

Corrigendum-6 to GeM Bid ref: GEM/2024/B/5406710 dated 17/09/2024 for Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

It is decided to amend the following in respect of the above RFP:

a. GeM bid document (Bid End date/ Bid Opening Date, Page no. 1 of 7):

Description	Existing details	Amended details
Bid End Date/Time	20/11/2024, 15:00:00	25/11/2024, 15:00:00
Bid opening Date/Time	20/11/2024, 15:30:00	25/11/2024, 15:30:00

b.

Sl. No	Section/ Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1.	Section C - Deliverable And Service Level Agreements	Sl. No. 5 Uptime	5.3 The selected bidder should consider high-availability (active-active) with zero RPO and RTO.	5.3 The selected bidder should consider high-availability (between DC & DR) either Active-Active or Active- Passive unless it is explicitly mentioned in RFP, wherever it is Active-Passive, RPO should be 15 minutes and RTO 120 minutes.
2.	Section C - Deliverable And Service Level Agreements	Sl. No. 7	Payment Terms	Amended Payment Terms
3.	SECTION F - OWNERSHIP & AWARDDING OF CONTRACT	10. Execution of Agreement	10.1. Within 21 days from the date of acceptance of the Purchase Order/LOI or within 30 days from the date of issue of Purchase Order/LOI whichever is earlier, the selected bidder shall sign a stamped "Agreement" with the Bank at Bengaluru as per Appendix-G. Failure to execute the Agreement makes the EMD liable for forfeiture at the discretion of the Bank and also rejection of the selected bidder	10.1. Within 38 days from the date of acceptance of the Purchase Order/LOI or within 45 days from the date of issue of Purchase Order/LOI whichever is earlier, the selected bidder shall sign a stamped "Agreement" with the Bank at Bengaluru as per Appendix-G. Failure to execute the Agreement makes the EMD liable for forfeiture at the discretion of the Bank and also rejection of the selected bidder
4.	Annexure-2	Pre-Qualification Criteria	Pre-Qualification Criteria	Amended Annexure-2 Pre-Qualification Criteria
5.	Annexure-10	Technical Evaluation Criteria	Technical Evaluation Criteria	Amended Annexure-10 Technical Evaluation Criteria

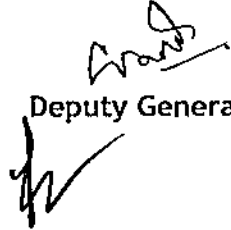


6.	Annexure-9	Functional and Technical Requirements	Functional and Technical Requirements	Amended Annexure-9 Functional and Technical Requirements
7.	Annexure-8	Scope of Work	Scope of Work	Amended Annexure-8 Scope of Work

All the other instructions and terms & conditions of the above RFP shall remain unchanged.

Please take note of the above amendments while submitting your response to the subject RFP.

Date: 16/11/2024
Place: Bengaluru


Deputy General Manager





6. Payment Terms

6.1. Payment Terms for Solutions and Hardware:

6.1.1. The payment schedule will be as under and will release after execution of contract agreement. Payment schedule will be as under for each of the in-scope solutions (SIEM, SOAR, UEBA, PIM, EDR, TIP, BAS, DAST, DLP, VM, Anti-DDoS, Anti-APT, NBA):

Sl. No	Payment Stages	% Of Payment	Condition/ Remarks (After deducting applicable penalties and Liquidated damages (if any) as per GeM Terms & conditions)
1.	Hardware cost (including OS & associated Software)	50%	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. The Applicable GST will be paid in full upfront.
		30%	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, Warranty period, on submission of invoices duly acknowledge by the Bank's Officials or Submission of Bank Guarantee of equivalent amount.
2.	<u>License cost</u>	100%	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.
3.	One time implementation cost	30%	On successful implementation in UAT of respective solution/services and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents.
		50%	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. NOTE: Sign-off will be provided on successful demonstration of all technical specification points of the respective solutions.
		15%	On successful completion of DR Drill of respective solution/services and on submission of Invoice and Acceptance/Sign off by the Bank on production of relevant documents.
		5%	On successful implementation of all NG SOC solutions and submission of Invoice and Acceptance/Sign off thereof by the Bank officials on production of relevant documents.
4.	AMC/ATS		Payment will be made yearly in advance subject to submission of Bank Guarantee of equivalent amount and the applicable penalty and LD, if any, shall be recovered by invoking the submitted Bank Guarantee for this purpose.



		<u>If Bank Guarantee is not submitted, Payment will be made Quarterly in arrears after deducting applicable penalties and Liquidated damages.</u>
5.	Additional requirement/ additional customization/ enhancement	100% payment will be released after Successful Go Live and on production of relevant documents, Acceptance/Sign off thereof by the Bank officials on production of relevant documents.
6.	Dedicated Onsite Resources	Payment for onsite resource charges will be paid proportionately as per attendance in monthly arrears after deducting applicable penalties and Liquidated damages.
7.	OEM Training	100% payment will be released yearly after successful completion of training for respective year and submission of Invoice and Acceptance by the Bank on production of relevant Training Certificates and documents.

- 6.1.2. Bank will release the payment on completion of activity and on production of relevant documents/invoices. Please note that Originals of invoices (plus One Copy) reflecting GST, GSTIN, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office and Manufacturer's/ Supplier's Warranty Certificate should be submitted while claiming payment in respect of orders placed.
- 6.1.3. The selected bidder has to submit installation report/Sign off report duly signed by the Bank officials of the respective Branch/offices in originals while claiming payment. The invoice and installation report should contain the product serial number of the items supplied.
- 6.1.4. Bank will not pay any amount in advance unless otherwise specified in this RFP.
- 6.1.5. Bank will not pay any amount in advance except Licenses charges for 2nd& 3rd year.
- 6.1.6. Payment shall be released within 30 days from the date of submission of relevant documents as per RFP terms.
- 6.1.7. The Bank shall finalize the installation and acceptance format mutually agreed by the selected bidder. The selected bidder shall strictly follow the mutually agreed format and submit the same for each location wise while claiming installation and acceptance payment.
- 6.1.8. The payments will be released through NEFT/ RTGS after deducting the application LD/ Penalty, TDS if any, by centrally by Head Office at Bengaluru and the selected bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code etc.
- 6.1.9. All licenses shall be provided/ purchased in the name of the Bank.

6.2. Payment Terms for Services:

- 6.2.1. Payment schedule will be for each of the in-scope services (Threat Intel Services + ASM, Breach Attack Simulation, Cyber Range, DDoS Drill).
- 6.2.2. 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.
- 6.2.3. The total cost or total contract price as defined in this RFP shall mean the total cost or price or value or charge towards providing the mentioned SOC Services to. The payments will be released only on acceptance of the order and on submission of contract performance guarantee.
- 6.2.4. The selected bidder shall be responsible for extending the validity date and claim period of all the bank guarantees as and when it is due on account of incomplete





- contract under guarantees. The bank will invoke the guarantee before expiry of validity if contract is not completed and the guarantee is not extended, accordingly.
- 6.2.5. Please note that Originals of invoices (plus One Copy) reflecting GST, State Code, HSN Code, State Name, Taxes & Duties, Proof of delivery duly signed by Bank officials of the respective Branch/office should be submitted while claiming payment in respect of order/s placed.
- 6.2.6. Payment shall be released within 30 days from submission of relevant documents as per RFP terms after deducting applicable TDS centrally at the Bank's office at DIT Wing, Naveen complex, 14, M G Road, Bengaluru-560001.
- 6.2.7. The payments will be released through NEFT/ RTGS after deducting the application LD/Penalty, TDS if any, centrally by Head Office at Bengaluru and the selected bidder has to provide necessary Bank Details like Account No., Bank's Name with Branch, IFSC Code etc.
- 6.2.8. The invoices should contain full details of all the items contracted by bank, as reflected in Annexure 17 and should not contain any clauses contrary to the terms of the contract and if any such clause exists in the Invoice/any other documents, the same will not be valid and cannot be held against the Bank.
- 6.3. Payment terms for resources:
- 6.3.1. Payment for Onsite Resources shall start after implementation sign off of respective solutions/ services and as per discretion of bank.
- 6.3.2. Vendor has to provide onsite resources from the date of sign off or as per banks requirement during implementation phase, if required.
- 6.3.3. Payment for the SOC operations, maintenance from 1st year to 5th year i.e., 60 months from the date of sign-off of the project (last solution Sign off). The total cost quoted under the Final Commercial Bill of Material - SOC Operating cost will be divided into 60 equal installments and will be paid to the System Integrator monthly in arrears on submission of invoice and other supporting documents.
- 6.3.4. Payment for onsite resource charges will be paid proportionately as per attendance in monthly arrears after deducting applicable penalties and Liquidated damages.



Annexure-2

Amended Pre-Qualification Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Ref: GEM/2024/B/5406710 dated 17/09/2024.

We have carefully gone through the contents of the above referred RFP along with replies to Prebid queries & amendment, if any and furnish the following information relating to Pre-Qualification Criteria.

Sl. No	Pre- Qualification Criteria	Documents to be submitted in compliance with Pre-Qualification Criteria	Bidders Response
1	Signing of Pre-Contract Integrity Pact	The bidder should submit signed Pre-Contract integrity pact on Non-Judicial Stamp Paper of Rs.500/- or more (as per respective state Stamp Act whichever is higher) as per Appendix-F.	
2	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 19/07/2024.	Certificate of local content to be submitted as per Annexure-5 as applicable.	
3	The Company operating should be legally compliant company and can be: a. A partnership firm or a Limited Liability Partnership duly registered under the Limited Liability Partnership Act, 2008. (OR) b. Company duly registered in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013. (OR) c. Proprietorship firm duly registered under the applicable shops and commercial Establishments Act and should be compliant to all the applicable laws.	Copy of Certificate of LLP registration. (OR) Copy of Certificate of Incorporation and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies. (OR) Copy of Certificate of registration under and Certificate of Commencement of business in case of Public Limited Company or Certificate of Incorporation in case of Private Limited Company, issued by the Registrar of Companies. For (c) Documentary proof for confirming registration of Proprietorship firm (e.g. Copy of Certificate of registration under shops and commercial Establishments Act., GST etc) Copy of Certificate of registration under shops and commercial Establishments Act.	
4	Bidder should be the Original Equipment Manufacturer (OEM)/ Original Software Owner (OSO)/ Original Software Developer (OSD) of Solution. (OR)	If the applicant is OSD/OSO, an Undertaking Letter has to submit in this effect. (OR) If the bidder is an authorized dealer/distributor, an authorization letter from their OEM and OSO/ OSD to deal/market their product in India and it should be valid	





	An authorized dealer/distributor of the proposed Solution.	for entire contract period from the date of submission of the bid.
5	The bidder should have an Average annual turnover of <u>Rs.250 Crores</u> (Two Hundred and Fifty Crore Rupees) during last 3 financial years (i.e., 2021-22, 2022-23 & 2023-24) from Indian operations. This must be the individual company turnover and not of any group of companies.	Bidder has to submit audited Balance Sheet copies for last 3 Years i.e., 2021-22, FY2022-23, 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.
6	Bidders should not be under debarment/blacklist period for breach of contract/fraud/corrupt practices by any Scheduled Commercial Bank/ Public Sector Undertaking/ State or Central Government or their agencies/ departments on the date of submission of bid for this RFP.	The bidder should submit self-declaration on the Company's letter head to this effect.
7	The Net Worth of the bidder should not be negative as on 31/03/2023 and also should not have been eroded more than 30% in the last three financial years ending on 31/03/2023.	The bidder should submit certificate from the Company's Chartered Accountant with UDIN to this effect. If Bidder is not able to submit audited balance sheet for 2023-24, they should provide provisional balance sheet signed by CA with UDIN
8	The bidder should have implemented/ managed on-prem security operations center with minimum 4 solutions along with SIEM (mandatory) and 3 among SOAR, UEBA, PIM/PAM, XDR/EDR, Anti - APT, DLP, Anti - DDOS, NBAD, DAM, WAF) in 2 organizations like BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI/ other equivalent government entities in India during last 5 financial years.	Bidder should provide the completion certificate/reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/invoices.
9	Bidder must not be an existing System Integrator (SI) managing banks datacenters (DC and DRC).	Letter of confirmation on letter head from bidder duly signed by an authorized signatory
10	Bidder should not be the existing Consultant for the NGSOC Implementation at Canara Bank	Letter of confirmation on letter head from bidder duly signed by an authorized signatory
11	The Bidder to confirm that all the technical and functional specifications and Scope of work of the RFP are covered in totality in the proposal submitted by the bidder	Bidder should provide an undertaking on his letter head
12	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	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.



	government entities in India during last 5 financial years.		
13	OEM should have provided on-prem SIEM solution with active implementation of at least 80,000 EPS in single entity of Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI/ <u>Private entities</u> in India, during last 5 financial 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.	
14	The OEM should have supplied SOAR solution in two Government Organizations/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 financial 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.	
15	The OEM should have supplied UEBA solution in two Government Organizations/ BFSI/Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 financial 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.	
16	The Bidder should have implemented/ managed the EDR/ XDR solution in Single entity with Government Organizations/ BFSI/ Private Sector/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 financial 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.	
17	OEM should have provided SaaS based EDR solution with minimum 40,000 endpoints in two Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 financial years as on date of 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.	
18	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 financial 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.	
19	OEM should have provided on-prem PIM/PAM solution with minimum 1,500 privileged users licenses or 10,000 servers licenses in two Government Organizations/ BFSI / PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI in India, during last 5 financial years as on date of 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.	
20	OEM for any technology / security solution/ solution for NGSOC and other security solutions should have support center in India with availability of 24x7	An undertaking should be submitted in a letterhead with complete postal address and contact details of such OEMs	





	onsite, telephonic, and remote support (Preferably in Mumbai, Bengaluru).	
21	The Bidder shall have minimum 100+ security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management (g) Infrastructure Management (h) Technology Architect	List of resources with employment details (Employee number, Designation, Qualification, certification (with number) & experience (in number of years) in the relevant field) in company letter head shall be submitted
22	The bidder shall submit duly filled and signed Manufacturer Authorization form (MAF) and declaration about back-to-back support from respective OEMs proposed as part of their bid. Validity of same should cover contract period from date of sign - off	Undertaking to this effect must be submitted in their letter head as per Format 16
23	The Bidder should agree and comply with the Bank's security policy and regulators i.e., Govt. of India/ RBI/ CERT-IN/ NPCI/ DeitY/ MeitY/ SEBI/AMFI etc. guidelines; industry guidelines as well as complying with other country's regulatory guidelines wherever applicable	Self-declaration cum undertaking to be submitted
24	The bidder should have support office in Bengaluru or Mumbai for 24x7 supports.	The Bidder should submit the details viz., address, phone no., email id and contact person Name & Mobile no. etc.,
25	The bidder should provide confirmation that any person/ Partnership/ LLP/ Company including any subsidiary or holding company/ proprietorship connected to bidder directly or indirectly has not participated in the bid process.	The bidder should submit letter of confirmation on the Company's letter head to this effect.
26	Any bidder (including OEM and OSD/OSO, if any) from a country which shares a land border with India will be eligible to bid, only if the bidder (including OEM and OSD/OSO) are registered with the Competent Authority. Bidder (entity) from a country which shares a land border with India means: a. An entity incorporated, established or registered in such a country; or b. A subsidiary of an entity	A declaration stating "We have read the clause regarding restrictions on procurement from a bidder of a country which shares a land border with India. We further certify that we and our OEM are not from such a country or if from such a country, has been registered with Competent Authority. We hereby certify that we and our OEM fulfills all requirements in this regard and are eligible to be considered" to be submitted in Company's letter head. [Where applicable, evidence of valid



	incorporated, established or registered in such a country; or c. An entity substantially controlled through entities incorporated, established or registered in such a country; or d. An entity whose beneficial owner is situated in such a country; or e. An Indian (or other) agent of such an entity; or f. A natural person who is a citizen of such a country; or g. A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.	registration by the Competent Authority shall be attached.]	
27	Authorization Certificate- Whether the Bid is authenticated by authorized person.	Bidder to submit a copy of the Power of Attorney or the Board Resolution and KYC documents evidencing the authority delegated to the authorized signatory.	

We confirm that the information furnished above is true and correct. We also note that, if there are any inconsistencies in the information furnished above, the bid is liable for rejection. All documentary evidence/ certificates confirming compliance to Pre-Qualification Criteria should be part of the RFP.

Date:
Place:

Signature with seal
Name:
Designation:



Annexure-10
Amended Technical Evaluation Criteria

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Ref: GEM/2024/B/5406710 dated 17/09/2024.

The technical evaluation of the bidder will be carried as per the details furnished below:

#	Evaluation Parameters	Documents to be submitted	Max marks	Marks Obtained
a.	<p>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.</p> <p>The SOC must be currently operational and running (a) 3 and above clients: 10 Marks (b) more than 1 and below 3 clients: 5 Marks</p> <p>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.</p>	<p>Bidder should provide the Satisfactory performance certificate from client and copy of purchase order/ contract agreement/ work order/ engagement letter/ Certificate of completion to this effect.</p>	10	
b.	<p>The OEM for SIEM must have supplied on-prem SIEM solution in BFSI/ PSU/ Government/ Private entities in India.</p> <p>Supply Experience:</p> <ul style="list-style-type: none"> Each reference of 80,000 EPS or 3.1 TB/ Day and above with minimum 400 branches/offices: 5 marks Each reference of 70,000 EPS or 2.8 TB/ Day and above: 4 marks. Each reference of 60,000 EPS or 2.4 TB/ Day and above: 3 marks. <p>Note: Max. 2 references will be considered.</p>	<p>OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/invoices.</p>	10	
c.	<p>The OEM for SOAR must have supplied on-prem SOAR solution in BFSI/ PSU/ Government entities in India.</p> <p>Supply Experience:</p> <ul style="list-style-type: none"> For 4 and above clients with minimum 5 Analyst/ User licenses having minimum 200 branches - 5 marks 	<p>OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.</p>	5	



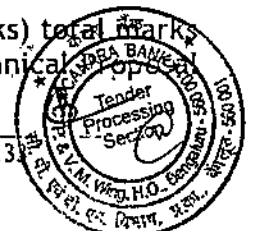
	<ul style="list-style-type: none"> For 2 clients with minimum 4 Analyst/ User licenses - 3 marks 		
d.	<p>The OEM must have supplied on-prem UEBA solution in BFSI/ PSU/ Government/ Private entities in India.</p> <p>Supply Experience:</p> <ul style="list-style-type: none"> Two references each of 15,000 endpoints having minimum 200 branches- 5 marks Two references each of 10,000 endpoints - 3 marks 	OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	5
e.	<p>The OEM must have supplied on-prem PIM/ PAM solution with 1000 privileged users in Banking segment in India.</p> <p>Supply Experience:</p> <ul style="list-style-type: none"> For 3 or more clients: 10 marks For 2 clients: 5 marks 	OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	10
f.	<p>The Bidder must have implemented/ managed EDR/ XDR solution in BFSI/ PSU/ Government/ Private entities in India.</p> <p>Implementation/ Management Experience:</p> <ul style="list-style-type: none"> For 3 clients of SaaS EDR/ XDR each with minimum 20,000 endpoints: 5 Marks For 2 clients of SaaS or On Prem EDR/ XDR each with minimum 15,000 endpoints: 4 Marks For 1 clients of SaaS or On Prem EDR/ XDR each with minimum 5,000 endpoints: 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.	5
g.	<p>The OEM must have implemented/ supplied SaaS EDR/ XDR solution in BFSI/ PSU/ Government entities in India.</p> <p>Implementation/ Supply Experience:</p> <ul style="list-style-type: none"> For 2 clients each with minimum <u>70,000</u> endpoints: 5 marks For 2 clients each with minimum 40,000 endpoints: 4 marks For 2 clients each with minimum 25,000 endpoints: 2 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.	5
h.	<p>The Bidder should have the experience in managing SIEM Solution in Organization(s) in India.</p> <p>Managing Experience:</p> <ul style="list-style-type: none"> For 2 clients each with minimum 1 lakh EPS or 4.0 TB/ Day: 5 marks For 1 client with minimum 1 lakh EPS or 4.0 TB/ Day: 4 marks For 1 client with minimum 50,000 EPS or 2.0 TB/ Day: 3 marks 	Bidder should provide the reference letter or email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.	5
i.	<p>The Bidder should have implemented or managed PIM/ PAM Solution in Organization(s) in India</p>	Bidder should provide the completion certificate/	5





	<p>Implementation/ Management Experience:</p> <ul style="list-style-type: none"> Each with 400 privileged users or 4000 servers - More than 7 clients: 5 Marks Each with 400 privileged users or 4000 servers - 3 clients to 7 clients: 4 Marks Each with 150 privileged users or 2000 servers - 2 clients: 3 Marks 	reference letter email from client along with copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices.		
j.	<p>Presentation by the Bidder:</p> <p>The broader outline of the presentation mentioned below:</p> <ol style="list-style-type: none"> Overview of the proposed solution Design Principle Implementation and Migration Strategy Implementation Plan Resource Planning SOC Maturity Roadmap Add-ons and Innovations 	The Presentation is as per the technical & functional requirement/ scope of work/ other terms as mentioned in RFP to the Bank.	25	
k.	<p>Resources:</p> <p>The bidder should have a minimum of 35 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CCNP Security/ <u>CompTIA Security Plus/ CEH.</u></p> <p>(a) >=75: 10 Marks (b) >= 50 and <75: 7 Marks (c) >=35 and <50: 5 Marks</p> <p>Note:</p> <ol style="list-style-type: none"> For CEH maximum 5 number of certified resources will be considered. <u>For one resource only one certification will be considered.</u> <u>Eg. If person 'A' has CISSP, CEH certifications it will be considered as one count.</u> 	Undertaking on bidder letter head needs to be submitted.	10	
c.	<p>The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions</p> <p>SIEM - 10 Proposed OEM certified resources PIM - 5 Proposed OEM certified resources SOAR - 5 Proposed OEM certified resources EDR - 5 Proposed OEM certified resources</p> <p>Note: All respective certified resources must be on direct payroll of Bidder.</p>	Bidder has to share the relevant certifications of the resources	5	
Total Marks			100	

Note: The bidder should score minimum 70% marks (i.e., 70 Marks out of 100 marks) for qualifying under Technical Evaluation. The bidders qualified under Technical Evaluation will be eligible for commercial opening.



Declaration: We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us, our response to this RFP is liable for rejection.

Date:
Place:

Signature with seal
Name:
Designation



Annexure-9
Amended Functional and Technical Requirements
 (Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of System Integrator for End-to-End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.
 Ref: GEM/2024/B/5406710 dated 17/09/2024.

Note:	
(a)	The specifications of proposed NG SOC system/ solution are detailed below. These specifications are only indicative but not exhaustive.
(b)	If the bidder feels that certain features offered are superior to what has been specified by the Bank, it shall be highlighted separately. Information regarding any modification required in the proposed solution to meet the intent of the specifications and state-of-the-art technology shall be provided. However, the Bank reserves the right to adopt the modifications /superior features suggested/ offered.
(c)	The bidder shall provide all other required equipment's and/or services, whether or not explicitly mentioned in this GeM bid, to ensure the intent of specification, completeness, operability, maintainability, and upgradability.
(d)	The bidder shall own the responsibility to demonstrate that the solution offered are as per the specification/performance stipulated in this GeM bid and as committed by the bidder either at site or in bidder's work site without any extra cost to the Bank.

The bidder should provide their response to the Technical and Functional Requirements by giving the compliance as Yes/ No. Explanations/ suggestions of the bidder against each requirement should be given in the Remarks column. If more explanation of a point is needed, documents can be attached to Remarks Column of the respective requirement.

All the below points are Mandatory/ Essential Technical/ Functional/ Features requirements. Non-compliance to any points shall lead to disqualification of the Bidder.

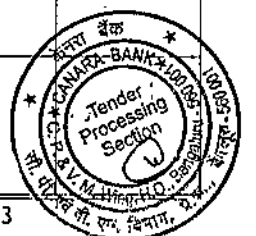
1. Technical Specifications of each SOC Solutions

1. Security Incident and Event Management (SIEM):

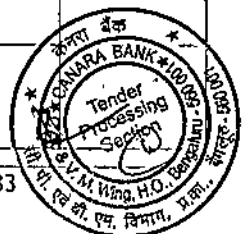
SI No	Technical and Functional Requirements	Compliance (Yes/No)	Remarks
Architecture			
1.	The proposed solution shall be hardware or software based with logically segregated into Collection, correlation, and Management layer. If the software appliance is proposed, the OEM shall provide all the required hardware to implement the solution		
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. Bidder must provide pricing for extra EPS required by bank during the contract period in bundle of 5000 EPS.		
3.	The proposed solution shall be capable of dual forwarding/ streaming/ replicating of raw logs from DC to DRC and vice versa. Storage must be arranged accordingly.		



4.	SIEM solution should support Disaster Recovery and sized for the DR site as well. The solution shall be sized to consider dual forwarding/ streaming/ replication from DC to DR and vice versa. Bidder shall provide necessary load balancer to distribute log ingestion across proposed log collectors (in DC and DR).		
5.	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. 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.		
6.	The solution must integrate with 3rd party directory systems as an authentication method. Solution should be integrated with LDAP or Active Directory solution for access provisioning to the SIEM system.		
7.	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 develop the parsers without any extra cost to bank.		
8.	SIEM solution should provide MITRE framework mapping and suggest TTPs across rules, alerts, and incidents		
9.	The solution must provide an open API mechanism to forward events /incidents /alerts to other platforms such as ITSM, SOAR, and any other SIEM solutions		
10.	The solution must use distributed computing to scale data collection and analytics and co-locates analytic processing with collection engines.		
11.	SIEM solution should have High Availability across all components within the system e.g., log collection, log correlation, management console etc. If it is required to have a LB to achieve the requirement, the OEM should factor the same also must have RAID redundancy (hard drives), Network Redundancy (Mgmt. interfaces), and Power-Supply module redundancy and 4x1G/10G network interfaces per server. (Bidder to explain architecture)		
12.	High Availability should use cluster set-up so that data could be shared between the nodes.		
13.	The solution collector must support the automatic load balancing and load sharing		
14.	The solution must have automated internal health checks and notify Bank in case of problems		
15.	The solution should have out of the box bi-directional integration with proposed SOAR solution.		
16.	The solution should not require additional license to deploy additional nodes/SIEM components i.e., for collection, processing, or HA requirements of the proposed solution.		
17.	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		
18.	The Proposed solution should have the capability to sync the use cases, configuration from DC to DR automatically.		
19.	The proposed solution must provide for secure user access via HTTPS, SSH.		
20.	The solution shall have out of the box parser for the log sources bank would ingest. If the solution does not have a parser for custom application/ log source the bidder / OEM shall develop and implement the same within the agreed timelines. The bidder shall ensure the		



	relevancy of the custom developed parser are maintained throughout the tenure of the contract		
21.	If the proposed solution has data replication functionalities, the same has to be achieved without relying on other third-party replication technologies on the operating system or storage level.		
22.	The solution should be able to integrate with incident management and ticketing tools like Service now, BMC, Proposed SOAR, UEBA, and TIP etc. but not limited.		
23.	The solution should have the ability to gather information on real time threats and zero-day attacks from anti-virus, IPS and IDS and analyses data against the information for any threats		
24.	The solution shall be able to provide the contextual enrichment for the parsed data to help triage alerts faster. This information can include details about the user, asset, IP address, geolocation, threat intelligence and vulnerability scan results.		
25.	The OEM must provide the sizing approach during the technical presentation.		
26.	The OEM shall provide Premium/Enterprise Support.		
27.	Solution must support STIX/TAXII and API method for consumption of threat intel feeds from different platforms. Also, it must have capacity to ingest custom threat intel feeds manually.		
Log Storage			
28.	The bidder 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.		
29.	SAN storage Systems should support Native Storage virtualization for centralized management and SAN Storage should support 99.99% Data Availability.		
30.	SAN Storages must Scale-Up & Scale out with support for intermix of different type of drives (NVMe SSDs, SAS SSDs).		
31.	No single point of failure, The SAN system should deliver Industry leading Performance at least 4 Lakh + IOPS and should be expandable.		
32.	End to End SAN Infra monitoring from a single management suite.		
33.	SAN system should support native remote replication for backup/DR purposes, i.e 2 way replication with Synchronous and Asynchronous		
34.	SAN system should allow intelligent compression & de-duplication per workload and can be disabled on non-compressible workloads.		
35.	The NAS system should be active-active architecture and should have unified capability i.e., should support block and file access with host connectivity for FC, iSCSI, CIFS and NFS. If external appliance required, it should be proposed with necessary licenses.		
36.	The NAS serving node should be purpose-built appliance and should not be a host based or running on general purpose OS or a simple SMB/ NFS configured file server.		
37.	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		
38.	The system must have dual controller and file system heads with automatic failover capabilities in case of one controller or head failure. The united component must be redundant against power supply, disk,		



	cooling fan and data path failures. The central storage system must support multi path automatic load balancing with no single point of failure.		
39.	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.		
40.	Storage should support in built Data Encryption, FIPS.		
41.	Minimum usable storage 1PB after RAID6/DRAID with 2 Nos of disk hot spare and later it should be expandable up to 2PB		
42.	Connectivity of Host and SAN should be through redundant SAN Switches (with SFP's) only as a part of Solution.		
Log Management			
43.	The Proposed solution should have capability to collect logs from different platforms like Microsoft Windows, Linux(All flavors) UNIX, MAC OS, AIX, Solaris, Firewalls, EDR, AV, WAF, Tenable - Nessus, Network devices, other security devices or solution, identified database servers, endpoint security management servers, web application firewalls, network firewalls ,Active Directory servers, Web servers, Private cloud (VMware, OpenStack) & cloud services (Aws/Azure/GCP/OCI), SAAS Solutions, O365, etc. as required by the Bank.		
44.	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		
45.	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.		
46.	Solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, IPsec, ODBC etc.)		
47.	The solution must support information (users, groups, etc.) collected from Directories (i.e., AD, LDAP) products.		
48.	The solution must not block, drop, or place grace period when system exceeds purchased EPS license/subscriptions limit		
49.	The solution must integrate with other security and network devices such as Firewalls, IPS, WAF, EDR, Switches, Routers etc.		
50.	Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage		
51.	Solution must be able to store logs in a separate system which would not be required to perform any real time correlation thereby minimizing the load on the Real time analysis.		
52.	Solution must provide agent-based collection of event logs preferably wherever not possible agent less log collection has to be provided without any additional license cost. Agent must be single lightweight agent. Solution must have a light footprint and agent based / agentless solution must have minimal/ no impact on performance of endpoints.		
53.	Solution must provide the ability to distribute both event collection and processing across the entire SIEM deployment.		





54.	SIEM shall support Connector Development tool/SDK /API availability for developing collection mechanism for home-grown or any other unsupported devices/ applications. The respective tool should be provided without any extra cost to Bank		
55.	The solution must ensure the communication between the SIEM components are encrypted		
56.	SIEM solution collector should forward the data to processing unit/component in real time without any delay.		
57.	The solution must normalize common event fields (i.e., usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network		
58.	The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
59.	The system should be able analyze logs with different event formats e.g., well-structured logs, natural language logs, multi-line logs etc.		
60.	The solution must provide a common taxonomy of events.		
61.	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields		
62.	The SIEM must provide searching & data/log management, including free form search.		
63.	The solution must provide near-real-time analysis of events.		
64.	The solution must provide more advanced event drill down when required.		
65.	The solution must provide a real-time streaming view that supports full filtering capabilities		
66.	The solution must provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, etc..		
67.	The solution must allow for custom defined tagging of events		
68.	The proposed solution should be horizontally scalable to support increase in EPS and should have global correlation capability on raw or metadata/normalized events (i.e., correlation of events if processed on multiple hardware/appliances)		
69.	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names		
70.	Solution should be able to define purging and retention rules for log storage.		
71.	The solution must monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes, then generate an alert (report / SMS /email). In the event of same device generating multiple device types of logs (For Example, same device generating Application logs and System logs), the log disruption should be identified properly without any false positives. Please describe how your solution meets this requirement.		
72.	The solution must provide an out of the box mechanism to discover and classify assets by system type (i.e., mail servers vs. data base servers) to minimize false positives associated with poor asset classification. Please describe how your solution meets this requirement.		
73.	The platform shall help to explore current and potential log source type MITRE-mapping coverage per rule, and suggest how the rule coverage can expand if new log source types are added to the environment.		
74.	Solution should do baselining of normal log ingestion rate regularly and alert for any unusual log ingestion rate(dips/spikes) per log source using ML/AI models.		



