केनरा बैंक Canara Bank

Corrigendum-5 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.

Sl. No	Section/ Annexure/ Appendix of GeM Bid	Clause No.	Existing Clause	Amended Clause
1.	Annexure-9	Functional and Technical Requirements	Functional and Technical Requirements	Amended Annexure-9 Functional and Technical Requirements
2.	Annexure-10	Technical Evaluation Criteria	Technical Evaluation Criteria	Amended Annexure -10 Technical Evaluation Criteria

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: 08/11/2024
Place: Bengaluru

Deputy General Manager

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

केनरा बैंक Canara Bank

Annexure-9

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

I. Security Incident and Event Management (SIEM):

Sl 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 with near zero RPO & RTO. It should also admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.		
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 systems should support 100 % Data Availability guarantee		
30.	SAN Storages must Scale-Up & Scale out with support for intermix of different type of drives (NVMe SSDs, NL SAS, SAS). Data tiering (Auto sub-LUN tiering) should be supported.		
31.	No single point of failure, The SAN system should deliver Industry leading Performance.		
32.	End to End SAN Infra monitoring from a single management suite.		
33.	SAN system should support native remote replication for backup/DR purposes. The storage system should support Zero RTO natively.		
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 symmetric active-active architecture and should have unified capability i.e., should support block and file access with host connectivity for FC, iSCSI, CIFA and NFS. If external appliance required, it should be proposed with necessary licenses.		
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.	Proposed NAS system should have purpose-built hardware acceleration through specialized hardware such as FPGA for superior performance.		
38.	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		
39.	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.		
40.	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.		
	Log Management		
41.	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.		
42.	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		
43.	The network assets are often changing IP addresses. The solution must maintain the asset database correctly even when IP address changes.		
44.	Solution must support industry log collection methods (syslog, WMI, JDBC, SNMP, IPsec, ODBC etc.)		
45.	The solution must support information (users, groups, etc.) collected from Directories (i.e., AD, LDAP) products.		
46.	The solution must not block, drop, or place grace period when system exceeds purchased EPS license/subscriptions limit		
47.	The solution must integrate with other security and network devices such as Firewalls, IPS, WAF, EDR, Switches, Routers etc.		
48.	Solution must have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage		
49.	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.		
50.	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.		
51.	Solution must provide the ability to distribute both event collection and processing across the entire SIEM deployment.		
52.	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		
53.	The solution must ensure the communication between the SIEM components are encrypted		

54.	SIEM solution collector should forward the data to processing unit/component in real time without any delay.		
55.	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		
56.	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.		
57.	The system should be able analyze logs with different event formats e.g., well-structured logs, natural language logs, multi-line logs etc.		
58.	The solution must provide a common taxonomy of events.		
59.	The solution must provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box normalized fields		
60.	The SIEM must provide searching & data/log management, including free form search.		
61.	The solution must provide near-real-time analysis of events.		
62.	The solution must provide more advanced event drill down when required.		
63.	The solution must provide a real-time streaming view that supports full filtering capabilities		
64.	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..		
65.	The solution must allow for custom defined tagging of events		
66.	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)		
67.	The solution must support user extended taxonomy of events and fields. The user must be able to add their own unique event names		
68.	Solution should be able to define purging and retention rules for log storage.		
69.	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.		
70.	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.		
71.	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.		
72.	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.		
73.	The solution must allow the adding/ modifying/ removing of log parsers from UI console without impacting log collection.		

74.	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		
75.	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.		
76.	Solution should have ability to restore / replay older logs for reporting, analysis, correlation, investigation, and forensics.		
77.	Solution should support IPV6 format.		
	Analysis		
78.	The solution must provide alerting based on observed anomalies and behavioral changes in network and security events.		
79.	The solution must support and maintain a history of user authentication activity on a per asset basis.		
80.	The solution must support a web-based GUI for management, analysis, and reporting.		
81.	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.		
82.	Solution should allow analyst to perform manual ad-hoc check to determine if the organization is infected with any Zero-day attack.		
83.	There should be provision available to create complex searches by means GUI, to support advance investigation on the data available in the platform.		
84.	The platform should provide a search experience which shall guides analysts in defining what they want to search for with ability to change.		
85.	The solution must provide alerting based on observed security threats from monitored devices and network activity		
86.	The solution must support a distributed model for correlation such that counters, sequences, identity lookups, etc. are shared across all collectors/loggers/aggregators.		
87.	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		
88.	The solution must provide the ability to correlate information across potentially disparate devices and flows information.		
89.	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.		
90.	The solution must observe anomalies other than just simple threshold basis		
91.	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.		
92.	The solution must provide alerting based upon established policy. (e.g., IM traffic is not allowed.)		

