Admins or Analysts to access and manage.	Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1482	233	Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5. End point is a complext project in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder who have demonstrated a smooth deployment and sustenance in such large environment in BFSI in India. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an opportunity to evalute Bidder capability or allow bidder to allign with such OEM'S who have great track record in BFSI in India. Hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5. Suggested Modified Clause: The OEM/Bidder must have PO reference of 50000 users and above SaaS EDR solution in last 5 years in BFSI/ PSU/ Government entities in India. •For 5 or more clients - 10 marks •For 4 clients - 5 marks •For 2 clients - 3 marks	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1483	233	Annexure-10	Technical Evaluation Criteria	Additional query	In the Scoring pattern, we request the bank to attach a decent score for OEM reference in SaaS based EDR reference and increase the score to 10 instead of 5. End point is a complext project in a distributed environment like Bank. With a user node of 85K, its always better to ask for OEM/Bidder who have demonstrated a smooth deployment and sustenance in such large environment in BFSI in India. Current Scoring Matrix in SaaS EDR does not add much value to the overall evaluation as large SaaS EDR deployments are mostly direct order or those bidders are not present in this large RFP. Banks looses an opportunity to evalute Bidder capability or allow bidder to allign with such OEM"S who have great track record in BFSI in India. Hence request the bank to ask bidder/OEM references and also increase the score to 10 instead of current 5. Suggested Modified Clause: The OEM/Bidder must have PO reference of 50000 users and above SaaS EDR solution in last 5 years in BFSI/ PSU/ Government entities in India. •For 5 or more clients - 10 marks •For 4 clients - 5 marks •For 2 clients - 3 marks	Bidder to comply with RFP terms and conditions.
1484	142	14. SoW for Proposed Services - Threat Inteligence Services - Clause - c	c)Detect & Stop Email Fraud/Phishing - Monitor fraudsters' emails spoofing of Bank's domains and take rapid action to takedown the same limiting the damage		Kindly Elaborate the scope as Email fraud detection is part of the email security. However, as part of the Threat Intelligent services we can investigate.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1485	145	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank - Clause - e	e)The Bidder shall perform Dark Net/Deep Web forum monitoring for bank registered brand. Bidder shall also monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc. where cybercriminals congregate to sell/buy services/tools/exchange knowledge for banks brand		Whatsapp Monitoring is not possible as the end to end communication is encrypted. However, we can initiate the takedowns.	Bidder to comply with RFP terms and conditions.
1486	146	14. SoW for Proposed Services - Dark Web/ Deep Web scanning for sensitive information pertaining to Bank: - Clause - m	m)Vendor has to takedown all the dark / deep web sensitive information pertaining to Bank without any extra charge to Bank.		Kindly elaborate the scope.	Bidder to refer Corrigendum-1.
1487	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The proposed solution shall be hardware or software based with logically segregated into Collection, correlation, and Management layer. If the software appliance is proposed, the OEM shall provice all the required hardware to implement the solution	Most of the NextGen SIEM verdors combine logging and correlation modules in a single appliance or software to optimize the number of servers or hardware requirements without impacting performance. Please confirm if the same is acceptable to the bank.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1488	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Bidder must provide pricing for extra EPS required by bank during the contract period in bundle of 5000 EPS.	Could you clarify the EPS capacity? Is the total EPS capacity 200K across DC and DR, scalable up to 300K? Or is the overall EPS capacity across DC and DR 100K, scalable up to 150K?	Clarification: 1,00,000 EPS for each site with Hardware Scalable up to 1,50,000 EPS (i.e At each site Hardware should support for min. 3 Lakh EPS)
1489	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Bidder must provide pricing for extra EPS required by bank during the contract period in bundle of 5000 EPS.	Please confirm if the bidder can propose enterprise licenses of the SIEM system that are not tied to EPS but rather to other criteria such as the organization's size (number of users or servers, for example). Because Enterprise licenses are trust-based, the solution doesn't restrict the number of devices such as servers, network devices, virtual machines, or other data sources integrated with the SIEM platform. The key advantage of enterprise licenses over EPS-based or GB per day licenses is that they are future proof (i.e., if EPS increases above what indicated in the RFP, then banks don't need to buy more licenses).	Yes, Bidder can propose enterprise licenses propotionally sized as per the RFP requirement