75.	The solution must allow the adding/modifying/removing of log parsers from UI console without impacting log collection.		
76.	The proposed solution must support the decoding of the common protocols/ports: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP, NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI and not limited to the above-mentioned ports/ protocols		
77.	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.		
78.	Solution should have ability to restore / replay older logs for reporting, analysis, correlation, investigation, and forensics.		
79.	Solution should support IPV6 format.		
Analysis			
80.	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events.		
81.	The solution must support and maintain a history of user authentication activity on a per asset basis.		
82.	The solution must support a web-based GUI for management, analysis, and reporting.		
83.	Solution should offer a global threat feed which must allow the analyst to perform search across various parameter like IPv4, IPv6, URL, vulnerability, Applications name, Malware, Spam.		
84.	Solution should allow analyst to perform manual ad-hoc check to determine if the organization is infected with any Zero-day attack.		
85.	There should be provision available to create complex searches by means GUI, to support advance investigation on the data available in the platform.		
86.	The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change.		
87.	The solution must provide alerting based on observed security threats from monitored devices and network activity		
88.	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors/loggers/aggregators.		
89.	SI proposed should provide capability to add the following systems for effective incident detection and correlation post completion of the SIEM deployment. a) Flow and packet-based threat Detection b) User Behavior analysis by Integration with flow analysis/ packet capture tool c) Threat Intelligence		
90.	The solution must provide the ability to correlate information across potentially disparate devices and flows information.		
91.	The solution must provide alerting based on observed anomalies and behavioral changes in network activity (flow) data. Describe any pre-packaged alerts and method for adding user-defined anomaly and behavior alerts.		
92.	The solution must observe anomalies other than just simple threshold basis		
93.	The solution must chain alerts into one single incident record, so when different rules are triggered and these activities are related with one single offense, then these triggers will generate only one incident record to avoid overloading the security operation team.		



94.	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)		
95.	The solution must generate and alert when a new service appears on the network or when new assets appear where they shouldn't or are not planned.		
96.	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
97.	The solution must provide UI based wizard/ capabilities to minimize false positives and deliver accurate results. Please describe how your solution meets this requirement.		
98.	The solution must limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.		
99.	The solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. Please describe how your solution meets this requirement. The solution should also have feature to capture analyst details who have worked analyzed/ investigate the alerts		
100.	The solution must support the ability to correlate against 3rd party security data feeds (i.e., geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically in the proposed SIEM solution. Please describe how your solution meets this requirement.		
101.	The solution must support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes. Please describe how your solution meets this requirement.		
102.	The solution must support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one-hour period of time. Please describe how your solution meets this requirement.		
103.	The solution must provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity. Please describe how your solution meets this requirement.		
104.	The solution must support historical correlation so users can re-run past events and flows on historical data, so new rules can be tested more precisely. Please describe how your solution meets this requirement.		
105.	The solution must be able to be updated regularly, to stay aware of the latest threat information and research available.		
106.	The solution must be able to analyze user activity to detect malicious insiders and determine if a user's credentials have been compromised.		
107.	The platform should Visualize alerts, network data, threats, malicious user behavior, and cloud environments from around the world in geographical maps, and auto updating charts.		
108.	The platform should offer an interface to help user in browsing the existing rule mapping across MITRE Framework & enabling them to map their custom rules to MITRE ATT&CK tactics and techniques.		
109.	The platform should offer user to tune their environment with the help of built-in analysis capability.		
110.	The platform should suggest new insights to prioritize the rollout of new use cases/apps to effectively strengthen the security posture.		



111.	The platform must automatically detect any logical or performance issues in the default or custom use cases/rules and provide a visual interface indicating the issue.		
112.	The platform must detect logical or performance issues, such as when a rule calls referenceable data but the object is blank for example: when a rule calls referenceable data of a bad process but the object/folder does not contain a list of bad processes.		
113.	The platform must detect logical or performance issues such as no rule referring to a data/object/folder.		
114.	The platform must detect any logical or performance-related issues. Such a rule uses a normalized event property/field, but the field is deactivated at the system level.		
115.	The platform must detect logical or performance issues, such as a rule that uses a performance-intensive test condition, such as regex or unparsed raw payload content, and so on.		
116.	The platform must provide information about the rules that are available with OEM (as part of the OEM update or content packs) but not deployed on the platform, as well as the name of the content pack and the coverage of the use case/rules from MITRE perspective.		
117.	Platform must be capable of Identify the topmost alert generating rules or event generating rules, and then provide the guide/steps to tune them.		
118.	Platform must help in Reducing the number of false positives by reviewing the most common configuration features like update network details, common reusable content, and server discovery based on recommendations		
119.	Should support integrating to Bank's existing VA tools (i.e., Tenable) bidirectionally to tag the offenses with list of vulnerabilities present in the associated assets of that offense.		
Reporting & Dashboard			
120.	The solution must provide a 'Dashboard' for quick visualization of security and network information.		
121.	The solution must support the automated distribution of reports		
122.	The solution must support the capability to provide historical trend reports.		
123.	Platform must provide capability to generate rules related reports from predefined templates, such as searches based on rule response and actions, log source coverage, and many others.		
124.	The platform shall support provision for dashboard specific to a single incident, which can offer various widgets, provision for sharing notes, representation of data in a graphical manner over a certain period and various rules triggered, rule s, model responsible in triggering of the offense.		
125.	The platform should allow to Import and export dashboards or share dashboard links with colleagues.		
126.	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, and generic APIs.		
127.	The platform should allow user to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates		
128.	The platform should allow user to Assign thresholds.		
129.	The solution must offer all the below built-in compliance modules out of the box at no additional cost but not limited to: a) PCI-DSS Compliance Module b) NIST c) GDPR Compliance Module		





	d) ISO Compliance Module and other regulatory bodies which is applicable to Bank		
130.	The proposed solution must offer all the reports out of the box at no additional cost		
131.	The proposed solution must have real-time visualization options, features and capabilities of the dashboard. A) Blacklist-based correlation. B) Whitelist based correlation		
132.	Proposed solution should have a dashboard to see the real time and history of EPS, Data sources integrated for the last 6 months		
133.	Solution should have option to check non reporting event sources and non-triggered/ zero hit use cases within the given timeframe		
134.	In case OEM supports Ingestion per day licensing then bidder has to provide scientific calculation sheet for EPS to Ingestion per day conversion by taking the average event size as <u>500</u> bytes for the sizing of solution on OEM Letter Head.		
Packet Capture			
135.	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, associated metadata and logs for 7 days. The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. Adequate storage shall be provisioned accordingly. The PCAP solution should also support selectively 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.		
136.	The proposed packet capture solution should ensure full packet and payload capture with network inflow/ outflow of data in DC& DR. Proposed solution should be a dedicated hardware with 2 X 1G/10G RJ45 and 6*10 Gig SFP+ slots for Fiber transmission and 1*1/10G management port.		
137.	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.		
138.	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 appliance and the storage should utilize Self-Encrypting Drives (SED). Should have OEM provided storage or 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.		



139.	<p>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 for sharing of network data (Packet + Meta data) in real time.</p> <p>Solution should create indexes for payload objects and not just rely on header information</p> <p>The solution should provide network traffic insight by,</p> <ul style="list-style-type: none"> • Classifying protocols and applications. • Reconstructed file such as a Word document, image, Web page and system files. • Full & Deep-packet inspection. • Cross correlation for Analysis & Aggregation. • Reconstruct sessions and analyze artifacts. • Preview artifacts and attachments. 		
140.	Solution should provide meaningful artefacts like email, FTP data files, 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.		
141.	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.		
142.	The solution should have the capability to extract data/ files from the captured network packets		
143.	The solution should have the functionality to reconstruct or replay with complete packet analysis of the network packets which will help to identify the entire transaction.		
144.	Solution should have the ability to support analysts by creating on the fly parsers from raw packet data captured and generate meta to trigger an incident (e.g., a future detection) without understanding how to create the parser.		

II. Security Orchestration and Automation (SOAR):

Sl. No	Technical Requirement	Compliance (Yes/No)	Remarks
Architecture, Integration & General Requirement			
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		
2.	All the hardware/ software etc. required for the solution shall be provisioned by the Bidder.		
3.	The solution must be able to support multi-tenancy.		
4.	The proposed solution should support High Availability in DC and DR site, the same shall be offered as part of the solution.		
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		

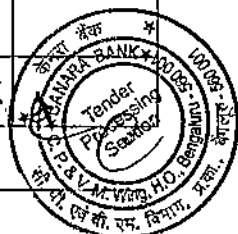




6.	The proposed solution should have Development environment where integration and playbooks shall be tested before deploying it to the production deployment.		
7.	The solution should be able to consume security alerts/incidents from SIEM, EDR, TIP, directly from any other Next Gen SOC and Cyber security solutions.		
8.	The solution should be able to provide bidirectional integration with All the solution and tools proposed as a part of Next Gen SOC		
9.	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.		
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		
11.	In solution there should not be any limit on number of playbooks and playbook steps or playbook execution or action execution		
12.	The solution should have the capability to integrate with banks Ticketing tool and ITSM tool (Service Now) to auto-assign incidents/tickets based on the type of alert/incident, asset owner/department, based on the availability of personnel in shift.		
13.	All the basic and advanced integrations with required playbook and connectors have to be provided by the Bidder/ OEM without any extra charge to bank. In case of new customizations, OEM has to provide, required professional services for 10 customized integrations with required playbooks and connectors every year or 50 customized integrations with required playbooks and connectors during contract period without any extra cost to Bank.		
14.	Solution should support Realtime ticket/incident mirroring feature OOB with Major ticketing systems like ServiceNow, Jira etc.		
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.		
16.	The solution should provide contextual analysis / quick reference into an indicator/object/event when viewing incident investigation data by auto-correlation with TIP, VM, EDR etc. without requiring navigating away from incident investigation.		
17.	AI Capabilities: - The solution should have capability to auto assign incidents/ tickets based on type of incident, asset owner, concerned department etc.		



18.	Chat/ Messaging capabilities: a. The solution should provide platform for users to discuss and collaborate. b. The solution should support auto documentation of chats/ actions.		
19.	The platform must provide capability to quickly integrate the existing security tools to generate deeper insights into threats, orchestrate actions and automate responses—all while leaving the data where it is i.e., using federated searches		
20.	Solution must be an open platform i.e., must connects tools like Qradar, ArcSight, Net witness, Splunk, ELK, CrowdStrike, carbon black, Azure Sentinel, Darktrace, GCP chronical, LogRhythm etc. for executing federated searches using prebuilt integration or/and have capability to build custom connections using an open-source python library.		
21.	The solution should be able to parse all necessary fields from proposed SOC solutions (SIEM, UEBA, NBA, PCAP) alerts, including but not limited to creation time, update time, source/destination IP, source country, category, system, rule-name, severity, etc.		
22.	The proposed solution should take response actions to Users like Password reset, Force Sign out, Disable User Account, etc.		
23.	The solution should provide visual representation of an incident, correlation of its elements, history of investigation and so on.		
24.	The Platform must support the integration with multiple 3rd party directory systems for authentication via SAML 2.0 etc.		
25.	The Platform must offer API's so that 3rd Party solutions such as ITSM tool can integrated with the platform and fetch/update alerts/cases/offense		
26.	The Platform must support Granular Role based access control. The administrator must be able to define role-based access to various functional areas of the solution. This includes being able to restrict a user's access to specific functions of the solution that is not within the scope of a user's role including, but not limited to, administration, reporting, incident assignment, playbook creation. Please describe how your solution meets this requirement.		
27.	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		
Analysis and Incident Management			
28.	The platform should provide a single, integrated platform for analyzing log, flow, vulnerability, user and asset data providing full visibility into all networks, applications, and user activity.		
29.	The Platform must support documenting Investigation notes/outcome and presented it in chronologically order.		
30.	The Platform must support export Investigation notes/outcome in pdf or csv format.		
31.	The Platform must provide information in such a way that analysts can quickly understand the source and impact of an attack, enabling teams to respond more effectively		
32.	Platform must have inbuilt Ability to gather actionable IOC based on the organization vertical/Geo and then run automated searches for related indicators of compromise across different datastores in the organization like SIEM, EDR, NDR, Data Lake etc.		
33.	OEM should integrate the threat Intelligence feeds with SOAR to check threat score, reputation etc.		





34.	The Platform provides a visual representation of enriched information HTML, markdown, feature-rich GUI.		
35.	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.		
36.	The Platform must support the creation of custom incident types, artifact tagging and any additional custom fields as you see fit.		
37.	The proposed platform must have built-in MITRE ATT&CK alignment for all the Automated/manual based investigation and should overlay the playbooks depicting the coverage against MITRE ATT&CK TTPs.		
38.	The solution must be able to create incident by parsing email notification.		
39.	The solution must provide UI based wizard to manually create incidents.		
40.	The solution must be able to support creation and deletion of automated incidents via API, Web URL, SIEM, Ticketing System.		
41.	The solution must be able to automatically extract email attachments from emails and store that for the related incidents as attachments.		
42.	The solution must be able to support storing of incident related files not limited to malware specimens, logs, screenshots.		
43.	The solution must include out-of-the-box playbooks based on SANS and NIST for incidents like Malware, Phishing, DOS and should support creation of multiple playbooks based on the SOC's Use case.		
44.	The solution must be able to provide incident response playbooks that consist of phases and tasks that guides the user on how to adequately response to the incident; integrating people, processes and technology.		
45.	The solution must provide a visual workflow editor to enforce sequencing of incident response activities.		
46.	The solution must include an in-product script editor with <u>autocomplete and syntax highlighting/GUI Driven Engine</u> , to support automation of incident response workflow.		
47.	The solution must include an in-product script editor with <u>run buttons/GUI Driven Engine</u> to facilitates debug and perform tests on scripts.		
48.	The solution must allow organizations simulate incidents, to test response plans, allowing them to identify gaps and refine processes before a real incident happens.		
49.	The Proposed Solution should have out-of-the-box bi-directional integration with the proposed SIEM solution & App on both platform (SIEM & SOAR)		
50.	The proposed solution should have out-of-the-box provision of closing incident simultaneously on SIEM and the proposed SOAR platform.		
51.	The proposed solution should have out-of-the-box capability to query or add IOC/Artifact to existing watchlist of the deployed SIEM solution.		
52.	The Proposed solution should have web-based application store which should host latest integrations available from the OEM this integration can be downloaded with no additional cost.		
53.	The proposed solution should have community portals and knowledgebase which can be used to learn about sample integration and forum to discuss issue or use cases.		
54.	The solution should have bidirectional integration capability with proposed SIEM solutions i.e., create case/ticket/incident from the alert raised by SIEM/ EDR, pull raw logs from SIEM/EDR, pull information		

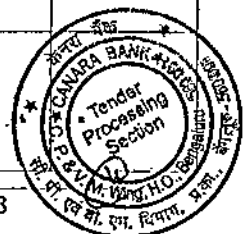


	related to rules triggered the alert, pull asset vulnerability details, update alert in SIEM/EDR and close SIEM/ EDR alert.		
55.	The solution should have capability to create flexible, multi-conditional and complex workflows		
56.	The solution should allow creation of manual tasks, automated tasks, combination of both and conditional tasks in playbooks		
57.	The solution should also allow scheduling and customization of tasks.		
58.	The solution should provide capability to embed scripts (Python or any other language) in the playbooks.		
59.	The solution should be capable to provide automated detailed post incident report about all the actions taken, root cause, collaborative actions/chats etc.		
60.	The solution must support creation of workflow which can have multiple task which can be executed sequentially or parallelly where parallel task can be executed independently while sequential task will depend on closure of previous task. In case any task or workflow encounter any issue, same should be displayed on the tool as part of status.		
61.	Solution should provide analysis about failed tasks/workflow in the UI itself		
62.	SOAR solution must allow analyst to create multiple playbooks and allow them to be manually or automatically saved with different names or versions		
63.	The solution should allow for viewing playbook name/version history for all or selected playbook either within the system or outside the system and provide option for restoring to an older playbook.		
64.	The solution must provide central management of incidents and administrative functions from a single web-based user interface. Please describe how your solution meets this requirement.		
65.	The solution must support the ability to correlate against 3rd party security data feeds (i.e., geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.		
66.	The solution must dynamically augment incident playbooks in real time to support a specific incident response workflow. Please describe how your solution meets this requirement.		
67.	The solution must provide the ability to contextually link incidents with similar artifacts.		
68.	The solution must provide the means for analysts to review the enrichments performed on the incident to arrive at conclusions about a security incident.		
69.	The solution must out-of-the-box integrate with external threat intelligence feed providers to provide data enrichment of incident artifacts.		
70.	The solution must, out-of-the-box, must provide visualization of incident correlation across IOCs and other artifacts automatically with timeline support.		
71.	The solution must allow users to take remedial steps directly from within the visualization of incident correlation enabling a rapid and efficient response.		
72.	The solution should offer graphical representation of all the artifact associated to a particular incident along with the timeline. It should enable the analyst to take action from withing the graphical view on any artifact i.e., this could be blocking a IP address or doing further investigation using any of the threat service available to solution.		





73.	The Solution should offer Timeline graph for each incident allowing display that can be set to display days, weeks, and months. It should also allow analyst to add milestones to call out important events within the timeline. Where the analyst can add a date, title, and description of your milestone.		
74.	The solution should allow adding custom table to incident layout allowing organization to track relevant fields based on use case. Such as Approval flow, Response time, Actions performed to name a few.		
75.	The solution must offer out-of-the-box support for auto creation of incident artifacts. Please describe how your solution meets this requirement.		
76.	The solution must be able to support logical segregation of incidents. This will be used to assign a specific group of incidents to a specific group of users/analysts		
77.	The solution must enable to delegate tasks to another user and to assign due dates		
78.	The solution must be able to support creation of Knowledge portal. This enables organizations to add important information, guidelines, and reference material for the Incident Response team.		
79.	The solution must provide long term trend analysis of incidents. Please describe how this requirement is met by the solution.		
80.	The solution must provide more advanced incident drill down when required. Please describe how this requirement is met by the solution.		
81.	The solution must provide the ability to correlate artifacts across potentially disparate incidents. Please describe how your solution meets this requirement.		
82.	The solution must support the ability to trigger action on external systems, for a related to an incident. For example, the solution should support the ability to block an intruder. Please describe how your solution meets this requirement.		
Reporting & Dashboard			
83.	The solution must support a web-based GUI for management, analysis and reporting. Please describe how your solution meets this requirement.		
84.	The solution must provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. Please describe how your solution meets this requirement.		
85.	Provide automated reports and dashboards for real-time measurement of key performance indicators (KPIs) such as MTTD and MTTR for overall SOC		
86.	The solution must deliver sample dashboards out-of-the-box (not limited to - Incident Over Time by Type, Open Incidents by Phase, Close Incident by Duration). Please describe how your solution meets this requirement.		
87.	The solution must deliver customizable dashboard widgets that can present relevant incident information to the users. Please describe how your solution meets this requirement.		
88.	The solution must maintain a database of incidents. The user must be able to search this database.		
89.	The solution must support and maintain a history of user activity per incident. Please describe how your solution meets this requirement.		
90.	The solution must provide reporting templates, to report on incident information, for the management team as well as the IT Security team via the GUI. Describe how the solution provides the ability to configure reports.		



91.	The solution should support reporting templates where users can add content blocks with preconfigured text or visual elements, such as charts, images, tables, and saved graphs, or placeholder sections that users can fill in after they create a report from the template		
92.	The solution must provide configurable reporting engine for customized report creation. Please describe how your solution meets this requirement.		
93.	The solution must support importing and exporting of configuration settings.		
94.	The Solution must support a flexible dashboard environment that allows users to leverage searches and views that can easily be deployed to a user's workspace.		
95.	The solution should serve as end-to-end incident management, incident response, investigation platform and single evidence repository		
96.	The Solution should provide ticketing functionality for the security team/IR team		
97.	The Solution should be able assign an incident to a user or a team		
98.	The solution shall have feature to configure SLAs pertaining to MTTD, MTTR, MTTC and have capabilities to notify respective incident owner/ manager for any potential SLA breach through SMS, email		
99.	The solution should be able to set reminders for tasks		
100.	The solution should be able to group incidents (e.g., Malware outbreak with time delay, every incident with this malware in one parent incident)		
101.	The solution should have customizability available for incident management		
102.	The solution should offer any auto-casing / auto-population based on the incident type or other relevant incident attributes		
103.	The solution must provide tagging capabilities on tickets. Tags must be customizable.		
104.	The solution must be able to aggregate information from past investigations on the ticket (such as link to a data source, comments, involved analyst, etc.)		
105.	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)		

III. User Entity Behavioral Analysis (UEBA):

Sl. No	Technical Requirement	Compliance (Yes/No)	Remarks
Architecture & General Specifications			
1.	The proposed solution is required to be deployed at on-premises. The bidder is required to size all the component for the solution proposed. If there is any performance issue during the contract period, bidder is required to provide software / hardware at no additional cost to the Bank		
2.	Proposed UEBA should be from the same OEM of the proposed SIEM solution.		
3.	The solutions deployed should be modular, scalable and should be able to address Bank's requirements for the next five years, with the deployed hardware and software.		





4.	The architecture should have High Availability in inbuilt into the product. The solution shall be deployed at Data center and Disaster Recovery Center of the Bank in high availability		
5.	The solution shall have 90,000 User & Entity licenses and procure additional licenses as per the requirement without compromising on system functionality or performance and OEM to provide unit price which shall be leveraged to place additional order as required during the tenure of the contract		
6.	The solution shall be sized to maintain six months data online		
7.	The solution shall have native integration available with existing AD, ServiceNow ITSM and proposed SIEM, SOAR.		
8.	The solution should have role-based access control. It should support SMS, Email and App based MFA		
Analysis			
9.	The solution should leverage Artificial Intelligence and machine learning for detecting anomalies.		
10.	The solution shall be able to detect risky and potentially abnormal user activity within the Bank's network such as but not limited to privilege escalation, lateral movement etc.		
11.	The solution shall be able identity threat behavior such as account hijacking and abuse of user accounts		
12.	The solution must be able to detect when strange users access a specific host, learn what users connect with specific assets such as a point-of-sale terminal and then alert when new users login.		
13.	The solution shall provide high privilege access anomaly detection for misuse, sharing, or takeover user accounts		
14.	The solution shall have self-learning behavioral analysis and dynamically model to identify any anomalous activity that falls outside of the normal pattern		
15.	The solution shall use unsupervised or 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.		
16.	UEBA should activate a rule for a set of users until a specified condition or specified time window.		



17.	The solution should leverage Machine learning to perform analytics to gain additional insight into user behavior with predictive modelling.		
18.	UEBA should perform the below mentioned scenario's as well.		
	Use Case for UEBA: Access and Authentication		
	Account accessing more high value assets than normal		
	More data being transferred then a normal to and from servers and / or external location		
	Privileged account accessing high-value servers from a new location for the first time		
	Account used for the first time in a long time		
	Rare privilege escalation		
	Accounts being used from peculiar locations,		
	User involved in previously malicious or threatening behavior		
	User an outlier within their peer group.		
19.	Exfiltration:		
	Data Exfiltration by Print		
	Data Exfiltration by Removable Media		
	Data Loss Possible		
	Initial Access Followed by Suspicious Activity on critical servers		
	Large Outbound Transfer by High-Risk User		
	Multiple Blocked File Transfers Followed by a File Transfer		
20.	Browsing behavior:		
	Browsed to Entertainment Website		
	Browsed to Gambling Website		
	Browsed to Information Technology Website		
	Browsed to Mixed Content/Potentially Adult Website		
21.	DNS Analysis		
	Potential Access to Blacklist Domain		
	Potential Access to DGA Domain		
	Potential Access to Squatting Domain		
	Potential Access to Tunneling Domain		
22.	Admin/Activity Based		
	Anomalous Account Created from New Location		
	User Access from Multiple Locations		
	User Geography Change		
	User Geography, Access from Unusual Locations		
Dashboard and Reports			
23.	The solution shall provide customizable dashboards, configurable policies, and risk model optimization		
24.	The solution shall provide various visualization options for deep-dive investigation, compliance, and reporting		
25.	The solutions shall have a "Single-pane-of-glass" view into high-risk user/ entity showing behavior pattern with respect to activities, locations, devices, sessions, usage, and risk trends		
26.	The solution shall enable bank to export report in CSV, Email, PDF format		
27.	The solution should have ability to schedule the report.		
28.	UEBA UI/panel should be integrated in SIEM dashboard. Thus, which will help in monitor desired elements of users' behaviors, risks, and trends from a single screen.		





29.	The solution should provide Privilege Access Intelligence via Access information & Activity Log to alert most Risky events as per device, User, Access, and behavior.		
30.	The solution should support contextual natural language search for query, investigation & threat hunting purpose. It should provide baselines, Peer Groups (Static & Dynamic) Analysis and User contextual Data while doing the investigation.		
31.	The solution should provide 360-degree view and single pane of glass for user/entity activities across all resources using linked analysis. The tool should be capable to provide Risky Activities, Anomalies/Outliers, Risk profiling, Asset & Device Usage, Transaction Timeline, MITRE ATT&CK Mapping information, Incident Information, Access & Peer Group Information as a single view, for quick analysis. This 360-degree view should be exportable as a Report with above mentioned information.		
32.	The solution should provide Cyber Kill chain mapping using the MITRE ATT&CK framework and suggest remediation.		
33.	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.		
34.	The solution should support the creation of personalized Dashboards & Sharing of Dashboards & Queries with specific Users & Roles (SOC Analyst, Auditor etc.).		
35.	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.		
36.	The solution should support bidirectional integration with core NGSOC solutions (SIEM, SOAR, threat Intel etc.)		
37.	The OEM shall be able to support Premium/Enterprise Support.		

IV. Endpoint Detection and Response (EDR):

Sl. No	Technical and Functional Requirement	Compliance (Yes/No)	Remarks
Architecture & General Requirement			
1.	The solution offered as SaaS platform with DC and redundant site shall be hosted in India to ensure data localization		
2.	The platform shall offer for 99.90% uptime		
3.	The vendor shall provide the list of telemetry data EDR agent collects on their letter head. It shall have a feature for Bank to disable sensor to control data collections as necessary		
4.	The OEM shall have necessary compliance certifications such as ISO 27001:2022 or SOC 2 Type II. The certification copy shall be produced if requested by the Bank		
5.	The OEM shall provide the Premium support		
6.	OEM shall perform half-early review of the deployed solution to cover the following but not limited to and provide a report suggesting the best practices 1. Architecture Review 2. Policy review 3. Agent Management Review 4. Exception reviews All the observations from OEM assessment/ regulatory audits/internal audits shall be closed by the bidder within the		



	defined SLA mentioned in the RFP, if there is any dependency on OEM, OEM shall support closing the identified issues without any additional cost to bank.		
7.	The solution shall size to store all telemetry data (including applicable forensic data) for 30 days and for incidents & alerts data 180 days on cloud		
8.	The OEM shall provide licenses for 85,000 endpoints and 5000 servers (which can be used interoperable) and have the fixed unit price for the entire duration of the contract which can be leveraged by the Bank to place additional order based on the requirement		
9.	The proposed OEM should have full-fledged operations along with a dedicated Technical Support Center running in India		
10.	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.		
11.	The proposed OEM offers comprehensive product lines/integration from hybrid cloud, endpoint, email and network security solutions geared towards layered security approach		
12.	The proposed solution should be hosted in India region to address the data sovereignty and localization. OEM or Bidder should have alternate infrastructure support arrangements available in India in case primary facilities are not available.		
13.	The proposed solution should not allow the user to uninstall or disable agent and should have password protection to disable configuration changes/ uninstall by unauthorized personnel/ malware.		
14.	The proposed solution should also support to install/ uninstall supported 3rd party security agents.		
15.	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.		
Threat Detection and Prevention			
16.	The solution should identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, crypto miners.		
17.	The solution should identify malicious behavior of executed files, running processes, registry modifications, or memory access and terminate them at runtime, or raise an alert (exploits, file less, Macros, PowerShell, WMI, etc.)		
18.	The solution should support the creation of rules to exclude specific addresses/IP ranges. Configure detection rules, policies, and response actions within the EDR solution.		
19.	The solution should identify and block privilege escalation, reconnaissance attacks (scanning).		
20.	The solution should identify, and block credential theft attempts occurring in memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).		
21.	The solution should identify user account malicious behavior, indicative of prior compromise, malicious interaction with data files, data exfiltration.		
22.	The solution should identify and block usage of common attack tools (Metasploit, Empire, Cobalt etc.).		
23.	The solution should support the display of entity and activity data, dynamic analysis (sandbox) and the means to execute forensic investigation.		





24.	The solution should support isolation and mitigation of malicious presence and activity on the endpoint, via remote operations.		
25.	The solution should support incident response automation.		
26.	The solution should include threat hunting		
27.	The solution should collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner.		
28.	The solution should rate the severity of security alerts.		
29.	The solution should automatically assign a risk score/severity to all objects in the protected environment.		
30.	The Endpoint Security Solution should be using a blend of AI/ML based advanced threat protection & detection techniques to eliminate threats entering in to bank network services to be delivered via an architecture that uses endpoint resources more effectively, preserve and optimize CPU, network utilization to their lowest value.		
31.	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.		
32.	The solution should be able to identify vulnerabilities with highly accurate machine learning - pre-execution and runtime, application control & EDR features.		
33.	The solution should support scheduled or on-demand scanning of endpoints/servers to detect known and unknown viruses and threats.		
34.	The Solution should have Automated Malware Analysis capabilities and real-time threat detection.		
35.	The solution should be able to detect and prevent hidden exploit processes that are more complex than a simple signature or pattern and evade traditional AV.		
36.	The solution should have strong anti-evasion capabilities. It should also accurately identify evasion capabilities of malware such as evasion by detecting sandbox environment.		
37.	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: <ul style="list-style-type: none"> • 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 		
38.	The solution should identify and block privilege escalation attacks Specially root level attacks like rootkit, boot kit or any other such malwares and provide Process monitoring mechanism.		
39.	The solution should be able to pinpoint the origin of attack and provide the entire attack path.		

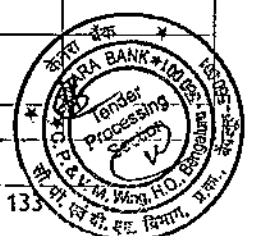


40.	The solution should collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner such as Eliminate the need of manual configuration of rules or policies or reliance of additional devices.		
41.	The solution should support isolation and mitigation of malicious presence and activity, locally on the endpoint.		
42.	The solution should allow Ingesting or fetch Indicators of Compromise (IOC) from third-party sources automatically.		
43.	The solution should Utilize both signature or signature-less detection and prevention techniques		
44.	The solution should detect and prevent memory based and/or file-less attacks		
45.	The solution should Contain the incident at the endpoint via automated actions and/or manually implemented by security analyst or other appropriate personnel		
46.	The solution should be able to provide a full attack process tree to track/identify all affected machines/patient zero		
47.	The solution should continuously record events on the endpoints and provide appropriate means of storage for later retrieval and forensics investigation		
48.	Analysts should be able to conduct RegEx, File, Hash, and value search across all endpoints.		
49.	Analysts should be able to review malicious activity and validation including analysis, tagging, notes, and workflows		
50.	The solution should be capable of basic forensic capabilities such as memory analysis, disk analysis, user and entity behavior analysis, and historical process mapping		
51.	The solution should provide SECURE LOG-IN using Multifactor Authentication		
52.	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		
53.	The solution should have a stateful attack analysis to detect the entire infection lifecycle and trace stage by stage analysis of the advanced attacks from system exploitation to outbound malware communication leading to data exfiltration.		
54.	The solution should detect and handle the presence of malicious files that have been written to the systems but not executed.		
55.	The solution should have capability to analyze obfuscated and encrypted malware.		
56.	The solution should have the ability to specify a list of alert exclusion rules for the selected objects.		
57.	The solution should provide protection from key loggers.		
58.	The solution should allow to configure different policies for different set of processes.		
59.	The solution should leverage file repudiation service such as prevalence, source, and age etc. to detect and prevent execution of malware files.		
60.	The solution should support device control to allow/ block USB devices that are connected to endpoint.		
61.	The solution should provide policy inheritance exception capabilities.		
62.	The solution should have the ability to lock down a computer (prevent all communication) except with management server.		





63.	Memory footprint - cache and signature database size should be limited and minimum, solution should have ability to deal with agent bloat problem, should have capability to take optimal use of network resources (for updates and intra VM communication for intelligence sharing (if any).		
64.	Memory monitoring - While the process is running in the memory, its behavior is observed to decide if it could be a virus.		
65.	Solution should support Single integrated workflow to analyze and respond to threats within Endpoint Security. Solution should support Enterprise Security Search to rapidly find and illuminate		
66.	The solution should support Data Acquisition to conduct detailed in-depth endpoint inspection and analysis over a specific time frame.		
67.	The solution should automate the complex, multi-step investigation workflows of security analysts from Historic data.		
68.	The solution should support to build AI / ML based intelligent models and databases to quickly expose suspicious behaviors, unknown threats, lateral movement, and policy violations		
69.	The solution should have outbreak prevention feature by blocking on the propagation techniques.		
70.	The solution should support remote shell to the machine to mitigate a malicious activity this includes network isolation, and remote access etc.		
71.	The solution should support the scanning of all the endpoints immediately after deployment of any new model/engine and signature on all the endpoints for presence of the malwares hitherto. The solution should also support various scanning options to clean dormant malwares - Real time scan, Scheduled Scan and on Demand Scan		
72.	The solution should have capabilities to detect/prevent/block/quarantine/clean all kind of cyber threats by EDR such as <ul style="list-style-type: none"> • Anti-malware • Rootkits/ grayware scanning for file system to prevent or stop spyware execution. • Should have capabilities to restore spyware/grayware if the spyware/ grayware is deemed safe. • Behavior Monitoring. • Device Control. • Real Time Scan Suspicious connection services 		
73.	The solution should be able to identify suspicious embedded object in document file like OLE & Macro extraction, Shell code & exploit matching.		
74.	The solution should show the assigned confidence/score in terms of Percentage/severity in the ML based detection logs.		
75.	The solution should have behavior monitoring module to constantly monitor endpoints for unusual activity in operating systems and installed applications.		
76.	Solution must support creation of rules to exclude specific addressed/ IP ranges and provide capability for Blacklisting malicious IPs/domains.		
77.	Solution must identify and block/alert on lateral movement (SMB relay, pass the hash)		
78.	Solution must have a Vulnerability visibility and Protection feature.		