93.	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.		
94.	The solution must provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions		
95.	The solution must provide UI based wizard/ capabilities to minimize false positives and deliver accurate results. Please describe how your solution meets this requirement.		
96.	The solution must limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.		
97.	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		
98.	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.		
99.	The solution must support correlation for a missing secuence. Example service stopped not followed by the service restarting within 10 minutes. Please describe how your solution meets this requirement.		
100.	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.		
101.	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.		
102.	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.		
103.	The solution must be able to be updated regularly, to stay aware of the latest threat information and research available.		
104.	The solution must be able to analyze user activity to detect malicious insiders and determine if a user's credentials have been compromised.		
105.	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.		
106.	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.		
107.	The platform should offer user to tune their environment with the help of built-in analysis capability.		
108.	The platform should suggest new insights to prioritize the rollout of new use cases/apps to effectively strengthen the security posture.		
109.	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.		

110.	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.		
111.	The platform must detect logical or performance issues such as no rule referring to a data/object/folder.		
112.	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.		
113.	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.		
114.	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.		
115.	Platform must be capable of Identify the topmost alert generating rules or event generating rules, and then provide the guide/ steps to tune them.		
116.	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		
117.	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		
118.	The solution must provide a 'Dashboard' for quick visualization of security and network information.		
119.	The solution must support the automated distribution of reports		
120.	The solution must support the capability to provide historical trend reports.		
121.	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.		
122.	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.		
123.	The platform should allow to Import and export dashboards or share dashboard links with colleagues.		
124.	The platform should allow user to create dashboard items that use the full power of native query language, dynamic search, and generic APIs.		
125.	The platform should allow user to fine-tune there with complete flexibility in dashboard layout and dashboard item refresh rates		
126.	The platform should allow user to Assign thresholds.		
127.	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		
128.	The proposed solution must offer all the reports out of the box at no additional cost		

129.	The proposed solution must have real-time visualization options, features and capabilities of the dashboard. A) Blacklist-based correlation. B) Whitelist based correlation		
130.	Proposed solution should have a dashboard to see the real time and history of EPS, Data sources integrated for the last 6 months		
131.	Solution should have option to check non reporting event sources and non-triggered/ zero hit use cases within the given timeframe		
132.	**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 600 bytes for the sizing of solution on OEM Letter Head.**		
	Packet Capture		
133.	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.		
134.	The proposed packet capture solution should ensure full packet and payload capture with network inflow/ outflow of data in DC. 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.		
135.	The proposed packet capture solution should also support future expansion of up to 20 Gbps using same hardware by only adding software license. There should not be any restriction forcing buying of new stack from scratch to support expansion up to 20 Gbps. This requires the solution to have a modular architecture with separate components for collection, data storage, reporting and correlation. The bidder shall provide unit software price which can be leveraged by Bank to procure additional software licenses as and when required during the tenure of the contract.		
136.	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.		
137.	The proposed packet capture solution should be able to perform Real time monitoring of Network traffic analysis to identify threats. Solution should have Deep Packet Inspection (DPI) to provide visibility in all layers of the OSI stack L2 to L7 layer conversations including application payload data in the network and for sharing of network data (Packet + Meta data) in real time. Solution should create indexes for payload objects and not just rely on header information The solution should provide network traffic insight by, • 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.		
138.	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.		
139.	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.		
140.	The solution should have the capability to extract data/ files from the captured network packets		
141.	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.		
142.	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 autocomplete and syntax highlighting, to support automation of incident response workflow.		
47.	The solution must include an in-product script editor with run buttons 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: • 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 be able to perform device control on endpoints by assigning rights to allow or deny the Read, Read/ Write, and block for USB and allow/block Bluetooth peripherals for Windows and Mac OS.		
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 • 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.		
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, Acunetix, Qualys 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: 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, CVE 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: 1. The Title. 2. The Location (URL and/or line of code). 3. Specific vulnerability description. 4. Risk likelihood, business impact, and severity. 5. Code snippets. 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 and IPMI 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, hwpx, iqy, 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, xlsm, xlam, xltm, xml, xht, xhtml, uri, 7z, ace, ang, 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, Beaconing 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		