1490	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Bidder must provide pricing for extra EPS required by bank during the contract period in bundle of 5000 EPS.	Please confirm if Bidder can propose GB per day licenses instead if EPS bases licenses?	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1491	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution shall be sized for 1,00,000 EPS for DC & DR each and sustainable up to 150,000 EPS per site during contract period without dropping or queuing of logs on any proposed SIEM components as per bank requirement and any additional Hardware, software, and storage except EPS licenses. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. Bidder must provide pricing for extra EPS required by bank during the contract period in bundle of 5000 EPS.	If GB per day licenses are allowed to be proposed, please confirm the average byte size which OEM shoud factore. As per our experience with large banks, we have seen average byte size to range between 700 bytes to 1200 bytes	Bidder has to provide scientific calculation sheet for EPS to Ingestion converstion taking the average event size as 800 byte for the sizing of solution on OEM Letter Head.
1492	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The proposed solution must support the data replication /dual forwarding without relying on other third-party replication technologies on the operating system or storage level with near zero RPO & RTO. It should also admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	Most SIEM vendors support 1+1 High Availablility which meets the availablility requirements for overall Solution. Capability of "decide on replication factor within DC and replication factor for DR" is OEM specific point. For better participating please make this open.	Bidder has to comply with RFP terms
1493	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The proposed solution must support the data replication /dual forwarding without relying on other third-party replication technologies on the operating system or storage level with near zero RPO & RTO. It should also admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.	SIEM will sent to alert /offense to SOAR along with all the Artifacts. Same can be replicated to DR SOAR. This does not require the SIEM to duplicate the alerts/offences in DR instance. Please confirm if same is accptable to the Bank	Not Acceptable, Bidder to comply with RFP terms and conditions.
1494	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	Solution should contain Generative AI based automatic/ custom use case rules builder based on Analyst prompt.	Generative AI might create rules that are not perfectly accurate or relevant for the specific environment. Misconfigured rules could either miss critical security events or generate too many false positives, making it hard for analysts to discern genuine threats. Also, Generative AI may struggle to fully understand the specific context or nuances of an organization's IT environment, leading to rules that don't fit well with the actual security landscape or operational needs. Not all OEM's uses GenAI for creating rules hence requesting Bank to relax this point.	Clause stands deleted. Bidder to refer Corrigendum-2.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1495	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	High Availability should use cluster set-up so that data could be shared between the nodes.	Typical high-availability will replicate 100% data to other nodes in the cluster. Sharing of data can lead to log loss. Please confirm if same is accptable to Bank	Bidder to comply with RFP terms and conditions.
1496	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution collector must support the automatic load balancing and load sharing	Log balancing or load sharing without an external load balancer is not possible. This is an OEM-specific point. Please relax on this point.	Kindly refer Technical specification of SIEM point 4
1497	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Incident and Event Management (SIEM)	The solution must not block, drop, or place grace period when system exceeds purchased EPS license/subscriptions limit	Please confirm if Bidder can propose Enterprise licenses of SIEM solution which are not bouded to EPS but to other factores like size of the organization (number of users in the organization or number of server in the organization etc). Enterprise license will never enforce any restriction (like drop or grace period) on the EPS ingestion.	Yes, Bidder can propose enterprise licenses propotionally sized as per the RFP requirement
1498	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	User Entity Behavioral Analysis (UEBA)	Proposed UEBA should be from the same OEM of the proposed SIEM solution.	Bank must adopt best in breed technology for SIEM and UEBA. Not all SIEM vendors provide Best in class UEBA and not all UEBA vendors provides Best in class SIEM. Also, todays Standalone UEBA solutions prvides bidirectional integration by collecting logs from SIEM and sending alerts to SIEM. Hence please relax this point by allowing 3rd party standalone UEBA vendors to participate in this RFP.	Yes