79.	Solution must have multiple techniques to address known, unknown, patched, unpatched threats with pattern/ signature based, behavior monitoring.		
80.	The solution shall have the feature of manually submitting the suspicious file samples which includes but not limited to Executables, Microsoft Office files, PDFs, Scripts, and binaries to sandbox for further analysis. If required, the Bank shall be able to submit unknown samples to OEM's research team for deeper investigation		
81.	Solution should deliver the multi-vector protection in the industry across a variety of endpoints, including end-of-support (EOS) operating systems.		
82.	The proposed solution shall be able to submit suspicious file samples manually for automated analysis.		
83.	The proposed solution console should support automatic sweeping tasks based on curated intelligence and manual sweeping tasks against custom intelligence to search the environment for IoCs.		
84.	The proposed solution shall be able to view information that has been obtained by analyzing the objects in the sandbox from EDR console		
Management Server, Agent and Reporting			
85.	The solution should support rapid and seamless installation across all endpoints and servers in the environment.		
86.	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.		
87.	The solution should have a light footprint for minimal impact on the endpoint/server performance.		
88.	The solution should provide encrypted communication between the central EDR server and the agents on the endpoints or servers.		
89.	The solution must have control over the Endpoint version push across bank infrastructure		
90.	The solution should support connection to Active Directory.		
91.	The solution should co-exist with all commodity and proprietary software on the endpoints/servers and provide seamless operation of the protected endpoint/ server without bluescreens or process crashes.		
92.	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.		
93.	The solution should provide full protection for endpoints and servers that are roaming and connected over internet.		
94.	The solution should ensure roaming agents should also report to the central console over internet all the time.		
95.	The solution should support deployment on multiple sites that report into a single management console.		
96.	The solution should support exporting the current configuration and import it later to the same or another computer.		
97.	The solution should allow enable/disable certain types of notifications.		
98.	The solution should centrally collect and process alerts in real-time.		
99.	The solution should support central distribution of updates with no user intervention and no need to restart endpoint or server.		
100.	The solution should support the 100% logging of events, alerts and updates.		





101.	The solution should support integration with email infrastructure to notify security personnel in case of alert		
102.	The solution should support integration with bank on premises proposed SIEM for ingesting all logs, proposed SOAR for getting all alerts and incidents, Bank's ITSM solution (Service Now) etc. products.		
103.	The solution should have feature to install/ enable and uninstall/ disable agents from the console.		
104.	The proposed solution should have the process for reviewing and redeploying malfunctioning agents must be ensured.		
105.	The solution should have option to configure policies based on the location of the endpoint, Desktop-wise and Server-wise. It should also have capability to create department wise or application-wise policy groups for servers and endpoints.		
106.	The solution should have feature to configure client communication interval which defines how often endpoints report their status and policy updates to central management console.		
107.	The solution should provide proactive, immediate notifications of serious system health issue for the solution.		
108.	The solution should facilitate manual or automatic quarantining of the system from the rest of the enterprise network, as well as kill and quarantine specific processes and malicious artifacts		
109.	The solution should provide functionality to automatically backup and restore files changed by the suspicious program.		
110.	The solution should continuously collect data on all the entities and their activities within the environment.		
111.	The solution should ensure all the binaries from the OEM (Vendor or system) that are Downloaded and distributed must be signed and signature verified during runtime for enhanced security.		
112.	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, 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.		
113.	The solution should provide all listed features of proposed Endpoint security solution in a single lightweight agent. Solution must have a light footprint and agent based / agentless solution must have minimal /no impact on performance of endpoints.		
114.	The solution should be able to defend endpoints on or off the Bank's network against ransomware, malware, Trojans, worms, spyware, ransomware, and adapts to protect against known / unknown variants and advanced threats like crypto malware, fileless malware and macro-based malware in order to detect and respond to the ever-growing variety of advanced malware threats, including file and fileless attacks and ransomware.		
115.	The solution should provide agent self-protection/Tamper-Protection to be configured via GUI or CLI.		
116.	The solution should support Central Management server of the Endpoint Security should be able to monitor the status of EDR service on the endpoints.		
117.	The solution should ensure Management console should have an option of various alerting methods such as SIEM, Email / SMS etc., integration.		



118.	The solution should ensure Management console should support API integration.		
119.	The solution should support Reporting options such as Scheduled/ on demand/Custom in CSV / PDF, or any other format desired by the Bank.		
120.	The solution should have ability to forward events to bank's on-prem SIEM system or centralized logging server for eventual correlation, reporting and archiving.		
121.	The solution should ensure Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.		
122.	The solution should have the ability to enable/disable certain types of notifications and must provide a central collection and processing of alerts in Realtime.		
123.	The solution should ensure Supporting common security integrations such as APIs etc.		
124.	The solution should provide timeline threat graphic views to deliver guided investigations for analysis of a wide range of skillsets along with virtual asset tagging		

Incident Management and Compliance

125.	The solution should provide the means to conduct Inventory Management.		
126.	The solution should cover incident response processes and workflows.		
127.	The solution should correlate endpoint detections with network and threat intelligence and vice versa.		
128.	The solution should ensure that the data at rest and data in transit should be encrypted as per best practices and also in line with Bank's Information Security Policy guidelines.		
129.	The proposed SaaS solution shall be SOC 2 Type 2 certified. The OEM shall provide valid certification copy to Bank for valid verification.		

Sandbox

130.	The proposed Sandboxing component should have the capability to scan the file size up to 50 MB.		
131.	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.		
132.	The AI-ML model-based or sandboxing should be able to overcome malware evasion techniques like staling code, blind spot, and environmental checks.		
133.	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.		

V. Privileged Identity Management (PIM)

Sl. No.	Technical Specification	Compliance (Yes/No)	Remarks
Architecture & General			
1.	The solution shall be deployed onsite in Bank's data center. The solution shall be cloud ready for future use		
2.	The proposed solution shall provide multi-tier architecture where the database and application level are separated		





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		
4.	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.		
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.		
6.	The bidder shall maintain 99.90% uptime and ensure all the hardware and software are part of the solution to meet the requirement		
7.	The proposed solution shall provide scalability where it is not limited by the hardware. Also, the solution shall provide modular design for capacity planning and scalability metrics		
8.	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption		
9.	The licenses shall only be applicable to the number of servers and the privileged users count asked in the RFP, there should not be any licensing limitation on the concurrent connections or password rotations.		
10.	The solution shall retain six months logs and video recording		
11.	The solution shall have feature to integrate with external storage such as SAN and NAS to store logs / video recordings		
12.	The solution shall have a secure password storage/vault and should have limited remote access to vault		
13.	All communication between system components, including components residing on the same server should be encrypted.		
14.	The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments		
15.	The solution should provide a method for creating new connectors with minimal intervention required from OEM.		
16.	The solution shall have a single console for unified administration and management of accounts/devices configured in DC and DR		
17.	The access to administrative console shall be restricted only from authorized client IP addresses.		
18.	The solution should enforce segregation of duties ensuring Administrators do not have access to view the password by default. The bidder has to configure a workflow to ensure necessary approval has been obtained before invoking show password.		
19.	The solution should have Auto-Onboarding/ discovery Feature for both User and Devices without having to do any manual activity and perform two-way reconciliation		
20.	The proposed solution shall have built-in options for backup or integration with existing backup solutions		
21.	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically		
22.	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution		
23.	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location		



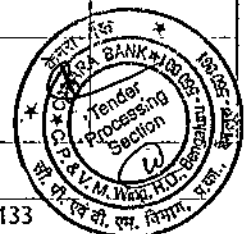
24.	The proposed solution shall support both clients based (in the case where browser is not available) as well as browser-based administration without any extra cost to bank.		
25.	The solution should support multiple active instances with load balancing and fully automatic failover at each component level to another active instance.		
26.	The solution should be able to integrate with enterprise authentication methods e.g., LDAP, RADIUS, and a built-in authentication mechanism.		
27.	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.		
28.	The solution should provide for self-service portal for users and devices for ease of on boarding both users and devices.		
29.	The solution shall have feature to manage system and application-level privilege accounts. OEM to support application integration		
30.	The solution should have feature to integrate with hardware and software tokens		
31.	The solution should have feature to integrate with SIEM, SOAR and ITSM systems		
32.	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.		
33.	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords		
34.	The solution should be able to onboard various systems including operating system accounts (Windows, Unix/Linux, Customized OS) and other infrastructure assets like Network devices, databases, application servers, etc.		
35.	The Solution Should support integration with devices like, Routers, Switches, Firewalls, UTM devices, NIPS, DDoS appliances, SIEM, HSM, WAF devices and Load Balancers for Web UI, GUI and CLI.		
36.	The solution should be able to integrate with a solution that provides a ready stack of APIs to help integrate with any HR or other such solutions that is the source of truth for identities within the organization.		
37.	The solution should be able to onboard the Organization structure from a directory store for ease of administration and be able to automatically onboard users into the privilege access management solution. The auto-onboarding capability should also be available for public cloud directories like AWS, Azure, GCP etc.		
38.	The solution should be able to identify orphan accounts on any target assets including auto-discovery of privileged accounts and reconciliation		
39.	The solution should be able to map privileged and personal accounts on various target systems		
40.	The solution should be able to identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key-related data, and ascertain the status of each key.		
41.	The solution should be able to integrate with public cloud infrastructure.		
42.	The solution should provide access to end-users based on least privilege principles. and then grant the user the ability to elevate users access based on certain roles and access approval methodologies with inbuilt dynamic workflows.		

Secret Management





43.	Secured Vault platform - main password storage repository should be highly secured (hardened machine, limited and controlled remote access, etc.)		
44.	"The solution should provide a robust and mature vault to manage credentials, passwords, Keys secrets, certificates and such other artifacts as one would like to vault		
45.	The solution should provide out of box connector integrating all standard systems (like HP tandem, Guardian etc.) to the Vault.		
46.	The solution should provide for auto vaulting features as soon as the system is on- boarded.		
47.	The solution should be able flexible to configure the policies and procedures of the organization, especially for passwords and secrets.		
48.	The solution should provide features to create local or general exceptions to the rules or policies.		
49.	The solution should be able to provide rotation capabilities at scale (across technologies)		
50.	The solutions should be able to create a sequence or automate events or actions based on technology requirements to ensure that any rotation activity is conducted without any manual intervention		
51.	The solution should be able to provide features for JIT (Just in time), on-demand, and time-based rotations of passwords		
52.	The solution should be able to automatically sync any out of sync passwords without using any external utilities (on target systems/applications)		
53.	A single person/user should not be able to check out any credentials, always two or four eyes' principles should be applied		
54.	Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online (break glass facility).		
	The solution should provide a high-velocity vault that is agile and dynamic to generate not only unique passwords/secrets but also unique credentials especially for cloud assets that are auto-scaled		
55.	The solutions should be able to onboard and support credential management for cloud and containerized environment		
56.	The solution should provide a secure method to facilitate access to managed assets in case of PAM failure for identified users (local vault) like fail safe features		
57.	The solution should have a central administration console for unified administration		
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		
Workflow & Notifications			
59.	The solution should have an inbuilt workflow to manage: i) Electronic/Dual Approval based Password Retrieval ii) Onetime access / Time Based / Permanent Access		
60.	Multi-level approval workflow with E-mail and SMS notification and delegation rules		
61.	Ability to provide for the delegation at all levels in the workflow		
62.	The solution should support a workflow approval process that is flexible to assign multiple levels of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).		

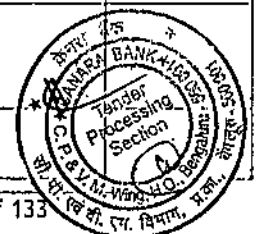


63.	The solution should support a workflow approval process that requires approvers to be in sequence before final approval is granted.		
64.	The solution should support workflow delegation capabilities		
65.	The solution should provide ready integration with service now and other ticketing ITSM tools for workflows		
66.	The solution should have the capability to provide alerts and notifications for critical PAM events over SMS & Email		
67.	The solution should have the capability to provide alerts and notifications for all administration/configuration activities over SMS & Email		
68.	The solution should have the capability to integrate with banks ITSM (Service Now, BMC Remedy, JIRA etc.), ATM Solution (Guardium OS), proposed SIEM, SOAR, Tenable and UEBA solutions for validating access.		
User and Password Management			
69.	The solution should set password options as per Bank's policy in days, months, years and compliance options via the use of a policy. After predefined configuration solution should rotate password.		
70.	The solution shall perform password change options which is parameter driven.		
71.	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.		
72.	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule		
73.	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods		
74.	The solution should allow user the option to provide read, write access based on time/days		
75.	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')		
76.	Ability to generate 'One-time' passwords as an optional workflow		
77.	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		
78.	The solution should automatically verify, notify and report all passwords which are not in sync with PIM		
79.	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.		
80.	The proposed solution should restrict the solution server administrators from accessing or viewing passwords or approve password requests. Solution should have Workflow based approach for providing viewing passwords and approve password or server access requests.		
81.	The solution should have provision for secure offline access of managed credentials in case of vault failure (break glass scenario)		
82.	Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online		
83.	The passwords and keys shall be stored in the vault with minimum AES 256-bit encryption		
84.	The solution shall be capable of managing the entire Software Key Lifecycle i.e., initiation, key generation, maintenance, supply, rotation, renewal, backup and restore, recovery, publish, revocation and destruction in automated manner		
85.	The solution must enforce auto- rotation for each password before the expiry of password.		





86.	The system shall allow Key caching, Key rotation and Key versioning without any downtime.		
87.	The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices, etc.		
88.	The solution shall allow single baseline policy across all systems, applications and devices (e.g. one single update to enforce baseline policy. It should support multiple policy also based on the requirement		
89.	The solution should restrict execution of risky commands execution (as per the regulatory guidelines) if the session is initiated with PIM. The PIM solution should have the list of Risky commands available out of the box. If not, the bidder shall build such list and configure it in the platform.		
90.	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.		
Logging & Reporting			
91.	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.		
92.	The solution should be able to support a session recording on any session initiated via PAM solution including servers, network devices, databases, and virtualized environments etc.		
93.	The proposed system shall support full color and resolution video recording		
94.	The proposed system shall support video session compression with no impact on video quality.		
95.	The solution shall have the ability to replay actual session recordings for forensic analysis		
96.	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video-based formats		
97.	The solution should be able to log/search text commands for all sessions of database even through the third-party utilities		
98.	All logs created by the solution should be tamper proof and should have legal hold		
99.	The solution shall restrict access to different reports by administrator, group, or role		
100.	The tool generates reports in at least the following formats: HTML, CSV, and PDF		
101.	The system shall have the ability to run all reports by frequency, on-demand, and schedule		
102.	The solution should be able to report password lockouts (failure logon attempts)		
103.	Ability to report password checkouts on systems and users requesting passwords		
104.	The solutions should provide advanced analytics capability and provide risk score on all the sessions and tasks done by users.		
105.	The PAM solution has automated report query capability		
106.	The solution shall rotate/change the password automatically when it is shared/viewed by Administrator		
107.	The solution shall balance the load between session managers. Any hardware or software or license required to achieve the functionality shall be provisioned by the OEM/bidder		
108.	The proposed solution shall have filesharing capabilities to share file using PAM		



109.	The solution shall have workflows which can be leveraged to build for managing third-party accesses		
110.	The solution shall record the transcript capturing all the activities		
111.	The removal of user account from PAM solution shall not delete the historical logs associated with the user which includes Past sessions video recording, audit train logs etc.		
112.	The solution shall have integration available for leading vulnerability management solutions such as Tenable, Qualys etc. to provide just in time privilege access to perform scans across the enterprise network		
113.	The bidder shall provide an UAT environment to test custom integration/policies as necessary		

VI. Threat Intelligence Platform (TIP):

Sl. No	Technical Specifications of TIP	Compliance (Yes/No)	Remarks
1. Data Centre			
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.		
2. General Feature and Functionality			
2.	The proposed solution automatically researches and scores each IOC imported using machine learning or other unsupervised techniques		
3.	The proposed solution must normalize input data into structured formatting.		
4.	The proposed solution must support creation of any number of collaborative groups and subgroups between any members or stakeholders, in order to share any intelligence, including IOCs, threat actor profiles, bulletins, etc		
5.	The proposed solution must support search across all IOCs, reports, threat actors, etc, including across any created or held by collaboration partners who provide trusted access to any intelligence they choose to share		
6.	The proposed solution must have the ability to integrate with Bank's third-party threat Intel vendor feeds		
7.	The proposed solution must have an automated means to curate Threat Intelligence Data. That is, the removal of duplicates, false positives, risk scoring, and aging out of IOC's.		
8.	The proposed solution should be able to match keywords in Observables, Sandbox, Bulletins, Vulnerabilities and Signatures and will be able to trigger various actions.		
9.	The proposed solution allows instant visibility on the Threat/Risk with further pivot capabilities into granular Tactical and Strategic contextualized and enriched reporting.		
10.	The proposed solution should provide out-of-the-box reports of threat activities related to the events data. Such as indicator matches, real-time forensics reports.		
11.	The proposed solution can perform retrospective data retrieval/search against all events received in the platform.		
12.	The solution must assist the organization's threat analysts by providing managed threat analytics algorithms to provide a high accuracy confidence score on new threat intelligence with no configuration required		
13.	The proposed solution should support bulk data uploads.		





14.	The solution needs to seamlessly integrate with the Bank's Network Time Protocol (NTP) and Active Directory (AD).		
15.	The proposed solution must allow the organization to utilize the solution's API to automate data processing using scripts and/or other data stores		
16.	The proposed solution must provide the ability to have intelligence imported quickly and easily into the system in all common formats		
17.	The proposed solution must allow the adding of analyst comments to threat intelligence including indicators and threat bulletins		
18.	The proposed solution must support the creation of tags on public or shared intelligence that are visible only to the organization. Ie. To allow tagging of shared intelligence that is unknowable to other organizations		
3. Data Ingestion			
19.	The proposed solution can automatically parse IOCs from unstructured source documents such as PDF, DOC, XLS, as well as web pages and blog posts		
20.	The proposed solution offers more than 100+ open-sourced intelligence and also provide Free Feeds' content as well.		
21.	The proposed solution must support the ability to automatically parse indicators from a phishing email sent to an assigned email inbox		
22.	The proposed solution must support the ability to automatically detonate any malware attached to a phishing email sent to an assigned email inbox, and capture any IOCs generated by the detonation as linked to the email		
23.	The proposed solution should generate a ticket or case for an analyst to assess, when phishing malware is detonated		
24.	The proposed solution must support either manually defined confidence scores or analytics-derived confidence scores, based on analyst preference.		
25.	The proposed solution's browser extension can import scraped contents into solution as indicators, report or create investigation.		
26.	The proposed solution must include support for ingesting all major OSINT and commercial intelligence sources with no configuration effort		
27.	The proposed solution must be able to ingest not only syslog, network traffic (NetFlow, Sflow) and events forwarded from SIEM but also support the ingestion of Threat Intelligence in multiple formats as well.		
4. Threat Intelligence Management			
28.	The proposed solution provides out-of-the-box enrichments and integration.		
29.	The solution must be feasible for integration with the Bank's newly proposed sandbox solution.		
30.	The proposed solution includes an analyst workbench with on-demand enrichments and link-analysis features to allow analysts to conduct detailed investigations		
31.	The proposed solution must allow creation of threat models including as a minimum, threat reports, malware entities, actor profiles, campaign notes, with the ability to associate IOCs and other relevant entities, in-line images and rich text formatting		
32.	The proposed solution's browser extension allows leveraging of MITRE ATT&CK Framework in investigations within the platform.		



33.	The proposed solution must support Threat Modelling such as Diamond, STIX, Kill chain, MITRE ATT&CK and allow users to assign phases during investigations.		
34.	The proposed solution must provide the ability to alert users of new additions to the platform regarding certain keywords hits and also automatically tag IOC's/Threat Bulletins that meet the requirements of the alert.		
35.	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.		
36.	The proposed solution must provide a Threat Management incident handling capability with the ability to create incidents and/or tickets depending on organizational workflow		
37.	The proposed solution should be capable of operationalizing threat matches and turn it into actionable intelligence		
38.	The proposed solution must support the rendering of any threat bulletin, or any other threat intelligence product created by the platform to human-readable PDF		
39.	The proposed solution must support export of atomic IOCs to CSV, PDF, STIX, OpenIOC.		
5. Integration and Dissemination			
40.	The proposed solution must has built, out of box integration with proposed SIEM, SOAR, ITSM (Service Now) etc.		
41.	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		
42.	The proposed solution must include applications to integrate and automatically manage a data feed from the solution to all security systems that the organization requires to use threat intelligence from the system		
43.	The proposed solution must support selective filter conditions for only high-severity or high-relevance indicators to a security system that has a limited capacity for IOCs		
44.	The proposed solution must permit indicators to be synchronized to a downstream system based on tags applied to the indicator, such as might result from an analyst tagging an indicator to be actioned by a security system		
45.	The proposed solution must support bi-directional sharing of threat intelligence using STIX documents with a TAXII server		
46.	The proposed solution must offer a documented SDK for developing integrations to other intelligence sources or feeds without the involvement of professional services or development		
47.	The proposed solution should offer a REST API		
48.	The proposed solution has bi-directional sharing between SIEM and Threat Intel platform such as Adaptive Response action.		



VII. Dynamic Application Security Testing (DAST):

Sl. No	Technical Specifications of DAST	Compliance (Yes/No)	Remarks
General Requirement			
1	The solution should have capability to scan web, mobile, APIs as well as single page applications.		
2	The solution should be capable to perform scans on internal as well as external applications.		
3	The solution should be capable to automate / schedule scans.		
4	The solution should be capable to perform Black box as well as Grey box testing.		
5	The solution shall support simultaneous Crawl & Audit during scans.		
6	The solution shall allow for multiple concurrent scans without latency using DC, DR scanners. Solution should allow independent scanning from DC and DR.		
7	The solution shall provide a built-in scan profiler to assist in tuning the scan configuration to a target server to improve the effectiveness and accuracy of the scan.		
8	The solution should allow for real-time review and investigation of vulnerabilities found while a test is still in progress.		
9	The solution should offer the capability to pause a scan for continuation later without the loss of data.		
10	The solution should have the capability to maintain false positive tags across scans		
Performance Requirement			
11	The solution should have the capability to view the actual attack during a scan session.		
12	The solution should have the capability to generate the rules to send to WAF.		
13	The solution should also come with the Interactive Application Security Testing feature.		
14	Integration with tools like POSTMAN, BURP or any other pentest tools etc. Further, it should also integrate with new tools which would be compatible or procured in future.		
15	Solution should have capability to provide reports which can be ingested to the GRC Solution such as RSA Archer		
16	The solution should support scanning only the vulnerabilities from previous scan, scan incremental, scan crawl and Audit from previous configurations		
17	The solution should have the REST & SOAP API to initiate/pause/stop/ scans and for various other functionalities		
18	The solution should be able to scan and test a wide breath of application security vulnerabilities.		
19	The solution should employ the latest algorithms and techniques to ensure the most accurate testing and minimize false positives		
20	The solution licensing should support concurrent/floating license		
21	The solution should support OAST Vulnerability detection		
22	The solution should support FAST proxy		
23	Solution must support Top 10 OWASP Standards, OWASP Application Security Verification Standard (ASVS), PCI DSS, ISO/IEC 27001, NIST Cybersecurity Framework, and SANS CWE TOP 25 Most Dangerous Software Errors. and provide reports based on these standards		



24	The solution should support distributed scan sensors/agents to run the scans and the solution should have capability to Automate security assessment in the CI/CD pipeline		
Solution Capabilities			
25	The solution supports Web Services security testing.		
26	The solution should provide REST/URL Rewriting (Variable) detection and support.		
27	The solutions should allow for custom checks to be added and modify.		
28	The solution should allow for a re-run of the entire scan with the same settings		
29	The solution should provide a shortcut to quickly re-test all vulnerabilities, retest based on severity		
30	The solution should provide automatic vulnerability signature updates via the internet. Updates may also be performed manually for offline machines.		
31	The solution should integrate with a defect-tracking system for easy creation of defects from within the solution itself.		
32	The solution shall have the ability to feed details of vulnerabilities found during a scan into Web Application Firewall and/or Intrusion Prevention Systems to block potential application exploits		
33	The proposed solution must be able to record macros against Web 2.0 applications		
34	The solution integrates and works out-of-the-box with a real-time application security technology within Java, C#, and .NET servers to: <ul style="list-style-type: none"> i. Gather internal, code-level vulnerability information by observing the attacks in the code as they happen in real-time. ii. Inspect parts of the application that it may not find through normal crawling. iii. Collect information about the internal behaviors of a target application during dynamic tests. iv. Detect new types of vulnerabilities, e.g., privacy violation and log fogging. v. Provide stack trace and line-of-code detail during dynamic web application scanning. 		
35	The solution should have the capability to export scan data in PDF, CSV and Excel format for upload to a web management console, to be correlated with security vulnerabilities found from static and interactive time testing. This offers a holistic view of the security status of applications and projects within an enterprise.		
Administration, Manageability and Reporting			
36	The solution comes with an array of out-of-the-box scan policies and all major compliance reports which may be further added to and customized.		
37	The solution provides the ability to compare and report on two different scans to enable a delta analysis, including a visual representation of vulnerability differences between the two scans and the ability to drill-down into the differences.		
38	Solution must provide Executive Summary Report, Remediation based Report, History reports, Scan comparison reports and Custom reports. The solution must be capable to generate report in following format:		



	<ol style="list-style-type: none"> 1. The Title. 2. The Location (URL and/or line of code). 3. Specific vulnerability description. 4. Risk likelihood, business impact, and severity. 5. <u>Detailed proof of concept.</u> 6. Specific remediation recommendations. 7. Affected links/parameters 8. References, CVE, CVSS & CWE etc. 		
Availability			
39	The solution must support deployment on premises at DC and DR.		
40	The solution must support CAPTCHA/ OTP/ Composite Login process configuration in the proposed solution.		
41	The solution should support 2FA/ MFA authentication.		
42	The solution should be able to skip an attack while the scan is in progress.		
43	The solution should support REST API scan and SOAP API scan and support Swagger, ODATA, gRPC, GraphQL, SOAP, Postman data types for API Scan.		

VIII. Anti - APT:

Sl. No	Technical Specifications of Anti - APT	Compliance (Yes/No)	Remarks
Key Functional Requirement			
1.	The bidders are intended to deploy Network Advance Threat Detection solution as a dedicated purpose-built platform deployed independently without any functional reliance on existing layers of security like NGFW, NG-Proxy etc. adhering to defense in depth architecture. The proposed solution must be capable to function on its own even if any of the layers of core underlying security get replaced or become non-functional.		
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.		
3.	The Bidders are expected to propose a solution that must detect zero-day, multi-stage, fileless and other evasive advanced attacks using dynamic, signature-less analysis in a safe, anti-evasive execution environment. The solution should be sized appropriately by the bidder including all other costs required for performance, scalability, and efficiency.		
4.	Anti-APT appliances must be deployed On-Prem. Other technologies such as Sandboxing and advanced technique for example: AI/ML analytics, automatic correlation and investigation can be performed on-Prem or cloud. Offered cloud components shall be hosted in India to ensure data localization.		
5.	The proposed solution must preferably be supplied as a purpose built dedicated physical appliance while central management ensuring performance and applicability to environment. Any components required to run the solution including hypervisor hardware & software must be supplied by the bidder.		
6.	Bank will procure additional licenses as per the requirement without compromising on system functionality or performance and OEM to		



	provide unit price which shall be leveraged to place additional order as required during the tenure of the contract		
7.	The bidders are required to provide integrated regular security threat intelligence content subscription as part of the solution. The security content must be integrated with the solution without any requirement to manually manage and update the feeds		
Technical Requirement			
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.		
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, TLS Concurrent connections of 5 Lakhs and appliance hardware scalable to accommodate future requirements up to 20 Gbps on the same hardware appliance on day 1.		
10.	The proposed hardware/appliance should have SSL inspection capability for internet traffic. However, in case the hardware/appliance does not have the capability for SSL inspection, bidder must supply an integrated enterprise grade SSL decryption and orchestration solution with packet broking functionalities for encryption/decryption of web/network traffic and further provide decrypted traffic to APT sensors for SSL inspection for the north-south traffic.		
11.	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.		
12.	Proposed solution/ appliance should have below hardware requirements: Anti APT solution/appliances should be supplied with minimum below port requirements with a separate dedicated management port with 10/100/1000GBASE-T. 4 X 1G/10G RJ45 4 X 10G SFP+ (With Bypass) 8 X 10G SFP+ or (6 x 10G SFP+ and 2 x 40G QSFP+)		
13.	The proposed solution must detect multi-flow, multi-stage, zero-day, polymorphic, ransomware and other evasive attacks in real time while also enabling back-in-time detection of threats		
14.	The solution must detect advanced threats using dynamic machine learning, AI and correlation engines detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights from real world victim breach intelligence Indicators		
15.	The solution must have signature-less, dynamic analysis engine that inspects suspicious objects to identify targeted, evasive and unknown threats. The engines must detect and block malicious objects based on high-fidelity machine, attacker and victim-intelligence.		
16.	The proposed solution must rapidly detect both known and unknown attacks with high accuracy and a low rate of false positives, while facilitating an efficient response to each alert		
17.	The solution must generate the alerts which include concrete real-time evidence to quickly respond to, prioritize, and contain targeted and newly discovered attacks.		
18.	The bidders must ensure the proposed solution Analysis component is a secure purpose-built appliance/ 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.		
19.	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.		
20.	The proposed sandboxing platform shall support minimum 100+ sandbox VMs (to support 100 parallel file executions) On-Prem or Auto-scaling in cloud model. The bidder to size the hardware according to the throughput given above.		
21.	Analysis engine must provide real-time protection against evasive attacks with micro tasking within Dynamic Analysis O.S VM's (Windows & 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.		
22.	The solution should leverage a sandbox technology, featuring a custom hypervisor/cloud sandbox 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.		
23.	The Internal Network Analysis solution should also be able to detect malicious post-exploitation activities such as attacker lateral movements between various zone like user workstation & servers. The solution should detect lateral movement indicating source & destination IP addresses, files transferred, commands executed, with detailed execution analysis of payload, files etc.		
24.	The solution must detect zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment and stop infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.		
25.	The solution must have multiple, dynamic machine learning, AI and correlation engines detect and block obfuscated, targeted and other customized attacks with contextual, rule-based analysis from real-time insights		
26.	The proposed solution must provide protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, crypto miners etc.		
27.	The solution must have capability to identify malicious exploits, malware, phishing attacks and command and control (CnC) callback while extracting and submitting suspicious network traffic to the dynamic analysis engine for a definitive verdict analysis.		
28.	The solution must support the detected threats mapping with riskware categorization, and mapping to MITRE ATT&CK framework		
29.	The proposed solution must support analysis of different file types listed below but not limited to for dynamic analysis, including portable executables (PEs), active web content, archives, images, Java, Microsoft and Adobe applications and multimedia etc. with a proven capability to analyze suspicious network session, flows with capabilities like code		



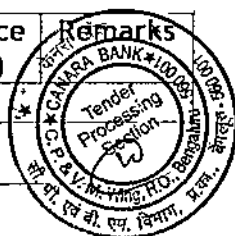
	analysis, that includes function, entropy and similarity analysis of Files, URL's, Objects, network flows, scripts. must be supported.		
30.	The proposed solution should support more than 80 files types for inspection in sandbox environment including alz, bat, cmd, cell, chm, csv, class, cla, com, dll, doc, docx, egg, ocx, drv, dot, dotx, docm, dotm, cpl, exe, sys, crt, scr, gul, hta, htm, html, hwp, hwp, ixy, jar, js, jse, jtd, lnk, mht, mhtml, mov, msi, odt, odp, ods, pdf, ppt, pps, pptx, ppsx, ps1, pub, rtf, shtml, slk, svg, swf, vbe, vbs, wsf, xls, xla, xlt, xlm, xlsx, xlsb, xltx, xlsx, xlam, xltm, xml, xht, xhtml, url, 7z, ace, amg, apk, arj, hqx, bz2, bzip2, cab, crx, gzip, gz, iso, lha, lharc, lzh, bin, macbin, eml, email, msg, msi, arc, rar, sis, sit, sitx, tar, tgz, tnef, winmail, dat, win, uue, wim, xz, zip, dmg, jar, class, cla, pkg, o, sh.		
31.	The proposed solution should utilize multiple machine learning, AI and correlation engines represent a collection of contextual, dynamic rules engines that detects and blocks malicious activity in real-time and retroactively, based on the latest machine-, attacker- and victim-intelligence.		
32.	The proposed solution should detect suspicious files uploaded to web servers through HTTP- POST and FTP protocols and provide mapping of methodology & alert techniques to MITRE ATT&CK framework. It should also detect attempted data exfiltration, Beacons including other Advanced techniques.		
33.	The solution must have capability to provide Back-in-time IOC threat analysis via integration of 3rd party Threat Intelligence, STIX or TAXII or Open IOC feeds with automated Investigation and analysis search function.		
34.	The solution must have built in functionality to detect genuine attacks, Advanced technology engines must be used to validate alerts detected by conventional signature-matching methods like IPS to identify and prioritize critical threats.		
35.	The solution must detect Event Type for Network Anomaly, OS Change, Checksum Match, VM Signature Match, CNC Signature Match etc. logged while analyzing any traffic or PCAP or objects		
36.	The Solution must have the dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses		
37.	The proposed Anti - APT solution should support operating system for sandboxing such as (Windows, Linux etc.)		
38.	Proposed solution shall have open IOC sharing framework so that the indicators can be shared with other security solution deployed at the Bank such as AV, EDR, SOAR, Firewall etc.		
39.	The solution should have SSL Decryption capabilities available out of the box		
40.	The proposed solution should be able to detect and prevent the persistent threats which may come in the form of executable files, PDF files, Flash files, RTF files and/or other objects.		
41.	The proposed solution shall have both out of band and inline deployment mode		
42.	The proposed solution should monitor traffic from multiple segments like WAN, DMZ, Proxy, MPLS links etc. simultaneously on a single appliance.		
43.	The proposed solution should have capabilities to ingest/ configure files, IP, URLs, and Domains to deny list and whitelist.		