केनरा बैंक CANARA BANK Tender Processing Section C.P. & V.M. Wing, H.O., Bangaluru - 560 001

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: • 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:

केनरा बैंक CANARA BANK Tender Processing Section H.O., Bengaluru - 560 001

केनरा बैंक Canara Bank

Annexure-10

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
1.	The Bidder must have successfully implemented or managed on-prem Security operation center (*SOC) during last 5 years in organizations like Government/ BFSI/ PSU/ RBI/ NPCI/ NSE/ BSE/ SEBI. The SOC must be currently operational and running (a) 3 and above clients: 10 Marks (b) more than 1 and below 3 clients: 5 Marks Note: * BFSI must be an organization having minimum of 1000 branches or 1 Lakh crore Business in India. * SOC - Bidder must have provided any of the two solutions (SOAR, UEBA, EDR/XDR, PIM/PAM, NBA, DLP, Anti-DDOS, Anti-APT, WAF, DAM) along with SIEM.	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.	10	
2.	The OEM for SIEM must have supplied on-prem SIEM solution in BFSI/ PSU/ Government/ Private entities in India. Supply Experience: • Each reference of 100,000 EPS and above with minimum 400 branches/ offices: 5 marks • Each reference of 80,000 EPS and above: 4 marks. • Each reference of 50,000 EPS and above: 3 marks. Note: Max. 2 references will be considered.	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	
3.	The OEM for SOAR must have supplied on-prem SOAR solution with minimum 5 Analyst/ User licenses in BFSI/ PSU/ Government entities in India. Supply Experience: • For 4 or more clients **having minimum 200 branches** - 5 marks • For 2 clients - 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	

4.	The OEM must have supplied on-prem UEBA solution in BFSI/ PSU/ Government/ Private entities in India. Supply Experience: • 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	
5.	The OEM must have supplied on-prem PIM/ PAM solution with 1000 privileged users in Banking segment in India. Supply Experience: • 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	
6.	The Bidder must have implemented/ managed EDR/ XDR solution in BFSI/ PSU/ Government/ Private entities in India. Implementation/ **Management** Experience: • 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 2 clients of SaaS or On Prem EDR/ XDR each with minimum 10,000 endpoints: 3 Marks • For 1 client of SaaS or On Prem EDR/ XDR each with minimum 5,000 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	
7.	The OEM must have implemented/ supplied SaaS EDR/ XDR solution in BFSI/ PSU/ Government entities in India. Implementation/ Supply Experience: • For 2 clients each with minimum 100,000 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	
8.	The Bidder should have the experience in managing SIEM Solution in Organization(s) in India. Managing Experience: • For 2 clients each with minimum 1 lakh EPS or 4.7 TB/Day: 5 marks • For 2 clients each with minimum 75,000 EPS or 3.6 TB/Day: 4 marks • For 2 clients each with minimum 50,000 EPS or 2.4 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	

9.	The Bidder should have implemented or managed PIM/ PAM Solution in Organization(s) in India **Implementation/ Management Experience:** • 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	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
10.	Presentation by the Bidder: The broader outline of the presentation mentioned below: 1. Overview of the proposed solution 2. Design Principle 3. Implementation and Migration Strategy 4. Implementation Plan 5. Resource Planning 6. SOC Maturity Roadmap 7. 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
11.	Resources: The bidder should have a minimum of 50 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CCNP Security/ CEH. **(a) >=75: 10 Marks** **(b) > 50 and <75: 5 Marks** Note: For CEH maximum 5 number of certified resources will be considered	Undertaking on bidder letter head needs to be submitted.	10
12.	The bidder should have the following OEM certification to get 5 marks for the below mentioned proposed solutions SIEM - 10 Proposed OEM certified resources PIM - 5 Proposed OEM certified resources SOAR - 5 Proposed OEM certified resources EDR - 5 Proposed OEM certified resources Note: All respective certified resources must be on direct payroll of Bidder.	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) total marks for qualifying under Technical Evaluation. The bidders qualified under Technical Proposal Evaluation will be eligible for commercial opening.

केनरा बैंक Canara Bank

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