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1499	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	User Entity Behavioral Analysis (UEBA)	The solution shall use unsupervised and supervised machine learning algorithms for anomaly detection mentioned below (a) Access high-value assets such as User starts accessing and downloading high-value assets with increased frequency. (b) Usage changes over time such as User activity deviates from normal over a short period of time or a gradual change over an extended period of time. (c) Assess frequency of assets such as User's volume of activity suddenly spikes or access to number of assets increases rapidly. (d) Usage deviates from peer group such as User pattern of activity starts deviating from the peer group. (e) Change in account privileges such as User attempts to change privileges on existing account or open new accounts on other systems. (f) Application misuse by sequence of actions: User performs a sequence of actions which no other user is performing. (g) Sensitive data leakage such as User manipulates http request / response parameter to download sensitive data (h) Application misuse by malware or bots such as A bot or malware attacks an application or access sensitive data (i) Dynamic adjustment of risk scores such as Dynamically adjust the risk score of rules when triggered against particular user or users	Most of the use cases can be achieved using either supervised or unsupervised or custom correlation rules or custom ML rule to deliver the required outcom. Please relax this point by stating - The solution shall use unsupervised/supervised/custom machine learning algorithms or custom rule for anomaly detection mentioned below:	Bidder to refer Corrigendum-1
1500	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	User Entity Behavioral Analysis (UEBA)	The solution should provide analytical capabilities pertaining to ML models such as Outliers, Peer- Group Analytics, Time-Series Analytics, Predictive Analytics, Geo-location & ISP Analytics, Pattern Match Analysis etc.	Please elobrate on the usecase of ISP analytics	Bidder to comply with RFP terms and conditions.
1501	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	AI Capabilities: a. Auto assigning analyst - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department, availability in shift, workload on analyst etc.	The requested feature do not require any AI capabilities. Its uses very basic automation script. Please relax this point.	Bidder to refer Corrigendum-1

केनरा बैंक CANARA BANK H.O. Tender Processing Section H.O., Bengaluru - 560 001 प्र.का., एस.बी., एस. विभाग, प्र.का., बेंगलूरु - 560 001

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1502	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	The solution should suggest contextual between incidents using machine learning.	There are other ways to achieve the same outcome without using ML like common artifacts of the incident etc.Please relax this point	Bidder to refer Corrigendum-2.
1503	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	The solution should provide shift management feature to upload shift schedule of users in any suitable format.	Not all SOAR vendors provide the same. Please relax this point	Bidder to comply with RFP terms and conditions.
1504	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	The solution must maintain a database of incidents. The user must be able to search this database using the embedded Elasticsearch. Please describe how your solution meets this requirement.	Use of elasticsearch for incident database is vendor specific point. Please remove "embedded Elasticsearch" from this requirement.	Bidder to refer Corrigendum-2.
1505	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	The solution should be able to group incidents (e.g., Malware outbreak with time delay, every incident with this malware in one parent incident)	Grouping of incident can be done on dashboard for visualization. Please confirm if same is accptable to Bank	Bidder to refer Corrigendum-2.
1506	165-232	Annexure-9/Functional and Technical Requirements/Technical Specifications of each SOC Solutions	Security Orchestration and Automation (SOAR)	The solution must be able to detect redundant alerts and hence, aggregate duplicates in one and only ticket (Number of aggregated tickets must be displayed)	Aggregating the redudant alert is a feature of SIEM and Aggregrated alerts can be send to SOAR for investigation. Please relax this point and most the SIEM and SOAR vendors have tight integration for deliver the desired outcome.	Bidder to comply with RFP terms and conditions.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1507	166	1.Technical Specifications of each SOC Solutions	I. Security Incident and Event Management (SIEM): Log Storage	Point no 29 to 40	Online storage shall be provided by the SIEM vendor on the server in-built/HCI storage with necessary uptime with failover & performance.SAN appears to be an overhead for the solution.	Bidder to comply with RFP terms and conditions.
1508	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	5. The solution should auto replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data	Replication of rules/playbook requirs minimum manual intervention / process between DC & DR with minimum configuration changes required as the assets/IP/User Creds may be different in DC & DR. Kindly modify clause as following "The solution should auto/manual replicate all the rules, data, etc., to DR site and vice versa for continuing the operations without any loss in data"	Bidder to comply with RFP terms and conditions.
1509	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	9. The solution shall have 500+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Different OEM's have different count of OOB integrations available. putting such a high number will make it a very limited OEM participation(might be only one) in the bid. We request the bank to modify the clause as The solution shall have 100+ out of the box integration available from day one. SI to develop any new integration as and when required by the Bank with no extra cost.	Bidder to refer Corrigendum-1.
1510	176	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	10. Solution should include 100+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank	Different OEM's have different count of OOB playbooks. putting such a high number will make it a very limited OEM participation(might be only one/two oem) in the bid. We request the bank to modify the clause as "Solution should include 50+ out-of-the- box playbooks for incidents like Ransomware Attack, Data Leakage, Malware Attack, DoS and DDoS attack, Phishing Attack, etc. and should support creation of multiple playbooks without any additional cost to Bank"	Bidder to comply with RFP terms and conditions.
1511	177	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	18. The solution should suggest contextual between incidents using machine learning.	We request the bank to modify the clause as "The solution should enrich alert/incident with contextual information using machine learning platform.	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1512	178	1.Technical Specifications of each SOC Solutions	II. Security Orchestration and Automation (SOAR):	36. Bidder should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc.	We request the bank to modify the clause as "Bidder/OEM should have their own threat intelligence service which shall be integrated with SOAR to check threat score, reputation etc."	Bidder to refer Corrigendum-1.
1513	2	Annexure 10 , Point no.6	The OEM must have supplied on-prem PIM solution with 1000 privileged users in Banking segment in India. 10 Marks		This gives undue advantage to one specific technology OEM (PIM Vendor). For all other technologies, the highest scoring is capped at 5 marks, However in case of PIM, the marking is very high. We highly recommend to reduce from 10 to 5 marks & provision the remaining 5 marks for other technologies which bank intends to procure.(Example: DAST/TIP)	Bidder to comply with RFP terms and conditions.
1514	2	Annexure 10 , Point no.10	Evaluation Criteria	Presentation by the Bidder:	Since this is a QCBS RFP & minimun marks required to qualify under technical evaluation is set at 70 marks, allocating 25 marks only for the bidder presentation can make it to difficult for bidders to qualify.	Bidder to comply with RFP terms and conditions.
1515	74	Annexure 2 - Pre-Qualification Criteria	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	The bidder should have implemented/ managed proposed on prem PIM solution in one Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 years as on date submission of Bids.	We request the bank to reconsider this point inline with Annexure-10 Technical Evaluation Criteria (234) and consider OEM references instead of bidder implemented references. This will ensure support requirements for next 5 years and also provide expertise of new age PIM products implemented elsewhere by us or OEM directly in India.	Bidder to comply with RFP terms and conditions.
1516	234	Annexure-10 Technical Evaluation Criteria	9) The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India - 500 privileged users with more than 5 clients - Score of 5 - 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	9) The Bidder should have implemented or managed PIM Solution with minimum of 500 privileged users in Organization(s) in Organization(s) in India - 500 privileged users with more than 5 clients - Score of 5 - 500 privileged users with more than 2 clients and upto and including 5 clients - Score of 2	Request the Bank to relax this clause and reduce the minimum number to 200. Suggested clause: The Bidder should have implemented or managed PIM Solution with minimum of 200 privileged users in Organization(s) in Organization(s) in India - 200 privileged users with more than 5 clients - Score of 5 - 200 privileged users with more than 2 clients and up to and including 5 clients - Score of 2	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1517	Page 87 of 291	Annexure-8 / Scope of Work	3. Sizing & Scalability Requirements	Sl. No. 15 SOC Solution - Cyber Range	Existing: Under Estimated Future Sizing (For 5 years) Participants: 5/ batch Hours: 40 hours per year When opting for **Cyber Range as a Service (CRaaS)** with a **yearly subscription** limited to **5 people per batch** and **40 hours per year**, the platform's utilization is minimal. The upfront investment covers the entire year, but usage is restricted, leading to underutilization of the service. Change: Under Estimated Future Sizing (For 5 years) Participants: 5/ batch Hours: 40 hours per month In contrast, using **CRaaS for 5 people per batch** with up to **40 hours per month** results in a more efficient and cost-effective use of the platform. With monthly access, the bank can conduct more frequent training sessions, increase hands-on experience for participants, and maximize the platform's value by leveraging it throughout the year instead of limited annual sessions. This provides greater flexibility and better return on investment.	Bidder to refer Corrigendum-1.

Pre bid queries replies for GeM bid ref.no. GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Sr. No.	Page No.	Section / Annexure / Appendix	RFP Clause	Sub-Clause/ Technical Specification	Bidder's Query	Bank's Response
1518	Page 155,156 of 291	Annexure-8 / Scope of Work	14. Scope of Work for Proposed services	c) Cyber Range	Addition: Cyber Range SaaS solution should support 50 or more users logging in simultaneously to play individual exercises. Each user should be able to engage in the same or different threat scenarios concurrently, without impacting the configurations, settings, or gameplay rules on other users' machines.	Bidder to comply with RFP terms and conditions.
1519	Page 245 of 291	Annexure-17 / Bill of Material	Table 2) Price for NGSOC Services	Sl. No. 3 Solution/Service - Cyber Range	Existing: Qty mentioned is Participants: 5/ batch Hours: 40 hours per year Change: Qty should be 1	Bidder to refer Corrigendum-1

Date: 22-10-2024
Place: Bengaluru

DEPUTY GENERAL MANAGER

CANARA BANK * 560001 * Tender Processing Section H.O. Bengaluru