44.	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal.		
45.	The solution should provide Sandboxing detailed report and playback for suspicious activity.		
46.	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.		
47.	The proposed solution should support Structured Threat Information expression (STIX) for user-defined detection and third-party integrations		
48.	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.		
49.	Continuously analyzes current and historical network metadata and correlates these related threat events into a single view for full visibility of the attack cycle		
50.	Should support advanced and sophisticated machine learning techniques to detect network traffic anomalies. Correlates the events and maps out every step of the attack, giving a better idea of how to respond and prevent future attacks.		
51.	The solution should be sized to handle the concurrent sessions		
Central Management - Admin and Operational			
52.	The bidders are asked to supply a Central Management solution in high availability mode over WAN between DC & DR to manage and administrate the overall deployed ecosystem, ensuring that sensors, components & appliances share the latest intelligence and correlate across multiple attack vectors to detect and prevent from cyber incidents.		
53.	The central management solution must help centralize the entire deployment management into a single console to manage configurations, threat updates, and software upgrades		
54.	The central management solution must have capability to enable remote management and dynamic configurations		
55.	The central management solution must enable blended threat prevention using multi-vector correlation of collected data events		
56.	The central management solution must be able to distribute and disseminate in real-time local threat intelligence to multiple deployments across your systems in an automated fashion		
57.	The solution must only be accessible via web UI/ plugins/ thick clients for Admins or Analysts to access and manage.		
58.	The proposed solution should support SNMP, syslog etc. for integration with all leading SIEM, SOAR, TIP, Firewall, AV, Proxy, EDR, ITSM (Service Now) solutions. The Solution components should also be providing access over REST APIs with detailed OEM documentation.		

IX. Breach Attack Simulation (BAS):

Sl. No	Technical Requirement	Compliance (Yes/No)	Remarks
Architecture & General Requirement			

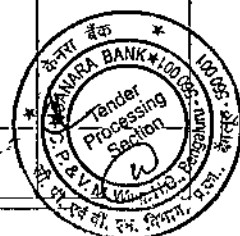


1.	The proposed solution must be SaaS model/ hybrid having cloud setup in India (complied with MeiTy) with 99.90% uptime.		
2.	The solution should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations.		
3.	The agent installed for assessments /simulations should be able to remove any malicious files or executables that were run on the system as part of the simulation activity.		
4.	The proposed solution should be able to provide the entire attack kill chain in accordance to MITRE attack framework. In case of change in MITRE attack framework, the tool has to adopt the revised/ changed framework.		
5.	The solution should Identify controls specific effectiveness of models (MITRE, NIST etc.).		
6.	The solution should support user management with support for different user roles like admin, user etc.		
7.	Solution should be able to export and import malware samples/hashes etc.		
8.	The solution should be able to detect the outbound exposure to malicious or compromised websites from the bank's endpoints and servers, etc.		
9.	The solution should have the ability to identify the device trajectory to map how hosts interact with files, including malware, across endpoint environment (e.g., if the file transfer was blocked or if the file was quarantined by antivirus) & security solution deployed in bank.		
10.	The solution should be able to generate detailed report covering the attacks which were successful and should detail the indicators of compromise (IoCs) and how the attack played out in the environment.		
11.	The content library of the solution should be updated periodically with new attack simulations.		
12.	All the simulations should be mapped to MITRE attack framework.		
13.	The solution should not be dependent on other solutions for sourcing threat feeds.		
14.	The solution should be able to integrate with ticketing platforms.		
15.	The solution should measure the time to detect and respond the attack simulation.		
16.	The solution should have the capability of providing attack blocking / prevention analysis.		
17.	The solution should have the capability to execute attack sequences to expose changes in effectiveness or identify risks.		
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) etc.		
19.	The solution must support proxy communications to the Internet. Simulation Agents installed must support proxy communications to the Breach & Attack simulation solution's cloud platform counterpart.		
20.	The Solution agent component must be installable as a software package (Publishing it through group policy) and can be included in Golden image.		
21.	For the proposed solution, Agents will be installed on minimum set of endpoints. Considering mentioned setup supplier should be able to run and provide all required use cases/simulations effectively.		
22.	The solution must be easily and automatically updated either from the server itself or via manual updates		
23.	For the proposed Solution, All installed agents/simulators should have capability to run assessments/simulations as local user privilege and/or admin user privilege		





24.	All data collected/processed should be secure in vendors cloud instance and to be stored only in India		
25.	For the proposed solution, The Supplier shall describe/provide assurance that when the customer deletes data, the data is completely gone and not resident anywhere on the supplier infrastructure within the solution.		
26.	For the proposed solution, The Supplier should ensure access to sensitive information is restricted to only personnel with a need to know basis with Granular User Role management.		
27.	For the proposed solution, The Supplier should notify the customer immediately when security vulnerability is discovered within the solution.		
28.	The solution must include discrete privileged and user account levels with specific permissions for each (e.g., RBAC)		
29.	The Solution should have Multi-Factor Authentication to access Platform.		
30.	The solution must include basic user policy controls for account access and password management		
31.	The proposed solution should respond with a generic error message regardless of whether the user ID or password was incorrect. The message should give no indication of the status of an existing account.		
32.	The solution must generate an audit log of all operations including individual user actions		
33.	The Supplier should ensure passwords for services shall not be displayed during authentication nor stored in an unencrypted form.		
34.	The Supplier proposed solution should secure audit logs from tampering.		
35.	The solution must directly integrate with the proposed SIEM solutions		
36.	The solution must validate network security control effectiveness.		
37.	The solution must validate email security control effectiveness / assessment (improper configuration or implementation of email filters)		
38.	The solution must include support for the POP3, IMAP, and SMTP email protocols with SSL and TLS.		
39.	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)		
40.	The solution should support red team activities (attack scenarios) and blue team activities (actionable remediation).		
41.	The solution should not add/create any performance degradation in the network.		
42.	The solution should be able to determine during an attack which security solutions were able to detect the attack and if they were not able to detect then should be able to suggest rules / configurations to be done on the security solutions.		
43.	The solution should be able to source latest critical threats in the industry and should be able to provide simulations immediately, not later than 1 day of discovery.		
44.	The solution should be able to simulate Real attacks and provide malware artefacts (capability to simulate real exploits and latest malware)		
45.	The solution should be able to test attacker lateral movement (once successfully within a network) - e.g., pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data		
46.	The solution should be able to detect data transfer to and from malicious domains / IPs / websites (Secure web gateway / proxy test).		



Use cases		
47.	Solution should have Ability to simulate breach methods across the complete cyber-attack kill chain including NIST, MITRE ATT&CK complete framework (e.g., infiltration, exfiltration etc.)	
48.	The solution should be able to detect the outbound exposure to malicious or compromised websites from the bank's endpoints and servers, etc.	
49.	The solution should have the ability to identify the device trajectory to map how hosts interact with files, including malware, across endpoint environment (e.g., if the file transfer was blocked or if the file was quarantined by antivirus) & security solution deployed in bank.	
50.	The solution should be able to generate detailed report covering the attacks which were successful and should detail the indicators of compromise (IoCs) and how the attack played out in the environment and eliminate specific weaknesses.	
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.	
52.	Determine which controls are most and least valuable, i.e., prioritization of controls.	
53.	The solution should have the capability of providing attack blocking / prevention analysis.	
54.	The solution should have the capability to execute attack sequences to expose changes in effectiveness or identify risks.	
55.	The solution should have the capability to integrate and consume threat feeds such as IOCs, IPs etc. from third party intelligence/regulators like CSITE, CERT-IN, etc.	
56.	The solution should provide RESTful API interface from third party.	
57.	The solution should have the capability of providing Detect, Alerting analysis including SIEM Correlation rule analysis.	
58.	The solution should have the capability to validate existing deployed Data Loss Prevention/Protection controls.	
59.	The solution should have the ability to execute batch attack scenario processing across multiple vectors including Network, Endpoint, Email and cloud.	
60.	The solution should have the facility to integrate with the existing VA Tool of the bank to obtain information about existing vulnerabilities.	
61.	Solution should be able to validate end-point security tool controls.	
62.	The solution should be able to import samples of sensitive data from solution such as DLP.	
63.	The solution should be able to test systems in case no agent is installed, like in the scenarios of remote exploitation, use of credentials, lateral movement etc.	
64.	The solution should include attacks simulations relevant to information technology targets.	
65.	The solution must include library of attacks that exploit common application vulnerabilities & Weaponize Known CVE's.	
66.	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g., CVSSV3)	
67.	Solution must provide timestamp of the attack across multiple geographies for all attack vectors for correlation & Validation.	
68.	Solution should have Ability to test data loss prevention (DLP) implementation, methodology, and configuration along with other exfiltration techniques to test outbound flows of data to ensure protection of critical information during simulation.	





69.	Solution should have Ability to simulate Infiltration techniques for breaching a network or infecting a host - Via Email, Web & WAF.		
70.	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc.		
71.	Solution should have Ability to test attacker lateral movement through a single machine (once successfully within a network) - e.g., brute force or pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data		
72.	Solution should support Ransomware simulations using latest Ransomware, malware samples/cases, etc.		
73.	Solution should support Email security assessment (improper configuration or implementation of email filters)		
74.	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing automated behavioral detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.		
75.	Solution should support Extracting credentials from memory (Endpoint privilege escalation test)		
76.	Solution should support Executing local privilege elevation exploits (Endpoint privilege escalation test)		
77.	Solution should support Transfer and/or execution of malware on a test system (Endpoint malware download and execution test)		
78.	Solution should support Access, connection, or data transfer attempt (Network segmentation test)		
79.	Solution should support Access or data transfer to a malicious site (Secure web gateway / proxy test)		
80.	Solution should support Proxy tests - HTTP/HTTPS inbound/outbound exposure to malicious or compromised websites (web malware, malicious scripts)		
81.	Solution should have Ability to deliver safe tests with no chances of interfering with business operations, and no user interference when deployed on production assets		
82.	Solution should have Ability to perform continuous analysis and Historical trending (alert, track, analyze, and remediate advanced malware that may at first appear clean or that evades initial defenses and is later identified as malicious) and there should not be cap on the number of times simulations are being performed for a particular device /device		
83.	Solution should have Ability to simulate breach methods based on attacker profile (APT) and data assets to be protected		
84.	Solution should have Mechanism to identify remediation options and recommendations, prioritize severity of test findings and actionable remediation for each security control.		
85.	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps that can be taken to lower the overall security risk highlighted by the simulations.		
86.	Solution should Continuously simulate breach methods to address changing risks, and track security posture via risk trending and historical reports.		
87.	Solution should have capability to test SIEM rules by simulating a multi-vector attack		
88.	Solution should have Ability to create custom use cases / simulations attacks according to the bank's requirement		



89.	Solution should Test effectiveness of security tools and controls (real behavior and outcome of controls) - e.g., identify configuration errors or defects		
90.	Solution Knowledge base should be extensive & should Describe how the library of breach and attack methods are created, managed, Updated and mapped to threat models.		
91.	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations		
92.	The proposed solution should have capabilities to allow for the detection or prevention of unauthorized modification of data.		
93.	Solution should be able to do a lateral movement assessment from a single endpoint		
94.	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC		
95.	The Supplier should verify SIEM alerts by simulating malicious activity (injecting events into a SIEM) to gauge whether it correlates them to generate the right alert (Monitoring SIEM tests)		
96.	The Supplier should address configuration, segmentation, or implementation errors throughout the entire lifecycle of a security product		
97.	Solution should check inbound and outbound penetration of web gateway.		
98.	Solution should have integrated Email phishing simulation module with the capability of accessing the responses.		
99.	The solution should support any cloud instances such as Azure, AWS, Oracle etc.		
100.	The solution should have the capability to provide the Indication of Attack (IoA) based on the tool intelligence of detecting IOCs, behavior, other contextual information etc. about the attacks.		
101.	The solution should have the capability to instrument attacks on each of the below vectors but not limited to: <ul style="list-style-type: none"> • Endpoint based attacks • Network based attacks • Email based attacks • Proxy • Attacks on cloud infrastructure • Any combination of the above 		
102.	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.		
103.	The solution should be able to perform attack by exploiting the missing patches on the system & report has to be generated highlighting issues due to missing latest patches.		
Dashboard			
104.	The solution must provide an intuitive dashboard that shows vulnerabilities, misconfigurations, gaps, and risks in the current security controls deployed.		
105.	The solution must provide a MITRE ATT&CK heatmap for both prevention and detection controls for the organization.		
106.	The solution must have the ability to provide a quantitative security score or equivalent rating to showcase the maturity of the detection or prevention technologies.		
107.	The solution must provide dashboards that display the strengths and weaknesses of current security controls for both prevention and detection.		





108.	The solution must provide a dashboard that shows organizations resilience against ransomware attacks.		
109.	The solution must provide a dashboard that shows a negative deviation from baseline security controls.		
110.	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.		
111.	The solution must allow cloning and editing of customized dashboards as and when required.		
112.	The solution must provide benchmarking and comparison results for organizations in the same industry.		
113.	The solution must include the ability to export primary dashboards, reporting in PDF format		
Reporting			
114.	The reports must provide details about each attack simulation executed along with its mitigation.		
115.	The solution must provide the assessment history and maintain a detailed audit trail for at least 12 months for auditing purposes.		
116.	The solution must store historical reports along with their timestamp, target system, target user, type of assessment executed, etc.		
117.	The solution must display a risk score for each assessment performed individually as well as the overall risk.		
118.	The report must have previous comparisons to show changes in current control, i.e., improved or deteriorated.		
119.	The solution should provide a consolidated report view for specific security control tests.		
120.	The report should show the number of test cases covered, percentage of control bypassed, overall and category-wise risk, etc.		
121.	The report should contain granular details, which include timestamps, payload information, risk, type of attack, target, description, mitigation, IOC or IOB, etc.		
122.	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.		
123.	The solution must provide industry-standard reporting templates, e.g., remediation guides, prevention and detection reports, overall security posture, and security control performance.		
124.	The solution must allow selecting datasets from existing results to create customized reports.		
125.	The solution must allow cloning and editing of customized reports as and when required.		
126.	The solution must provide reporting for executive, scenario, and recommendation reports in PDF or CSV formats as appropriate.		
127.	The solution must provide different types of reporting, including executive-level, scenario-level, a recommendations report that outlines best practices, and vendor-specific recommendations for failed assessments.		
128.	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.		
129.	The solution must provide visual representations of attack paths and potential lateral movement within the network to aid in understanding the attack's potential impact.		

Declaration:



1. We hereby confirm that we have various certificates/bench mark testing standards for the items quoted to meet the intent of the Bid.
2. We hereby confirm that we have back-to-back arrangements with third party software/ cloud for providing continuous and un-interrupted support to meet SLAs obligations as per bid terms.
3. We hereby confirm that the information submitted above is true to the best of our knowledge. We understand that in case any discrepancy is found in the information submitted by us our tender is liable to be rejected.

Date:
Place:
Designation:

Signature with seal
Name:



Annexure-8
Amended Scope of Work

(Should be submitted on Company's letter head with company seal and signature of the authorized person)

SUB: Selection of System Integrator for End to End implementation of Next Generation Security Operations Center (NGSOC) in Canara Bank.

Ref: GEM/2024/B/5406710 dated 17/09/2024

1. SOC Solutions & Services

Summary of the solutions required by the Bank as a part of the project of "NGSOC and in scope security solutions" are provided below:

S. NO	Solution	Requirement	Deploy Mode
1.	SIEM	As per the Technical Specifications and Scope of Work	On-Prem
2.	PCAP	As per the Technical Specifications and Scope of Work	On-Prem
3.	UEBA	As per the Technical Specifications and Scope of Work	On-Prem
4.	SOAR	As per the Technical Specifications and Scope of Work	On-Prem
5.	EDR	As per the Technical Specifications and Scope of Work	SaaS
6.	DAST	As per the Technical Specifications and Scope of Work	On-Prem
7.	PIM	As per the Technical Specifications and Scope of Work	On-Prem
8.	TIP	As per the Technical Specifications and Scope of Work	On-Prem
9.	Anti - APT	As per the Technical Specifications and Scope of Work	On-Prem
10.	DLP	Retained Solution - As per Scope of Work	On-Prem
11.	NBA	Retained Solution - As per Scope of Work	On-Prem
12.	Anti - DDOS	Retained Solution - As per Scope of Work	On-Prem
13.	VM	Retained Solution - As per Scope of Work	On-Prem
S. NO	Services	Requirement	Deploy Mode
1.	BAS (Breach Attack Simulation)	As per the Scope of Work	SaaS
2.	Threat Intel Services	As per the Scope of Work	SaaS
3.	Cyber Range	As per the Scope of Work	SaaS



4.	DDOS Drill	As per the Scope of Work	SaaS
----	------------	--------------------------	------

2. Scope of Work

- a. Bank intends to implement NGSOC and other Security Solutions for protecting information assets at Primary Data Centre at Bengaluru and Disaster Recovery Site at Mumbai. Bank expects Bidder to provide full-fledged services including but not limited to design, supply, implementation, configuration, customization, integration, migration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, arrangement with OEM and any other activities related to or connected to the cyber security solutions, devices, applications & technologies together at the Bank during the entire contract period of 5 years.
- 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.
- c. Supply all required infrastructure and manpower for operations of NGSOC and other security solutions as per the detailed scope mentioned in this RFP.
- d. Deploy qualified personnel in Bank's premises at Bengaluru and Mumbai for configuration, monitoring and management of in scope NGSOC solutions.
- e. Inventory management of all assets (Hardware and Software etc.) supplied as part of the RFP.
- 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.
- g. 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.
- h. Supporting the Risk Management Process of the Bank by mitigating the risks for the assets under the scope of NGSOC.
- i. Managing reporting and logging of security alerts/ incidents through proposed SOAR & bank existing Service Now ITSM tool and closing the same as per the agreed SLA.
- j. Deliver and implement the solutions & services to the Bank in compliance with International Standards such as ISO, PCI-DSS, etc. and advisories issued from regulatory authorities and statutory directions.
- k. Ensure that the supplied NGSOC solutions and services top-of-the-line in terms of specifications, support, compatibility with other products. Also, they should be up to date in terms of product releases, version upgrades, patches, and other service packs.
- l. The service delivery (SLA Management) and periodic reporting should be done through automated dashboards.
- 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.
- n. Provide forensic support, which is limited to sharing of evidences from in-scope security solutions and support on investigation.
- o. Ensure continual improvement of NGSOC operations, incorporating industry best practices, closure of audit observations and regulatory guidelines.
- p. Ensure graceful transition from existing CSOC of the Bank to new NGSOC along with migration activities.
- q. The proposed solutions implemented by the Bidder should adopt evolving threat and technological advancements, including quantum computing.





3. Sizing & Scalability Requirements

Canara Bank intends to implement captive NGSOC. The implementation, migration, upgradation, management, monitoring of NGSOC will be at Bank’s premises.

The broad level requirements are mentioned below:

Sl. No	SOC solution	Present Sizing	DC and DR applicability for NGSOC	HA in DC and DR for NGSOC	Estimated Future Sizing (For 5 years)	Remarks
1	SOAR	NA	Yes	Yes	15 Agent license	
2	UEBA	NA	Yes	Yes	90,000 users/ Entity licenses	
3	Breach Attack Simulation	NA	NA	NA	SaaS model supporting 99.90 percent uptime Report Frequency: monthly basis	
4	Threat Intelligence Management Platform	NA	Yes	No	5 user licenses	
5	DAST	NA	Yes	No	600 Application licenses along with the hardware	
6	Anti-DDoS	Refer Annexure	Yes	Yes	2 AED 8100 appliances with 5Gbps software licenses. Extension of licenses aligned with new appliances One appliance each in DC, DR	
7	DLP	Refer Annexure	Yes	Yes	Upgrade the licenses to 90k for Endpoint and Network DLP Licenses along with new hardware	
8	NBA	Refer Annexure	Yes	Yes	Upgrade the licenses to 3 lakh FPS license along with the new hardware and additional features	
9	Threat Intel Services	NA	NA	NA	SaaS model with 99.90 percent uptime Reporting frequency - every month	
10	VA	2300 licenses	Yes	Yes	5000 licenses along with the new hardware	

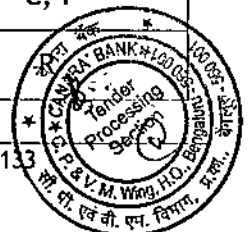


11	SIEM	30K EPS (Per site)	Yes	Yes	1,00,000 EPS sustainable to 1,50,000 EPS for each DC and DR
12	PCAP	NA	Yes	NO	10GBPS software throughput & 20 GBPS hardware capacity
13	PIM	750 privileged user licenses	Yes	Yes	1500 privileged users licenses required along with the UAT environment
14	EDR	NA	NA	NA	90, 000 licenses (85,000 for Endpoints & 5000 for Servers) 99.90% SaaS Uptime
15	Anti-APT	NA	Yes	Yes	20 Gig Hardware Capacity with 10Gig on day one TLS Inspection Throughput at DC, DR
16	Cyber Range	NA	NA	NA	10 user licenses with unlimited platform access & 40 hours per year live team exercise. At any particular time, bank should have privilege of modify/ delete/ update user IDs.
17	DDoS Drill	NA	NA	NA	Number of applications per year - 3 Number of test cases: 10 minimum

4. Responsibility Matrix:

1. SOC Governance & Program Management

Service	Activity	Canara Bank	OEM	System Integrator
Governance & Strategy				
SOC Governance & Program Management	SOC vision, mission, and objectives	A, R	I	C, I
	Update SOC governance structure and roles	A, R	I	C, I
	Maintain SOC policies, procedures, and standards	A, R	I	C, I
	Define SOC metrics and key performance indicators (KPIs)	A, C	I	

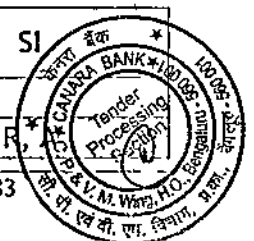




Develop method to track SOC metrics and KPIs	A, R	I	C, I
Provide SOC metrics and KPIS	A	I	R
Track SOC Metrics and KPIs	R, A	I	C, I
Provide strategic guidance to improve SOC metrics and KPIs	R, A	I	C, I
Implement recommendations to improve SOC metrics and KPIs	A, C	I	R
Periodic review of SOC Metrics and KPIs	A, C	I	R
Program Management			
Develop overall SOC management plan	C	I	A, R
Manage project scope and timeline	C	I	A, R
Coordinate and manage project resources	C	I	A, R
Track project progress and milestones	C	I	A, R
Report project status and risks to stakeholders	C	I	A, R
Risk Management			
Identify and assess SOC risks	A, R	I	C, I
Develop risk mitigation strategies	A, R	I	C, I
Implement and monitor risk controls	A, C	I	R
Report on risk status and remediation progress	A	I	R
Compliance Management			
Identify applicable regulations and standards	R, A	I	C, I
Ensure SOC compliance with requirements	A, C	I	R
Conduct regular compliance audits and assessments	A, I	C	R
Report on compliance status and findings	A, I	I	R
Communication & Reporting			
Establish communication channels and protocols	R, A	I	C, I
Provide regular updates on SOC progress and performance	A, C	I	R
Report on SOC incidents and response actions	A, C	I	R
Communicate SOC value and ROI to stakeholders	A, C	I	R

II. Threat Management

S.No	Activity	Bank	Bank's IT Operation	SI
Security Monitoring				
1	24*7 Monitoring of security events and alerts	C, I	I	



2	Perform Initial Triage	C, I	C	R, A
3	Provide necessary details requested by SOC Team	A, I	R	C
4	Raise Security Incidents	C, I	C	R, A
5	Escalate incident to SME as necessary	C, I	I	R, A
6	Provide Daily, weekly, and Monthly report	C	I	R, A
Incident Response				
7	Maintain incident response plan	A, I	C	R
8	Create playbooks for incident triage and investigation	C	C	R, A
9	Investigate security incidents	C, I		R, A
10	Create containment, Eradication and Recovery plan	A, C, I	C	R
11	Implement containment, Eradication and Recovery plan	A	R	C, I
12	Create investigation report and lesson learned document	C, I	C, I	R, A
13	Track the lesson learned until closure	C, I	C, I	R, A
14	Implement suggested lesson learned action items	C, R	C, R	R, A
Dashboards and Reports				
15	Provide Daily, weekly, and Monthly report	C	I	R, A
16	Track Meantime to Detect (MTTD), Mean Time to Respond (MTTR) and Mean time to Close (MTTC)	C, R	I	R, A
17	Provide strategy to improve MTTD, MTTR and MTTC	C, R	I	R, A

III. Platform Management

S.No	Activity	Bank	Bank's IT Operation	SI	OEM
SIEM, UEBA					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, A		R	
3	License Management	C, A		R	C
4	SOP creation and maintenance	C, I		R, A	C
5	Log source integration	C, I	R	R, A	
6	Troubleshooting Log source issues	C, I	C, I	R, A	
7	Log Baselining	C, I	C, I	R, A	
8	Backup management	C, I	C, I	R, A	
9	Major version upgrades	C, I	C, I	R, A	C
10	Minor upgrades	C, I	C, I	R, A	C
11	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
12	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
13	Use case creation, testing and finetuning	C, I	C, I	R, A	C
14	Creation of parser for unknow log sources	C, I	C, I	R, A	R
15	Create dashboards and reports	C, I	C, I	R, A	C
16	Reduce False Positive Alerts	C, I	C, I	R, A	C
17	Perform DR drill	A, C, I	C, I	R	
18	Perform Backup testing	C, I	C, I	R, A	
19	Integration with SOAR and ITSM tools	C, I	C, I	R, A	





20	Integration with Directory services, SIEM and SOAR	C, I	C	R, A	
21	Rule and Policy Management	C, I		R, A	
22	Performance Management	C, I	C	R, A	C
23	Integration with Security solutions and Directory services	C, I	C, I	R, A	
SOAR					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, A		R	
3	License Management	C, A		R	C
4	SOP creation and maintenance	C, I		R, A	C
5	Integration with Security solutions and Directory services	C, I	C, I	R, A	
6	Create custom integration	C, I	C, I	R, A	C
7	Creation and testing of playbooks	C, I	C, I	R, A	C
8	Reduce False Positive Alerts	C, I	C, I	R, A	C
9	Management of Playbooks which includes troubleshooting, version control etc.	C, I	I	R, A	
10	Major version upgrades	C, I	C, I	R, A	R
11	Minor upgrades	C, I	C, I	R, A	C
12	Create dashboards and reports	C, I	C, I	R, A	C
13	Perform DR drill	A, C, I	C, I	R	C
14	Perform Backup testing	C, I	C, I	R, A	C
15	Follow-up with OEM for issues/defects	C, I	C, I	R, A	R
16	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
17	Perform daily health check-up	C, I	C, I	R, A	
EDR					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C
4	Agent Package creation based on the Operating systems	C, I	C, I	R, A	C
5	SOP creation and maintenance	C, I		R, A	C
6	Installation of agents via centralized solution	C, I	R	C	
7	Troubleshooting agent installation	C, I	C, I	R, A	C
8	Agent compliance monitoring	C, I	C, I	R, A	
9	Policy Management	C, I	C, I	R, A	
10	Reduce False Positive Alerts	C, I	C, I	R, A	C
11	Exception Management	C, I	C, I	R, A	C
12	Integration with SOAR and SIEM	C, I		R, A	C
13	Create dashboards and reports	C, I	C, I	R, A	C
14	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
15	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
PIM					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	
4	Exception Management	C, I	C, I	R, A	





5	Application onboarding	C, I	C, I	R, A	C
6	User access flow design	C, I	C, I	R, A	
7	User onboarding	C, I	C, I	R, A	
8	PAM agent installation on the systems/servers	C, I	R	C, I	
9	Access Policy creation and management	C, I	C, I	R, A	C
10	MFA configuration and management	C, I	C, I	R, A	C
11	Reduce False Positive Alerts	C, I	C, I	R, A	C
12	Backup management	C, I	C, I	R, A	
13	Major version upgrades	C, I	C, I	R, A	R
14	Minor upgrades	C, I	C, I	R, A	C
15	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
16	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	R
17	Create dashboards and reports	C, I	C, I	R, A	C
18	Perform DR drill	C, I	C, I	R, A	C
19	Perform Backup testing	C, I	C, I	R, A	C
20	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	A	R
21	Integration with SOAR and ITSM tools	C, I	C, I	R, A	C
NBA					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C
4	SOP creation and maintenance	C, I		R, A	C
5	Network configuration to capture the flows	C, I	R	C, I	C
6	Policy Management	C, I	C, I	R, A	
7	Reduce False Positive Alerts.	C, I	C, I	R, A	C
8	Backup management	C, I	C, I	R, A	
9	Major version upgrades	C, I	C, I	R, A	C
10	Minor upgrades	C, I	C, I	R, A	C
11	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
12	Integration with SOAR and ITSM tools	C, I	C, I	R, A	C
13	Create dashboards and reports	C, I	C, I	R, A	C
14	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
Anti-DDoS					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C
4	SOP creation and maintenance	C, I		R, A	C
5	Onboarding applications	C, I	R	C, I	C
6	Policy Management	C, I	C, I	R, A	
7	Reduce False Positive Alerts	C, I	C, I	R, A	C
8	Backup management	C, I	C, I	R, A	
9	Major version upgrades	C, I	C, I	R, A	C
10	Minor upgrades	C, I	C, I	R, A	C
11	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C



12	Integration with SOAR and ITSM tools	C, I	C, I	R, A	C
13	Create dashboards and reports	C, I	C, I	R, A	C
14	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
DLP					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C
4	Agent Package creation based on the Operating systems	C, I	C, I	R, A	C
5	SOP creation and maintenance	C, I		R, A	C
6	Installation of agents via centralized solution	C, I	R	C	
7	Troubleshooting agent installation	C, I	C, I	R, A	C
8	Agent compliance monitoring	C, I	C, I	R, A	
9	Policy Management for both Network and Endpoint DLP	C, I	C, I	R, A	
10	Reduce False Positive Alerts	C, I	C, I	R, A	C
11	Exception Management	C, I	C, I	R, A	C
12	Backup management	C, I	C, I	R, A	
13	Major version upgrades	C, I	C, I	R, A	C
14	Minor upgrades	C, I	C, I	R, A	C
15	Integration with SOAR and SIEM	C, I		R, A	C
16	Create dashboards and reports	C, I	C, I	R, A	C
17	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
18	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
VA/DAST					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C
4	SOP creation and maintenance	C, I		R, A	C
5	Create policy according to the OS, Application and Device type	C, I	C, I	R, A	
6	Perform Scan and application testing as per the defined schedule	C, I	C, I	R, A	
7	Reduce False Positive Alerts	C, I	C, I	R, A	C
8	Track vulnerabilities until closure	C, I	C, I	R, A	
9	Exception Management	C, I	C, I	R, A	C
10	Integration with SOAR and SIEM	C, I		R, A	C
11	Create dashboards and reports	C, I	C, I	R, A	C
12	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
13	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
Threat Intelligence Platform					
1	Perform daily health check-up	C, I	C, I	R, A	
2	User Access Management	C, I		R, A	
3	License Management	C, I		R, A	C



4	SOP creation and maintenance	C, I		R, A	C
5	Database onboarding	C, I	C, I	R, A	
7	Reduce False Positive Alerts	C, I	C, I	R, A	C
8	Backup management	C, I	C, I	R, A	
9	Major version upgrades	C, I	C, I	R, A	C
10	Minor upgrades	C, I	C, I	R, A	C
11	Follow-up with OEM for issues/defects	C, I	C, I	R, A	C
12	Integration with SOAR and ITSM tools	C, I	C, I	R, A	C
13	Create dashboards and reports	C, I	C, I	R, A	C
14	Fix vulnerabilities identified in the platform within the defined SLA	C, I	C, I	R, A	C
Breach Attack Simulation					
1	Create synthetic test cases	C, I	C, I	R, A	C
2	Perform Synthetic test	C, I	C, I	R, A	C
3	Prepare Lesson Learned document	C, I	C, I	R, A	
4	Fix the identified gaps	C, I	R	R, A	
5	Create dashboards and reports	C, I	C, I	R, A	C

5. Manpower Requirement

This is the minimum manpower requirement per shift. Bidder shall factor the total resource required to meet the below requirement.

Threat Management

Analyst Type	Morning	General	Afternoon	Night
L1	6	0	6	2
L2	2	0	2	1
L3	0	2	0	0
Project Manager	0	1	0	0

Use case Engineering & Automation

Analyst Type	Morning	General	Afternoon	Night
L1	0	0	0	0
L2	0	2	0	0
L3	0	1	0	0

Endpoint Security

Analyst Type	Morning	General	Afternoon	Night
L1	1	0	1	1
L2	1	0	1	0
L3	0	2	0	0

Network Security

Analyst Type	Morning	General	Afternoon	Night
L1	0	2	0	



L2	0	3	0	0
L3	0	0	0	0

PIM Specialist

Analyst Type	Morning	General	Afternoon	Night
L1	0	0	0	0
L2	0	3	0	0
L3	0	1	0	0
OEM (L3)	0	1	0	0

SIEM, SOAR & UEBA Engineer

Analyst Type	Morning	General	Afternoon	Night
L1	0	0	0	0
L2	0	2	0	0
L3	0	2	0	0
L3 (SOAR)	0	1	0	0

Vulnerability Management, BAS, ASM, DAST

Analyst Type	Morning	General	Afternoon	Night
L1	0	0	0	0
L2	0	2	0	0
L3	0	1	0	0

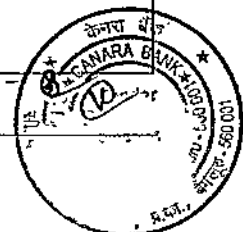
6. Manpower Roles and Responsibilities

Resources Requirement		
L1 Triage Analyst		
S.No	Role & Responsibilities	Resources/Shift
1	24*7*365 monitoring of security alerts and events generated by SIEM and other in scope security solutions (both on-prem and SaaS solution)	6resources 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
2	Triage potential security incidents and assigned severity based on the defined criteria	
3	Perform preliminary analysis to validate whether an alert represents a true security incident	
4	Investigate basic indicators of compromise (IOCs) and determine the scope and impact of the incident	
5	Escalate confirmed incidents to SOC L2 analysts with all relevant information	
6	Accurately document all findings, actions taken, and evidence collected during the triage process	
7	Maintain detailed logs of incident activities for further analysis and reporting	
8	Follow established incident response playbooks and standard operating procedures	



9	Execute predefined use cases and scripts to gather additional information about alerts	Mumbai respectively
10	Monitor the health and performance of security monitoring tools and systems	
11	Report any issues or anomalies with the security tools to ensure continuous monitoring	
12	Participate in training and development programs to enhance cybersecurity skills	
Skills Required:		
1	Understanding of networking and security concepts.	
2	Familiarity with common cyber threats and attack vectors.	
3	Proficiency in using proposed security monitoring tools and SIEM platforms.	
4	Analytical skills to assess and validate security alerts.	
5	Good communication and documentation skills.	
6	Ability to follow established procedures and protocols.	
7	The triage analyst shall have minimum 2 years of experience in Monitoring and responding to cyber threats, possess at least one of the following certifications, a) Security+ b) CEH c) ECSA	

L2 Incident Responder		
S. No	Role & Responsibilities	Resources/Shift
1	24*7 analysis of the alerts escalated by the L1 Team	2 resources per shift for Morning and Afternoon and 1 resource in night shift.
2	Lead and coordinate response activities for High and medium security incidents	
3	Perform root cause analysis to determine the origin and impact of incidents	
4	Develop and implement containment, eradication, and recovery strategies	
5	Correlate data from multiple sources to identify and respond to security events	
6	Develop and maintain incident response playbooks and runbooks	
7	Ensure standard operating procedures (SOPs) are followed and updated as needed	
8	Escalate critical incidents to SOC L3 or other senior incident responders when necessary	
9	Review all the alerts handled by SOC L1 Triage team and provide suggestions to improve triaging of the alerts	
10	Document all actions taken during incident investigations and response	
11	Prepare detailed incident reports and post-incident reviews	
12	Communicate findings and recommendations to management and relevant stakeholders	
13	Participate in security audits and assessments	



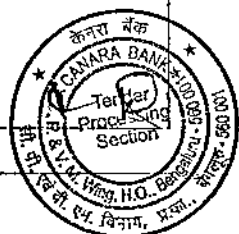
14	Conduct regular reviews of incident response processes to identify areas for improvement
15	Provide SIEM finetuning recommendations to reduce the false positive alerts
16	Suggest new SIEM use cases to improve threat detection coverage
17	Provide mentorship and guidance to L1 analysts

Skills Required:

1	Strong understanding of networking and security fundamentals.
2	Proficiency in analyzing logs and network traffic.
3	Experience with malware analysis and reverse engineering.
4	Knowledge of scripting and automation (e.g., Python, PowerShell).
5	Excellent problem-solving and analytical skills.
6	Strong communication and documentation skills.
7	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) CISSP f) Any SIEM Certification

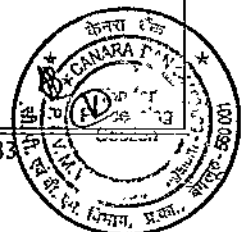
L3 Incident Investigator

S.No	Role & Responsibilities	Resources/Shift
1	08*5 analysis of the alerts escalated by the L2 or L1 Team	2 Resources in General shifts
2	Lead the response to critical security incidents.	
3	Coordinate with other teams to contain, mitigate, and remediate incidents.	
4	Develop and execute advanced incident response strategies and playbooks.	
5	Gather and analyze evidence from compromised systems.	
6	Conduct malware analysis to understand the behavior and impact of malicious code.	
7	Analyze logs, network traffic, and other data sources to trace the origins of attacks.	
8	Proactively hunt for threats within the network and endpoints.	
9	Utilize threat intelligence to identify emerging threats and vulnerabilities.	
10	Develop and refine threat detection use cases and signatures.	
11	Perform in-depth root cause analysis to understand how incidents occurred and their impact.	
12	Identify security gaps and weaknesses exploited by attackers.	
13	Provide recommendations for improving security controls and preventing future incidents.	
14	Work closely with other IT and security teams to coordinate response efforts.	
15	Provide guidance and mentorship to L1 and L2 analysts.	
16	Document all actions taken during incident response in detail.	
17	Prepare comprehensive incident reports and post-incident reviews.	



18	Communicate findings, impact, and recommendations to senior management and stakeholders.
19	Evaluate and recommend new security tools and technologies to enhance incident response capabilities.
20	Continuously improve incident response processes and playbooks.
21	Develop automation scripts to streamline incident response tasks.
22	Conduct training sessions for SOC staff to improve their incident response skills.
23	Stay current with the latest threats, attack techniques, and security best practices.
24	Participate in industry conferences, workshops, and training programs.
Skills Required:	
1	Deep understanding of networking, operating systems, and security principles.
2	Expertise in digital forensics, malware analysis, and reverse engineering.
3	Strong analytical and problem-solving skills.
4	Proficiency in using advanced security tools and technologies.
5	Excellent communication and documentation skills.
6	Ability to handle high-pressure situations and make critical decisions.
7	Continuous learning mindset to stay updated with the evolving threat landscape.
8	The L3 Incident investigator shall have minimum 7 years of experience in Incident response; possess at least one of the following certifications, 1) CHFI 2) GCFA 3) GCFE 4) CISSP

Platform Engineer - SIEM, SOAR and UEBA		
S.No	Role & Responsibilities	Resources/Shift
1	08*6 general shift and provide on call support for critical issues	4 Resources in General shifts <u>L2</u> Resources with 4-6 Years of experience and <u>L3 (8*5 support and On demand support during off hours)</u> resources with 6-9 Years of experience
2	Platform management for SIEM, SOAR, UEBA, NBAD, DLP, Anti-APT, Deception, VM, and any other in scope solutions.	
3	Log Source Management, Ensure timely integration of log sources	
4	SIEM Rule Management - Ensure rules are up to date to reduce false positives	
5	Performance Tuning: Optimize SIEM performance to ensure efficient processing and alerting.	
6	Compliance and Reporting: Generate reports for compliance and audit requirements.	
7	Integrate UEBA solutions with existing security infrastructure.	
8	Model Development: Develop and fine-tune machine learning models to detect abnormal activities.	
9	Provide insights and context to support security investigations.	
10	Reduce false positives by fine-tuning alerting mechanisms.	
11	Create automated workflows to streamline security operations."	
12	Implement and manage incident response playbooks.	
13	Integrate SOAR platforms with various security tools and systems.	



14	Enhance the efficiency of security operations through orchestration and automation.
15	Track and report on the effectiveness of automation and response efforts.
16	Platform Management: The installation, configuration, maintenance, update, upgrade of SIEM, UEBA, SOAR, Anti - APT, NBA, DLP, Deception, VA and any other in scope solutions.
17	Work closely with other security teams to enhance threat detection, investigation, and response processes.
18	Provide training and support to security analysts on the use and capabilities of these platforms.
19	Ensure that the platforms meet regulatory and compliance requirements.
20	Perform health check-up daily and share the reports with the stakeholders
21	Perform major and minor upgrades of the platform
22	Ensure all the components are up to date (n-1)
23	Monitor the availability of all the deployed components
Skills Required:	
1	Deep understanding of networking, operating systems, and security principles.
2	Have designed and implemented the proposed solutions in at least 2 clients
3	Strong analytical and problem-solving skills.
4	Proficiency in using advanced security tools and technologies.
5	Excellent communication and documentation skills.
6	Ability to handle high-pressure situations and make critical decisions.
7	Continuous learning mindset to stay updated with the evolving threat landscape.
8	The platform engineer shall have minimum 4-9 years of experience in managing the proposed solutions with OEM certification

Endpoint Security Specialist		
S.No	Role & Responsibilities	Resources/Shift
EDR		
1	08*6 general shift and provide on call support for critical issues	2 Resources in General shifts 2 Resources in Mrng shift & Second shift 1 in night shift. On call support whenever required to handle High and Critical issues
2	Deploy, configure, and maintain Endpoint Detection and Response (EDR) platforms.	
3	Create and deploy EDR agent packages using centralized solutions such as SCCM	
4	Policy Development: Develop and enforce security policies and procedures for endpoint protection.	
5	Ensure endpoints are up to date with the latest security patches and software updates.	
6	Configure EDR policies to align with organizational security requirements.	
7	Customize detection rules to enhance threat detection capabilities.	
8	Provide regular updates to management on the status of endpoint security.	

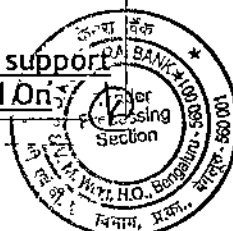


9	Conduct training sessions for employees on best practices for endpoint security.	L3 (8*5 support and On demand support during off hours)
10	Raise awareness about emerging threats and how to avoid them.	
11	Stay updated on the latest trends and advancements in endpoint security.	
12	Evaluate and recommend new EDR tools and technologies.	
13	Participate in threat intelligence sharing to enhance the organization's security posture.	
14	Work closely with IT teams to ensure seamless integration of EDR solutions with existing infrastructure.	
15	Troubleshoot any agent related issues along with IT team	
16	Collaborate with the Security Operations Center (SOC) and other security teams to improve overall threat detection and response capabilities.	
17	Support any internal and external audit and provide necessary logs/reports within the agreed timeline	
18	Close all the identified vulnerabilities within the defined timeline	
19	Liaise with vendors and service providers to manage and optimize EDR solutions.	
20	Create Agent installation SOPs for various operating systems which can be followed by IT team for manual installation of agents	
21	Create and maintain knowledgebase capturing the known issues and the solutions	
DLP		
1	08*6 general shift and provide on call support for critical issues	
2	Deploy DLP solutions on servers, endpoints, and cloud services.	
3	Troubleshoot agent related issues along with IT Team	
4	Configure DLP policies and rules for both network and endpoint DLP to identify and protect sensitive data.	
5	Ensure the DLP solution is properly integrated with existing security tools and infrastructure.	
6	Develop DLP policies based on organizational data protection requirements.	
7	Classify and categorize data to apply appropriate DLP rules.	
8	Regularly review and update DLP policies to address new threats and business needs.	
9	Conduct periodic audits to ensure DLP policies are effectively enforced.	
10	Ensure DLP policies comply with relevant data protection regulations (e.g., GDPR, HIPAA).	
11	Generate reports for compliance audits, highlighting data protection measures and incidents.	
12	Provide regular updates to senior management on the effectiveness of the DLP program.	
13	Conduct training sessions for employees on data protection best practices and DLP policies.	
14	Raise awareness about the importance of data security and how to handle sensitive information.	
15	Work closely with IT, legal, and compliance teams to align DLP policies with business objectives.	
16	Collaborate with data owners to understand data flows and protection requirements.	



17	Liaise with vendors and service providers to optimize the performance of the DLP solution.
18	Perform Health check daily and share the report
19	Ensure all the components are up to date (n-1)
20	Monitor the availability of all the deployed components
21	Support any internal and external audit and provide necessary logs/reports within the agreed timeline
22	Close all the identified vulnerabilities within the defined timeline
23	Create Agent installation SOPs for various operating systems which can be followed by IT team for manual installation of agents
24	Create and maintain knowledgebase capturing the known issues and the solutions
Deception	
1	Deploy deception agents as per the requirement
2	Ensure all the agents are healthy and have the latest update
3	Troubleshoot agent related issue along with the IT team
4	Integrate deception solutions with the SIEM and SOAR solution
5	Manage policies to ensure all the activities pertaining to deception decoys are captured and sent to SIEM solutions
Skills Required:	
1	Deep understanding of networking, operating systems, and security principles.
2	Have designed and implemented the proposed solutions in at least 2 clients
3	Strong analytical and problem-solving skills.
4	Proficiency in using advanced security tools and technologies.
5	Excellent communication and documentation skills.
6	Ability to handle high-pressure situations and make critical decisions.
7	Continuous learning mindset to stay updated with the evolving threat landscape.
8	The platform engineer shall have following experience L1 Resource - Minimum 2 years, L2 Resource with 4-6 Years L3 Resource with 6-9 Years of experience in managing the proposed solutions and have OEM certifications

PIM Specialist		
S.No	Role & Responsibilities	Resources/Shift
1	08*6 general shift and provide on call support for critical issues	5 Resources in General shift. On call support whenever required to handle High and Critical issues
2	Deploy and configure proposed PIM solution	
3	Configure policies and settings to ensure secure management of privileged accounts.	
4	Integrate PIM systems with other security tools and infrastructure.	
5	Develop and implement access control policies for privileged accounts.	
6	Ensure that privileged access is granted only to authorized personnel based on their roles and responsibilities.	
7	Regularly review and update policies to align with security best practices and regulatory requirements.	
		L3 (8*5 support and On

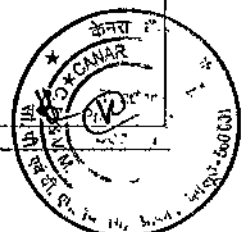


8	Ingest PIM logs with SIEM and SOAR for privilege account misuse cases
9	Conduct periodic audits of privileged account activities to ensure compliance with policies.
10	Respond to security incidents involving privileged accounts, including unauthorized access and account compromise.
11	Investigate incidents to determine the root cause and take corrective actions.
12	Work with other security teams to mitigate risks and prevent recurrence.
13	Perform regular maintenance tasks to ensure the optimal performance of PIM systems.
14	Apply patches and updates to PIM software to address vulnerabilities and improve functionality.
15	Optimize system configurations to enhance security and efficiency.
16	Provide support for issues related to PIM systems, escalating to L3 support when necessary.
17	Troubleshoot technical problems and resolve issues in a timely manner.
18	Assist users with PIM-related queries and provide guidance on best practices.
19	Generate reports on privileged account usage and security incidents.
20	Maintain documentation of PIM policies, procedures, and incident response actions.
21	Provide regular updates to management on the status and effectiveness of the PIM program.
22	Conduct training sessions for users on the proper use of privileged accounts and PIM systems.
23	Raise awareness about the risks associated with privileged account misuse and the importance of PIM.
24	Stay updated on the latest trends and technologies in Privileged Identity Management.
25	Evaluate and recommend new PIM tools and features to enhance security.
26	Work closely with IT, security, and compliance teams to align PIM policies with organizational goals.
27	Collaborate with vendors and service providers to ensure the effective operation of PIM solutions.
28	Engage with other stakeholders to ensure privileged account management practices meet business needs.

demand support during off hours)

Skills Required:

1	Expertise in leading PIM tools such as CyberArk, Beyond Trust, Thycotic, Arcos or Centrify
2	Strong understanding of the architecture, deployment, and configuration of PIM systems
3	Experience integrating PIM solutions with various IT and security systems (e.g., Active Directory, SIEM, IAM)
4	Knowledge of API integration and custom connector development
5	Proficiency in scripting languages (e.g., PowerShell, Python, Bash) for automation and customization
6	Experience in automating PIM tasks and workflows
7	Experience in preparing for and supporting audits related to privileged access management.



8	Experience in managing security projects from conception to completion
9	The PIM engineer shall have following experience L2 Resource with 4-6 Years L3 Resource with 6-9 Years of experience in managing the proposed solutions and have OEM certifications.

Network Security Specialist - NBAD, Anti -APT and Anti-DDoS

S.No	Role & Responsibilities	Resources/Shift
1	08*6 general shift and provide on call support for critical issues	5resources in General shift On call support whenever required to handle High and Critical issues <u>L3 (8*5 support and On demand support during off hours)</u>
2	Implement and manage Anti-DDoS solutions	
3	Deploy and maintain Network Behavior Anomaly Detection (NBAD) systems	
4	Optimize Anti-DDoS and NBAD systems for performance and accuracy	
5	Implement strategies to mitigate the impact of DDoS attacks, such as rate limiting, traffic filtering, and IP blacklisting.	
6	Generate reports on DDoS incidents, including attack vectors, sources, and mitigation effectiveness	
7	NBAD - Configure policies and thresholds to identify deviations from normal network behavior	
8	Lead the response to active DDoS attacks, coordinating with internal teams and external partners as necessary	
9	Investigate network anomalies detected by NBAD systems to determine if they are indicative of security incidents	
10	Work closely with network, security, and operations teams to coordinate defense efforts	
11	Liaise with vendors to ensure the effective operation and support of Anti-DDoS and NBAD solutions	
12	Maintain up-to-date documentation of Anti-DDoS and NBAD policies and procedures	
13	Integrate NBAD and Anti-DDoS solution with proposed SIEM solution	
Skills Required:		
1	Expertise in DDoS protection solutions such as Cloudflare, Akamai, Arbor Networks, and Radware.	
2	Proficiency in deploying and managing NBAD systems like Darktrace, Cisco Stealthwatch, and Vectra AI	
3	Proficiency in scripting languages (e.g., Python, Bash, PowerShell) to automate tasks and analyze data.	
4	Experience in developing automation scripts for traffic analysis and incident response	



5	<p>Shall have minimum 6 years of experience in managing the proposed solutions and have any of the mentioned certifications</p> <p>CISSP (Certified Information Systems Security Professional) CompTIA Security+ CCNA Security (Cisco Certified Network Associate Security) CCNP Security (Cisco Certified Network Professional Security) Certified DDoS Protection Specialist (CDPS) - Arbor Networks</p>
---	--

Project Manager		
S.No	Role & Responsibilities	Resources/Shift
1	Lead and manage the Security Operations Center (SOC) team to ensure effective monitoring, detection, and response to security incidents	<p>1 resource in General shift</p> <p>On call support whenever required to handle High and Critical issues</p>
2	Oversee the incident response process, ensuring timely and effective resolution of security incidents	
3	Train, and develop SOC team members to maintain a high level of expertise and performance	
4	Develop and implement SOC strategies, policies, and procedures to enhance security operations. Detailed Responsibilities	
5	Provide leadership and direction to the SOC team, ensuring alignment with Bank's goals and objectives	
6	Manage the day-to-day operations of the SOC, including staffing, scheduling, and performance management	
7	Oversee the incident response process, ensuring incidents are identified, investigated, and resolved promptly	
8	Coordinate with other teams and stakeholders during incident response to ensure effective communication and resolution	
9	Conduct post-incident reviews to identify lessons learned and improve future response efforts	
10	Develop and implement SOC policies, procedures, and playbooks to guide security operations and incident response	
11	Ensure policies and procedures are regularly reviewed and updated to reflect changes in the threat landscape and organizational needs	
12	Conduct regular performance reviews and provide feedback to team members	
13	Develop and implement long-term strategies to enhance the effectiveness and efficiency of the SOC	
14	Identify areas for improvement and implement initiatives to enhance SOC capabilities and performance	
15	Collaborate with other security teams, IT departments, and business units to ensure a coordinated approach to security	
16	Communicate security incidents and risks to senior management and other stakeholders	
17	Represent the SOC in meetings, presentations, and discussions with internal and external stakeholders	
18	Ensure accurate and timely documentation of security incidents, investigations, and actions taken	





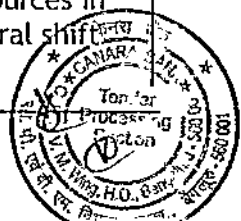
19	Generate regular reports on SOC activities, incident trends, and key performance indicators (KPIs).
20	Adhere to SOC SLA and share monthly trend report
21	Provide management with insights and recommendations based on SOC analysis and findings
22	Oversee the implementation, and management of security tools and technologies used by the SOC
23	Ensure tools and technologies are properly configured, maintained, and optimized for performance
24	Evaluate new security solutions and technologies to enhance SOC capabilities
Skills Required:	
1	Minimum 12 Years of experience in Security operation center and have 4 years as SOC Manager
2	Knowledge of incident response frameworks (e.g., NIST, SANS).
3	Proficiency in using and managing SIEM, SOAR and UEBA
4	Knowledge of relevant security standards and regulations (e.g., ISO 27001, GDPR, HIPAA).
5	Excellent verbal and written communication skills
6	Shall have any two certifications from the mentioned list, Cyber Security - Any One 1) CISSP (Certified Information Systems Security Professional) 2) GCIH (GIAC Certified Incident Handler) 3) GCFA (GIAC Certified Forensic Analyst) Incident and Program Management - Any One 4) ITIL (Information Technology Infrastructure Library) 5) PMP (Project Management Professional)

SIEM Use case and SOAR Automation Specialist		
S.No	Role & Responsibilities	Resources/Shift
1	Work with security teams to understand their requirements and translate them into SIEM use cases	3 resources in General shift On call support whenever required to handle High and Critical issues
2	Design, implement, and test SIEM use cases to detect specific types of security threats	
3	Continuously optimize use cases to improve detection accuracy and reduce false positives	
4	Develop and implement SIEM rules and correlation logic to detect security incidents	
5	Tune alerts to minimize false positives and ensure they are actionable	
6	Create and maintaining parsers/connectors in SIEM and SOAR	
7	Set appropriate thresholds for alerts based on analysis and threat intelligence	
8	Ensure data is normalized and enriched for effective correlation and analysis	
9	Develop and maintain log parsing rules to accurately ingest and process data	



10	Maintain detailed documentation of SIEM use cases, including design, implementation, and tuning procedures
11	Generate reports on the performance and effectiveness of SIEM use cases
12	Work closely with stakeholders, including SOC analysts, incident responders, and IT teams, to ensure use cases meet their needs
13	Collaborate with SIEM vendors to troubleshoot issues and implement new features
14	Innovate and experiment with new use case ideas to enhance the SIEM's detection capabilities
15	Design and develop automated workflows to address common security operations tasks and incidents
16	Write and maintain scripts (e.g., Python, PowerShell) to support automation tasks
17	Create and implement playbooks that automate the response to security incidents.
18	Develop use cases for automation based on common incident scenarios and threat patterns
19	Automate the enrichment of security alerts with contextual information to improve decision-making
20	Integrate various security tools (e.g., SIEM, EDR, ITSM (Service Now), firewalls, Threat intelligence platforms) with the SOAR platform.
21	Continuously optimize automated workflows to reduce false positives and enhance detection accuracy.
22	Tune the performance of automated workflows to ensure they operate efficiently and effectively.
23	Establish a feedback loop with security teams to gather input on automation performance and make necessary adjustments.
24	Monitor the performance and health of the SOAR platform and automated workflows
25	Maintain detailed documentation of automated workflows, playbooks, and scripts.
Skills Required:	
1	Proficiency with proposed SOAR and SIEM solutions
2	Experience in configuring, managing, and optimizing SOAR and SIEM platforms
3	Strong skills in scripting languages (e.g., Python, PowerShell, JavaScript) for developing automation scripts
4	Experience in writing and maintaining scripts to automate security tasks and processes
5	Experience in utilizing RESTful APIs to enable communication between different security tools
6	Experience in converting MITRE TTPs to Misuse cases for better detection and response
7	Shall have 7 Years of experience and proposed OEM certifications

Vulnerability Management & DAST Specialist		
S. No	Role & Responsibilities	Resources/Shift
1	Deployed resource shall ensure regular remote backups with retention capabilities, ensuring data restoration for at least the past 3 years.	2 resources in General shift





2	The deployed resource shall be assigned to handle any activities requested by the bank related to the Vulnerability Management (VM) solution.	On call support whenever required to handle High and Critical issues
3	The deployed resource should be responsible for deploying agents and the scanner within the bank's infrastructure.	
4	The deployed resource should be able to create customized dashboards as per the bank's requirements.	
5	The deployed resource should have at least 4 years of experience in security, particularly in Nessus and Tenable or any other Vulnerability Management (VM) solution, DAST solutions, deployments, updates, patching, and migrations.	
6	The deployed resource should also be capable of performing VA/PT and DAST scan as and when required by the bank.	
7	Deployed Resource should support deployment, testing & scanning activities required by the Bank as when required.	
8	Deployed resource should be able to implement automation in the VAPT process & integration of different solutions	

Skills Required:

1	Deployed resource should have good hands-on experience in Application Security Testing, Network Security Testing, Vulnerability Assessment & Penetration Testing.
2	Deployed resource should have excellent knowledge in Networking, network Security, Databases, Operating Systems etc.
3	The deployed resource should hold relevant security certifications, such as RHCE, CEH, CISSP, OSCP and CCNA.
4	Deployed resource should have good hands-on experience in Application Security Testing, Network Security Testing, Vulnerability Assessment & Penetration Testing.

Attack Surface Management & Breach Attack Simulation Specialist

S. No	Role & Responsibilities	Resources/Shift
1	Deployed resource should have expertise in Attack Surface Management (ASM), Breach and Attack Simulation (BAS), Vulnerability Management (VM) solution.	1 resource in General shift
2	The deployed resource shall be assigned to handle any activities requested by the bank related to the Attack Surface Management (ASM), Breach and Attack Simulation (BAS), Vulnerability Management (VM) solution.	On call support whenever required to handle High and Critical issues
3	The deployed resource should be able to create customized dashboards as per the bank's requirements.	
4	The deployed resource should also be capable of performing VA/PT scans as and when required by the bank.	
5	Deployed Resource should support Security testing & scanning activities as and when required by the bank.	
6	Deployed resource should be able to implement automation in the VAPT process & integrate different solutions such as GRC, SIEM, ITSM, etc.	
7	Deployed resource should have good hands-on experience for Application Security Testing, Network Security Testing, Vulnerability Assessment & Penetration Testing.	
8	Deployed resource should have expertise in Networking, network Security, Databases, Operating Systems etc.	



9	Deployed resource should be able to conduct penetration tests to exploit identified vulnerabilities and assess their impact.
10	Strong understanding of network protocols, operating systems (Windows, Linux), and application security.
11	Resource should be able to develop and execute test plans, scenarios, and scripts.
12	Deployed resource shall have Strong analytical and problem-solving abilities, Excellent written and verbal communication skills, Ability to work independently and as a part of team.
13	Work closely with IT and development teams to remediate identified vulnerabilities.
14	Provide guidance and expertise on security best practices.

Skills Required:

1	Proficient in using tools such as Nessus, Nmap, Metasploit, Burp Suite, and Wireshark etc.
2	The deployed resource should hold relevant security certifications, such as RHCE, CEH, CISSP, OSCP, CCNA, GPEN.

SOAR Specialist

S. No	Role & Responsibilities	Resources/Shift
1	Develop and design the overall SOAR architecture to meet security and automation needs.	1 resource in General shift
2	Define integration strategies with existing security tools and platforms.	On call support whenever required to handle High and Critical issues
3	Ensure the SOAR system is scalable to handle growing security operations.	
4	Create and maintain security playbooks for automating incident response procedures.	
5	Analyze security incidents and determine automation opportunities.	
6	Continuously improve existing playbooks for efficiency and effectiveness.	
7	Conduct thorough testing and validation of playbooks to ensure accuracy.	
8	Map data flows between different systems and ensure data consistency.	
9	Create custom scripts and connectors to facilitate integrations.	
10	Implement robust error handling and troubleshooting mechanisms for integrations.	
11	Provide technical guidance and mentorship to the team.	

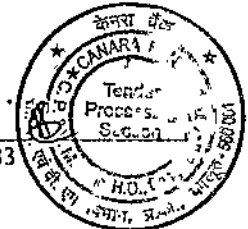
To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored -

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.

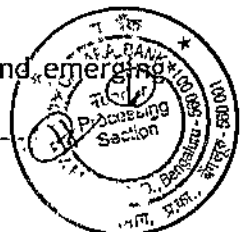
3. SOC Automation Engineer (L3) - Rs.25 Lakhs per year.



7. Scope of Work for Bidder/ System Integrator (SI)

The general scope based on which the NGSOC to be made operational are as under and the selected bidder /SI is expected to do following but not limited to:

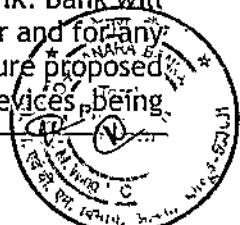
- The bidder should maintain accurate and updated inventory of all Hardware and Software being used for NGSOC and in scope solutions, including but not limited to Appliances, Servers, Virtual Machines, Software, and Licenses. Same shall be submitted to Bank as and when demanded.
- Bidder should involve respective OEM/ PS to carry out seamless migration of existing configuration, policies, data, and backup without affecting Bank's operations.
- 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).
- The Bidder is responsible to close all the Audit, VAPT and assessment observations of NG SOC solutions conducted by Bank in timely manner.
- Bidder should bring all the tools and equipment (Including cables, SFP, transreceivers) for successful commissioning of hardware and software for successful implementation of Solution.
- Bidder should supply products as specified, and services which include development, integration, management, maintenance, audit compliance, training, and knowledge transfer in respect of NGSOC and security solutions as detailed in the subsequent sections.
- Bidder has to provide all the SOC solutions with capacity of 10 Gig port interfaces.
- NGSOC implementation plan submitted by the Bidder should ensure optimum utilization of tools, technologies, and services which are part of the project
- A comprehensive strategy and Standard Operating Procedure (SOP) including the High Level Architecture Diagram with port details and data flow and Business Continuity & Disaster recovery diagram should be provided by the Bidder for all NGSOC solutions and services proposed under this RFP.
- 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.
- Compliance in gaps identified during various audits 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 should be closed by the Bidder in the proposed solution within the prescribed timeframe.
- 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.
- Bidder shall ensure that all the NGSOC and other security solutions have in-built AI/ML capabilities that significantly enhance the NGSOC team's ability to detect, prevent and respond to modern day cybersecurity threats.
- Bidder should ensure the proposed solutions should flexible enough to integrate with new technologies and standards as they emerge.
- The Bidder should ensure the proposed solutions should be compatible with or able to integrate with quantum-resistant technologies and encryption methods.
- The Bidder should ensure the proposed solutions should comply with current and emerging standards and regulations related to cybersecurity and quantum computing.



- Preparation of all documents related to deployment architecture, operation, and maintenance including the SOPs, user manuals & process documents etc. for all the underlying processes, roles and responsibilities of the personnel. Provide the complete set of Operation and System Manuals of all the systems/components provided as part of the NGSOC and other security solutions implementation in Hardcopies.
- 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.
- The bidder would be responsible for updates, patches, bug fixes, and version upgrades for the entire infrastructure without any additional cost to the Bank during the contract period. The same needs to be performed as per the Bank's policy.
- The bidder should provide the latest stable version of the solutions. The bidder would be responsible for replacing the out-of-support, out-of-service, end-of-life, and undersized, faulty infrastructure elements at no extra cost to the Bank during the entire contract period of 5 Years. In case of any such scenarios, replacement is to be done before the due date of the product/service and the intimation is to be given to the Bank at least one month before
- The solutions implemented as part of NGSOC should be in hot-standby with BC (Business Continuity) set-up at Bank's DR (Disaster Recovery) site. The Bidder would be responsible for installation, testing, commissioning, configuring, patching, regular backup, warranty, and maintenance of the system.
- The Bidder would be responsible for all technical support for maintaining the required uptime for NGSOC and in scope solutions as per SLA terms.

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.

- The Bidder would be the single point of contact for any matters requiring OEM support. The Bidder should have back-to-back agreements with respective OEMs to ensure onsite support for each solution. The Bidder should submit a letter issued by OEM in this regard.
- If the Bidder lacks the expertise for a particular in-scope tool, then the OEM shall provide implementation and professional services or support, for its own solution, on behalf of the Bidder, without any extra cost to Bank. In the absence of such an arrangement, the Bidder will be held accountable for OEM's inaction and penalty charges would be levied on the Bidder as per the SLA terms.
- 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.
- 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.
- Bidder will manage NGSOC operations in consultation with the Bank's team. The bidder shall deploy qualified personnel in the Bank's premises (as defined in Manpower Requirements) on a 24x7x365 basis for monitoring; management and operations of NGSOC and other security solutions.
- All the tools/ application/ OS supplied as part of the project should be latest and supplied with Enterprise-wide Licenses and all the licenses should be in the name of Canara Bank. Bank will have the right to use the tools for the functions provided by the tools in any manner and for any number of branches, offices, subsidiary units, joint ventures, or RRBs or in any future proposed Mergers, irrespective of the number of users, geographical location of the devices being



monitored. Bank will also have a right to relocate any one or all the tools to different locations without any extra cost to the bank.

- Bidder shall provide a list and details of licenses procured and also maintain the inventory database of all the licenses including any open-source tools/utilities and the updates installed. Bidder should intimate the Bank about impending expiry of licenses, AMC, ATS and other contracts at least 3 months in advance to allow Bank to ensure renewal of such contracts on timely basis.
- 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.
- Bidder should take appropriate license, support/ patches to be provided by OEM or by the bidder. No community support will be permitted for any tools
- The Bank has a complex infrastructure with multiple resources maintained and managed through multiple vendors. So, for seamless implementation close coordination is required with other vendors and bank personnel. A robust documentation system needs to be in place for all to understand the process and its responsibilities. Therefore, the Bidder has to provide the documentation for the project including but not limited to references regarding scope, functional and operational requirements, resource requirements, project design/plan, product description, guidance for best practices, implementation guidelines, user acceptance test plan, operation manual, user manual, procedure for each solutions, security implementation, training materials, evaluation scoreboards and matrices, etc.
- The Bidder is expected to size the hardware/appliance/storage as per the requirements of RFP document in the next stage of the procurement process. The Bidder's response should include the calculations / logic used to arrive at the sizing. In case any further clarification related to the sizing of hardware is required, Bidder can visit the bank to meet Chief Information Security Officer (Security Operation Centre) and seek clarification.
- Bidder / System Integrator (SI) should provide health reports and utilization details that may affect the day-to-day normal functionality of existing IT infrastructure.
- Adherence to agreed SLA and periodic monitoring and reporting of the same to the bank through a portal, which should be accessible to the Bank officials over intranet.
- 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.
- The bidder should commit to provide regular updates and patches to address new vulnerabilities and threats. This includes updates to counteract advancements in quantum computing and other emerging technologies.
- Bidder must ensure the high availability of all the NGSOC solutions wherever mentioned and other security solutions (In case a device goes down at DC, the function being performed by the device should be taken over by a corresponding device at DR site and vice versa).
- 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.
- 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.
- Bidder shall provide required load balancers for the NGSOC.



- NGSOC setup/infrastructure is subject to audit by Internal teams of Bank and/or third party such as International Organization for Standardization (ISO) 27001, ISO 31000, ISO 27017, ISO 27701, ISO 22301, PCI- DSS, regulatory & statutory authorities such as RBI, Cert-In, NCIPC, IT Act 2000 and subsequent amendments, DPDP act 2023 and various guidelines in place. It shall be the responsibility of the Bidder to provide necessary information and support to the auditors with concurrence of the Bank.
- 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.
- The Bidder shall take over operations and management of the currently running CSOC setup till NGSOC implementation is completed.
- 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.
- The Bidder should invariably ensure that backups for all the NGSOC solutions are taken in coordination with Bank's IT Team as per the Bank Policy.

8. Design and Implementation of NGSOC and other security solutions

- The architecture should be designed with consideration of OEM and Bank's existing infrastructure and DR/BCP plans for placement of various solutions, and optimum utilization of tools, technologies, and services.
- 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.
- The architecture should be designed with redundancy and no single point of failure. Bidder should involve OEM while designing the architecture incorporating industry best practices.
- The architecture should be vetted by respective OEM. For vetting respective OEM is expected to send email confirmation to bank and implementation to be done post approval from the Bank.
- Bidder will be responsible for the end-to-end setup of the NGSOC as per proposed architecture in close coordination with the respective OEMs.
- Bidder will also review the proposed architecture periodically and suggest and implement any changes as required by the Bank.
- The Bidder shall prepare documentation such as policies, SOPs, administrator, and user guides for all the solutions. It should cover all operation activities such as configuration, raising alerts, designing, and customizing reports, incident management, log monitoring and archiving, Business Continuity, agent deployments, backup, and recovery as applicable to various solutions implemented for NGSOC. The same has to be reviewed and share it with Bank once in a year.
- Bidder should provide knowledge transfer and training as per training schedule to Bank officials on the technology, functionality, and operations of the NGSOC.
- All the hardware Components/ servers/ appliances to be provided with Dual Power Supply.
- All Power cables must be of India Make and power supply must be redundant for all hardware.
- Bidder has to quote for highest/ premium/ enterprise support available from all the OEMs along with the documentation/ datasheet specifying the details of all the deliverables like



service part code, features etc. Bank will release the payment after verification of documentation of highest / premium / enterprise supports from OEM's.

9. NGSOC Operations

The Bidder is expected to perform the below operations but not limited to:

- The Bidder would be responsible for maintaining continued trouble-free operation of NGSOC solutions and other security solutions proposed, including Hardware/ Software/ Operating System/ Middleware and arrange to resolve or repair any issues preventing the same.
- Bidder should provide 24x7x365 onsite service availability for monitoring of the devices/servers/applications under scope and support for NGSOC and in scope solutions.
- The Bidder shall ensure monitoring of all the solutions in scope and underlying hardware, software, storage and network. Bidder will be also responsible for any escalation or trouble-shooting requirements. Bidder will also be liable for the closure of incidents/events as per SLA terms.
- Bidder shall monitor security devices/security logs to detect malicious or abnormal events and raise alerts for any suspicious events that may lead to security breaches in Bank's environment.
- 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.
- Bidder shall do pro-active and continuous monitoring of security events throughout Bank's network and infrastructure through correlation and analysis of logs from servers, network devices, security devices and application systems. The security monitoring service shall include following components:
 - Creation of Log baseline for Bank's infrastructure.
 - 24x7x365 logs and availability monitoring for Bank's infrastructure and business applications.
 - Rapid response to incidents.
 - Create awareness among stakeholders for handling of Security incidents.
- 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.
- Bidder shall ensure that all logs (raw or normalized) data must remain within the Bank's premises and for SaaS Solutions data must remain within jurisdiction of India.
- Further Bidder must follow the best practices for all compliances related to data and its security.
- 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:
 - Top Management (Organization level view)
 - Department Heads (View the data associated with their function group/business line)
 - CISO (Complete and detailed dashboard of the Security posture of the organization set-up being monitored through this NGSOC).
 - System Administrator (View of systems associated with this administrator)
 - Network / Security Administrator (View of devices/equipment for which they are an administrator)
 - Application Administrator (View of systems associated with this administrator)



- Auditor (Internal Auditors, IT Auditors, ISO Certification Auditor, or any other authorized official of the organization).
- Bidder must ensure that once the logs are written to the disk/ database no one including SIEM, or database/system administrator should be able to modify or delete the stored raw logs.
- Bidder must ensure that for each security incident, the solution should provide real-time remediation guidance.
- Bidder should develop custom plug-ins/connectors/agents for business application monitoring.
- Bidder should undertake Service availability monitoring of devices/servers configured and submit a report in case of service non-availability of the devices along with the status.
- 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.
- Bidder shall also assist during any other drill or assessments performed by the Bank.
- The Bidder must ensure that the observations arising out of audits are closed on top priority and to the satisfaction of the Bank, regulator, and its appointed auditors. Extreme care should be taken by the Bidder to ensure that audit observations do not get repeated in subsequent audits. Such non-compliance by Bidder shall attract penalty.
- The Bidder should proactively inform the Bank about potential security threats/vulnerabilities, new global security threats/zero-day attacks in circulation, suggest and implement suitable countermeasures to safeguard Bank's IT assets and customer data against such evolving threats/attacks along with the analysis.
- The Bidder shall monitor logs of various types of operating systems, network, security devices & solutions using log analysis tools on 24X7X365 basis.
- The Bidder shall perform Log correlation for in-depth monitoring and remedial actions on a daily basis.
- The Bidder should ensure rapid response to incidents/ alerts raised by security devices and/or monitoring systems.
- The Bidder should evaluate incidents and implement/recommend remedial measures.
- The Bidder should perform detailed Incident Analysis to identify the origin of threats, mitigation thereof, initiation of logical measures to prevent recurrence, which should be acceptable to Bank.
- The Bidder should implement required solutions for local log retention supported by log analysis tool for offline monitoring and reporting.
- The Bidder should ensure prudent measures based on advisories to the Bank on relevant threats and vulnerabilities supported with mitigation against identified risk exposure.

10. Security Device Management and Administration

- Device lifecycle management, License management and OEM co-ordination must be governed by the Bidder under Bank's supervision.
- The change management of all the devices, both hardware and software, must be adhering to the standards and policies set by the Bank and respective SLA will be applicable to the bidder.
- In case of any hardware/software malfunctioning, patch management, firmware upgradation or any other activities which require OEM support, the Bidder shall coordinate with the respective OEM of the solutions for faster resolution.
- SI Should ensure that all the solutions to be upgraded to the latest N-1 within 30 days from the latest version release date in UAT and within 60 days in Production. In case of non-availability of UAT, the same needs to be upgraded to latest N-1 in DR and then in production within 60 days from the latest version release date.
- The Bidder is expected to fine-tune the configuration/operational/process settings based on the trends identified as part of Advanced Threat Monitoring and should be part of the continuous improvement plan.
- 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.



- 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.

Scope for the onsite Management team includes but not limited to the following:

- System Hardening
- Update/Upgrade/Patching
- Backup/Restore
- Configuration Management
- Configuration Review and Performance Tuning
- Change Management
- Security Intelligence and Feeds
- Access Management
- NGSOC Manual/SOP Preparation and Review
- Security Device Problem Management
- DR Drill of Security Solutions
- Endpoint Management for DLP and EDR, troubleshoot endpoint related issues using remote session in case of endpoint is corrupted or not reporting.
- Security Inventory Management
- License & AMC Management
- OEM/Bidder Liaising for technical support
- Document and Record Management
- Reporting and designing of Dashboard
- Compliance Management
- Rule Base, signature and user management.
- Risk Analysis prior to configuration of any new server.
- Rule base optimization
- Co-ordination with OEM / vendor for up-to-date implementation of patches
- Quarterly management reporting for the configuration management and recovery testing
- Fault Management
- Compliance with internal policies, regulatory & legal requirements
- Risk assessment for the security devices
- Database management of all security solutions

Scope of work for the monitoring team includes but not limited to:

- Monitoring of security devices for any suspicious activities
- Reporting/escalations and lifecycle management for incidents or alerts
- Crisis Management
- Reporting and Dashboard
- Support in Threat Hunting/Red team exercises
- Forensic Analysis of any breach
- Monitoring of various logs
- Monitoring of resource utilization and daily report submission to the Bank.

11. Incidents and Problem Management



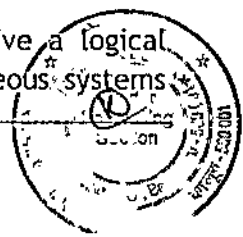
- The Bidder should provide detailed procedures for managing incidents - describing each phase of the process - prepare, identify, contain, eradicate, recover, and learn from the incidents responded to.
- The Bidder shall assist the Bank to establish a process for identifying, preventing, detecting, analyzing & reporting all Information Security incidents as per the internal policies of the bank, this may revise time to time.
- 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.
- The incident management solution should provide complete life cycle management of tickets from incident generation till closure of the incident. The solution should have the capability to structure rule-based workflow and calendar/event-based alerting capability.
- 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.
- The Bidder shall develop and maintain the up-to-date Escalation Matrix to handle security incidents efficiently.
- The incident management solution should facilitate time/event-based automated escalation of tickets as per the escalation matrix defined by the Bank.
- The Bidder should assist the Bank in investigating Information Security (IS) incidents through various modes like forensic evidence collection & preservation, log analysis etc.
- The Bidder shall arrange for troubleshooting any problem / issue reported in the context of security solutions & devices under the scope for NGSOC, and coordinate with the respective OEM / vendor till resolution. Troubleshooting should be performed within an accepted time limit as per SLA or as mutually agreed both Bank and the Bidder.
- Bidder shall be responsible to provide Root Cause Analysis (RCA) report for any problem / issue reported in the context of security solutions & devices under the scope for NGSOC.
- The Bidder should provide an alert mechanism solution to send alerts through SMS/e-Mail for any malicious activity observed in security solutions and other devices under the Bidder's scope. Bidder will track the status of the ticket opened in this context.
- 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.
- The bidder shall leverage proposed SOAR solution to automate incident investigation and response leveraging structured playbooks.
- The bidder shall create a roadmap to improve MTTD, MTTI and MTTR associated with security incidents.

12. Scope of Work for Proposed Solutions

Bidder shall deploy and manage the below-mentioned NGSOC solutions and security tools in Bank's premises to improve the security posture of Bank.

1. Security Information & Event Management (SIEM)

- The SIEM solution must enable Bank to collect, correlate, analyze, and derive a logical conclusion from logs, events, and information received by it from heterogeneous systems



including Networking and Security systems, OS, Web servers, Applications, Databases, all security solutions, other infrastructure etc. on 24x7x365 basis.

- Bidder shall offer a complete solution that shall include hardware, software, all licenses, upgrades, updates, and subscriptions required for meeting the requirement for correlating and analysis of events.
- The Bidder should offer the SIEM device with all requisite modules for the collection of logs, monitoring, and displaying of events on individual device or on a correlation basis, to facilitate administrators to take proactive actions for the prevention of security threats that might occur on network access devices.
- 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.
- The offered solution shall provide storage and correlation of logs from various devices in Bank's network.
- The Bank intends to implement SIEM with a centralized dashboard to monitor various IT Security threats originating across the organization. The solution should provide a single dashboard with the correlation of threats originating in the form of events across various networks, security, and system devices in the organization.
- Deploy the SIEM for the in-scope infrastructure and security tools.
- Integration of log sources from various devices/servers/network devices/ security devices/applications/APIs with SIEM as part of the implementation
- Bidder should discuss and develop use cases with Bank & Implement in the project phase.
- The bidder should configure/ migrate the use-cases deployed in the current SIEM to the newly procured SIEM.
- Bidder should carry out fine-tuning of use cases based on the evolving requirement in the ongoing operations phase.
- In case the systems are not able to send the logs to SIEM, the SIEM should be capable to fetch the logs from the point of failure.
- 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.
- Bidder will be responsible to store logs in an industry standard format, preferably in non-proprietary formats.
- Bidder/ OEM should develop parsers for all log sources without any cost to the Bank.
- Bidder/ OEM 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.
- The Bidder has to identify and document all the data sources that need to be integrated with the SIEM, such as firewalls, intrusion detection/prevention systems, antivirus solutions, servers, and applications.
- The Bidder will be responsible for performing the testings of the SIEM solutions which are as:
 - Functional Testing: Validate that the SIEM system functions as expected, including data collection, correlation, alerting, and reporting.
 - Performance Testing: Ensure the SIEM solution performs efficiently under load, especially during peak events.
- The Bidder has to document RCA for all incident, ensuring accurate and detailed records are maintained. Document lessons learned and integrated them into SOC processes, training, and threat detection strategies.



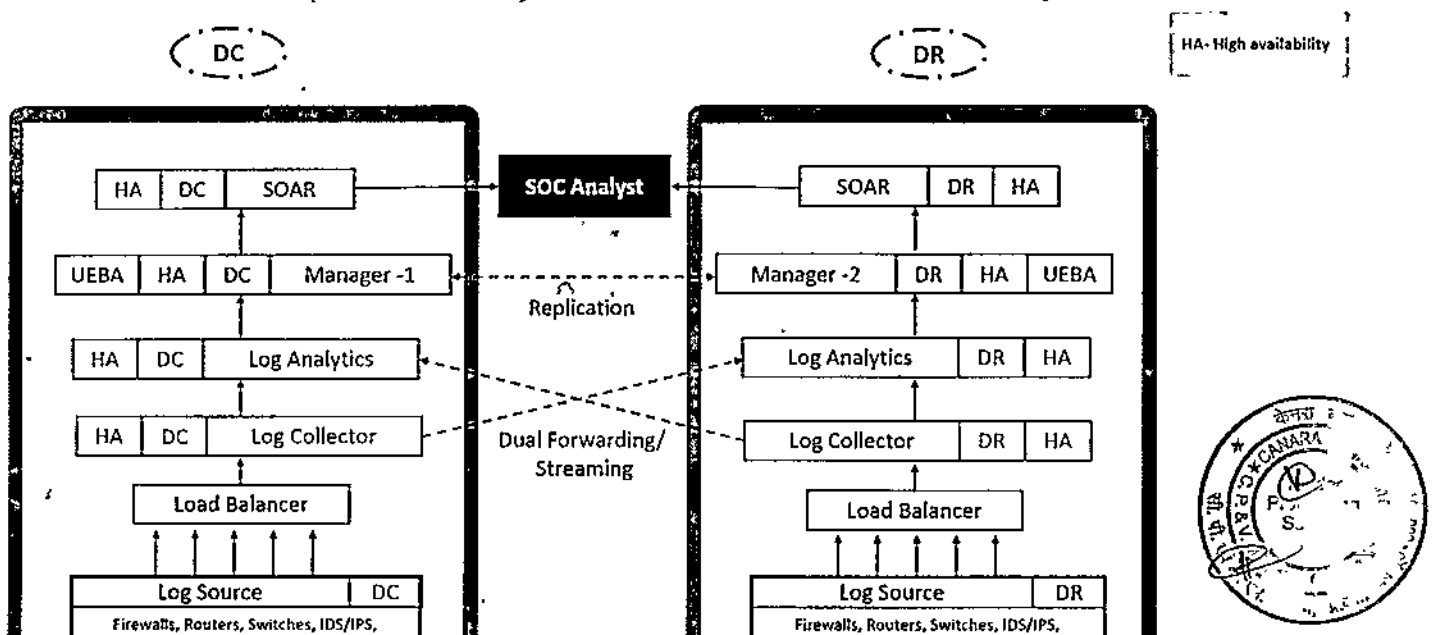
- The Bidder must provide regular reports (Daily/Weekly/Monthly/Quarterly) on security trends, alert volumes, and SOC activities. The reports should include but not limited to the following details:
 - Total alerts triggered
 - Open/Closure status of alerts
 - SLA status
 - Root Cause Analysis (RCA) wherever applicable
 - False positive ratio
 - Improvements/Suggestions
 - Rules Triggered
 - Pending Activities
 - SIEM/PIM Servers Onboarding status
- The Bidder has to track the following Metrics and share the details with Bank:
 - Mean Time to Detect (MTTD)- The average time taken to detect a security incident after it occurs.
 - Mean Time to Respond (MTTR)- The average time taken from the detection of an incident to its resolution.
- Bidder should generate various report as per requirement and create a customized dashboard to provide an overview of the security landscape of the organization. Further, dashboard should be provided with MITRE framework & other frameworks as per requirement of the Bank
- Bidders should integrate the proposed SIEM with a ticketing tool for automated ticket generation.
- The OEM has to perform half yearly/yearly health check-up of the solution and provide the comprehensive report to Bank.
- SIEM solution should be patched as and when required or in case new updates are available.
- The solution shall provide the following functionality:
 - Log Collection
 - Log Storage
 - Event Co-relation
 - Alerting
 - Dashboarding and Reporting
- SIEM tool and related components
 - The Bidder must provide monitoring & security analysis of the infrastructure through SIEM solution on 24x7 basis.
 - Monitor all security incidents using SIEM solution deployed at DC and DR and integrated with various infrastructure devices and security solutions of bank. The solution should integrate with Network devices / Security solutions / Servers / Applications / Database of Bank.
 - Provide continuous threat hunting to strengthen cyber security posture.
- Log collection
 - 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.
 - The log baseline should be in line with global best practices. In case the systems/applications are writing logs to the local hard disks, solution should be capable to pull the logs from these devices through secure transfer.
 - Server logs collection to be monitored and alert to be raised, if logs not received after a threshold time, dashboard to be provided for the same. System should automatically initiate SMS/Email to respective stakeholders in case of non-reporting logs.



- Only in the case where remote log collection is not feasible, Bidder should install agent on the servers and applications for collection of logs. Raw logs should be made available in case of legal requirement.
- Bidder shall develop a framework to detect log stoppage issue based on the criticality of the log sources.
- Bidder to troubleshoot log stoppage issue along with the system owners.
- Log aggregation and normalization
 - Logs collected from all the devices should be aggregated as per configured parameters.
 - Logs from multiple disparate sources should be normalized in a common format for event analysis and correlation.
 - Log collected on SIEM solution should be forwarded orchestration / analytical solution.
- Log archival.
 - Logs collected from all the devices should be stored in a tamper proof format on the archival device in the compressed and encrypted form. Collection of Logs and storage should comply with the Regulatory requirement and should maintain a chain of custody to provide the same in the court of law in case the need arises.
 - For correlation and report generation purpose, 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.
 - Retrieval of archived logs should not require any proprietary tools/protocol and should be retrievable using open standards/protocols or else the retrieval tool should be provided to the Bank without any additional cost.
- Log correlation
 - Collected logs should be correlated according to various predefined criteria for generation of alert and identification of the incident. Correlation rules should be customized by the vendor / System Integrator on a regular basis to reduce false positives. In any case false negatives will not be permitted. In case of detection of any such incident, correlation rules must be customized immediately to capture such incidents.
- Alert generation
 - Solution should be capable to generate alerts, register and send the same through message formats like SMTP, SMS, Syslog, SNMP as per user configurable parameters.
- Event viewer / dashboard / reports / incident management
 - SIEM Solution should provide web-based facilities to view security events and security posture of the Bank's Network and register incidents.
 - Solution should have drill down capability to view deep inside the attack and analyze the attack pattern. Dashboard should have filtering capability to view events based on various criteria like geographical location, Device type, attack type etc.
 - Dashboard should have Role based as well as Discretionary access control facility to restrict access to incidents based on user security clearance level.
 - Solution should provide various reports based on user configurable parameters and standard compliance reports like ISO 27001:2013/2022, ISO 31000:2018, ISO 27017:2019, ISO 27701:2019, ISO 22301:2019, PCI-DSS etc., and from regulatory and statutory authorities.
 - The Bidder will customize incident management / dashboard / reports for the Bank and will modify them as per the changing requirement of the Bank.
- Integration with in-scope monitored devices and interoperability.



- The Bidder is responsible for integrating SIEM solution with the hardware items & security solutions. As the system integrator the Bidder will also be responsible for integrating all in scope security solutions/devices with the SIEM solution for log monitoring, correlation.
 - 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.
 - The SIEM solution should have tight integration with proposed UEBA, SOAR, TIP. It should also have tight integration with Bank's existing solutions like Microsoft -AD.
 - The SIEM solution should support integration of all windows, Linux, HP-Tandem, UNIX flavoured Operating systems and OEM should develop the connectors wherever applicable without any extra cost to the Bank.
- Development of connectors/parsers for customized applications/devices
 - While it is expected that connectors for all the standard applications, APIs and devices will be readily available in the collector and Log management devices, connectors not available for devices will need to be developed. It is the responsibility of the Bidder to develop connector applications for all devices.
 - The solution shall support the various Use Cases to provide log collection, event correlation, alert generation, and escalation.
 - SIEM Use case Management
 - The bidder shall ensure all the current SIEM use cases are transferred to the Next Gen SIEM solutions.
 - Bidder to develop new use cases as per the Bank's requirement.
 - Bidder to perform quarterly rule review which should include the following but not limited to,
 - Total number of rules triggered alerts
 - False positive vs True Positive
 - MITRE ATT&CK Coverage
 - Number of rules with no events
 - Bidder to fine-tune to the rules based on the feedback received from Bank or SOC team
 - Bidder to incorporate change management process in rule management
 - Bidder to enhance the MITRE ATT&CK coverage and share the progress-report
 - Bidder to ensure up-to-date reference sets/Watchlist leveraged in SIEM use case
 - Perform quarterly review of watchlist and remove stale indicators
 - Bidder to fix the gaps identified by OEM or Auditor as part of the assessment
 - Bidder to manage access provisioning and de-provisioning to the platform.
 - Bidder to perform monthly access reconciliation and share the report with the Bank



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)

Note: The Bidder should refer above mentioned diagram for SIEM Implementation

II. PCAP.

- The solutions should be able to execute all data acquisition tasks in the network. The capture rate should be sufficient to perform full packet capture and packet inspection of traffic without any loss of data or degradation of performance.
- The proposed PCAP solution should capture the network traffic and support replay functionality.
- It should capture and record all network packets in full (both header and payload).
- The proposed PCAP solution should be capable of capturing traffic through port mirroring. Bidder/OEM should suggest to the Bank, the best possible placement of PCAP solution for obtaining its optimum utilization.
- 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 perform end-to-end management of PCAP solutions which includes but not limited to
 - Daily Health check-up of all the deployed components
 - Policy Management which includes creation, modification and retirement
 - User access management
 - Monthly user access reconciliation
 - Integration with SIEM
 - Creation of dashboard and Reports
 - Support during Audit and assessment
 - Close of Vulnerabilities associated with PCAP solutions
 - Ensuring the product is up to date as per Bank's defined policy
 - Backup to be configured by the bidder as per Bank's policy
 - Implement change management process aligned with Bank's policy
 - OEM coordination in case of issues where support required.

III. Security Orchestration, Automation and Response (SOAR)

- Bank intends to use SOAR as orchestration, automation and remediation engine which should automate incident triage by leveraging artificial intelligence, Machine learning and self-learning capabilities to provide measurable reduction in time gaps between incident detection, analysis, and closure by continuous optimization of workflows, playbooks to lessen the dependency on NGSOC Admins and NGSOC Engineers.
- Solution should provide automated remediation of threats on IT infrastructure (OS, DB, networking techs etc.), security implementation / threat prevention / mitigation technologies in real-time basis and update its conclusive action taken status back into security monitoring technologies immediately.



- 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.
- The intention should be to free up the personnel resources/ NGSOC analysts/ IT teams from routine job and encourage them to invest their time more into threat hunting and advanced threat detection & prevention efforts.
- Having hundreds of inbuilt playbooks for threat detection & prevention technologies/ applications, IT infrastructure, their makes, models & versions, the SOAR should analyze incident and prioritize & perform triage leveraging joint efforts by personnel resources and technologies, create / update playbooks and thus standardize response to security incidents.
- SOAR should endeavor to build & customize playbooks leveraging its analytical abilities powered by AI/ML. Thus, the SOAR should support push and pull mechanism - push instruction into systems and pull data, information, logs from IT infrastructure using APIs, light weight / simple scripts etc. and pull mechanism is to extract relevant info, logs, data, emails, information, alerts from NGSOC technologies, IT Infra, emails (to read IOCs etc.).
- SOAR licenses should be strictly based on number of active users/ analysts as defined in the scope of work. There should be no limitation / restriction in SOAR licenses based on the number of events coming to the SOAR or the number of playbooks or actions performed by the SOAR.
- The bidder shall develop custom integration as necessary within the defined timeline.
- Bidder shall develop custom playbooks as per the requirements. There should not be any limitation on the number of playbook bidder should develop during the tenure of the contract.
- Bidder to manage Dev, Prod DC and DR instances of SOAR and ensure all the components are up to date as per the defined policy of the Bank.
- 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.
- Bidder to troubleshoot playbook related errors.
- Bidder to manage access provisioning and de-provisioning to the platform.
- Bidder to perform monthly access reconciliation and share the report with the Bank.

IV. User and Entity Behavior Analytics (UEBA)

- UEBA as a part of analytical engine of NGSOC shall deeply compliment SIEM.
- It should profile and analyze the activities of users and IT infrastructure objects from their digital footprint standpoint, to identify outliers who are (users) or which are (entities) inadvertently or deliberately performing unexpected activities thereby showing signs of behavior different than their peers in same team, group, business / IT unit or function, region, zone, delegated powers / authority etc.
- Solution should provide early warning or prediction must be done at very early stage by exploiting inbuilt deep analytics powered by AI/ML.
- 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.
- Integrate with existing and proposed security solutions.
- Identify and integrate respective log sources such as Active Directory, Network Traffic etc.
- Define normal behavior baseline for user and entities.
- Use historical data collected in SIEM to train the UEBA models.
- Create alert thresholds based on the risk level of detected anomalies.



- Implement automated response actions for high fidelity alerts.
- Regularly update the UEBA model to address evolving threats.
- Fine-tune models to reduce false positives and provide high fidelity alerts.
- Create custom dashboards and reports as per Bank's requirements.
- Develop SOPs and How to Document for managing the operations.

V. Endpoint Detection & Response (EDR)

- The successful bidder has to provide detailed solution document, project implementation plan, architecture diagram and provision for the proposed solution.
- All feature customization, enabling, disabling, and parametrization during the contract period to be ensured by successful bidder/OEM without any additional cost to the Bank.
- 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.
- Fixing of Comprehensive Security Review findings, after first setup and thereafter as and when carried out by Banks requirement and any other security or compliance audit findings within the prescribed time limits. Solution will be rolled out only after closure of all security findings by the Bank.
- For all type of technical support services/premium support & SLA where involvement of OEM is required, there should be a back-to-back agreement between successful bidder & OEM.
- Bidder will ensure Services from the OEM to be available round the clock during the contract period.
- OEM should be pioneer in releasing the signatures and updates of AI&ML models proactively as and when new IT Threats are identified, locally or globally. In case, new threats are declared and any other OEM has the remediation for these new threats, then the OEM is responsible for releasing the signature / pattern/AI&ML models within 06 Hrs, to protect the Bank from these new threats.
- Signature/remediation for all new malware or IT-Threats must be deployed across all endpoints within their availability on the solution.
- Bidder to provide the 24x7x365 support for Implementation, Integration, Maintenance, Administration, Onsite-Support etc. during contract period of 5 years.
- Bidder to install and manage 90,000 endpoint agents, agent management includes,
 - Creating installation package for different operating systems
 - Creating agent installation guide for Bank's IT to refer
 - Provide SCCM package to push the agent remotely.
 - Troubleshoot agent installation failed instances
 - Ensure agent compliance is 99.5% across all the supported operating systems.
 - Group agent based on the location, Department, or business units.
 - Create policy based on the various groups.

Description of Deliverables

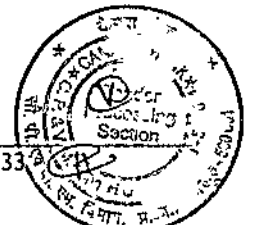
- Implementation plan should be provided for roll out of the 85000 Endpoints including, 5000 servers.
- It will be the responsibility of the selected bidder to ensure 100% communication status of Endpoint Agents and to take corrective steps in co-ordination with the Bank, to resolve agent communication issues and ensure 100% communication of endpoints with central management servers.



- The scope of the project also includes training & handholding to the designated staff of the Bank.
- The software / hardware / licenses / AMC / management / maintenance / developer / warranty / VAPT / patching will be responsibility of the bidder during the contract period of 5 years.
- Implementation documents related to configuration, migration, and customization including other documentation such as Operations & administration manual, Standard Operating Procedure (SOP) for various modules and roles/responsibilities, etc.
- The bidder should update and maintain the solution and ensure that the update and upgrades of all the components are implemented in a timely manner. The bidder should also ensure that the latest versions recommended by OEMs of all the components in the solution are configured in the production at any point of time during the contract period.
- The delivered solution should ensure scalability as per Bank's requirements and ensure immediate response to the end users.
- OEM is responsible to release the detection for alerts released by RBI, cert-in and any other advisories from India or foreign location proactively.
- Bidder is responsible for follow-up with OEM and arrange the latest signature/patterns to the Bank in case any malware/ransomware/ alert released by advisories in India or any other foreign countries.
- Bidder to create policies as per the recommendation from the OEM to detect latest threats.
- Bidder to perform periodic review of configuration and policies to ensure relevancy of the same.
- OEM to perform half-Yearly assessment of the proposed solution and share the operating and control effectiveness report with the Bank.
- Bidder to provide support during any audit/assessment and ensure all the identified observations are closed within the agreed timeline.

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.
- Bidder has to ensure that OEM shall design the solution and ensure the solution is implemented as per the agreed design.
- The OEM has to provide undertaking on company letter head that the architecture recommended is as per the OEM best practices and deployment plan. Post implementation, the bidder must provide Certificate from the OEM, certifying that the implementation has been done in line with the OEM best practices and the deployed solution meets all the technical/functional requirements of the solution.
- Any other components like middleware hardware/software/licenses etc. required in connections with the work will be supplied and maintained by the Bidder.
- The Bidder will integrate the PIM solution with Bank's proposed SIEM solution, Vulnerability Management tool etc. without any additional cost
- 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.





- The proposed PIM solution\ architecture should be able to consume existing PIM logs which enable bank to view and analyze existing logs\ videos. Migration efforts will be in the scope of SI.
- The Solutions should be deployed in the Bank's existing DC and DR Sites and wherever Bank migrates its servers in future.
- The solution deployment should be compliant with Bank's IS, IT and Cyber policies, internal guidelines, regulatory requirements and country wide regulations and laws from time to time.
- 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.
- The Bidder will be responsible for day-to-day management, administration, monitoring, and support.
- The Bidder will be responsible for Installations, uninstallations, onboarding, deboarding, etc.
- The Bidder shall have Proactive and agile response on any new upgrade, global level alerts.
- The Bidder will be responsible for configuring, testing and roll-out/add-on components/packages available in PIM solution.
- The Bidder has to ensure configuration management / backup PIM solution (DB, Application, and Staging).
- The Bidder has to ensure weekly database related housekeeping activities and report to Bank team.
- The Bidder will be responsible for the timely planning and implementing the upgrades, updates and patches as recommended by OEM and roll out across the Bank.
- The OEM has to perform half yearly/yearly health check-up of the solution and provide the comprehensive report to Bank.
- The Bidder will be responsible for providing necessary support, guidelines, and training's from time to time to Bank Tech support and users.
- The Bidder will be responsible to analyze, troubleshoot & resolve PIM related issues raised by users at server or desktop level.
- The Bidder will be responsible for the creation of PIM application users, creation of server and user groups, retrieve PIM logs on demand.
- Ensure proper escalations to the OEM support for quick resolution.
- The Bidder will be responsible for the log call with OEM Back-end Support team for escalated issue.
- The Bidder will be responsible for monitoring and ensuring the overall health of PIM Servers.
- The Bidder will be responsible for publishing reports as per defined intervals.
- Patch the system in line with OEM patch releases.
- The Operations team has to do version upgrades of all underlying software / Middleware as per respective OEM recommendations.
- The Bidder will be responsible for conducting DR Drills for PIM solution as per bank defined policy and emergency DR cutovers as per Bank's requirement.
- The Bidder has to maintain and periodically update SOPs and other documents as per Bank policy.
- The Bidder will be responsible for responding to audit queries related to PIM solution and ensure all the observations are closed within the defined timeline.
- The Bidder will be responsible for assisting other internal teams in troubleshooting real time issues.
- The Bidder will be responsible for mitigating vulnerabilities or observations reported during security audits, VA&PT, and regulatory technology audits (internal, external, and concurrent).



- The Bidder will be responsible for resolving technical issues & coordinating with OEM as escalation follow-up for long pending Tickets & calls.

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:

- The Bidder will be responsible for creating High Level design document which should have Scope, Objective, Design consideration and architecture.
- The Bidder must ensure to get the OEM approval for the design and implement the solution as per the agreed design.
- The Bidder must ensure all the components are installed and meeting the requirements of the RFP.
- 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.
- The Bidder will be responsible for Integrating proposed TIP solution with SIEM, SOAR, EDR, and other security tools.
- The Bidder will be responsible for configuring the TIP to align with Bank's workflows.
- The Bidder must ensure to implement automation for data enrichment, threat scoring, and alerting.
- The Bidder will be responsible for configuring workflows for incident response and threat hunting.
- Perform periodic validation of integration, data flow, and automation configurations.
- Train security analysts and relevant personnel on TIP operations, use cases, and best practices.
- Perform De-duplication, normalization, and enrichment of threat data.
- Identify emerging threats, vulnerabilities, and trends.
- Trigger automated incident response actions based on threat intelligence; such as blocking IPs or isolating systems leveraging SOAR.
- The Bidder will be responsible for creating Threat Intelligence which shall cover IoC life Cycle Management.
- Provide stale IoC details to respective stakeholders for action
- Create automation to remove stale/expired IoCs from respective security controls leveraging SOAR.
- The Bidder will be responsible for sharing the curated threat intelligence with internal stakeholders and trusted external partners.
- The Bidder will be responsible for regularly update and patch the TIP to ensure security and performance.
- The Bidder will be responsible for performing continuous tuning to improve detection and automation accuracy.
- The Bidder must ensure to generate reports on threat trends, incidents, and TIP effectiveness.
- The Bidder will be responsible for maintaining documentation on workflows, configurations, and operational metrics.

VIII. Dynamic Application Security Testing (DAST)





- The Bidder will be responsible for providing detailed report of identified vulnerabilities, including a description, impact, proof of concept (if applicable), and recommendations for remediation.
- The Bidder will be responsible for actionable remediation steps for each identified vulnerability, including references to best practices and relevant security standards.
- After the Bank has implemented remediation measures, Bidder has to conduct a follow-up test to confirm that the vulnerabilities have been effectively mitigated.
- The Bidder must ensure that testing methodologies align with relevant industry standards and regulations such as OWASP TOP 10, SANS CWE TOP 25 Most Dangerous Software Errors & any other industry standards etc.
- The Bidder will be responsible for providing weekly updates on the testing progress, any critical findings, and potential blockers.
- The Bidder will be responsible for immediately report any critical vulnerabilities that could significantly impact the organization's security posture, even if the testing is ongoing.
- The Bidder ensure to conduct a debriefing session with the organization's security team, explaining the findings, risks, and remediation strategies.
- The Bidder will be responsible to comprehensive vulnerability reports, including technical details, risk ratings, and remediation recommendations.
- The Bidder will be responsible for sharing Executive summary reports tailored for management, highlighting key risks and suggested actions.
- The Bidder must ensure to provide the documentation of all testing processes, methodologies, and tools used.
- The bidder shall be responsible for planning, executing, and reporting on all aspects of the DAST process, ensuring alignment with the organization's security objectives.
- The bidder shall follow-up with relevant stakeholders to close the vulnerabilities.
- The bidder shall provide support during the audit & assessment and close identified weaknesses in the DAST solution and processes within the agreed timeline.
- Bidder shall be responsible for updating and upgrading the solution as per the Bank's policies and procedures.

IX. Anti-APT and Sandboxing

- The Bank intends to implement an Anti-APT solution to protect its north south and east west network from known, unknown and zero-day malware attacks, infiltration attacks.
- Bidder should install and configure an Anti-APT solution to protect against web and email attacks.
- Bidder should suggest the required changes to be done to integrate Anti-APT solution to integrate with the existing infrastructure.
- Bidder should integrate Anti-APT solution with the proposed SIEM, SOAR solution.
- The proposed solution should support currently available operating systems to perform inception for malware, zero day and stealth attacks etc.
- Bidder to perform end-to-end management of Anti-APT solutions which includes but not limited to
 - o Daily Health check-up of all the deployed components
 - o Policy Management which includes creation, modification, and retirement
 - o User access management
 - o Monthly user access reconciliation
 - o Integration with SIEM
 - o Creation of dashboard and Reports



- o Support during Audit and assessment
- o Close of Vulnerabilities associated with Anti-APT solutions
- o Ensuring the product is up to date as per Bank's defined policy
- o Backup to be configured by the bidder as per Bank's policy
- o Implement change management process aligned with Bank's policy
- o OEM coordination in case of issues where support required.

13. Solutions under tech refresh

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.

It is expected that the Bidder shall take over operation of the mentioned solutions and manage end-to-end without any dependency on the Bank or incumbent partner

- Bidder to note that all the validity of the licenses (existing and proposed) for the tech refreshed solutions should start and end according to the contract period.

S. No	Solution *	OEM
1	Anti DDoS	Arbor AED
2	Network Behaviour Analytics (NBA)	Cisco Stealthwatch
3	Data Loss Prevention (DLP)	Forcepoint
4	Vulnerability Assessment (VA)	Tenable SC

*Further details of the solution along with architecture diagram will be shared to the selected Bidder

a. Anti - DDOS

Existing setup:

- Primary appliances (AED 8100)
- Secondary appliances (APS 2600)

Upgrade:

- Primary appliance (AED 8100) will be retained, and the support will be extended as per the RFP timelines.
- Secondary appliance APS 2600 reached End of Support, which will be upgraded to AED 8100 for which end of life/support is not yet announced.

Additional feature:

- Procurement of central manager with hardware to manage all DC and DR appliances.

Note: Please refer *Annexure - 17(C) Sizing of Hardware of Retained Solutions* for the hardware sizing requirement

Scope for Anti - DDOS:





- Analyze the existing NetScout Anti-DDoS infrastructure, configuration, and performance metrics.
- Specify performance, scalability, reliability, and security expectations.
- Conduct gap analysis and Compare current capabilities with desired functionalities.
- Design and implement the overall architecture of the new Anti-DDoS solution in DC and DR and configure HA.
- Plan integration with existing network infrastructure and security systems.
- Install, configure and maintain the Anti-DDoS appliances.
- Integrate with proposed SIEM Solution to generate alerts for any Anti DDoS violations.
- Develop and implement DDoS protection rules and policies.
- Integrate with banks SIEM, SOAR, ITSM (Service Now), Threat Intel Platform, Threat Intel Services using STIX TAXII or REST API.
- Evaluate system performance under normal and peak load conditions.
- Coordinate with banks DDoS Drill service provider during drills.
- Weekly automated backup for configuration and data.
- Monitor events from Anti DDoS and suggest / take appropriate action to the bank of ongoing basis.
- Integrate with banks existing scrubbing services. Monitor and coordinate with services provider in case any issue.
- Monthly review policies and protection groups to reduce occurrence of false positives.
- Coordinate, Integrate and maintain website certificates in solution.
- Data Migration: Transfer relevant data from the old to the new system.
- Cutover Planning: Develop a detailed cutover plan.
- Cutover Execution: Implement the cutover process.
- Validation: Verify system functionality after cutover.
- Knowledge Transfer: Transfer knowledge to operations and support teams.
- Operational Procedures: Develop standard operating procedures.
- Monitoring and Management: Establish monitoring and management processes.
- Incident Response Plan: Create a plan for handling DDoS attacks.
- Evaluation: Assess project success against defined objectives.
- Project Documentation: Finalize project documentation.

Maintenance Scope of work -

a. System Monitoring and Health Checks

- Real-time monitoring: Continuously monitor the Anti-DDoS system's performance, resource utilization, and overall health.
- Key performance indicators (KPIs): Track critical metrics such as attack volume, mitigation efficiency, and system latency.
- Alerting: Establish thresholds and notifications for abnormal system behavior.
- Log analysis: Regularly review system logs for potential issues or security incidents.

b. Software Updates and Patches

- Patch management: Maintain an up-to-date inventory of software components.
- Vulnerability assessment: Regularly assess the system for vulnerabilities.
- Patch testing: Thoroughly test patches in a controlled environment before deployment.
- Patch deployment: Apply security patches and updates promptly.

c. Configuration Management

- Configuration baseline: Establish and maintain a baseline configuration.



- **Change management:** Implement a change control process for configuration modifications.
- **Configuration-auditing:** Regularly review and verify system configurations.
- **Configuration backup:** Maintain regular backups of system configurations.

d. Performance Optimization

- **Performance tuning:** Optimize system performance through configuration adjustments and resource allocation.
- **Capacity planning:** Assess system capacity and plan for future growth.
- **Bottleneck identification:** Identify and address performance bottlenecks.
- **Performance testing:** Conduct regular performance tests to measure system efficiency.

e. Security Management

- **Access control:** Implement strict access controls to protect system resources.
- **Security audits:** Conduct regular security audits to identify vulnerabilities.
- **Incident response:** Develop and maintain an incident response plan.
- **Security awareness:** Provide security training to system administrators.

f. Documentation and Knowledge Management

- **System documentation:** Maintain up-to-date system documentation.
- **Knowledge base:** Create and maintain a knowledge base for troubleshooting and best practices.
- **Operational procedures:** Document standard operating procedures for system management.

g. Support and Incident Management

- **Help desk support:** Provide timely support for user inquiries and issues.
- **Incident management:** Establish procedures for handling and resolving incidents.
- **Problem management:** Identify and address recurring issues.
- **Service level agreements (SLAs):** Maintain service level expectations and performance metrics assigned by bank.

h. Regular Review and Improvement

- **Performance evaluation:** Regularly assess the effectiveness of the maintenance activities.
- **Continuous improvement:** Identify opportunities for improvement and implement changes.
- **Best practices adoption:** Stay updated on industry best practices and incorporate them into the maintenance plan.

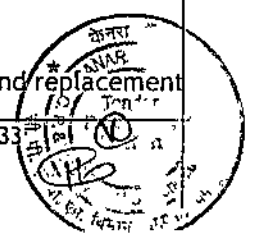
b. DLP

Existing setup:

- 80k endpoint DLP Licenses (managed by SOC)
- 80k network DLP licenses inbuilt in Bank Proxy solution (managed by IT-NOC team)

Upgrade:

- As part of upgrading the solution, Bank is procuring Additional licenses (90k in total) and replacement



of hardware (along with network DLP) to meet the requirement. The bidder shall plan for 10% YoY growth and size the hardware accordingly.

- At present OEM for both Endpoint DLP & Network DLP (Proxy) are same i.e. Forcepoint. Hence, it is recommended to have centralized management console to govern the DLP policies effectively. All the 90k licenses validity will be 5 years from date of implementation sign off

Additional feature:

- DLP Discovery

Note: Please refer *Annexure - 17(C) Sizing of Hardware of Retained Solutions* for the hardware sizing requirement.

Scope for DLP:

- The Bidder to ensure successful deployment of DLP solution (Endpoint, Network) in the Bank as per the architecture suggested by the Bank.
- Bidder has to integrate the Network DLP with Bank's existing Forcepoint Proxy for prevention of data leakage (During contract period, if there is any OEM/architecture (on-prem or cloud) change in Proxy solution, Bidder has to integrate Network DLP with new Solution without any cost/ extra license to the Bank).

Note: Architecture will be shared to the selected Bidder.

- The Bidder to ensure that all the existing policies are migrated to the new DLP solution.
- The Bidder to ensure the required DLP policies are configured for both Endpoint and Network proxy from the management console.
- The Bidder to ensure the configuring the backup in co-ordination with Bank's IT team and managing the same on day to day basis as per the Bank's guidelines.
- The Bidder to ensure performing regular updates of patches / firmware upgrades as per the broad scope defined. Non compliance of that will invoke penalties as per the SLAs.
- The Bidder to ensure that the latest DLP agents are pushed to all the endpoints.
- The Bidder has to perform quarterly DR Drills and ensure that BCP / DR setup is tested as per the bank's guidelines.
- The Bidder has to create new policies (custom and leverage default) using various data classifiers as per Bank's requirement and should be well versed with using dictionary (normal and weighted) advanced regex, scripts, fingerprinting etc.
- The Bidder has to perform data discovery and configure data discovery policies as per the Bank's requirement and provide observation reports regularly.
- The Bidder has to ensure the solution uptime as per the defined SLAs.
- The Bidder has to integrate the DLP incidents with either SecOps or Bank's ITSM tool and need to close the tickets as per the agreed SLAs.
- The Bidder has to integrate DLP solution with SIEM / SOAR for forwarding all the incidents, admin, access, error and audit logs.
- The Bidder should ensure ICAAP integration from Network DLP to present proxy solution and new proxy solution after Proxy upgrade by respective bank team.
- The Bidder has to configure anti - tampering settings for all the endpoints agents and maintain the same.
- The Bidder has to configure drip DLP policies as per the Bank's requirement.



- The Bidder has to configure threat based DLP policies.
- The Bidder has to verify and monitor Risk score based incidents triggered in the DLP solution.
- The Bidder has to configure automatic workflows to trigger notifications to relevant stakeholders for auctioning the alerts / incidents.
- The Bidder should integrate DLP solution with Email Gateway and configure automatic email templates according to Bank's requirement.
- The Bidder should configure and manage encryption / password protection / fingerprinting of the data as per the Bank's requirement.
- The Bidder has to ensure the reporting of all the endpoints and perform sanitization of the endpoints reporting status duplication etc.
- The Bidder has to perform review regularly to identify and configure various domains / applications and use them in the policies wherever required for blacklisting / whitelisting in co-ordination with Bank's team.
- The Bidder has to ensure regular review and fine tuning of the classifiers policies in both Endpoint and Network DLP.
- The Bidder has to manage Endpoint removable media whitelisting as per Bank's requirement.
- The Bidder has to create all relevant documentation such as SOP (Standard Operating Procedures), Health monitoring, installation / uninstallation of agents or any other adhoc requests from Bank.
- The Bidder has to configured and customize various dashboards and reports as per Bank's requirement.
- The Bidder should perform trend analysis to action accordingly and provide relevant reports. Also, provide compliance reports for regulatory / internal audits.
- The Bidder has to provide user / customer trainings and ensure support whenever required.
- The Bidder has to perform discovery of Network inventory and data flow analysis.

c. NBA

Current setup:

- 60k Flow Per Sec (FPS) at DC and DR
- SMC Manager and flow collectors at DC and DR

Upgrade:

- 3 lakh FPS (planning to integrate internal firewall where expected flow is 1.5 to 2 lakh).
- SMC Manager and flow collector at DC and DR

Additional requirement:

- Flow sensor, Datastore and Telemetry broker for gaining visibility of other segmented networks.

Note: Please refer *Annexure - 17(C) Sizing of Hardware of Retained Solutions* for the hardware sizing requirement

Scope of Work for NBA:

Design/ Deployment /implementation Scope:

- Analyze the existing CISCO Stealthwatch NBA infrastructure, configuration, and performance.



metrics.

- Implement the overall architecture of the new NBA solution in DC and DR (Architecture diagram will be given to the Selected Bidder)
- Install, configure the new NBA appliances, and migrate all the existing configurations to the new Set-up.
- Implementing NBAD with Management console, 3-node data store cluster, telemetry brokers, Flow Collectors, ISE PIC for managing both DC,DR of NBAD solution.

Integration of Network devices:

Plan integration with existing network infrastructure and security systems. Provide the detailed configuration guide for the integration of OEM specific network devices separately. Integrate banks critical routers and firewalls including perimeter and internal DC and DR network devices considerably avoiding duplication of flows. Proxy syslog has to be integrated with Converged analytics. NAC Clear pass logs to be integrated with ISE PIC.

System Health: Evaluate system performance under normal and peak load conditions.

Implementation: Integrate Active Directory services for host details, TACACS & AD integration for authentication. Threat intel feeds has to be integrated to solution to directly look up for the IoC reputation. Integrate Converged analytics with data store for getting threats related to proxy logs similar to GTA.

Reporting & non reporting: Provide Troubleshooting guide for verifying the non-reporting network device configuration.

Incident Management: Integrate with proposed SIEM Solution to trigger NBA related alarms for swift IR. Integrate the NBA critical alarms to proposed Incident Management ticketing solution for incident remediation closure records.

Monitoring and Management: Establish monitoring and management processes. Develop and implement new use cases and policies by observing the network traffic of our Bank environment along with fine tuning of the existing policies. Review policies to reduce occurrence of false positives. Monitor events from NBA solution and provide play book for the same.

Annual Health check: Perform annual health checks for the solution to identify the gaps and for further improvement.

Backup: Weekly backup of configuration & 180 days backup of Alerts required in the data store and in standalone environment. Flow logs should be available for minimum of 180 days in the data store for forensic investigation. SOP for the same should be provided.

Adhoc Activities:

- **DR-Drill:** Conduct quarterly DR Drills. Provide SOP for conducting DR drill.
- **Host Classifier:** Install host classifier application under deployment stage.
- **Data Migration:** Transfer relevant configuration from the old to the new system.
- **Knowledge Transfer:** Transfer knowledge to operations and support teams annually.
- **Operational Procedures:** Develop standard operating procedures.
- **Incident Response Plan:** Create a plan for handling Alarms /Security events.
- **Evaluation:** Assess project success against defined objectives.
- **Project Documentation:** Finalize project documentation.

Maintenance Scope of work -

1. System Monitoring and Health Checks

- **Real-time monitoring:** Continuously monitor the NBA system's performance,



utilization, and overall health.

- Key performance indicators (KPIs): Track critical metrics such as Alarm volume, mitigation efficiency, and system latency.
- Alerting: Enable email notification for system alarms to make the action swiftly. Also, check for the packets rate and Bytes transferred, network latency, server response on NetFlow and fine tune the threshold of Security event alarms.
- Log analysis: Regularly review NetFlow logs for potential issues or security incidents.

2. Software Updates and Patches

- Patch management: Maintain an up-to-date inventory of software components.
- Vulnerability assessment: Regularly assess the system for vulnerabilities.
- Patch testing: Thoroughly test patches in a controlled environment before deployment.
- Patch deployment: Apply security patches and updates promptly.

3. Configuration Management

- Configuration: Establish and maintain configuration record of before and after changes.
- Change management: Implement a change control process for configuration modifications on polices, users access, system configurations, host group addition or deletion or host group whitelisting, version upgrades etc.
- Configuration auditing: Regularly review and verify system configurations.
- Configuration backup: Maintain regular backups of system configurations.

4. Performance Optimization

- Performance tuning: Optimize system performance through configuration adjustments and resource allocation.
- Capacity planning: Assess system capacity and plan for future growth.
- Bottleneck identification: Identify and address performance bottlenecks.
- Performance testing: Conduct regular performance tests to measure system efficiency.

5. Security Management

- Access control: Implement strict access controls to protect system resources.
- Security audits: Conduct regular security audits to identify vulnerabilities.
- Incident response: Develop and maintain an incident response plan.
- Security awareness: Provide security training to system administrators.

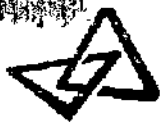
6. Documentation and Knowledge Management

- System documentation: Maintain up-to-date system documentation.
- Knowledge base: Create and maintain a knowledge base for troubleshooting and best practices.
- Operational procedures: Document standard operating procedures for system management.

7. Support and Incident Management

- Help desk support: Provide timely support for user inquiries and issues. Provide TAC support till the Project ends.
- Incident management: Establish procedures for handling and resolving incidents.
- Problem management: Identify and address recurring issues.
- Service level agreements (SLAs): Maintain service level expectations and performance.





metrics assigned by bank.

8. License Compliance: Ensure license support till end of Project.

9. Regular Review and Improvement

- Performance evaluation: Regularly assess the effectiveness of the maintenance activities.
- Continuous improvement: Identify opportunities for improvement and implement changes.
- Best practices adoption: Stay updated on industry best practices and incorporate them into the maintenance plan.

d. Vulnerability Assessment (VA)

Current setup:

- 1 Nessus scanner server
- 1 Tenable SC server
- 2300 licenses available

Upgrade:

- 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,

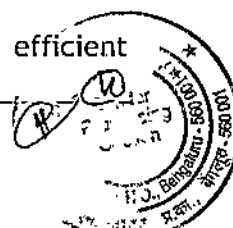
Additional requirement:

- Replication for the DC and DR will be configured.
- Tenable SC plus will provide Asset Exposure Scores (AES), Asset Criticality Rating (ACR) and Vulnerability Priority Rating (VPR) helpful for vulnerability management program.

Note: Please refer *Annexure - 17(C) Sizing of Hardware of Retained Solutions* for the hardware sizing requirement

Scope of Work of VA

- Bank requires a combined deployment of both Agent-based and Agentless scanners (Distributed Scanner) for the Vulnerability Management (VM) solution, tailored to fit the bank's specific needs.
- Bidder should suggest the required changes to be done to integrate VA solution with the existing infrastructure.
- Bidder must ensure the policies to be configured for the proposed VA solution.
- The Bidder will be responsible for sharing the Compliance Auditing files / scripts for the VA solution as per the Bank's requirement.
- 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.
- The Bidder will be responsible to conduct scans using credentials, keys, certificates, and integration with Privileged Identity Management (PIM).
- Perform compliance audits and reviews on IT assets as per the bank's Secure Baseline Document (SCD).
- The Bidder must ensure to provide customizable executive-level reports, patch reports, and technical reports in both Excel and PDF formats.
- The Bidder must offer mitigation recommendations in reports or dashboards for efficient patching of assets.



- The Bidder must ensure that the solution can identify and exclude false positives from reports.
- The Bidder will be responsible for performing regular maintenance and upgradation of the deployed solution to comply with banks or regulatory requirements.
- The Bidder will be responsible for providing technical support for the existing solution and suggest necessary changes and integrate the VA solution with the bank's existing infrastructure.
- The Bidder will be responsible for configuring policies for the VA solution and provide Compliance Auditing files/scripts as required by the bank.
- 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.
- The bidder must provide technical support for the existing solution and suggest necessary changes to integrate the VA solution with the bank's existing infrastructure.
- Regular maintenance of the deployed solution must be done to comply with regulatory requirements.
- The Bidder must ensure to take regular remote backups with retention capabilities, ensuring data restoration for at least the past 3 years.
- The bidder shall follow-up with relevant stakeholders to close the vulnerabilities
- The bidder shall provide support during the audit & assessment and close identified weaknesses in the VM solution and processes within the agreed timeline
- Bidder shall be responsible for updating and upgrading the solution as per the Bank's policies and procedures.

14. Scope of Work for Proposed services

a) Threat Intel Services

Current setup:

Currently Bank is having the following services from M/s Izoologic -

- Anti Phishing,
- Anti Pharming,
- Anti Malware,
- Anti Trojan,
- Rogue attack,
- Website defacement
- Dark web monitoring.
- Domain Name Monitoring
- Website Monitoring
- Social Media Monitoring for Bank and top executives of bank.

Upgrade:

Bank is preferring 2 brand monitoring and takedown partners to gain broader coverage, diverse expertise, and faster takedown response time additional services.

Additional requirement:

Bank is looking for the following services in addition to the services provided by M/s Izoologic.

- Attack Surface Monitoring



- IP reputation check
- Hash check
- Whois check
- IP Geo Location
- OU Details
- File or URL Sandboxing

Since Bank is currently using Izologic threat intelligence services, the Bidder should manage the existing Threat Intel services along with proposed Threat Intel services.

Detailed scope for the same is mentioned below.

Threat intelligence Services

Threat Intelligence Services should include below mentioned activities which includes but not limited to:

- a) Detection and Intelligence - Quickly find and confirm evidence of phishing, pharming, DNS Poisoning, Hacking, Smishing, Social Engineering attacks and other attacks at scale by using different proprietary machine learning classification and AI algorithms.
- b) Expedited Attack Takedown - Rapidly removal of identified threats and restoration of website/ account before customers or employees or public/ media become aware of a disruption.
- 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
- d) To perform round-the-clock (24X7X365) proactive cyber-threat monitoring across the surface with deep and dark web monitoring, Bidder shall maintain up-to-date whitelist/ fingerprint of all bank's internet-facing Assets, which includes but not limited to:
 - i. Authorized Social Media Accounts and websites /URLs.
 - ii. Domains and Sub-domains/Sub-directories respective IP addresses and associated web applications.
 - iii. Authorized Mobile Applications and Whitelist of URLs of download points
 - iv. Name server IP addresses
 - v. Authorized Sites - third party sites authorized to use Subscriber Trademark or Copyright Information and Brand name.
 - vi. Trademark and Copyright Documentation/ that is infringing our Brand name/ Identity.
 - vii. Key Executive Staff/VIP and other End User Details relevant to forming the whitelist for the Solution.
- e) The solution should identify if any of bank employee's credentials are leaked or sold online/ dark web/ deep web. The solution must update the list as and when any new breaches occur and make swift effort to and report at the earliest before someone alerts.
- f) The solution should identify leaked documents, APIs, Credentials, card data, login ID/ passwords, KYC and sensitive data of the Bank.
- g) The solution should monitor open security forums, like Pastebin, GitHub, GitLab, Bit Bucket etc

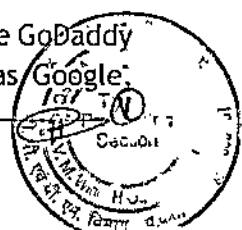


ingesting data from multiple code sharing and open security forums and report any such sensitive data/ code leaks by partners and employees having mention of the bank or its public assets such as Domains, Subdomains, IPs, etc.

- h) The solution should monitor and report YouTube and twitter videos which are abusing, spreading wrong news, hacking tutorials against bank's functions and businesses etc.
- i) The solution should use any technique or combination of techniques such as scanning of web server referrer logs and / or Digital watermarking/ or monitoring chat rooms used by hackers etc. to identify fraudulent techniques, scams, data trade and vulnerabilities targeting bank systems.
- j) The solution should monitor the global list of websites - like .com/ .org/ .bd/ .net and other domains and alert the moment any website similar to bank is registered.
- k) The solution should identify, and report Internationalized domain name (IDN) homograph attacks such as Misspelt domains, Punycode characters; Typo squatting domain attack, similarly spelt domains, Logo infringement detection, Imposter domains with MX Record, etc. Typo squat domains should be automatically continuously monitored for any change in state from Parked domain to hosted domain with WHO-IS information and the solution should provide Who-IS and DNS information for identified Typo squat Domains and relevant threat priority based on the intelligence gathered.
- l) Solution should provide for identification of fake recruitment schemes claiming affiliation with the bank.
- m) Solution should not impact the functioning of Canara Bank website. Any configuration on the Bank's infrastructure for the purpose of monitoring should not impact or degrade the performance of the bank's website.

Early Phishing Detection

- (a) Wide coverage of web, social media and email sources to detect newly configured phishing attacks, often before they are fully launched.
- (b) 24x7x365 real monitoring for phishing attacks.
- (c) The solution should alert bank against any phishing URLs/ pages that are often used for phishing and take all necessary steps for their takedown.
- (d) Implementation of real time detection mechanisms and alerts.
- (e) Implementation of tools for detecting anti- phishing mechanisms such as referrer logs, watermarks etc.
- (f) Track hosting of phishing sites through implementation of watermark or any other means.
- (g) Monitoring similar domain name registration.
- (h) Provide need based analysis on suspicious e-mail messages.
- (i) Should have mechanism to call, Mail or send SMS to Bank on the basis of severity of incident.
- (j) Website domain tracking analysis to detect phishing sites.
- (k) Blocking of the phishing sites from search engines and domain registration providers like GoDaddy and others. The bidder needs to have tie ups with search engine providers such as Google.





Mozilla, Microsoft and agencies like Cert-in for blocking the phishing sites.

- (l) Taking down of phishing sites anywhere in the world either on Bidders' own reach or through partnerships, however, the bidder will be solely responsible for any activity performed by the partner. The Bidder should have alternative response mechanisms other than web site take down to minimize impact of phishing.

Domain & Social Media for Impersonation Monitoring:

- A. Scan Bank's brand continuously and combat fake social media accounts and content such as Facebook, Twitter, LinkedIn etc. and domain registrations to find fake social profiles, malicious mentions and similar domains, bot twitter handles etc. that impersonate our Bank and compromise customer information.
- B. 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.

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.
- b) Detect and remove unauthorized applications imitating Banks official app from third- party app stores. Help Bank to reduce the risk of customers inadvertently downloading imposter apps.
- c) Monitor any fraudulent mobile applications targeting Bank's customers to capture their credentials for fraudulent transactions.
- d) Proactive Monitoring of major Mobile App stores and blocking/Shutting down of Malicious App/Trojan used against the bank.
- e) Taking down of fraudulent mobile apps/ APKs in the world including those circulated on social media platforms like WhatsApp etc. targeting Canara Bank Customers.
- f) The service provider should monitor of all major mobile application marketplaces for counterfeit, copycat apps, or apps infringing trademarks, linking to pirated content, attempting phishing attacks or distributing malware.
- g) Prompt submission of enforcement notices and for the removal of rogue or infringing applications.

Dark Web/ Deep Web scanning for sensitive information pertaining to Bank:

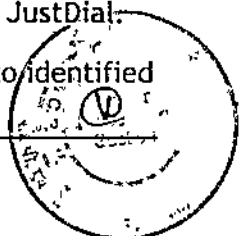
- a) The solution should crawl through multiple dark web forums to detect if someone is asking information or any data is leaked using bank's public assets such as domains, subdomains, IPs and pre-defined keywords.
- b) Monitor Cyber Crime Forums on clear web as well as dark web/deep web.
- c) Monitor Networks known to be sources of attacks and /or points of collection of compromised data.
- d) Maintain or have direct access to data from honey pots or network or sensors.



- 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
- f) The bidder /OEM needs to monitor sensitive data such as but not limited to Personal Identifiable Information (PII) such as Customer/Employee data, compromised banking credential/account monitoring, Credit card / Debit card BIN range monitoring of the bank, technical information/data used to target corporate systems, Vulnerability exploit monitoring and correlation with respect to the bank infrastructure, Hacktivist tracking and intelligence correlation with respect to the bank.
- g) The solution must have capability in tracking Customer vertical Threat actor groups as well as various ransomware operations targeting BFSI sector.
- h) The solution must provide data/information/intelligence related to threat actor, attack campaign, analysis report, tactics, techniques and protocols (TTPs) and profile the Threat Actors.
- i) The solution must provide Intelligence in near real-time as new information or context is gathered from various sources.
- j) Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without Bank actually going onto Dark web to look for evidence.
- k) The Solution/Service must monitor of hacker's activities related to Bank in Dark web much before it becomes public. The solution must provide the monitoring of the following:
 - i Exposed Top Managements/ Executives/ VIPs credentials as decided by bank Impersonation
 - ii Executive mentions/ Discussion on Top Management on Dark Web
- l) The solution/ service should incorporate a range of multi-layered monitoring services and analysis techniques and correlates data across a range of resources including: Tor, onion and alternative networks. Dark Net blogs, forums, chat rooms, Logs and Cookies, IRC conversations, Black market and criminal auction sites, Ransomware leaks.
- m) Vendor should monitor and inform all dark/ deep web sensitive information pertaining to bank.

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
- (b) Any newly launched websites and Mobile Application by the Bank in future to be scanned and brought to the notice of bank on same day.
- (c) Search engines (like Google, Yahoo, Bing 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.
- (d) The service provider is required to perform takedown services (unlimited) subject to identified threat and subsequently bank's approval.



- (e) Bidder must have capability for monitoring of look-alike domain name registrations and alerting the Bank in case of detection.
- (f) Social Media Monitoring of 20 Top level executives of Bank.
- (g) Detection and advisories of the attacks anywhere in the world within the minimum possible time. For the purpose of detection, service provider may use any technique or combination of techniques.
- (h) Take up and coordinate the cases with CERTS and/or other legal agencies of any country in consultation with Bank.

Web Site / Web App related Monitoring:

- a) The successful bidder should detect/ identify defacement of Bank website and corresponding Webpages through a combination of automated scans and manual analysis and reported immediately before anyone notices.
- b) The analysis should be done in a manner that only genuine defacements are informed to Bank and false positives are minimized.
- c) The solution should support Authenticated scanning with different authentication methods.
- d) The services are required for providing with comprehensive scanning of URLs/Websites and provide report in various possible ways.
- e) The solution should be able to provide website page scanning without skipping (No skipping of page scanning)
- f) The bidder has also to suggest suitable counter measures to safeguard against the threats and advise /assist to eradicate it on utmost priority.
- g) The Bank reserves the right to go for takedown with other agencies. The Bidder should consult with the Bank before going for takedown.
- h) Threat intelligence feed should identify new global threats around the globe like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc.
- i) Collection of Threat intelligence from the various sources should be automated, using technologies such as machine learning and Deep Language Processing, which allows mass collection of intelligence with low false positives, in real-time.
- j) Threat Intelligence of IOCs must be delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc. The contextualized threat information should be delivered in a simple and easy to digest format.
- k) Platform should support STIX and TAXII format and API Based integration with SIEM and SOAR.

Attack Surface Monitoring:

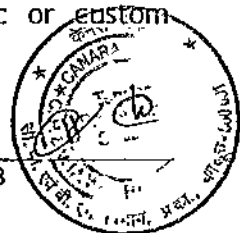
- a) The proposed solution shall identify publicly exposed IT infrastructure including Domains, Sub-Domains, IP Addresses, DNS Records, etc. and help bank to detect shadow IPs.
- b) The solutions should be capable of finding subdomains, IP addresses, web and mobile applications through different active & passive information gathering techniques not limited to Google Dorking, reverse IP, DNS reconnaissance, other public search engines.



- c) The proposed solution shall identify potentially orphaned applications, and services.
- d) The proposed solution shall identify exposed pre-production systems.
- e) The proposed solution shall identify the Tech Stack of the exposed services and applications.
- f) The proposed solution shall identify CVEs in the internet-facing infrastructure (passive enumeration)
- g) The proposed solution shall identify exposed services like RDP, SMB, Databases, LDAP and other high-risk ports with version detection. And should provide the CVE or CWE reference numbers and links with mitigation/fix.
- h) The proposed solution shall identify domain-level security issues such as subdomain takeover risks, DNS misconfigurations, WHOIS information, etc.
- i) The proposed solution shall identify and create an inventory of all exposed Web applications, Websites, Domain, APIs, Mobile applications and IP addresses exposed.
- j) The proposed solution should run port scanning on daily basis for at least 1000 top well-known ports and once in a week for all ports (0-65535) and provide the daily reports.
- k) The solution should provide the rescan report within 24hours for any observation upon requested.
- l) The solution should provide the detailed POC for all observations which can be downloaded, and should include but not limited to the URL/IP affected, detail observation, mitigation, CVE/CWE, reference links etc.
- m) The proposed solution shall identify application misconfigurations in CORS, SSL Certificates, exposed admin Panels, missing security web headers, exposed directory indexing, sensitive files/info exposure (logs, txt, excel, doc).
- n) Application/Cloud Testing should be based but not limited to the OWASP TOP 10, SANS CWE TOP 25 Most Dangerous Software Errors & any other industry standards etc.
- o) The proposed solution shall identify vulnerabilities in Bank's public Assets without sending huge amount of request like Brute forcing.
- p) The proposed solution shall discover exposed Database Servers & Cloud Buckets (due to misconfigurations, etc.) before the attackers do.
- q) The proposed solution shall be able to validate the Current IP attribution is using DNS, Netblock, and Keywords to improve accuracy.
- r) The proposed solution shall be able to provide Service and OS Fingerprinting to determine the services including their versions running on the open ports on Bank's networks.
- s) The proposed solution shall be able to perform Network Vulnerability Assessment to validate passive risks and remove false positives.
- 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.
- u) The Solution should be capable to provide the active or inactive assets.
- v) The proposed solution shall be able to detect observations related to weak encryption certificates, SPF, DKIM, DMARC DNS Sec and DS keys misconfigurations.



- w) The proposed solution shall be able to perform Network-level Risk scanning to identify misconfigured servers, services, and devices.
- x) The proposed solution must have the Risk center which prioritized and validated list of risks/severity for vulnerabilities and assets. The solution should be able to justify the severity and prioritization of observations and assets based on their documentation.
- y) The solution should maintain the knowledge base and FAQs for quick reference and troubleshooting.
- z) Any query/ticket should be resolve within 24 Hours and a Single Point of contact should be available for faster response/escalation.
- aa) The proposed solution able to prioritizes events via various techniques such as AI, machine learning, safe exploitation, correlation, and using custom-defined rules.
- bb) The solution shall be able to perform hunting for low hanging targets susceptible to various threat actors.
- cc) The proposed solution shall be able to run various adversary TTP based playbooks (e.g. nation state actors, ransomware actors) to find which assets (related vulnerabilities) can be low hanging targets for attackers
- dd) The solution shall be able to access to Triage Centre to get access to critical ports and services within 24 hours of creation.
- ee) The solution should be flexible to mark false positive based on banks input and artifacts for observations as well as asset discovered.
- ff) The solution should be capable of finding any data breaches that may impact Canara Bank assets, employees and clients, reputation.
- gg) The proposed solution must have the Basic Web Application Scanning such as:
- i. Black-box Dynamic Application Security Testing (DAST) on the web applications from the internet mimicking an attacker or hacker.
 - ii. OWASP Top 10 attacks on Web Applications.
 - iii. Monitor and Identify Critical Vulnerability on CMS (WordPress / Drupal etc).
- (hh) The solution should monitor SSL certificates regularly for HTTP compression attacks like BREACH, TLS compression attacks like BEAST, Padding Oracle Attacks - Poodle, vulnerable SHA1 algorithm, periodically scan and alert for expiring SSL certificates prior 15, 30, and 60 days, periodically scan and alerts old versions of SSL certificates, etc and any latest attacks available at that time.
- (gg) The solution should provide an option for adhoc/on demand scans as per required frequency to verify infrastructure asset's vulnerability/misconfiguration remediation.
- (ii) The Bidder should benchmark Canara Bank web facing infrastructure and suggest controls required to minimize impact from phishing attacks/ related threats.
- (jj) The OEM through its solution should accept bank's request to add specific or custom Surface/Deep/Dark web source for continuous/ specific external threat monitoring.



(kk) The OEM solution should provide end users to mark threats as High/Medium/Low as per their business preference including marking non-threat.

(ll) The solution should monitor compromised servers for forensic information related to the Bank till the primary incident is closed.

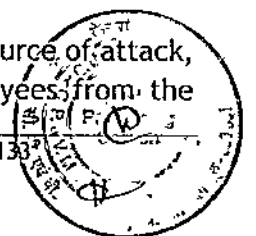
(mm) The solution should support scanning of static and dynamic links and also specify how the suspicious hidden web links/ pages will be detected.

Other Services & Requirements:

- a) Assistance to the bank for coordination with law enforcement agencies, regulators, statutory bodies, CERT-IN etc.
- 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.
- c) The solution shall provide correlation capability and actionable intelligence with respect to historical reference to threats.
- d) The solution shall provide inbuilt issue tracker to track incident/issues/takedowns etc.
- e) Bidder should ensure OEM training (Comprehensive/detailed) is provided along with certification to the members of Canara Bank and training to existing vendors. Training should be done prior to implementation and post implementation (This is mandatory requirement).
- f) The solution shall provide end users to collaborate on the platform.
- g) Alternative response mechanisms other than web site take down should be explored to minimize impact of phishing such as baiting, automatic dummy responses to phishing site using fictitious details.
- h) The solution shall be able to support all major international languages and Indian local languages specifically Hindi and Kannada for identifying chatters/phishing emails etc.

Incident Alerting and Reporting:

- a) Identified incidents with basic research and actionable alerts should be communicated immediately with a unique Incident ID number through dashboard, email and/ or push integration as per bank's requirements. There should be a defined incident categorization available for different types of incidents based on criticality (Eg. High, Medium, Low) for SLA purposes.
- b) The solution should clearly define actions for each identified incident and assist in taking those remedial actions wherever needed.
- c) The solution should provision unlimited user's access.
- d) A round-the-clock email, telephone and remote assistance support, with a designated/named Technical Manager, should be provided.
- e) The OEM shall conduct QBR with Bank's leadership team and provide the situational and the roadmap to reduce the external attack surface of the Bank
- f) The solution should gather forensic information such as IP address, exact URL, source of attack, images, screen shots, email, compromised credentials, data of the Bank employees from the



attacks and other relevant details and share the same with the bank. Bidder to ensure that necessary due care and chain of custody is maintained in handling the evidence such that it is permissible in the court of law.

Service Level Agreements

- a) 24x7x365 monitoring of banks unlimited domains/ sub - domains/ websites etc. and mobile apps.
- b) Alert within 20 minutes of attack/compromise/down/not reachable.
- c) Initial response to the incident within 20 minutes with action plan on taking down and other alternative response mechanisms.
- d) Take down of Phishing Site, within 12 hours of incident and fraudulent mobile apps within 24 hours.
- e) Round the clock monitoring of fraudulent mobile apps and any phishing attacks with 99.90% uptime.
- f) In case of defacement of any of the Bank's website and corresponding web pages, the bidder should notify the Bank over call in the shortest time.
- g) The bidder shall provide Threat Intelligence/ Cyber Intelligence/ Darknet services and monitor Darknet for the information and documents related to Bank and share the data related to cards (Debit Cards, Credit Cards, Financial Information, PII and PHI data etc.) with the Bank on daily basis.
- h) The Bidder to provide the comprehensive SLA's in their proposal.
- i) Any deviations in the SLA for countries of conflict such as Iraq, Africa, Somalia etc. needs to be mutually agreed between bank and the selected bidder in the contract agreement.

Dashboard & Reporting

It should include comprehensive centralized dashboard with below features:

- a) Demonstrating the identified threats and their status, consolidated numbers of threats grouped based on their characteristics, type etc., along with customizable dashboard.
- b) Risks and threats identified through the Anti-Phishing and threat intelligence services.
- c) Depicting activities like logging of incidents, ascertaining status of current/closed incident, generating reports of the reported incidents etc. as per requirement. It should include monthly/quarterly reports containing details of median/average of all incidents closed in the quarter etc.
- d) The portal should deliver a real-time view of all the components of Bank's digital threat protection. An all-encompassing dashboard illustrates threat data, including volume by source and category, and takedown status. Users can also set up email alerts, create online or printed reports, request takedowns. Data should be readily integrated with other systems with REST APIs.
- e) Providing incident reports on phishing attacks and fraudulent apps involving threat analysis and threat categorization.
- f) The OEM should extend full support to the Bank for setup, configuration, training and sales support of the dashboard portal.



- g) The dashboard should display high- and low-level customizable reports, option to process ad-hoc queries, capacity to download extracted data etc.
- h) The solution should provide centralized view of threats / attempts / attacks on Bank's web-facing assets/ websites, with recommendation on mitigation techniques.
- i) The bidder should provide monthly analysis and fraud intelligence reports (both high level - summarized and low level - detailed) to bank.
- j) Reporting to Bank in line with regulatory requirements about all the attacks and providing detailed information through email & online dashboard.
- k) Daily/Weekly/Monthly/Annual and other ad hoc reports to be provided as per the requirement and format provided by the bank.
- l) Monthly and other ad hoc reports to be provided as per the requirement and format provided by the bank.

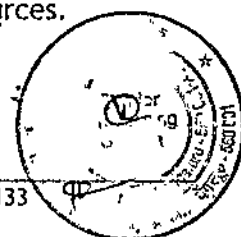
b) Breach Attack Simulation (BAS)

Canara Bank is procuring Breach and Attack Simulation Solution to enhance the security posture of the Bank. The scope includes supply and implementation of the solution. The period of contract will be 5 years. The scope of solution is to achieve functionalities like effectively running multiple attack simulation scenarios on the endpoints, Network / web gateways, email gateway etc. and provide an insight into the current security posture of the bank.

High-level scope of services to be rendered by bidder to the Bank, including but not limited to the following:

Implementation

- a) Bank has envisaged to implement the solutions in Hybrid mode where, there will be broker placed within the Bank's environment to communicate with the SaaS platform.
- b) Bidder shall size and implement the broker to handle the communications.
- c) Bidder to provide HLD document before implementation which shall have the following but not limited to
 - i. Design Approach
 - ii. Technical Specifications
 - iii. License Details
 - iv. Component Details
 - v. Prerequisites (Sizing, Connectivity and Port Requirement)
- d) It is expected that the bidder shall provide all the components required for the implementation and shall factor the same. If any component missed in the proposal, the same shall be provided without any additional cost to the Bank.
- e) Create agent if necessary to perform the synthetic test. Bank shall provide the asset post receiving the requirement from the bidder.
- f) Installation and management of the agents' part of the solutions
- g) Create user accounts in the platform and provide access considering need-to-know basis.
- h) Bank shall approve all the access requests to the platform. Bidder to establish the process for the same and obtain approval from the Bank.
- i) Create LLD and maintain the LLD documentation.
- j) Build SOPs and "How to Documents" for the Bank's consumption.
- k) Provide Pre and Post implementation training for the Bank's designated resources.
- l) Perform user acceptance test and obtain approval from the Bank.
- m) Fix any gaps identified during the UAT within the agreed timeline.



- n) If a solution fails to meet the technical requirements of RFP during the implementation/before sign-off phase, Bank reserves the right to reject the solution with no cost to the Bank and recover all payments made for that solution.
- o) The Proposed Breach and Attack Simulation solution should provide a single platform for running attack simulations to benchmark the performance of deployed security controls against the latest cyber-threats / attacks. The solution should also provide an insight into the security tools which are utilized to prevent from the attack in case the simulation is not successful. Also, the solution should suggest rules/controls to prevent attack in case the simulation is successful. The bidder should expand the coverage of the scope as and when the functional capability is developed during the contract period without any extra cost
- p) The solution deployed should be compliant with Bank's IS, IT and Cyber Security policies, internal guidelines, regulatory requirements and countrywide regulations and laws from time to time.
- q) The bidder shall be responsible for preparation and updating (periodically or as and when there are considerable changes) of all the documents pertaining to the proposed solution with all components.
- r) The bidder shall ensure OEM provides training of the proposed solution to Bank officials during the contract period along with complete training material / documentation.
- s) The bidder's solution must comply with guidelines of RBI/ MeitY/PCI or any other guidelines of GOI or any regulatory authorities in respect of Breach and Attack Simulation Tool issued from time to time.

Operations

- a) Bidder should carry out simulations in a controlled/isolated environment without causing any interference to production environment.
- b) Bidder should deliver safe simulations without any interference with the existing setup and chance of spreading any malware / infected files to other systems should be completely restricted.
- c) Bidder should provide Proof and trace of Attack for manual assessment / simulation which can be produced as artefact for successful simulated breaches
- d) Bidder should ensure that the simulation activity should not add/create performance degradation in the Bank's network.
- e) Bidder should be able to conduct simulation in both the scenario, i.e., inside-out and outside-in.
- f) The solution agent, if any, being used for assessments/simulations should have the capability to run as local user privilege or admin user privilege.
- g) Bidder should be able to initiate attacks using minimum set of access and should not require administrative privileges outright to execute simulations. In case, the simulation requires admin access, the necessary permission needs to be obtained before carrying out the activity.
- h) Bidder should ensure that any malicious files or executables that were run on the system as part of the simulation activity should be removed completely. The solution being used for conducting such simulation should have the capability in this regard.
- i) Bidder should be able to provide the entire attack kill chain in accordance to MITRE attack framework. In case of change in MITRE attack framework, bidder has to adopt the revised / changed framework to provide the report.
- j) Bidder should be able to determine during an attack which security solutions were able to detect the attack and if they were not able to detect then should be able to suggest rules / configurations / remediation to be done on the security solutions.
- k) Bidder should be able to perform simulation using latest Ransomware, malware samples/cases, etc.
- l) Bidder should be able to check any outbound flows of data / critical information, outlined by bank, during simulation. Such simulation should cover exfiltration methods such as SFTP, removable media, on various cloud services like Gdrive etc.
- m) Bidder should be able to detect data transfer to and from malicious domains / IPs / websites (Secure web gateway / proxy test).



- n) Bidder should be able to simulate Infiltration techniques for breaching a network or infecting a host.
- o) Bidder should be able to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc.
- p) Bidder should be able to simulate Real attacks and provide malware artefacts (capability to simulate real exploits and latest malware)
- q) Bidder should be able to test attacker's lateral movement (once successfully within a network) - e.g., pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data.
- r) Bidder to conduct the simulation to check robustness of the email security used by the bank (improper configuration or implementation of email filters).
- s) Bidder to conduct the simulation to check robustness of the endpoints of the bank.
- t) Bidder should carry out attack to test robustness of AV by executing malicious content which can check if the signatures are getting identified in AV including the behaviour.
- u) Bidder should be able to perform privilege escalation during endpoint assessment.
- v) Bidder should simulate real full kill chain i.e., from the initiation of attack till the completion highlighting all the impact such as data exfiltration, lateral movement etc.
- w) Bidder should be able to simulate access, connection or data transfer attempt while performing Network segmentation test.
- x) Bidder should be able to detect the outbound exposure to malicious or compromised websites from the Banks endpoint / server.
- y) The solution being used for simulation should integrate with the Security Operations Centre tools (SIEM) and judge the effectiveness of the same by simulating multi-vector attack.
- z) The solution being used should support red team activities (attack scenarios) and blue team activities (actionable remediation).
- aa) The bidder should provide the option to create custom use cases/ simulations based on new attacks or bank's requirements.
- bb) Bidder should ensure that there is no dependency on other solutions for sourcing threat feeds.
- cc) Service provider should measure the time to detect and respond the attack simulation.
- dd) Bidder shall provide detailed assessment report with contextualized recommendation for the Bank.
- ee) Bidder shall track the recommendations until closure.
- ff) Bidder to perform monthly review and share plans to improve the security risk score provided by the platform.
- gg) Bidder to ensure all the Audit/Assessment observations pertaining to BAS are closed within the agreed SLA
- hh) Bidder to provide Audit and Assessment support as and when required. Provide necessary data to auditors as per the requirements.
- ii) Bidder to provide weekly, Monthly and Quarterly reports capturing the KPIs.

c) Cyber Range

Bank expects Cyber range as service as mentioned in the BOM. Cyber range content should be inclusive of both scenarios and labs. Scenarios are prebuilt content designed to simulate both offensive and defensive enterprise security operations for information technology and operational technology using industry recognized tools and infrastructure.

Labs are defined as self-paced individual experiences focusing on specific learning objectives.

In addition to offering the services listed above, the vendor is expected to submit proposals that consider the following requirements:

- Pre-packaged content ready to be integrated into curriculum for key cybersecurity topics including, but not limited to, cryptography, network security, computer security, software security, offensive security, defensive security, digital forensics on network traffic and digital devices, and incident response.
- Scenarios which support municipal cybersecurity are a high priority. These scenarios could



promote general cybersecurity awareness, incident response across local government or team training events focused on emergency services, schools, or utilities are a special interest for this RFP.

- Cyber range exercises must vary in length and complexity as to be suited for different audiences and skill levels.
- Capability to have concurrent range scenarios and/or labs running at any given time at one facility or across multiple facilities.
- Allows participants on-premises and remote to access any given scenario and labs simultaneously.
- The Bidder has to provide the Labs (such as Network Security, Endpoint Security, Cloud and Application Security labs etc.) and scenarios (such as MITRE ATT&CK, Threat Emulation, Incident Response, Red & Blue Team exercises, OT Security etc.) as part of the training.
- Provides training and support for range administrators.
- Ability to provide range participants with overviews of the range scenarios and labs and formal performance feedback, including correct answers and hints at the conclusion of range scenarios and labs.
- Provides instrumentation for individual and team performance assessments.
- Capability to develop custom content.
- Ability for Bank's officials to tailor content to meet the needs of their development.
- Ability to add new content in the future, as well as an ability to collaborate with Bank's officials to build new content.

d) DDoS Drill

1. Evaluate the existing DDoS mitigation strategies and identify capacity related things.
2. Create realistic DDoS attack scenarios that mimic potential real-world threats.
3. Engage with relevant stakeholders to ensure alignment and understanding of the drill objectives and procedures.
4. Set up a controlled environment to conduct the DDoS drills without impacting actual business operations.
5. Simulate various types of DDoS attacks, including volumetric, protocol, and application layer attacks.
6. Test the SOC's ability to detect and respond to DDoS attacks in real-time.
7. Assess the effectiveness of the incident response procedures and the SOC team's readiness.
8. Gather data on response times, mitigation effectiveness, and overall system performance during the drill.
9. Analyze the collected data to identify strengths and weaknesses in the current DDoS mitigation strategies.
10. Provide detailed reports on the drill outcomes, including identified vulnerabilities and recommended improvements.
11. Conduct training sessions for SOC personnel to enhance their understanding and response capabilities regarding DDoS attacks.
12. Offer actionable recommendations to improve DDoS defense mechanisms and incident response plans.
13. Provide SOP and review DDOS SOP yearly once to Bank to handle DDOS attacks in future.
14. Plan and execute follow-up drills to ensure continuous improvement and readiness.
15. Collect feedback from all stakeholders to refine and enhance future DDoS drill exercises.

15. Scope of work for OEMs



The OEM[S] should be committed to the success of the project during actual implementation by being involved in implementation of the project till its completion. The OEMs should be involved in the overall implementation, support, sustenance, etc. for each of the proposed solutions by the bidder as per the scope of work defined in RFP.

Bidder shall ensure that the OEM is involved in the implementation of the project till its completion. A letter from the product OEM confirming the same have to be submitted in the technical bid. The OEMs must give the certificate to the Bank post implementation, confirming the implementation of their products with best industry practices and the standards and no zero-day threats or malware in the installed device or appliance.

The following are the tentative expectations (but not limited to) with respect to OEM involvement during the contract period, however the bank reserves the right to change the scope:

1. Review of SOC Requirements Specification document, considering all quantitative and qualitative aspects related to configuration of the solution from an industry leading practices perspective and in tune with regulatory guidelines.
2. Review of solution architecture to assess the extent to which same will support SOC requirements and review gaps/ customizations, if any
3. Review of information requirements and supporting processes with respective to completeness and quality
4. Review of functional configuration by duly benchmarking against defined scope and business requirements
5. Review of test strategy, scenarios and test cases developed for supporting the configuration for conducting UAT of the solution configured.
6. Review of UAT environment, plans, mapping of test cases and functional requirement specification and tracking mechanism for resolution of issues.
7. Review transition plan and approach.
8. Sign-off by Bidder and OEM for Go live of respective component.
9. Bidder shall furnish teaming agreement with OEM for the above scope of work and submit the same as part of the bid. This teaming agreement should include but not limited to the ownership of the activities, timelines and resources associated with the activities.
10. OEM should certify that the solution/product is implemented satisfactorily as per RFP terms.
11. OEM should be fully responsible for the successful implementation and Go-live Sign-off of their respective solutions.
12. For above scope of work, OEM shall produce following deliverables during implementation:
 - SOC Review report with recommendations for resolution of any gaps
 - Review Report on solution architecture and information requirements with recommendations for resolution of gaps
 - Report on functional configuration check done containing the observations on UAT test strategy,
 - UAT test cases and scenarios,
 - UAT plan, etc.
13. The Bidder should further provide the deliverables and sign-off for each of the deliverables at various stages of migration, upgradation, customization, and implementation.
14. OEM has to provide the respective solutions hardening documents, best practices and SOPs.
15. Further, the Bidder should arrange for sign-off by OEM for each of the critical stages of migration, upgradation, customization, and implementation.
16. The OEM shall provide premium support
17. OEMs should provide extended support wherever required at each deployment location for their respective solutions during the implementation phase for:
 - Validation of solution design and architecture
 - Continuous monitoring of implementation at each location.
 - Provide SME support to working teams.



- Ensure customization is in line with Bank's requirements.
- OEM sign-off would be necessary after implementation of its products.

18. The OEM shall conduct product certification (Beginner / Associate/ Administrator) training for 5 Bank nominated personnel every year till the contract, the same can be added in BOM (Bill of Material).
19. The OEM shall conduct half-Yearly assessment which should include the following,
- o Functional Effectiveness: The solution has been leveraged to its full potential.
 - o Operation Effectiveness: The solution has been operated as per the defined standard and industry leading best practices.

a. Other General Requirements

Implementation & Integration

- (a) In addition, the bidder is responsible for impact assessment and modification of NGSOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations.
- (b) Integration, Automation in NGSOC and other solutions: Implement the possible automations in NGSOC operations and security solutions, integrate all security solutions with the core NGSOC components.
- (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.
- (d) In case end of life/end of support for any proposed solution including software, hardware, license, and appliance is declared by OEM within contract period, Bidder shall provide upgraded version of the products without any additional cost to the Bank.
- (e) Integrate each solution with SIEM solution to provide a single view of events generated.
- (f) Bidder is responsible for developing and implementing the security configuration hardening of all the devices and software that are procured for NGSOC. Also, all solutions must be periodically reviewed as per guidelines and configure as and when required.
- (g) Any interfaces required with existing applications/ infrastructure within the bank should be developed by the bidder for successful implementation of the NGSOC as per the defined scope of bank.
- (h) The responsibility of integration of new solutions with existing SIEM lies with the Bidder selected through this RFP.
- (i) Development and implementation of processes for management and operation of the NGSOC including (but not limited to) the following processes:
- Configuration and Change Management
 - Incident and Escalation management processes
 - Daily standard operating procedures Training procedures and material
 - Reporting metrics and continuous improvement procedures
 - Data retention and disposal procedures
 - BCP and DR plan and procedures for NGSOC
 - Security Patch management procedure
- (j) Implement necessary security measures for ensuring the information security of the proposed NGSOC and other Security Solutions.
- (k) Provide necessary documentation for the operation, integration, migration, customization, and training of each of the solutions in scope.



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.
Pre-Implementation: Training will be provided to the Bank personnel/ NGSOC team on the product architecture, functionality, and the design for each solution under the scope of this RFP.
Post Implementation: Training will be provided to the bank personnel/ NGSOC team on operations, alert monitoring, policy configuration for all in-scope solutions, routine operations, management, monitoring, etc.
- (b) The Bidder is required to provide all trainees with detailed training material and 3 additional copies to the bank for each solution as per the scope of work of the bank. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution. Training material soft copy also needs to be submitted by the Bidder.
- (c) All out of pocket expenses related to training shall be borne by the selected Bidder.
- (d) The Bidder may utilize the OEM resources in case the Bidder does not have adequately experienced resources for providing 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.

c. Reporting and Security Dashboard

The bidder should provide periodic reports which includes but not limited to How many incidents came, What is the Average TAT (Turn Around Time) for that, How many pending incidents are to be work on, what is the RCA (Root cause Analysis) for those incidents, measure activities conducted, Review of SIEM and PIM integration, Review of Rules/ use cases/ policies of SOC solutions, No. of zero hit rules, no of false positives, improvement or fine tuning done to reduce false positives etc. to the Bank as per the following requirements:

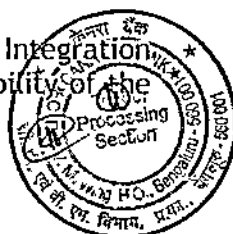
- Daily Reports: Critical reports should be submitted every day.
 - Weekly Reports: Any day of week as decided by Bank.
 - Monthly Reports: 1st week of each month.
 - In addition to this Bank may ask for any custom report at any point of time.
- A. The Bidder is expected to detail every report which it will provide to the Bank related to the services and activities performed by it in the NGSOC.
- B. The Bidder is expected to provide SOPs for all the in-scope solutions and review same at least once a year. After reviewing the same has submitted to Bank.
- C. Dashboard should be provided as an integrated view by integrating with the following tools.
- Risk baseline
 - Asset database
 - Security event/log monitoring tool
 - Vulnerability scanning/ Management tool.
 - Incident management process
 - Security Analysis, Mitigation, and reporting
 - Other security solutions, Technologies and devices as required by Bank.



- 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
- E. Dashboard should display the asset list and capture details including name, location, owner, value, business unit, IP address, platform details etc.
- F. Dashboard should display risk baseline corresponding to multiple categories for IT infrastructure, applications, and processes.
- G. Dashboard should display the security status of IT infrastructure assets of the Bank. The dashboard should have a graphical display of asset security status based on locations, business units, Value, Platform, owner, Overseas Branch, ZO, Zone, Region, Branch, etc.
- H. Dashboard should capture the status of all applications of the Bank. Dashboard should have a graphical display of application security status based on locations, business units.
- I. Dashboard should capture risks in each asset. Dashboard should have the provision to click on the asset and track mitigation status corresponding to risks.
- J. The Bank should be able to benchmark and track mitigation for new global threats and vulnerabilities using the dashboard. The applicability of new threats to the Bank's assets should also be displayed. A drill down of assets affected by new threats, vulnerabilities and status of mitigation should also be supported.
- K. SLA data should be captured in the dashboard with compliance details.
- L. SLA reports as agreed upon by the Bank should be generated on a daily/monthly/quarterly basis.
- M. Exclusive dashboard for uptime / down time of IT Assets, Number of Log generated / Analyzed/ Recommendation etc. Dashboard should be available for following:
- Top Management (Bank View)
 - Department Heads (View to the data associated with their function group / business line)
 - CISO & VH (Vertical Head) of DIT (complete and detailed dashboard of Security posture of the organization set-up being monitored through this SOC)
 - System Administrator (for the systems associated with this administrator).
 - Network / Security Administrator (for devices/equipment for which he is administrator)
 - Application Administrator
 - Auditor (Internal Auditors, IT Auditor, ISO Certification Auditor, any other authorized official of the Bank or Regulator)
- N. All deliverables including reports, incidents / alerts, their closure, vulnerabilities reported and closed, dashboards, query optimization, indexing, automation based on AI/ML, backup & recovery activities etc. should undergo Quality Assurance process by SOC Admin & SOC Engineer onsite resources of the bidder & respective OEM on ongoing basis.

16. System Integration Testing (SIT) and User Acceptance Testing (UAT)

1. There will be a UAT by the Bank for the tools deployed and NGSOC and other security solution operations wherever applicable.
2. The Bank shall commence the UAT as and when each product and service are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to the bank. The results thereafter will be jointly analyzed by all concerned parties including OEMs.
3. UAT will cover acceptance testing of all the product/services, integration with NGSOC tools (Primarily SIEM) and integration of NGSOC with all targeted devices/systems.
4. Once UAT of all the tools of NGSOC are individually completed, then a System Integration Testing shall be carried out by the Bidder to ensure the complete inter-operability of the



NGSOC tools among themselves and integration with the existing infrastructure (targeted devices/systems) of the Bank as specified in the RFP.

5. The Bidder is expected to make all necessary modifications to NGSOC solution including customizations, interfaces, appliances, integration, software etc., if there are performance issues and errors identified by the Bank. These deviations/ discrepancies/ errors observed will have to be resolved by the Bidder immediately.
6. Complete acceptance must adhere to the stipulated timelines.
7. The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP.
8. The Bank will accept the solution on satisfactory completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the Bank.
9. The Bank will conduct an acceptance test before accepting each solution supplied under this project. In the acceptance test, the solution should be completely operational, the solution should comply with its respective technical specification, the solution should integrate with the applicable devices / systems available with the Bank.
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.
11. In case of a discrepancy in facilities /services provided, the Bank reserves the right to cancel the entire contract.

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)
2. Bank currently has a SOC setup in its Data Centre premises at DC & DR. Current SOC setup has integrated with all critical servers, firewalls, security appliances and network devices etc. The proposed SIEM tool should be configured in such a way that all the log sources, configurations, use cases from existing SIEM are migrated to the proposed SIEM.
3. 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.
4. Periodic health checks should be carried out on-site, by the OEM every half yearly to ensure the quality of implementation and operations. On a need basis health checkup exercise shall be conducted.

18. Project Implementation Team

- a. During implementation phase, Bidder will place its team comprising of Bidder's and OEM/OEMs resources for implementation of NGSOC along with proposed solution.
- b. The implementation team will be responsible for design, implementation, integration, fine tuning, and other activities required during implementation phase.
- c. A senior management member from the Bidder shall be identified as the Project Manager (PM) who shall also be part of the steering committee for implementation at the Bank.
- d. The responsibilities of PM are outlined below:
 - Lead implementation effort.
 - Primarily accountable for successful implementation of the project across bank.
 - Act to remove critical project bottlenecks.
 - Identification of working team members, and team leads.
 - Single point of contact for Bank's senior management.



- Ensure implementation timelines are met to achieve desired result.
- Monitor Change management activities during implementation.
- Identify and implement best practices across the Bank.
- Co-ordinate with OEM/OEMs for successful implementation of solutions.
- Periodic reporting to bank on the implementation status, issues/ challenges faced and how these are handled.

(e) EMs 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.

(f) OEM sign-off would be necessary after implementation of its products. In addition to this, OEM/OEMs will also perform half-yearly/yearly health check-up of their solutions implemented in Bank and provide comprehensive report to Bank.

(g) Bidder will also have two separate teams i.e., Monitoring team and Management Teams for handling day to day operations of NGSOC.

(h) Bidders need to provide approximate number of on-site resources in order to meet the service level agreements mentioned in this RF. Bidder should mention number of resources required for managing the NGSOC in the Bill of Material.

Both teams should work on 24x7 basis during contract period.

We hereby comply with the above Scope of Work without any deviations.

Date:

Place:

Designation:

Signature with seal

Name:

