



Sub: Request for Proposal for Procurement of Breach and Attack Simulation Solution. Ref: RFP No. GEM/2026/B/7692320 dated 20.06.2026

Corrigendum-1

Clarification:

S.No	Page No.	Clause No.	Clause Name	Description	Query Details	Bank's Response
1	34	A.1	Implementation, Deployment and Operational	The services must be deployable in a production environment hosted on an India-based MeitY-approved cloud models. The deployment must be provisioned on a dedicated instance to ensure data isolation and compliance with regulatory requirements.	Please confirm if required hardware and OS can be provided on ndia-based MeitY-approved cloud	Adhere to RFP clause. The Bidder/OEM shall provision and manage all required hardware and operating system components as part of the solution on a dedicated instance hosted on an India-based MeitY-empanelled cloud service provider, ensuring full compliance with regulatory, security, and data localisation requirements of the Bank.
2	34	A.2	Implementation, Deployment and Operational	The solution should provide hybrid approach, utilizing both manual methods and automated tools to conduct simulations.	Clarification is required regarding the manual testing requirements. Typically, testing is highly automated, with minimal or no manual intervention	Adhere to RFP clause. The solution shall primarily support automated execution of attack simulations. A hybrid approach may be adopted, wherein limited manual intervention is permitted/required for scenario customization, validation, or analysis.
3	34	A.3	Implementation, Deployment and Operational	The solution should support agentless or lightweight agents, wherever required, to ensure ease of deployment. The simulation agent/sensor must be compatible with Windows and non-Windows operating systems, including but not limited to Ubuntu,RHEL, and CentOS etc.	In some cases Pentera require distributes architecture, it depend upon network segmentation coverage, please provide details of segmentation so we could provide our recommendation.	Adhere to RFP clause. Detailed requirements/inputs will be shared to successful bidder, if required, during implementation.
4	34	A.3	Implementation, Deployment and Operational	The solution should be capable of initiating simulations with minimal access and must not require administrative privileges by default. If administrative access is necessary for a specific simulation, the required permissions must be obtained prior to conducting the activity.	The required access level depends on the type of assessment. Black-box testing does not require credentials. However, Gray-box assessments and ransomware simulations require the necessary credentials to perform the testing.	Adhere to RFP clause
5	34	A.7	Implementation, Deployment and Operational	The simulation agent/sensor should support both automatic updates from the host device and manual updates when required. Additionally, the solution agent, if used for assessments or simulations, must have the capability to operate with either local user privileges or administrative privileges.	Pentera doesn't update automatically, we provide online update option which required manual effort for update	Adhere to RFP clause. The agent/sensor must be capable of being automatically updated and upgraded through the central console without requiring manual upgrades on endpoint systems.
6	34	A.12	Implementation, Deployment and Operational	The simulation agent/sensor should be deployed on a minimum number of endpoints/servers. Within the given setup, the bidder must be capable of executing and delivering all required use cases and attack simulations effectively.	Need clarity on use case, agent/sensor should be deployed on a minimum number of 12 endpoints/server meant 12 different network ? Also please confirm if those different networks are connecting to each others	Adhere to RFP clause. Solution must be capable of executing all required use cases and attack simulations based on solution deployment architecture with minimum number of endpoints/server. (please note 12 endpoints/servers is not specifically mentioned in RFP document)
7	34	A.16	Implementation, Deployment and Operational	The OEM shall provide comprehensive training to the Bank's team (15 members for 2 days), including sessions on tool usage, simulation customization, campaign execution,report interpretation, and updates to the threat library. Additionally, detailed product 16 manuals, configuration guides, SOPs (operational manual), and a knowledge transfer document shall be provided post-deployment. The training program shall include a minimum of two instructor-led sessions, along with access to on-demand learning resources in initial six months.	Please specify the total hrs for training	Adhere to RFP clause. It is 8 hours per day.
8	36	B.5	Data Protection	The solution must provide granular user role management to ensure that access to information is restricted strictly on a need-to-know basis. It should support Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and integration with AD,LDAP, and SAML.	Please confirm which MFA solution need to integrate	Adhere to RFP clause. Apart from others, the solution should support Multi-Factor Authentication (MFA) which can be OTP, PIM, Token, Email, TOTP etc.
9	37	C.1	Integration Interoperability	The solution must be vendor-agnostic and should support seamless integration with existing systems such as SIEM, SOAR, AV/EDR/XDR, DLP, Threat Intelligence Platforms (TIP), firewalls, ticketing tools, M365, and others, as required.	Please provide the details of the platform which need to integrate	Adhere to RFP clause. Platform details will be shared to successful bidder, if required, during implementation.

10	37	D.2	Functional and Technical Requirements	The OEM must ensure that the solution incorporates the latest industry threats and is capable of enabling corresponding simulations within one day of the discovery of any new threat. The solution should support simulation of zero-day attacks to validate specific threats and associated security controls. Additionally, the threat library must be regularly updated using inputs from various threat intelligence sources, including regulators such as CERT-In and others.	As pentera execute exploit, and we validate for post exploit scenarios as well, hence pentera follow safe by design fundamental and create payload exploit in our Lab, hence we take 5 to 7 days to craft the payload and test it to make sure that payload is safe and non destructive. please confirm if this point can be extended by 5 days after discovery of new vulnerabilities	Adhere to RFP clause.
11	37	D.6	Functional and Technical Requirements	The solution should have the capability to integrate with and consume threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, and others, to enable the creation of customized simulation use cases.	Pentera don't allow to modify or add any open source payload or IOC, as those are not safe to run on production environment. However pentera has its own threat intelligence feed to meet this requirement, please confirm if this suffice the requirement	Adhere to RFP clause. The solution should also use threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, etc apart from others
12	37	D.10	Functional and Technical Requirements	The proposed solution shall support the creation of custom attack scenarios by integrating threat samples from both external and internal sources. It should enable the Bank to design and execute tailored simulations across Windows endpoints and other OS, network infiltration, web applications (including malicious payloads), and email-based attacks, leveraging both imported threat intelligence and the solution's built-in threat repository.	Pentera provide pre define attack scenarios which have holistic coverage for Black Box, Gray Box, ransomware emulation and other scenarios, but pentera doesn't allow to customize these scenarios, please confirm if this meet the requirement	Adhere to RFP clause. Bank expects that the solution includes the ability to adapt and tailor simulations to the Bank's specific environment, architecture, and evolving dynamic threat landscape.
13	37	D.11	Functional and Technical Requirements	The proposed solution should offer ready-to-use static threat templates for emerging and recommended threats, which can be further customized by users to meet specific requirements.	This is feature of threat intelligence platform	Adhere to RFP clause. In the context of a Breach and Attack Simulation (BAS) solution, this requirement is intended to ensure availability of predefined simulation scenarios aligned to emerging and commonly observed threats. These templates should support simulation execution for security validation purposes.
14	37	D.14	Functional and Technical Requirements	The proposed solution should use real-world malicious attack payloads but not limited to: a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaigns	Pentera does cover all points except - Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) As it is part of application security testing, please confirm if customer want to validate their applications as well?	Adhere to RFP clause. The Bank clarifies that the inclusion of "Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities)" is not intended to mandate full-fledged application security testing (AST) capabilities, such as detailed SAST/DAST or code-level testing etc. The intent is to validate security controls surrounding applications.

15	37	D.20	Functional and Technical Requirements	Email Gateway Security Simulation Requirements a. Comprehensive Threat Simulation – The solution must simulate real-world malicious email behaviors, including attachments, embedded links, forged file extensions, multi-layered payloads, MIME-type evasion, and threats such as ransomware, worms, trojans, exploits, and potential code execution. Simulations must cover both common and uncommon file types across Windows, macOS, and Linux platforms. b. Advanced Evasion Testing – The solution must assess the effectiveness of email gateway controls, including sandboxing, real-time inspection, and Content Disarm & Reconstruction (CDR), by simulating techniques such as file type spoofing, MIME validation bypass, and multi-stage attack chains. c. Custom Attack Capabilities – The solution must support uploading, cloning, and modifying custom malicious files, URLs, and templates to simulate organizationspecific scenarios, without executing live malware. d. Realistic yet Safe Payloads – The solution should utilize both real and simulated malware samples to replicate attacker tactics, techniques, and procedures (TTPs). All test payloads must be non-destructive and automatically removed from target mailboxes after the simulation. e. Detailed Reporting & Remediation Guidance – Following simulations, the solution must provide detailed reports outlining the attack flow, identified detection gaps, and actionable remediation recommendations to strengthen email gateway security.	Pentera doesn't validate security controls individually, rather pentera validate security controls efficacy while real word attack is happening, please confirm if requirement is to validate security control individually or holistically	Adhere to RFP clause.
16	37	D.28	Functional and Technical Requirements	AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM top 10.	Please confirm if this point can be deliver through services ?	Adhere to RFP clause. The requirement is desirable not mandatory.
17	44	E.5	Executive Dashboard & Reporting	The solution should provide reports in both executive summary and detailed technical formats. It must also support data export in CSV, PDF, and JSON formats, and enable seamless integration of generated reports with other systems.	The PDF report is available in the platform, it suffice the requirement ?	Adhere to RFP clause.
18	45	F.3	General	The bidder must provide relevant documentation, such as SOC 2 reports, VAPT reports, and CERT-In empanelled audit reports, pertaining to their infrastructure audit processes.	As pentera is global organization hence we don't produce CERT-In empanelled audit reports, but all others report can be produces as required	Adhere to RFP clause.

19	45	F.13	General	<u>Threat Simulation, Analytics, and Security Validation Capabilities</u> • Threat Campaign Creation – The solution shall support the creation of threat campaigns based on industry sector, geography, threat actor profiles, malware families, and attack trends. • Enriched Threat Libraries – Threat libraries shall include detailed metadatasuch as publication date, severity, targeted platforms, mapped MITREATT&CK techniques, and associated vulnerability references. • Dynamic Threat Updates – The solution shall support dynamic threat collections that automatically incorporate newly released threats based on predefined criteria. • Threat Filtering & Prioritization – The solution should enable filtering and prioritization of threats based on the organization's risk profile and business context. • Historical Threat Intelligence – The solution should maintain historical threat intelligence data for trend analysis and forensic investigations. • Health Monitoring & Alerts – The solution shall provide health monitoring for deployed agents, sensors, and integrations, with alerting capabilities for any failures. • Concurrent Simulation Execution – The solution shall support simultaneous execution of multiple simulations across distributed locations and diverse attack vectors. • Browser-Based Testing – The solution should include browser-based testing capabilities for rapid validation of selected web security controls. • Containerized Deployment Support – The solution shall support deployment of assessment components in containerized environments, including Kubernetes, where required. • Detailed Outcome Reporting – The solution shall provide granular pass/fail results for each simulated technique and attack stage, and continue assessment of subsequent stages wherever safely feasible, even if earlier stages are blocked. • Configurable Execution Controls – The solution shall support configurable execution timing, pacing, and scheduling of attack simulations.	Customization on payload would not be available.	Adhere to RFP clause.
20				MSE/NSIC registered bidders are exempted from submitting the bid security.	Please advise if Medium category bidders are also exempted for bid security	Adhere to RFP clause.
21	2	A.1	Implementation, Deployment, and	The services must be deployable in a production environment hosted on an India-based MeitY-approved cloud models. The deployment must be provisioned on a dedicated	Please confirm whether a deployment on a dedicated instance hosted on an MeitY-empanelled Cloud Service	Adhere to RFP clause. Deployment on a dedicated instance hosted in India on a MeitY-empanelled
22	12	D.28	AI and LLM Model Security Testing	AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the	Please clarify whether AI/LLM security testing capability (OWASP LLM Top 10) is a mandatory pass/fail	Adhere to RFP clause. The requirement is desirable not mandatory.
23	12	D.29	VMs and Container Platforms Security	SOW Section D.29 requires the solution to 'enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments' and simulate 'VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and	Please clarify whether VM and Container Platform Security Testing (SOW D.29) is a mandatory pass/fail technical requirement or a preferred/aspirational	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM
24	37	Section III 1) Scope of Work Technical and Functional Specification	D - 6 Functional and Technical Requirements	The solution should have the capability to integrate with and consume threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, and others, to enable the creation of customized simulation use cases	Global BAS platforms "integrate" only with global threat intel, however can "consume" the threat feeds. Requesting to change the clause to only "consuming the threat feeds"	Adhere to RFP clause. The solution should also use threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, etc apart from others
25	39	Section III 1) Scope of Work Technical and Functional Specification	D - 16 - k Functional and Technical Requirements	DDoS and application-layer floods	These threats are not simulatable safely and can create potential damage to the environment. Requesting to remove this category of threat simulations	Adhere to RFP clause. The requirement is desirable not mandatory.

26	39	Section III 1) Scope of Work Technical and Functional Specification	D - 16 - I Functional and Technical Requirements	Deepfake & synthetic media-based phishing,	This is a phishing campaign related feature, not a BAS feature, and should be considered from a dedicated phishing campaign solution. Kindly remove this clause	Adhere to RFP clause. The requirement is desirable not mandatory.
27	54	Section III 1) Scope of Work Technical and Functional Specification	F - 11 General	The OEM must demonstrate readiness for future cryptographic transitions and provide support for, or a defined and time-bound roadmap toward, Post-Quantum Cryptography (PQC) standards and compliance	Requesting for this clause to be removed as an evaluatory criteria. We are willing to showcase our planned capabilities in this domain, however sharing information about the same at bidding stage is not desirable. There needs to be an NDA in place before sharing any such information. Also, the evaluation criterion needs to be understood	Adhere to RFP clause. The requirement is desirable not mandatory.
28	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	The proposed solution should use real-world malicious attack payloads but not limited to:- a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaigns	(i) Supply chain & third-party compromise simulations - Outside the scope of Breach and Attack Simulation which tests internal infrastructure security. (j) DoS/DDoS: Could the Bank define the acceptable scope of DoS/DDoS simulation within a live production banking environment? We respectfully submits that executing volumetric network-layer DDoS against live Bank infrastructure would be operationally destructive and inconsistent with the 'safe, non-disruptive manner' qualifier stated in this clause. We propose relaxation of these points.	Adhere to RFP clause. The points (i) and (j) are now desirable not mandatory.

29	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	The proposed Solution should include, but not be limited to, a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI, b. Prevalent ransomware variants, c. Vulnerabilities exploited by state and non-state actors, d. Business email compromise and advanced phishing campaigns, e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions, f. Insider threat simulations, g. Fileless malware and living-off-the-land techniques, h. OWASP Top 10 web, API and mobile application vulnerabilities, i. Cloud and SaaS compromise scenarios, j. ATM and payment switch targeted attacks, k. DDoS and application-layer floods, l. Deepfake & synthetic media-based phishing, m. Cloud SaaS configuration drift detection, n. API supply chain compromise, o. Mobile banking application attacks (Android/iOS), and p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations. The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility.	The RFP uses 'should include, but not be limited to' language for this requirement, suggesting a non-exhaustive scope. We request the Bank's position on the following sub-items: (j) ATM and payment switch targeted attacks: Are ATM-specific malware simulation scenarios involve targeting ATM-adjacent Windows endpoints? (l) Deepfake & synthetic media-based phishing: Not part of Attack Simulation Platform purview (m) Cloud SaaS configuration drift detection: Is this a BAS simulation requirement or a CSPM (Cloud Security Posture Management) capability? (o) Mobile banking application attacks (Android/iOS): Is a dedicated mobile application testing agent or mobile-specific attack module required or targetted testing of Mobile-compatible web applications? (p) AI/LLM model poisoning / OWASP LLM Top 10 Please define scope and appropriate process of AI/LLM model testing, are you testing the infrastructure on which on-prem models are deployed, or testing the prompts/guardrails connecting back on Frontier models. Please highlight in detail.	Adhere to RFP clause. (j) Yes, ATM and associated systems (e.g., Windows-based management servers, endpoints, middleware etc.), Payment switch applications and interfaces, Network-level attacks impacting ATM transaction flows. (m) Solution should detect the drift in configuration by analysing the risk score of the asset in consideration. (o) Dedicated mobile agents are not mandatory. Solution should support mobile relevant attack scenarios (e.g API abuse, session hijacking, credential theft etc.). Simulated testing may be performed via backend APIs, mobile compatible web interfaces. (l) and (p) points have been made desirable not a mandatory requirement.
30	79	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	d. Security Control Assessment – The solution must assess the effectiveness of real-time file inspection, sandboxing, and Content Disarm & Reconstruction (CDR) mechanisms implemented at the web gateway for detecting and preventing malicious downloads.	Could the Bank confirm the web gateway / secure web gateway (SWG) vendor deployed in its environment? Validation of sandboxing and CDR effectiveness depends on integration with or visibility into the SWG's alert and log output.	Adhere to RFP clause. The details will be shared to successful bidder, if required, during implementation.
31	82	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	Internal Network Attack - Lateral Movement a. The solution must simulate attacks to test internal network configurations, segmentation policies, and lateral movement techniques to evaluate how attackers could spread and reach critical assets. b. Must allow attacks to start from a single compromised workstation without pre-deployed agents or payloads, using evasion techniques and privilege escalation to mimic real-world threats. c. Should simulate common credential access methods, including token/hash extraction, password spraying, Kerberos attacks, and Local Administrator Password Service (LAPS) exploitation, along with privilege escalation techniques. d. Must scan the network to discover systems, accounts, shares, and services, using legitimate network protocols (SSH, RDP, SMB, WMI, etc.) and port scanning to emulate realistic attacker behavior. e. Should allow targeting specific IP ranges, users, or assets, with options to include/exclude systems, control attack speed, and encrypt internal communications to bypass existing defenses. f. Must provide clear visualization of attack paths, compromised endpoints, techniques used, and highlight critical assets reached, producing actionable reports with evidence and timestamps.	Requirement D.27(b) states attacks must start 'from a single compromised workstation without pre-deployed agents or payloads.' Could the Bank clarify the intended interpretation: (a) Does 'without pre-deployed agents or payloads' mean no agents are required on any host in the environment (fully agentless propagation), or does it mean no agents are pre-staged on LATERAL MOVEMENT TARGET hosts i.e., one agent on the initial compromised host is permitted? Our understanding is that since, an initially 'compromised' workstation is provided to start the Lateral Movement Activity, with the Attacker (in this case BAS Platform) already having read/write/execute access on the Machine. Then, the final outcome of the Lateral Movement activity does not change at all even if there is a Pre-installed attacker agent available on the system. If we use a powershell/cmd script Or we use the Agent binary, the end outcome of Lateral Movement Activity (Output/Alerts/Events/Logs) remains the same. Requesting the bank to relax this requirement.	Adhere to RFP clause. Clause D.27(b) is intended to ensure realistic adversary emulation and true lateral movement validation. The requirement does not mandate a fully agentless environment across all hosts. One agent on the initial compromised host is permitted to initiate the attack sequence.

32	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM top 10.	Could the Bank confirm: (a) Is a dedicated AI/LLM security testing module required at Go-Live, or can OWASP LLM Top 10 coverage (prompt injection, insecure output handling, sensitive data exposure via AI APIs) delivered through the existing WAF module and custom attack creator satisfy this requirement? (b) Does the Bank have specific AI/LLM systems deployed (e.g., ADYA AI Chatbot) that need to be in scope for security testing? If so, what type of AI system is it (LLM API, embedded model, third-party service)? We request the bank to highlight in-detail the complete scope, deployment, and proposed outcomes of the AI and LLM Model Security Testing since this is currently a high level requirement. Alternatively, please relax this requirement.	Adhere to RFP clause. The requirement is desirable not mandatory.
33	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	VMs and Container Platforms Security Testing a. Comprehensive Environment Assessment – The proposed solution should enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments. b. Advanced Threat Simulation – The solution should simulate scenarios such as VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and sandbox escape to assess the robustness of virtualization and container security mechanisms.	Could the Bank confirm: (b) For sub-item (b) specifically, 'VM evasion' and 'sandbox escape' are hypervisor-level attack simulations that are distinct from attacks executed on a VM-hosted OS. Does the Bank require simulation of attacks against the hypervisor or virtualization layer itself (e.g., VM escape to underlying host), or attacks on workloads running within VMs? (c) Does the Bank have containerized workloads or Kubernetes clusters in scope? Alternatively, please relax this requirement.	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM breakout scenarios, and control plane exposure.
34	27	8.1: Sno.2	Eligibility Criteria	The bidder should have minimum average annual turnover of Rs. 7 Crores (Rupees Five Crores only) (Rs. 4 Cr – Rupees Ten Crores only for MSE/Startups Bidders) from Indian operations in each of the latest three financial years i.e., 2023-2024, 2024-25 and 2025-26. This must be the individual company turnover from India Operations and not that of any group of companies.	Requested you to amend this clause as: The bidder should have minimum average annual turnover of Rs. 7 Crores (Rupees Five Crores only) (Rs. 4 Cr – Rupees Ten Crores only for MSE/Startups Bidders) from Indian operations in each of the latest three financial years i.e., 2022-2023, 2023-24 and 2024-25. This must be the individual company turnover from India Operations and not that of any group of companies. (because FY 2025-26 financial data are under audit and will take 2 to 3 months)	Adhere to RFP clause. Please refer 8.1 Eligibility criteria S.No 9 and Note c. page no. 30
35	29	8.1: Sno.9	Eligibility Criteria	The net worth of bidder firm should not be negative on 31/03/2026 and also should not have eroded by more than 30% (thirty percent) in the last three financial years ending on 31/03/2026.	Requested you to amend this clause as: The net worth of bidder firm should not be negative on 31/03/2025 and also should not have eroded by more than 30% (thirty percent) in the last three financial years ending on 31/03/2025. (because FY 2025-26 financial data are under audit and will take 2 to 3 months)	Adhere to RFP clause. Please refer 8.1 Eligibility criteria S.No 9 on page no. 29 and Note c. on page no. 30
36	49	Sno.2 (milestone timeline)	Timeframe for completion of activities	Within 4 weeks from date of Purchase Order	Requested you to amend this clause as: Within 6 weeks from date of Purchase Order	Adhere to RFP clause

37	49	Sno.3 (milestone timeline)	Timeframe for completion of activities	Within 5 weeks from the date of Purchase Order	Requested you to amend this clause as: Within 7 weeks from date of Purchase Order	Adhere to RFP clause
38	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	The proposed solution should use real-world malicious attack payloads but not limited to:- a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaigns	(i) Supply chain & third-party compromise simulations - Outside the scope of Breach and Attack Simulation which tests internal infrastructure security. (j) DoS/DDoS: Could the Bank define the acceptable scope of DoS/DDoS simulation within a live production banking environment? We respectfully submits that executing volumetric network-layer DDoS against live Bank infrastructure would be operationally destructive and inconsistent with the 'safe, non-disruptive manner' qualifier stated in this clause. We propose relaxation of these points.	Adhere to RFP clause. The points (i) and (j) are now desirable not mandatory.
39	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	The proposed Solution should include, but not be limited to, a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI, b. Prevalent ransomware variants, c. Vulnerabilities exploited by state and non-state actors, d. Business email compromise and advanced phishing campaigns, e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions, f. Insider threat simulations, g. Fileless malware and living-off-the-land techniques, h. OWASP Top 10 web, API and mobile application vulnerabilities, i. Cloud and SaaS compromise scenarios, j. ATM and payment switch targeted attacks, k. DDoS and application-layer floods, l. Deepfake & synthetic media-based phishing, m. Cloud SaaS configuration drift detection, n. API supply chain compromise, o. Mobile banking application attacks (Android/iOS), and p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations. The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility.	The RFP uses 'should include, but not be limited to' language for this requirement, suggesting a non-exhaustive scope. We request the Bank's position on the following sub-items: (j) ATM and payment switch targeted attacks: Are ATM-specific malware simulation scenarios involve targeting ATM-adjacent Windows endpoints? (l) Deepfake & synthetic media-based phishing: Not part of Attack Simulation Platform purview (m) Cloud SaaS configuration drift detection: Is this a BAS simulation requirement or a CSPM (Cloud Security Posture Management) capability? (o) Mobile banking application attacks (Android/iOS): Is a dedicated mobile application testing agent or mobile-specific attack module required or targetted testing of Mobile-compatible web applications? (p) AI/LLM model poisoning / OWASP LLM Top 10 Please define scope and appropriate process of AI/LLM model testing, are you testing the infrastructure on which on-prem models are deployed, or testing the prompts/guardrails connecting back on Frontier models. Please highlight in detail.	Adhere to RFP clause. (j) Yes, ATM and associated systems (e.g., Windows-based management servers, endpoints, middleware etc.), Payment switch applications and interfaces, Network-level attacks impacting ATM transaction flows. (m) Solution should detect the drift in configuration by analysing the risk score of the asset in consideration. (o) Dedicated mobile agents are not mandatory. Solution should support mobile relevant attack scenarios (e.g API abuse, session hijacking, credential theft etc.). Simulated testing may be performed via backend APIs, mobile compatible web interfaces. (l) and (p) points have been made desirable not a mandatory requirement.

40	82	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	Internal Network Attack - Lateral Movement a. The solution must simulate attacks to test internal network configurations, segmentation policies, and lateral movement techniques to evaluate how attackers could spread and reach critical assets. b. Must allow attacks to start from a single compromised workstation without pre-deployed agents or payloads, using evasion techniques and privilege escalation to mimic real-world threats. c. Should simulate common credential access methods, including token/hash extraction, password spraying, Kerberos attacks, and Local Administrator Password Service (LAPS) exploitation, along with privilege escalation techniques. d. Must scan the network to discover systems, accounts, shares, and services, using legitimate network protocols (SSH, RDP, SMB, WMI, etc.) and port scanning to emulate realistic attacker behavior. e. Should allow targeting specific IP ranges, users, or assets, with options to include/exclude systems, control attack speed, and encrypt internal communications to bypass existing defenses. f. Must provide clear visualization of attack paths, compromised endpoints, techniques used, and highlight critical assets reached, producing actionable reports with evidence and timestamps.	Requirement D.27(b) states attacks must start 'from a single compromised workstation without pre-deployed agents or payloads.' Could the Bank clarify the intended interpretation: (a) Does 'without pre-deployed agents or payloads' mean no agents are required on any host in the environment (fully agentless propagation), or does it mean no agents are pre-staged on LATERAL MOVEMENT TARGET hosts i.e., one agent on the initial compromised host is permitted? Our understanding is that since, an initially 'compromised' workstation is provided to start the Lateral Movement Activity, with the Attacker (in this case BAS Platform) already having read/write/execute access on the Machine. Then, the final outcome of the Lateral Movement activity does not change at all even if there is a Pre-installed attacker agent available on the system. If we use a powershell/cmd script Or we use the Agent binary, the end outcome of Lateral Movement Activity (Output/Alerts/Events/Logs) remains the same. Requesting the bank to relax this requirement.	Adhere to RFP clause. Clause D.27(b) is intended to ensure realistic adversary emulation and true lateral movement validation. The requirement does not mandate a fully agentless environment across all hosts. One agent on the initial compromised host is permitted to initiate the attack sequence.
41	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM top 10.	Could the Bank confirm: (a) Is a dedicated AI/LLM security testing module required at Go-Live, or can OWASP LLM Top 10 coverage (prompt injection, insecure output handling, sensitive data exposure via AI APIs) delivered through the existing WAF module and custom attack creator satisfy this requirement? (b) Does the Bank have specific AI/LLM systems deployed (e.g., ADYA AI Chatbot) that need to be in scope for security testing? If so, what type of AI system is it (LLM API, embedded model, third-party service)? We request the bank to highlight in-detail the complete scope, deployment, and proposed outcomes of the AI and LLM Model Security Testing since this is currently a high level requirement. Alternatively, please relax this requirement.	Adhere to RFP clause. The requirement is desirable not mandatory.
42	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	VMs and Container Platforms Security Testing a. Comprehensive Environment Assessment – The proposed solution should enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments. b. Advanced Threat Simulation – The solution should simulate scenarios such as VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and sandbox escape to assess the robustness of virtualization and container security mechanisms.	Could the Bank confirm: (b) For sub-item (b) specifically, 'VM evasion' and 'sandbox escape' are hypervisor-level attack simulations that are distinct from attacks executed on a VM-hosted OS. Does the Bank require simulation of attacks against the hypervisor or virtualization layer itself (e.g., VM escape to underlying host), or attacks on workloads running within VMs? (c) Does the Bank have containerized workloads or Kubernetes clusters in scope? Alternatively, please relax this requirement.	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM breakout scenarios, and control plane exposure.

43	34	SECTION – III	Scope of work - Technical and Functional Specification	The services must be deployable in a production environment hosted on an India-based MeitY-approved cloud models. The deployment must be provisioned on a dedicated instance to ensure data isolation and compliance with regulatory requirements.	Core Appliaction can we deployed on Private cloud with required hardware and supported OS, OEM need GPU enabled machine with Nvida GeForce RTX 20xx, 30xx, 40xx and 50xx series card and Ubuntu 22.04 OS Please confirm if required hardware and OS can be provided on India-based MeitY approved cloud.	Adhere to RFP clause. The Bidder/OEM shall provision and manage all required hardware and operating system components as part of the solution on a dedicated instance hosted on an India-based MeitY-empanelled cloud service provider, ensuring full compliance with regulatory, security, and data localisation requirements of the Bank.
44	34	SECTION – III	Scope of work - Technical and Functional Specification	The solution should support agentless or lightweight agents, wherever required, to ensure ease of deployment. The simulation agent/sensor must be compatible with Windows and non-Windows operating systems, including but not limited to Ubuntu, RHEL, and CentOS etc.	OEM core is agent less solution, we need to deploy core application on dedicated machine post that deployment OEM don't deploy any other agents on any other machine. In some cases it require distributes architecture, it depend upon network segmentation coverage, please provide details of segmentation so we could provide our recommendation.	Adhere to RFP clause. Detailed requirements/inputs will be shared to successful bidder, if required, during implementation.
45	34	SECTION – III	Scope of work - Technical and Functional Specification	The simulation agent/sensor should support both automatic updates from the host device and manual updates when required. Additionally, the solution agent, if used for assessments or simulations, must have the capability to operate with either local user privileges or administrative privileges.	OEM doesn't update automatically, we provide online update option which required manual effort for update	Adhere to RFP clause. The agent/sensor must be capable of being automatically updated and upgraded through the central console without requiring manual upgrades on endpoint systems.
46	35	SECTION – III	Scope of work - Technical and Functional Specification	The simulation agent/sensor should be deployed on a minimum number of 12 endpoints/servers. Within the given setup, the bidder must be capable of executing and delivering all required use cases and attack simulations effectively.	Need clarity on use case, agent/sensor should be deployed on a minimum number of 12 endpoints/server meant 12 different network ? Also please confirm if those different networks are connecting to each others	Adhere to RFP clause. Solution must be capable of executing all required use cases and attack simulations based on solution deployment architecture with minimum number of endpoints/server. (please note 12 endpoints/servers is not specifically mentioned in RFP document)
47	36	SECTION – III	Scope of work - Technical and Functional Specification	The solution must provide granular user role management to ensure that access to information is restricted strictly on a need-to-know basis. It should support Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and integration with AD, LDAP, and SAML	RBAC and SSO integration is available, Please confirm which MFA solution need to integrate	Adhere to RFP clause. Apart from others, the solution should support Multi-Factor Authentication (MFA) which can be OTP, PIM, Token, Email, TOTP etc.
48	37	SECTION – III	Scope of work - Technical and Functional Specification	The solution must be vendor-agnostic and should support seamless integration with 1 existing systems such as SIEM, SOAR, AV/EDR/XDR, DLP, Threat Intelligence Platforms (TIP), firewalls, ticketing tools, M365, and others, as required.	Please provide the details of platform which need to integrate	Adhere to RFP clause. Platform details will be shared to successful bidder, if required, during implementation.
49	37	SECTION – III	Scope of work - Technical and Functional Specification	The OEM must ensure that the solution incorporates the latest industry threats and is capable of enabling corresponding simulations within one day of the discovery of any new threat. The solution should support simulation of zero-day attacks to validate specific threats and associated security controls. Additionally, the threat library must be regularly updated using inputs from various threat intelligence sources, including regulators such as CERT-In and others.	As solution execute exploit, and we validate for post exploit scenarios as well, hence OEM follow safe by design fundamental and create payload exploit in their Lab, hence it take 5 to 7 days to craft the payload and test it to make sure that payload is safe and non destructive. please confirm if this point can be extended by 5 days after discovery of new vulnerabilities	Adhere to RFP clause.
50	76	SECTION – V	PART I - Technical and Functional Requirements	The solution should have the capability to integrate with and consume threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, and others, to enable the creation of customized simulation use cases.	OEM don't allow to modify or add any open source payload or IOC, as those are not safe to run on production environment. However OEM has its own threat intelligence feed to meet this requirement, please confirm if this suffice the requirement	Adhere to RFP clause. The solution should also use threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, etc apart from others
51	76	SECTION – V	PART I - Technical and Functional Requirements	The proposed solution shall support the creation of custom attack scenarios by integrating threat samples from both external and internal sources. It should enable the Bank to design and execute tailored simulations across Windows endpoints and other OS, network infiltration, web applications (including malicious payloads), and email-based attacks, leveraging both imported threat intelligence and the solution's built-in threat repository.	OEM provide pre define attack scenarios which have holistic coverage for Black Box, Gray Box, ransomware emulation and other scenarios, but OEM doesn't allow to customize these scenarios, please confirm if this meet the requirement	Adhere to RFP clause. Bank expects that the solution includes the ability to adapt and tailor simulations to the Bank's specific environment, architecture, and evolving dynamic threat landscape.

52	76-77	SECTION – V	PART I - Technical and Functional Requirements	The proposed solution should use real-world malicious attack payloads but not limited to: a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaigns	OEM does cover all points except - Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) As it is part of application security testing, please confirm if customer want to validate their applications as well?	Adhere to RFP clause. The Bank clarifies that the inclusion of “Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities)” is not intended to mandate full-fledged application security testing (AST) capabilities, such as detailed SAST/DAST or code-level testing etc. The intent is to validate security controls surrounding applications.
53	78	SECTION – V	PART I - Technical and Functional Requirements	Email Gateway Security Simulation Requirements a. Comprehensive Threat Simulation – The solution must simulate real-world malicious email behaviors, including attachments, embedded links, forged file extensions, multi-layered payloads, MIME-type evasion, and threats such as ransomware, worms, trojans, exploits, and potential code execution. Simulations must cover both common and uncommon file types across Windows, macOS, and Linux platforms. b. Advanced Evasion Testing – The solution must assess the effectiveness of email gateway controls, including sandboxing, real-time inspection, and Content Disarm & Reconstruction (CDR), by simulating techniques such as file type spoofing, MIME validation bypass, and multi-stage attack chains. c. Custom Attack Capabilities – The solution must support uploading, cloning, and modifying custom malicious files, URLs, and templates to simulate organizationspecific scenarios, without executing live malware. d. Realistic yet Safe Payloads – The solution should utilize both real and simulated malware samples to replicate attacker tactics, techniques, and procedures (TTPs). All test payloads must be non-destructive and automatically removed from target mailboxes after the simulation. e. Detailed Reporting & Remediation Guidance – Following simulations, the solution must provide detailed reports outlining the attack flow, identified detection gaps, and actionable remediation recommendations to strengthen email gateway security.	OEM doesn't validate security controls individually, rather it validate security controls efficacy while real word attack is happening, please confirm if requirement is to validate security control individually or holistically	Adhere to RFP clause.
54	84	SECTION – V	PART I - Technical and Functional Requirements	The bidder must provide relevant documentation, such as SOC 2 reports, VAPT reports, and CERT-In empanelled audit reports, pertaining to their infrastructure audit processes.	As OEM is global organization hence we don't produce CERT-In empanelled audit reports, but all others report can be produces as required	Adhere to RFP clause

55	87-88	SECTION - V	PART I - Technical and Functional Requirements Threat Simulation, Analytics, and Security Validation Capabilities • Threat Campaign Creation – The solution shall support the creation of threat campaigns based on industry sector, geography, threat actor profiles, malware families, and attack trends. • Enriched Threat Libraries – Threat libraries shall include detailed metadatasuch as publication date, severity, targeted platforms, mapped MITREATT&CK techniques, and associated vulnerability references. • Dynamic Threat Updates – The solution shall support dynamic threat collections that automatically incorporate newly released threats based on predefined criteria. • Threat Filtering & Prioritization – The solution should enable filtering and prioritization of threats based on the organization's risk profile and business context. • Historical Threat Intelligence – The solution should maintain historical threat intelligence data for trend analysis and forensic investigations. • Health Monitoring & Alerts – The solution shall provide health monitoring for deployed agents, sensors, and integrations, with alerting capabilities for any failures. • Concurrent Simulation Execution – The solution shall support simultaneous execution of multiple simulations across distributed locations and diverse attack vectors. • Browser-Based Testing – The solution should include browser-based testing capabilities for rapid validation of selected web security controls. • Containerized Deployment Support – The solution shall support deployment of assessment components in containerized environments, including Kubernetes, where required. • Detailed Outcome Reporting – The solution shall provide granular pass/fail results for each simulated technique and attack stage, and continue assessment of subsequent stages wherever safely feasible, even if earlier stages are blocked. • Configurable Execution Controls – The solution shall support configurable execution timing, pacing, and scheduling of attack simulations.	Customization on payload would not be available	Adhere to RFP clause
56	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements The proposed solution should use real-world malicious attack payloads but not limited to:- - Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. - Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) - Email-based attacks (phishing, spear-phishing, malicious attachments/links) - Proxy evasion techniques - Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) - Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) - Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) - Insider threat simulation (malicious insider data exfiltration scenarios) - Supply chain & third-party compromise simulations - DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. - Advanced Persistent Threat (APT) - Any combination of the above, or full kill chain attack campaigns	(i) Supply chain & third-party compromise simulations - Outside the scope of Breach and Attack Simulation which tests internal infrastructure security. (j) DoS/DDoS: Could the Bank define the acceptable scope of DoS/DDoS simulation within a live production banking environment? We respectfully submits that executing volumetric network-layer DDoS against live Bank infrastructure would be operationally destructive and inconsistent with the 'safe, non-disruptive manner' qualifier stated in this clause. We propose relaxation of these points.	Adhere to RFP clause. The points (i) and (j) are now desirable not mandatory.

57	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements The proposed Solution should include, but not be limited to, a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI, b. Prevalent ransomware variants, c. Vulnerabilities exploited by state and non-state actors, d. Business email compromise and advanced phishing campaigns, e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions, f. Insider threat simulations, g. Fileless malware and living-off-the-land techniques, h. OWASP Top 10 web, API and mobile application vulnerabilities, i. Cloud and SaaS compromise scenarios, j. ATM and payment switch targeted attacks, k. DDoS and application-layer floods, l. Deepfake & synthetic media-based phishing, m. Cloud SaaS configuration drift detection, n. API supply chain compromise, o. Mobile banking application attacks (Android/iOS), and p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations. The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility.	The RFP uses 'should include, but not be limited to' language for this requirement, suggesting a non-exhaustive scope. We request the Bank's position on the following sub-items: (j) ATM and payment switch targeted attacks: Are ATM-specific malware simulation scenarios involve targeting ATM-adjacent Windows endpoints? (l) Deepfake & synthetic media-based phishing: Not part of Attack Simulation Platform purview (m) Cloud SaaS configuration drift detection: Is this a BAS simulation requirement or a CSPM (Cloud Security Posture Management) capability? (o) Mobile banking application attacks (Android/iOS): Is a dedicated mobile application testing agent or mobile-specific attack module required or targetted testing of Mobile-compatible web applications? (p) AI/LLM model poisoning / OWASP LLM Top 10 Please define scope and appropriate process of AI/LLM model testing, are you testing the infrastructure on which on-prem models are deployed, or testing the prompts/guardrails connecting back on Frontier models. Please highlight in detail.	Adhere to RFP clause. (j) Yes, ATM and associated systems (e.g., Windows-based management servers, endpoints, middleware etc.), Payment switch applications and interfaces, Network-level attacks impacting ATM transaction flows. (m) Solution should detect the drift in configuration by analysing the risk score of the asset in consideration. (o) Dedicated mobile agents are not mandatory. Solution should support mobile relevant attack scenarios (e.g API abuse, session hijacking, credential theft etc.). Simulated testing may be performed via backend APIs, mobile compatible web interfaces. (l) and (p) points have been made desirable not a mandatory requirement.
58	82	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements Internal Network Attack - Lateral Movement a. The solution must simulate attacks to test internal network configurations, segmentation policies, and lateral movement techniques to evaluate how attackers could spread and reach critical assets. b. Must allow attacks to start from a single compromised workstation without pre-deployed agents or payloads, using evasion techniques and privilege escalation to mimic real-world threats. c. Should simulate common credential access methods, including token/hash extraction, password spraying, Kerberos attacks, and Local Administrator Password Service (LAPS) exploitation, along with privilege escalation techniques. d. Must scan the network to discover systems, accounts, shares, and services, using legitimate network protocols (SSH, RDP, SMB, WMI, etc.) and port scanning to emulate realistic attacker behavior. e. Should allow targeting specific IP ranges, users, or assets, with options to include/exclude systems, control attack speed, and encrypt internal communications to bypass existing defenses. f. Must provide clear visualization of attack paths, compromised endpoints, techniques used, and highlight critical assets reached, producing actionable reports with evidence and timestamps.	Requirement D.27(b) states attacks must start 'from a single compromised workstation without pre-deployed agents or payloads.' Could the Bank clarify the intended interpretation: (a) Does 'without pre-deployed agents or payloads' mean no agents are required on any host in the environment (fully agentless propagation), or does it mean no agents are pre-staged on LATERAL MOVEMENT TARGET hosts i.e., one agent on the initial compromised host is permitted? Our understanding is that since, an initially 'compromised' workstation is provided to start the Lateral Movement Activity, with the Attacker (in this case BAS Platform) already having read/write/execute access on the Machine. Then, the final outcome of the Lateral Movement activity does not change at all even if there is a Pre-installed attacker agent available on the system. If we use a powershell/cmd script Or we use the Agent binary, the end outcome of Lateral Movement Activity (Output/Alerts/Events/Logs) remains the same. Requesting the bank to relax this requirement.	Adhere to RFP clause. Clause D.27(b) is intended to ensure realistic adversary emulation and true lateral movement validation. The requirement does not mandate a fully agentless environment across all hosts. One agent on the initial compromised host is permitted to initiate the attack sequence.

59	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM top 10.	Could the Bank confirm: (a) Is a dedicated AI/LLM security testing module required at Go-Live, or can OWASP LLM Top 10 coverage (prompt injection, insecure output handling, sensitive data exposure via AI APIs) delivered through the existing WAF module and custom attack creator satisfy this requirement? (b) Does the Bank have specific AI/LLM systems deployed (e.g., ADYA AI Chatbot) that need to be in scope for security testing? If so, what type of AI system is it (LLM API, embedded model, third-party service)? We request the bank to highlight in-detail the complete scope, deployment, and proposed outcomes of the AI and LLM Model Security Testing since this is currently a high level requirement. Alternatively, please relax this requirement.	Adhere to RFP clause. The requirement is desirable not mandatory.
60	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	VMs and Container Platforms Security Testing a. Comprehensive Environment Assessment – The proposed solution should enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments. b. Advanced Threat Simulation – The solution should simulate scenarios such as VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and sandbox escape to assess the robustness of virtualization and container security mechanisms.	Could the Bank confirm: (b) For sub-item (b) specifically, 'VM evasion' and 'sandbox escape' are hypervisor-level attack simulations that are distinct from attacks executed on a VM-hosted OS. Does the Bank require simulation of attacks against the hypervisor or virtualization layer itself (e.g., VM escape to underlying host), or attacks on workloads running within VMs? (c) Does the Bank have containerized workloads or Kubernetes clusters in scope? Alternatively, please relax this requirement.	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM breakout scenarios, and control plane exposure.
61	50	6) Service Level Agreement (SLA)		Penalties for delay, non-performance and 5% per day salary deduction	In respect of Para No. 6 (SLA): The Bidder proposes that total SLA penalties including liquidated damages should be subject to an overall cap of 10% of the	Adhere to RFP clause
62	50	6) Service Level Agreement (SLA)		Strict milestone timelines	In respect of Para No. 6 (Milestone Timeline): The Bidder requests inclusion of a dependency clause clarifying that timelines shall be extended to the extent of delays attributable to the Bank, including delay in	Adhere to RFP clause
63	52	7) Contract Period		Termination with 180 days' notice	In respect of Para No. 7: The Bidder proposes that the notice period for termination be reduced from 180 days	Adhere to RFP clause
64	52	8) Sub-Contracting		Subcontracting not permitted	In respect of Para No. 8: The Bidder requests that subcontracting to affiliates or specialized partners be permitted with prior written consent of the Bank,	Adhere to RFP clause
65	52	10) Insurance		Extensive insurance obligations and penalty for non-submission	In respect of Para No. 10: The Bidder proposes that insurance requirements be limited to commercially reasonable levels aligned with contract value. Further, deduction of 10% of warranty invoice for non-	Adhere to RFP clause
66	53	12) Liquidated Damages (LD)		0.5% per week up to 10%	In respect of Para No. 12: The Bidder proposes that Liquidated Damages shall be the sole and exclusive remedy for delays and that total LD shall be capped at	Adhere to RFP clause
67	53	14) Performance Security		5% Bank Guarantee requirement	In respect of Para No. 14: The Bidder requests reduction of Performance Security from 5% to 3% of contract value and limiting the claim period to the	Adhere to RFP clause

68	53	15) Limitation of Liability
69	54	16) Indemnity Clause
70	55	20) Intellectual Property Rights
71	56	21) Acceptanc e of
72	58	25) Terminatio n for
73	58	26) Terminatio n for
74	59	27) Force Majeure
75	58	24) Exit Requirem ents
76	60	29) Confidenti ality
77	62	33) Substitutio n of Team Members
78	56	23) Settlement of
79	63	37) Taxes and Duties
80	63	40) General Terms and Conditions

Liability capped but no exclusion for indirect damages	In respect of Para No. 15: The Bidder proposes inclusion of standard exclusions stating that the Bidder shall not be liable for any indirect, incidental, consequential, or special damages including loss of profits, business interruption, or reputational loss.	Adhere to RFP clause
Broad indemnity obligations	In respect of Para No. 16: The Bidder proposes that indemnity obligations be mutual and limited to direct losses only. Further, the Bidder shall not be liable for claims arising due to Bank's misuse, modifications, or	Adhere to RFP clause
Source code escrow requirement	In respect of Para No. 20: The Bidder requests clarification that source code escrow obligations shall be limited only to custom developments made specifically for the Bank and not proprietary software/platforms.	Adhere to RFP clause
Blacklisting for withdrawal post PO	In respect of Para No. 21: The Bidder proposes that the blacklisting clause be moderated and applied only in cases of wilful default, excluding situations beyond the	Adhere to RFP clause
Bank's unilateral right without compensation	In respect of Para No. 25: The Bidder proposes inclusion of termination compensation covering committed costs, non-cancellable orders, and resources	Adhere to RFP clause
Immediate termination rights	In respect of Para No. 26: The Bidder requests inclusion of a minimum cure period of 30 days to	Adhere to RFP clause
Limited scope and strict notification period	In respect of Para No. 27: The Bidder proposes inclusion of broader force majeure events such as pandemics, cyber incidents, and government actions,	Adhere to RFP clause
Mandatory free transition support	In respect of Para No. 24: The Bidder proposes that exit support beyond a reasonable transition period be	Adhere to RFP clause
Perpetual obligations	In respect of Para No. 29: The Bidder proposes limiting confidentiality obligations to a period of 3-5 years post termination, except for confidential data requiring	Adhere to RFP clause
Strict restrictions on replacement	In respect of Para No. 33: The Bidder proposes that substitution be allowed with prior notice and subject to availability of equivalent qualified resources, with	Adhere to RFP clause
3 arbitrator panel and Chennai jurisdiction	In respect of Para No. 23: The Bidder proposes appointment of a sole arbitrator for faster resolution	Adhere to RFP clause
Bidder responsible for all taxes	In respect of Para No. 37: The Bidder requests clarification that prices are exclusive of applicable taxes, which shall be payable by the Bank as per	Adhere to RFP clause
Full liability for employees and agents	In respect of Para No. 40: The Bidder proposes limiting liability to acts performed within the scope of employment and under the Bidder's control, excluding	Adhere to RFP clause

81	38 & 77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	14. The proposed solution should use real-world malicious attack payloads but not limited to:- a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaigns	(i) Supply chain & third-party compromise simulations - Outside the scope of Breach and Attack Simulation which tests internal infrastructure security. (j) DoS/DDoS: Could the Bank define the acceptable scope of DoS/DDoS simulation within a live production banking environment? We respectfully submits that executing volumetric network-layer DDoS against live Bank infrastructure would be operationally destructive and inconsistent with the 'safe, non-disruptive manner' qualifier stated in this clause. We propose relaxation of these points.	Adhere to RFP clause. The points (i) and (j) are now desirable not mandatory.
82	77	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements	16. The proposed Solution should include, but not be limited to, a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI, b. Prevalent ransomware variants, c. Vulnerabilities exploited by state and non-state actors, d. Business email compromise and advanced phishing campaigns, e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions, f. Insider threat simulations, g. Fileless malware and living-off-the-land techniques, h. OWASP Top 10 web, API and mobile application vulnerabilities, i. Cloud and SaaS compromise scenarios, j. ATM and payment switch targeted attacks, k. DDoS and application-layer floods, l. Deepfake & synthetic media-based phishing, m. Cloud SaaS configuration drift detection, n. API supply chain compromise, o. Mobile banking application attacks (Android/iOS), and p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations. The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility.	The RFP uses 'should include, but not be limited to' language for this requirement, suggesting a non-exhaustive scope. We request the Bank's position on the following sub-items: (j) ATM and payment switch targeted attacks: Are ATM-specific malware simulation scenarios involve targeting ATM-adjacent Windows endpoints? (l) Deepfake & synthetic media-based phishing: Not part of Attack Simulation Platform purview (m) Cloud SaaS configuration drift detection: Is this a BAS simulation requirement or a CSPM (Cloud Security Posture Management) capability? (o) Mobile banking application attacks (Android/iOS): Is a dedicated mobile application testing agent or mobile-specific attack module required or targetted testing of Mobile-compatible web applications? (p) AI/LLM model poisoning / OWASP LLM Top 10 Please define scope and appropriate process of AI/LLM model testing, are you testing the infrastructure on which on-prem models are deployed, or testing the prompts/guardrails connecting back on Frontier models. Please highlight in detail.	Adhere to RFP clause. (j) Yes, ATM and associated systems (e.g., Windows-based management servers, endpoints, middleware etc.), Payment switch applications and interfaces, Network-level attacks impacting ATM transaction flows. (m) Solution should detect the drift in configuration by analysing the risk score of the asset in consideration. (o) Dedicated mobile agents are not mandatory. Solution should support mobile relevant attack scenarios (e.g API abuse, session hijacking, credential theft etc.). Simulated testing may be performed via backend APIs, mobile compatible web interfaces. (l) and (p) points have been made desirable not a mandatory requirement.

83	82	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements Internal Network Attack - Lateral Movement a. The solution must simulate attacks to test internal network configurations, segmentation policies, and lateral movement techniques to evaluate how attackers could spread and reach critical assets. b. Must allow attacks to start from a single compromised workstation without pre-deployed agents or payloads, using evasion techniques and privilege escalation to mimic real-world threats. c. Should simulate common credential access methods, including token/hash extraction, password spraying, Kerberos attacks, and Local Administrator Password Service (LAPS) exploitation, along with privilege escalation techniques. d. Must scan the network to discover systems, accounts, shares, and services, using legitimate network protocols (SSH, RDP, SMB, WMI, etc.) and port scanning to emulate realistic attacker behavior. e. Should allow targeting specific IP ranges, users, or assets, with options to include/exclude systems, control attack speed, and encrypt internal communications to bypass existing defenses. f. Must provide clear visualization of attack paths, compromised endpoints, techniques used, and highlight critical assets reached, producing actionable reports with evidence and timestamps.	Requirement D.27(b) states attacks must start 'from a single compromised workstation without pre-deployed agents or payloads.' Could the Bank clarify the intended interpretation: (a) Does 'without pre-deployed agents or payloads' mean no agents are required on any host in the environment (fully agentless propagation), or does it mean no agents are pre-staged on LATERAL MOVEMENT TARGET hosts i.e., one agent on the initial compromised host is permitted? Our understanding is that since, an initially 'compromised' workstation is provided to start the Lateral Movement Activity, with the Attacker (in this case BAS Platform) already having read/write/execute access on the Machine. Then, the final outcome of the Lateral Movement activity does not change at all even if there is a Pre-installed attacker agent available on the system. If we use a powershell/cmd script Or we use the Agent binary, the end outcome of Lateral Movement Activity (Output/Alerts/Events/Logs) remains the same. Requesting the bank to relax this requirement.	Adhere to RFP clause. Clause D.27(b) is intended to ensure realistic adversary emulation and true lateral movement validation. The requirement does not mandate a fully agentless environment across all hosts. One agent on the initial compromised host is permitted to initiate the attack sequence.
84	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements AI and LLM Model Security Testing a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM Top 10.	Could the Bank confirm: (a) Is a dedicated AI/LLM security testing module required at Go-Live, or can OWASP LLM Top 10 coverage (prompt injection, insecure output handling, sensitive data exposure via AI APIs) delivered through the existing WAF module and custom attack creator satisfy this requirement? (b) Does the Bank have specific AI/LLM systems deployed (e.g., ADYA AI Chatbot) that need to be in scope for security testing? If so, what type of AI system is it (LLM API, embedded model, third-party service)? We request the bank to highlight in-detail the complete scope, deployment, and proposed outcomes of the AI and LLM Model Security Testing since this is currently a high level requirement. Alternatively, please relax this requirement.	Adhere to RFP clause. The requirement is desirable not mandatory.
85	83	SECTION-V PART I - Technical and Functional Requirements	D: Functional and Technical Requirements VMs and Container Platforms Security Testing a. Comprehensive Environment Assessment – The proposed solution should enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments. b. Advanced Threat Simulation – The solution should simulate scenarios such as VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and sandbox escape to assess the robustness of virtualization and container security mechanisms.	Could the Bank confirm: (b) For sub-item (b) specifically, 'VM evasion' and 'sandbox escape' are hypervisor-level attack simulations that are distinct from attacks executed on a VM-hosted OS. Does the Bank require simulation of attacks against the hypervisor or virtualization layer itself (e.g., VM escape to underlying host), or attacks on workloads running within VMs? (c) Does the Bank have containerized workloads or Kubernetes clusters in scope? Alternatively, please relax this requirement.	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM breakout scenarios, and control plane exposure.

86	29			The Bidder should hold professional or higher level of partnership with OEMs in India for supply and support of equipment's (applicable if OEM is not the bidder)..	Request Bank to amend as below The Bidder should hold partnership with OEMs in India for supply and support of equipment's (applicable if OEM is not the bidder).	Adhere to RFP clause
87				3.The solution should support agentless or lightweight agents, wherever required, to ensure ease of deployment. The simulation agent/sensor must be compatible with Windows and non-Windows operating systems, including but not limited to Ubuntu,RHEL, and CentOS etc.	please provide details of segmentation whether it is distributed segmentation	Adhere to RFP clause. Detailed requirements/inputs will be shared to successful bidder, if required, during implementation.
88				6.The simulation agent/sensor should support both automatic updates from the host device and manual updates when required. Additionally, the solution agent, if used for assessments or simulations, must have the capability to operate with either local user privileges or administrative	Request to consider only manual update as some OEM do not support automatic update	Adhere to RFP clause. The agent/sensor must be capable of being automatically updated and upgraded through the central console without requiring manual upgrades on endpoint systems.
89				11.The bidder/OEM shall provide post-implementation technical support for all components and services on a 24x7x365 basis, within the timelines stipulated by the Bank.	Request to accept for remote online support	Adhere to RFP clause
90	36	Section III		B Data Protection, Privacy, and Governance		
91				8.The proposed solutions must comply with all applicable data protection and privacy regulations issued by the Government of India, RBI, CERT-In, and other regulatory authorities within the stipulated timelines of availing service.	PI provide further clarity on the same	Adhere to RFP clause. The bidder/OEM should comply with all applicable data protection and privacy regulations issued by the Government of India
92				The proposed solution must support configurable retention policies for simulation logs,telemetry, and audit data in alignment with the Bank's internal data governance standards. Archived data must be encrypted, securely stored within India, and made retrievable within defined timelines upon request. The bidder shall also detail the mechanisms for secure data archival, data purging upon expiration of retention periods,and the controls implemented to manage access to archived data and egress of data.Ingestion of data should not be chargeable.	PI provide further clarity on the same.	Adhere to RFP clause. The bidder/OEM should maintain retention of logs for atleast 180 days as per CERT-In Guidelines and should comply with all applicable data protection and privacy regulations issued by the Government of India
93	37			Simulating Attacks on Proxy Security a. Malicious Traffic Detection – The solution must evaluate the web gateway's effectiveness in detecting and blocking malicious traffic, including access to known malicious websites/IPs, phishing domains, malware distribution sites, command-and control (C&C) servers, and exploit hosting platforms, leveraging continuously updated threat intelligence.	please confirm if requirement is to validate security control individually or holistically	Adhere to RFP clause.
94	35	1) Scope of work Technical and Functional Specification		The bidder/OEM shall provide post-implementation technical support for all components and services on a 24x7x365 basis, within the timelines stipulated by the Bank	We request bank to Amend this clause as below:- The OEM shall provide post-implementation technical support for all components and services on a 24x7x365 basis, within the timelines stipulated by the Bank	Adhere to RFP clause
95	47	1) Scope of work Technical and Functional Specification		The OEM must demonstrate readiness for future cryptographic transitions and provide support for, or a defined and time-bound roadmap toward, Post-Quantum Cryptography (PQC) standards and compliance.	We request bank to remove this clause as its not applicable	Adhere to RFP clause. The requirement is desirable not mandatory.

96	38	1) Scope of work Technical and Functional Specification	D. Functional and Technical Requirements:- 14. The proposed solution should use real-world malicious attack payloads but not limited to: a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers. b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration) c. Email-based attacks (phishing, spear-phishing, malicious attachments/links) d. Proxy evasion techniques e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs) f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities) g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.) h. Insider threat simulation (malicious insider data exfiltration scenarios) i. Supply chain & third-party compromise simulations j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner. k. Advanced Persistent Threat (APT) l. Any combination of the above, or full kill chain attack campaign	We Request to Amend the Points as below:- c. Email-based attacks (phishing links, spear-phishing links, malicious attachments/links) f. Validate security control protecting Web and Mobile application & APIs (Including OWASP Top 10 categories) We Request to remove the Points which is Out of Scope:- i. <Point to be removed - Out of scope> j. <Point to be removed - Out of scope as DOS and DDoS nature is disruptive>	Adhere to RFP clause. The points (i) and (j) are now desirable not mandatory.
97	39	1) Scope of work Technical and Functional Specification	D. Functional and Technical Requirements:- The proposed Solution should include, but not be limited to, a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI, b. Prevalent ransomware variants, c. Vulnerabilities exploited by state and non-state actors, d. Business email compromise and advanced phishing campaigns, e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions, f. Insider threat simulations, g. Fileless malware and living-off-the-land techniques, h. OWASP Top 10 web, API and mobile application vulnerabilities, i. Cloud and SaaS compromise scenarios, j. ATM and payment switch targeted attacks, k. DDoS and application-layer floods, l. Deepfake & synthetic media-based phishing, m. Cloud SaaS configuration drift detection, n. API supply chain compromise, o. Mobile banking application attacks (Android/iOS), and p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations. The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility	We Request to Amend / Remove the Points as below:- h. Validate security control protecting web, API and mobile application vulnerabilities following OWASP Top 10 Category, j. <Point to be removed - ATM and payment switch out of scope> k. <Point to be removed - Out of scope DDoS and application-layer floods are disruptive attacks > l. < Point to be removed - Out of scope as Deepfake & synthetic media-based phishing targets user and not security control> n. < Point to be removed - Out of scope API supply chain compromise out of domain, no control over their security> o. Validate security control protecting Mobile banking application attacks (Android/iOS)	Adhere to RFP clause. (j) Yes, ATM and associated systems (e.g., Windows-based management servers, endpoints, middleware etc.), Payment switch applications and interfaces, Network-level attacks impacting ATM transaction flows. (m) Solution should detect the drift in configuration by analysing the risk score of the asset in consideration. (o) Dedicated mobile agents are not mandatory. Solution should support mobile relevant attack scenarios (e.g API abuse, session hijacking, credential theft etc.). Simulated testing may be performed via backend APIs, mobile compatible web interfaces. (l) and (p) points have been made desirable not a mandatory requirement.
98	45	1) Scope of work Technical and Functional Specification	F. General The implementation shall be carried out exclusively by the OEM at the Bank's Head Office in Chennai (onsite)	We Request to amend this clause as below:- The implementation shall be carried out by Bidder with the assistance of OEM at the Bank's Head Office in Chennai (onsite).	Adhere to RFP clause
99	47	1) Scope of work Technical and Functional Specification	F. General 11. The OEM must demonstrate readiness for future cryptographic transitions and provide support for, or a defined and time-bound roadmap toward, Post-Quantum Cryptography (PQC) standards and compliance.	We Request to remove this Points:- < Point to be removed - PQC readiness and roadmap is subject to evolving protocol standards globally. >	Adhere to RFP clause. The requirement is desirable not mandatory.

100	47	1) Scope of work Technical and Functional Specification		Threat Simulation, Analytics, and Security Validation Capabilities • Browser-Based Testing – The solution should include browser-based testing capabilities for rapid validation of selected web security controls. • Containerized Deployment Support – The solution shall support deployment of assessment components in containerized environments, including Kubernetes, where required.	We Request to remove this Points:- • Browser-Based Testing – Point to be removed, as its redundant, the target control is web gateway/proxy. Any malicious traffic initiated via command line, tools, browser must be protected by inline web gateway control.. We Request to Amend the Points as below:- • Containerized Deployment Support – The offered solution should assess Kubernetes and container security.	Adhere to RFP clause. The solution must provide, at minimum, Kubernetes security validation covering cluster misconfigurations, RBAC weaknesses, container and VM breakout scenarios, and control plane exposure.
101	50	5) Payment Terms		Solution cost: 25% of total solution cost would be paid (Quarterly in arrears, from the date of issuance of Go-Live certificate) On-site support Resource payment: 25% of total resource cost would be paid (Quarterly in arrears, from the date of issuance of Go-Live Certificate)	We Request to amend this clause as below:- Solution cost: 90% of total solution cost would be paid against Delivery of License & 10% against issuance of Go-Live certificate On-site support Resource payment: Resource Monthly cost would be paid (Monthly in arrears, from the date of Deployment of the resources)	Adhere to RFP clause
102	27	8.1	BAS Experience	Mandatory experience in two BAS implementations.	As an MSME bidder participating with an authorized OEM, is any relaxation available in the mandatory BAS implementation experience criteria under applicable Government/MSME procurement guidelines?	Adhere to RFP clause
103	27	8.1	BAS Experience	Experience eligibility.	Will experience in Cyber Security Assessment, VAPT, Red Teaming, Attack Surface Management (ASM), Continuous Security Validation, or similar cybersecurity engagements be considered equivalent to BAS implementation experience for meeting the eligibility criteria?	Adhere to RFP clause. The bidder/OEM should have experience in deployment and maintenance of specific BAS solution.
104	27	8.1	OEM Experience	Eligibility with OEM.	If the bidder participates with an authorized OEM, can the OEM's BAS implementation experience be considered for meeting the mandatory BAS experience requirement?	Adhere to RFP clause. If the bidder participates through an authorized OEM, the OEM's BAS implementation experience may be considered for meeting the mandatory BAS experience requirement.
105	27	8.1	Support Office	Office location requirement.	Kindly clarify whether having a support office in either Mumbai OR Chennai is sufficient to meet the eligibility requirement.	Adhere to RFP clause. Support office in either Mumbai OR Chennai is acceptable.
106	Scope of Work	24x7 Support	Helpdesk	Support requirements.	Can the mandatory 24x7 Helpdesk and support services be provided through the authorized OEM on behalf of the bidder instead of being maintained directly by the bidder?	Adhere to RFP clause. The OEM of the solution should have Online Helpdesk / Management Support Centre Setup in India 24x7.
107	8.1	Supporting Documents	Experience Proof	Supporting documents for experience.	Will Go-Live Certificates, Completion Certificates, Customer Acceptance Certificates, or Satisfactory Performance Letters be accepted where a separate Performance Certificate is not available?	Adhere to RFP clause. Yes, subject to satisfactory verification of the scope and completion status
108		General			Kindly confirm that Bidder along with its affiliate including its subsidiaries shall participate in the bid. The contracting and invoicing for proposed services/goods specified in this RFP will be managed by bidder or its wholly owned subsidiary	The bidder has to be anyone out of bidder itself, its affiliate or OEM.

Amendment:

S.No	Page No.	Clause No.	Clause Name	Description	Query Details	Bank's Response
1	8.1 (4)	28	Eligibility Criteria	The bidder must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion.	We understand OEM relevant certifications can also be considered here. Please confirm. Can this be changed as Either the OEM or the Vendor to have any of the two	Amendment: The point may be read as "The bidder/OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian

2	8.1 (3)	27	Eligibility Criteria	The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years	We understand non-BFSI private organizations will also be considered here. Please advise.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
3	3	8.1 Eligibility Criteria	Eligibility Criterion 3	Eligibility Criterion 3 requires the bidder to have 'successfully provided Breach and Attack Simulation services in at least TWO PSU/Government/BFSI private organizations in India, during last Five years.'	Please clarify whether the deployment and operationalisation of a BAS platform (such as Cymulate) as a Systems Integrator / Channel Partner for a PSU/BFSI client qualifies as 'providing BAS services', or whether only standalone BAS engagement services (without a platform) are considered. Please also confirm whether the client organisation needs to be a current active user of the platform.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
4	3	8.1 Eligibility Criteria	8.1 Eligibility Criteria	The bidder must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018,	Can this be changed as Either the OEM or the Vendor to have any of the two	Amendment: The point may be read as "The bidder/OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion of their BAS setup."
5	27	8.1: Sno.3	Eligibility Criteria	The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.	Requested you to amend this clause as: The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
6	49	Sno.4 (milestone timeline)	Timeframe for completion of activities	On-site support resource deployment	Please share the qualification criteria of the required resources and whether the required resources will be on roll OR off roll	Amendment: Note - The person should be proficient in the proposed solution and should have OEM certification.
7	Page 2	Point 8.1 - 3	Eligibility Criteria	The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years	Should the Purchase Order/Work Order be for the same product proposed by the partner in this tender or any equivalent Breach Attack Simulation solution.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
8	Page 2	Point 8.1 - 4	Eligibility Criteria	The bidder must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion. The Cloud service provider (CSP) must be MeitY-approved Cloud service provider	We are a MSE – we have one certification – ISO 27001-2022 as mentioned in the document. We are also ISO 9001/2000 certified – can this be considered as the other certification to qualify for this tender, request your kind consideration. MeitY approved Cloud service provider – is this required for On Prem solution?	Amendment: The point may be read as "The bidder/OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion of their BAS setup."
9	27	8.1 Eligibility Criteria	3	The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.	We request to relax this clause for wider participation & competitive bidding & amend the clause as follows: "The bidder must have successfully provided Breach and Attack Simulation services in at least TWO ONE PSU/ Government/ BFSI private organizations in India, during last Five years."	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
10	27	8.1		Eligibility Criteria The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.	Reeuest to include OEM experience for the eligibility criteria The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI /private organizations in India, during last Five years.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
11	27			The bidder must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion. The Cloud service provider (CSP) must be MeitY-approved Cloud service provider.	Request to accept ISO 27001:2013 as this involves Cyber Security	Amendment: The point may be read as "The bidder/OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion of their BAS setup."

12	27	8.1 Eligibility Criteria		3. The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.	We request bank to Amend this clause as below:- 3. The bidder must have successfully provided Breach and Attack Simulation services in at least ONE PSU/ Government/ BFSI private organizations in India, during last Five years. Proposed Solution should have deployed Minimum Four PSU/ Government/ BFSI private organizations in India, during last Five years.	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
13	27	8.1	Certifications	Required certifications.	If the bidder possesses ISO/IEC 27001:2022 certification and the proposed OEM holds the remaining prescribed certifications, will the eligibility criteria be considered complied with?	Amendment: The point may be read as "The bidder/OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion of their BAS setup."
14		PQC term		The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years	Instead of Bidder , request you consider Bidder/OEM for giving the reference PO	Amendment: The point may be read as "The bidder/OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years."
15	27	8.1 ELIGIBILITY CRITERIA / S. No. 2		The bidder should have minimum average annual turnover of Rs. 7 Crores (Rupees Five Crores only) (Rs. 4 Cr – Rupees Ten Crores only for MSE/Startups Bidders) from Indian operations in each of the latest three financial years i.e., 2023 2024, 2024-25 and 2025 26. This must be the individual company turnover from India Operations and not that of any group of companies.		Amendment: The bidder should have minimum average annual turnover of Rs. 7 Crores (Rupees Seven Crores only) (Rs. 4 Crores – Rupees Four Crores only for MSE/Startups Bidders) from Indian operations in each of the latest three financial years i.e., 2023 2024, 2024-25 and 2025 26. This must be the individual company turnover from India Operations and not that of any group of companies.
16	27	8.1 ELIGIBILITY CRITERIA / S. No. 3		The bidder must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.		Amendment: The bidder/ OEM must have successfully provided Breach and Attack Simulation services in at least TWO PSU/ Government/ BFSI private organizations in India, during last Five years.
17	27	8.1 ELIGIBILITY CRITERIA / S. No. 4		The bidder must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion. The Cloud service provider (CSP) must be MeitY-approved Cloud service provider.		Amendment: The bidder/ OEM must have at least any two of the below mentioned Certifications such as SOC 2, SOC 3, ISO 20000, ISO 27018, ISO 27001-2022, ISO 27017, ISO 22301, NIST, CSA-STAR or Indian equivalent certifications acceptable as per Bank's discretion of their BAS setup . The Cloud service provider (CSP) must be MeitY-approved Cloud service provider.
18	71	SECTION-V		Technical BID - Technical and Functional Specification Compliance		Amendment: Revised Technical and Functional Specification Compliance attached as Annexure-I
19	49	4) Timeframe for completion of activities / S.No. 4		On-site Support Resource Deployment (Phase-I)		Amendment: On-site Support Resource Deployment (Phase-I) Note - The person should be proficient in the proposed solution and should have OEM certification.

Ref: RFP No. GEM/2026/B/7692320 dated 20.06.2026		ANNEXURE-I	
A	Implementation, Deployment, and Operational	Requirement-Mandatory (M) / Desirable (D)	Compliance (Yes / No)
1	The services must be deployable in a production environment hosted on an India-based MeitY-approved cloud models. The deployment must be provisioned on a dedicated instance to ensure data isolation and compliance with regulatory requirements.	M	
2	The solution should provide hybrid approach, utilizing both manual methods and automated tools to conduct simulations.	M	
3	The solution should support agentless or lightweight agents, wherever required, to ensure ease of deployment. The simulation agent/sensor must be compatible with Windows and non-Windows operating systems, including but not limited to Ubuntu, RHEL, and CentOS etc.	M	
4	The simulation agent/sensor component must be deployable as either a software package or a pre-configured image/golden image.	M	
5	The services must support internet communication via proxy. The simulation agents deployed must also support proxy communication with the corresponding service platform. The proposed services should be OEM-agnostic with respect to proxy configurations.	M	
6	The simulation agent/sensor should support both automatic updates from the host device and manual updates when required. Additionally, the solution agent, if used for assessments or simulations, must have the capability to operate with either local user privileges or administrative privileges.	M	
7	The solution should be capable of initiating simulations with minimal access and must not require administrative privileges by default. If administrative access is necessary for a specific simulation, the required permissions must be obtained prior to conducting the activity.	M	
8	The bidder shall provide architectural, network, and data flow diagrams, along with Standard Operating Procedure (SOP) documents for installation and configuration, as well as any other supporting artifacts required by the Bank for deployment.	M	
9	The implementation of the BAS platform and configuration of policies including fine tuning shall be carried out directly by the OEM.	M	
10	The solution should have the capability to conduct testing across the DMZ and LAN (including VLANs) without bypassing existing network segmentation controls.	M	

11	The bidder/OEM shall provide post-implementation technical support for all components and services on a 24x7x365 basis, within the timelines stipulated by the Bank.	M	
12	The simulation agent/sensor should be deployed on a minimum number of endpoints/servers. Within the given setup, the bidder must be capable of executing and delivering all required use cases and attack simulations effectively.	M	
13	The bidder should define measurable Key Performance Indicators (KPIs) to assess the platform's effectiveness, including metrics such as simulation success rates, reduction in detection gaps over time, and system uptime.	M	
14	The bidder must clearly specify the licensing model of the proposed solution, whether it is based on the number of endpoints, subscription, number of simulations per month, users, or any other applicable metric.	M	
15	The solution should support seamless scalability to accommodate growth in endpoints, expansion of attack libraries, and evolving organizational requirements without any performance degradation. Additionally, the bidder should describe the flexibility of the license to allow scaling up or down during the contract period.	M	
16	The OEM shall provide comprehensive training to the Bank's team (15 members for 2 days), including sessions on tool usage, simulation customization, campaign execution, report interpretation, and updates to the threat library. Additionally, detailed product manuals, configuration guides, SOPs (operational manual), and a knowledge transfer document shall be provided post-deployment. The training program shall include a minimum of two instructor-led sessions, along with access to on-demand learning resources in initial six months.	M	
17	Simulations shall be conducted under strict safety controls to ensure no disruption to services, no alteration of production data, and no risk of data corruption or exposure that could lead to reputational or regulatory impact. The bidder must ensure that simulated attack scenarios do not affect the Bank's infrastructure at any point in time.	M	
18	The solution, whether operating in agent-based or agentless mode, must not result in significant CPU, RAM, or network resource utilization on the Bank's systems and network infrastructure during simulations.	M	
19	The proposed solution should be a comprehensive BAS platform, delivering all functionalities related to breach and attack simulations, aligned with the Bank's current and future IT infrastructure requirements.	M	

20	The solution must be capable of performing simulations without altering or bypassing existing security controls and rules. No whitelisting or special allowances will be provided, except for the necessary connectivity between the agent and the proposed application server (on Cloud).	M	
B	Data Protection, Privacy, and Governance		
1	All telemetry data collected by the proposed services must be processed securely. The bidder should provide a comprehensive overview of the data lifecycle, covering all stages from data generation and ingestion into the cloud to its final permanent deletion or erasure, along with appropriate evidence.	M	
2	For the proposed services, the bidder shall provide assurance, along with supporting evidence, that no Personally Identifiable Information (PII), Sensitive Personally Identifiable Information (SPII), or any personal data governed under the DPDP Act is transmitted from the Bank's environment to the OEM's cloud instance.	M	
3	All captured logs, attack results, and sensitive data must be stored exclusively within India's geographical boundaries and must not be shared outside the Bank under any circumstances.	M	
4	For the proposed solution, the bidder shall provide assurance that any data deleted by the Bank is permanently and irreversibly erased, and does not remain within the OEM's or bidder's infrastructure or services in any form. The bidder must also be able to provide verifiable evidence of such deletion, if required.	M	
5	The solution must provide granular user role management to ensure that access to information is restricted strictly on a need-to-know basis. It should support Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and integration with AD, LDAP, and SAML.	M	
6	The solution must generate tamper-proof audit logs covering all operations, including actions performed by individual users.	M	
7	The proposed solution must not store or transmit credentials in clear text or in an unencrypted form.	M	
8	The proposed solutions must comply with all applicable data protection and privacy regulations issued by the Government of India, RBI, CERT-In, and other regulatory authorities within the stipulated timelines of availing service.	M	
9	For the proposed solution, the OEM/Supplier must promptly notify the Bank upon discovery of any security vulnerability within the solution.	M	

10	The proposed solution must support configurable retention policies for simulation logs, telemetry, and audit data in alignment with the Bank's internal data governance standards. Archived data must be encrypted, securely stored within India, and made retrievable within defined timelines upon request. The bidder shall also detail the mechanisms for secure data archival, data purging upon expiration of retention periods, and the controls implemented to manage access to archived data and egress of data. Ingestion of data should not be chargeable.	M	
C Integration and Interoperability			
1	The solution must be vendor-agnostic and should support seamless integration with existing systems such as SIEM, SOAR, AV/EDR/XDR, DLP, Threat Intelligence Platforms (TIP), firewalls, ticketing tools, M365, and others, as required.	M	
D Functional and Technical Requirements			
1	The bidder should be capable of mapping and presenting the complete attack kill chain in alignment with the MITRE ATT&CK framework. In the event of any updates or modifications to the MITRE ATT&CK framework, the OEM must adopt the revised framework and reflect the changes in the reporting.	M	
2	The OEM must ensure that the solution incorporates the latest industry threats and is capable of enabling corresponding simulations within one day of the discovery of any new threat. The solution should support simulation of zero-day attacks to validate specific threats and associated security controls. Additionally, the threat library must be regularly updated using inputs from various threat intelligence sources, including regulators such as CERT-In and others.	M	
3	The solution should have the capability to conduct simulations using the latest ransomware and malware samples or scenarios, with periodic updates to ensure continued relevance.	M	
4	The solution should include a comprehensive breach library and attack playbooks that target common application vulnerabilities and leverage weaponized known CVEs (Common Vulnerabilities and Exposures).	M	
5	The solution must be capable of reporting vulnerabilities and security gaps with CVEs and appropriate risk severity classifications (Critical, High, Medium, Low, and Informational), based on established cybersecurity risk assessment models and frameworks such as DREAD, CVSS, and NIST.	M	

6	The solution should have the capability to integrate with and consume threat intelligence feed such as IOCs, hashes, and IPs from regulated entities like CSITE, CERT-In, RBI, and others, to enable the creation of customized simulation use cases.	M	
7	The solution should support both signature-based and behavior-based assessments at endpoints/Servers/Applications.	M	
8	The proposed solution should deliver technology- or vendor-specific remediation signatures, along with prioritized mitigation recommendations.	M	
9	The proposed solution should provide the actual payload or content used during threat execution, rather than only Indicators of Compromise (IOCs) in the threat details. Additionally, the solution must deliver comprehensive attack details mapped to the MITRE ATT&CK framework.	M	
10	The proposed solution shall support the creation of custom attack scenarios by integrating threat samples from both external and internal sources. It should enable the Bank to design and execute tailored simulations across Windows endpoints and other OS, network infiltration, web applications (including malicious payloads), and email-based attacks, leveraging both imported threat intelligence and the solution's built-in threat repository.	M	
11	The proposed solution should offer ready-to-use static threat templates for emerging and recommended threats, which can be further customized by users to meet specific requirements.	M	
12	The proposed solution should provide ready-to-use dynamic threat templates for security posture management, such as readiness against ransomware and advanced persistent threat (APT) groups.	M	
13	The proposed solution should be capable of automatically incorporating newly added attacks into dynamic templates without requiring any user intervention.	M	
	The proposed solution should use real-world malicious attack payloads but not limited to:-		
	a. Endpoint-based attacks (malware execution, privilege escalation, LOLBins persistence techniques) including servers.	M	
	b. Network-based attacks (infiltration, lateral movement, credential theft, exfiltration)	M	
	c. Email-based attacks (phishing, spear-phishing, malicious attachments/links)	M	
	d. Proxy evasion techniques	M	
	e. Attacks on cloud infrastructure (misconfiguration exploitation, IAM privilege abuse, exposed APIs)	M	

14	f. Attacks on Web and Mobile Applications & APIs (including OWASP Top 10 vulnerabilities)	M	
	g. Active Directory-based attacks (pass-the-hash, golden ticket, Kerberoasting, Password Spraying etc.)	M	
	h. Insider threat simulation (malicious insider data exfiltration scenarios)	M	
	i. Supply chain & third-party compromise simulations	D	
	j. DOS and DDoS (Network and application based) / Resource exhaustion attacks in a safe, non-disruptive manner.	D	
	k. Advanced Persistent Threat (APT)	M	
	l. Any combination of the above, or full kill chain attack campaigns	M	
15	The proposed Solution should allow all the simulated attacks to be managed from one Central Console.	M	
16	The proposed Solution should include, but not be limited to,		
	a. The latest global and regional attack trends, top MITRE ATT&CK techniques observed in BFSI,	M	
	b. Prevalent ransomware variants,	M	
	c. Vulnerabilities exploited by state and non-state actors,	M	
	d. Business email compromise and advanced phishing campaigns,	M	
	e. Advanced persistent threat (APT) scenarios targeting Indian financial institutions,	M	
	f. Insider threat simulations,	M	
	g. Fileless malware and living-off-the-land techniques,	M	
	h. OWASP Top 10 web, API and mobile application vulnerabilities,	M	
	i. Cloud and SaaS compromise scenarios,	M	
	j. ATM and payment switch targeted attacks,	M	
	k. DDoS and application-layer floods,	D	
	l. Deepfake & synthetic media-based phishing,	D	
	m. Cloud SaaS configuration drift detection,	M	
	n. API supply chain compromise,	D	
	o. Mobile banking application attacks (Android/iOS), and	M	
	p. AI model poisoning / prompt injection attacks, OWASP LLM top 10 and supply chain compromise situations.	D	
	The solution should allow the bank to modify and create campaigns to simulate real-world threats with full flexibility.	M	

17	The proposed solution should utilize actual threat payloads for security control assessment, rather than relying on 'PCAP replay' techniques for web application attacks.	M	
18	The solution must include mechanisms to track, measure, and minimize false positives and false negatives. It should validate attack outcomes by correlating simulation results with logs from EDR/XDR, SIEM, or firewall systems to determine whether simulated threats were detected, blocked, or missed. This correlation must be clearly reflected in reports to enhance SOC effectiveness and support the tuning of security controls.	M	
19	The proposed solution should support both HTTP and HTTPS protocols to simulate inbound and outbound attack scenarios, including network infiltration (e.g., malicious file downloads) and data exfiltration techniques, for effective assessment of security controls.	M	
20	Email Gateway Security Simulation Requirements		
	a. Comprehensive Threat Simulation – The solution must simulate real-world malicious email behaviors, including attachments, embedded links, forged file extensions, multi-layered payloads, MIME-type evasion, and threats such as ransomware, worms, trojans, exploits, and potential code execution. Simulations must cover both common and uncommon file types across Windows, macOS, and Linux platforms.	M	
	b. Advanced Evasion Testing – The solution must assess the effectiveness of email gateway controls, including sandboxing, real-time inspection, and Content Disarm & Reconstruction (CDR), by simulating techniques such as file type spoofing, MIME validation bypass, and multi-stage attack chains.	M	
	c. Custom Attack Capabilities – The solution must support uploading, cloning, and modifying custom malicious files, URLs, and templates to simulate organization-specific scenarios, without executing live malware.	M	
	d. Realistic yet Safe Payloads – The solution should utilize both real and simulated malware samples to replicate attacker tactics, techniques, and procedures (TTPs). All test payloads must be non-destructive and automatically removed from target mailboxes after the simulation.	M	
	e. Detailed Reporting & Remediation Guidance – Following simulations, the solution must provide detailed reports outlining the attack flow, identified detection gaps, and actionable remediation recommendations to strengthen email gateway security.	M	
	Simulating Attacks on Proxy Security		

21	a. Malicious Traffic Detection – The solution must evaluate the web gateway’s effectiveness in detecting and blocking malicious traffic, including access to known malicious websites/IPs, phishing domains, malware distribution sites, command-and-control (C&C) servers, and exploit hosting platforms, leveraging continuously updated threat intelligence.	M	
	b. Malware Download Simulation – The solution must simulate the download of malicious payloads such as executables, ransomware, worms, trojans, and other malware (both known and custom), including multi-layered malicious files, from legitimate domains or file hosting platforms across Windows, macOS, and Linux systems.	M	
	c. Policy Enforcement Validation – The solution must test web gateway policy enforcement across categories such as social media, hacking, spyware, adult content, downloads, and other restricted content to assess the effectiveness of configured controls.	M	
	d. Security Control Assessment – The solution must assess the effectiveness of real-time file inspection, sandboxing, and Content Disarm & Reconstruction (CDR) mechanisms implemented at the web gateway for detecting and preventing malicious downloads.	M	
	e. Custom Simulation & Cleanup – The solution must support uploading and simulating custom malicious files and URLs, allow customization of playbooks/templates, and ensure that any malicious artifacts bypassing controls are automatically removed upon completion of the simulation.	M	
22	<u>Simulating Attacks on Web Application Firewall</u>		
	a. Comprehensive WAF Testing – The solution must evaluate WAF capabilities against OWASP Top 10 vulnerabilities and other known attack payloads, including SQL Injection, time-based attacks, Cross-Site Scripting (XSS), command injection, file inclusion, XML-based injections, Server-Side Request Forgery (SSRF), path traversal, NoSQL injection, WAF bypass techniques, remote code execution (RCE), and other web and API-based attacks.	M	
	b. Diverse and Safe Payload Coverage – The solution should include a wide range of payload categories (OS-specific, database-specific, encoding variations), covering blind, error-based, encoded, and evasion techniques, without using destructive or irreversible exploits.	M	
	c. Automated Parameter Mapping & Testing – The solution must automatically discover and map HTTP requests, forms, and parameters of web applications, and perform targeted simulations on identified inputs to validate WAF detection and prevention effectiveness.	M	
	d. Safe Production Testing – The solution must enable secure testing on live production WAF environments without requiring UAT or test clones, ensuring no service downtime, data loss, or unintended false positives.	M	

	e. Custom Payload Support – The solution must allow uploading and executing customer-defined attack payloads to address organization-specific security use cases.	M	
23	<u>Simulating Attacks against Data Leak Prevention (DLP)</u>		
	a. Exfiltration Technique Assessment – The solution must evaluate both host-based and network-based DLP controls against a variety of data exfiltration techniques, including removable media, SFTP, Telnet, HTTP/HTTPS, email, browser uploads, and other channels.	M	
	b. Customizable Testing Capabilities – The solution must support customization, cloning, and modification of playbooks/templates, and allow uploading of custom keywords, phrases, and files for targeted testing.	M	
	c. Cross-Platform Simulation – Simulations must be executable across Windows, macOS, and Linux environments.	M	
	d. Detailed Reporting – Reports must clearly indicate whether each exfiltration method was permitted, detected, or blocked, along with the success or failure status of each attempted data transfer.	M	
24	<u>Simulating Emerging Cyber Threat Exposure</u>		
	a. Up-to-Date Threat Intelligence Simulation – The solution shall maintain a continuously updated library of Indicators of Compromise (IOCs) representing active threat actors, and leverage these to simulate emerging threats for evaluating the effectiveness of email gateways, web gateways, and endpoint security controls.	M	
	b. Safe Threat Delivery Simulation – The solution shall simulate the delivery of known malicious URLs or files to test detection and blocking capabilities across email and proxy/web gateways, ensuring no operational impact to the environment.	M	
	c. Endpoint Malware Detection Testing – The solution shall simulate endpoint-based malware detection by securely deploying and removing malicious test files (IOCs) on designated target systems, with complete cleanup ensured after each simulation.	M	
	d. Evidence Retention & Integration – The solution shall retain detailed evidence, including timestamps for each simulated threat event, and support integration with EDR and SIEM platforms to validate detection, alerting, and incident response workflows.	M	
	<u>Simulating Attacks on Endpoint Security Controls</u>		

25	a. Comprehensive Detection Assessment – The solution must evaluate both signature-based detection (e.g., known malware and recent exploits) and behavior-based detection mechanisms, including ransomware, trojans, worms, rootkits, APT techniques, browser exploitations, and multi-stage or chained attack scenarios across Windows, macOS, and Linux endpoints.	M	
	b. Defense Evasion Simulation – The solution must simulate advanced evasion techniques such as payload obfuscation, fileless or in-memory execution, staged payloads, and “Living off the Land” (LotL) techniques, with the capability to challenge endpoint defenses, including EDR/XDR bypass and tampering scenarios.	M	
	c. Control Effectiveness Evaluation – The solution must assess the effectiveness of individual endpoint security controls as well as their combined operation (e.g., AV, EDR, Group Policy, system hardening), and provide clear visibility into coverage gaps.	M	
	d. Customizable and Safe Simulations – The solution must support customization, cloning, and modification of attack playbooks/templates, ensuring that all simulations are safe, non-destructive, and executed only on designated test systems.	M	
	e. Evidence Retention & Integration – The solution must retain detailed evidence with timestamps, ensure complete cleanup of all simulated payloads post-execution, and support integration with EDR and SIEM platforms for real-time correlation of simulation events.	M	
26	<u>Simulating Attacks against the Complete Security Stack</u>		
	a. End-to-End Attack Simulation – The solution must support the creation of multi-stage attack scenarios to comprehensively evaluate all deployed security controls across the organization.	M	
	b. Real-World Threat Emulation – The solution must simulate tactics, techniques, and procedures (TTPs) used by real-world threat actors across the entire cyber kill chain, including malware such as ransomware, trojans, and worms.	M	
	c. Realistic Attack Vectors – The solution should enable attack initiation through common vectors such as email and malicious URLs, replicating real-world scenarios including file execution, command-and-control (C2) communication, and data exfiltration.	M	
	d. Automated Kill-Chain Execution – Full kill-chain attack simulations must be capable of running automatically, without requiring manual intervention, as and when required.	M	
	e. Advanced Evasion Techniques – The solution must incorporate defense evasion methods such as payload obfuscation, staged execution techniques, and the use of native system tools (Living off the Land).	M	

	f. Customization, Evidence & Safety Controls – The solution should support cloning, modification, and creation of attack playbooks, maintain audit-ready evidence with timestamps, ensure complete cleanup after simulations, and strictly restrict execution to designated test environments.	M	
	Internal Network Attack - Lateral Movement		
	a. The solution must simulate attacks to test internal network configurations, segmentation policies, and lateral movement techniques to evaluate how attackers could spread and reach critical assets.	M	
	b. Must allow attacks to start from a single compromised workstation without pre-deployed agents or payloads, using evasion techniques and privilege escalation to mimic real-world threats.	M	
27	c. Should simulate common credential access methods, including token/hash extraction, password spraying, Kerberos attacks, and Local Administrator Password Service (LAPS) exploitation, along with privilege escalation techniques.	M	
	d. Must scan the network to discover systems, accounts, shares, and services, using legitimate network protocols (SSH, RDP, SMB, WMI, etc.) and port scanning to emulate realistic attacker behavior.	M	
	e. Should allow targeting specific IP ranges, users, or assets, with options to include/exclude systems, control attack speed, and encrypt internal communications to bypass existing defenses.	M	
	f. Must provide clear visualization of attack paths, compromised endpoints, techniques used, and highlight critical assets reached, producing actionable reports with evidence and timestamps.	M	
	AI and LLM Model Security Testing		
28	a. Comprehensive Security Assessment – The solution should be capable of testing the security of Artificial Intelligence (AI) systems and Large Language Models (LLMs) by simulating real-world cyberattack scenarios including OWASP LLM top 10.	D	
	VMs and Container Platforms Security Testing		
29	a. Comprehensive Environment Assessment – The proposed solution should enable evaluation of security controls and identification of gaps across virtual machine (VM) and containerized environments.	M	
	b. Advanced Threat Simulation – The solution should simulate scenarios such as VM evasion, resource exhaustion, privilege escalation, isolation weaknesses, and sandbox escape to assess the robustness of virtualization and container security mechanisms.	M	
E	Executive Reporting & Dashboards		
1	The solution should provide executive dashboards and reports, with the capability to customize them as per specific requirements.	M	

2	The proposed solution should retain historical assessment data and provide capabilities for comparative analysis over time.	M	
3	The bidder should provide confirmation that all reports stored within the solution are encrypted and accessible only to authorized Bank personnel.	M	
4	The service provider must deliver comprehensive details of compromises and attack flows, including impacted assets, exploited vulnerabilities, remediation measures, and corresponding mapping to the MITRE ATT&CK framework.	M	
5	The solution should provide reports in both executive summary and detailed technical formats. It must also support data export in CSV, PDF, and JSON formats, and enable seamless integration of generated reports with other systems.	M	
6	The solution must include graphical dashboards that present the results of security effectiveness validation in a clear and insightful manner.	M	
7	The solution must include at least one graphical dashboard that presents quantitative results, showing both the numeric count and the percentage distribution of attacks across each stage.	M	
8	The solution dashboard must provide summary reports along with graphical visualizations of the results of executed attack simulations.	M	
F	General		
1	The OEM should be capable of enhancing or integrating the solution to meet new regulatory requirements on an ongoing basis, with minimal effort.	M	
2	The selected bidder shall provide the following documents as part of the project deliverables: Original product manuals for the proposed solution Standard Operating Procedures (SOPs) for installation and configuration Troubleshooting manual Executive summary report for management Functional and operational requirements documentation Project design and implementation plan Product description documentation Best practices guidance and implementation guidelines Business continuity, archival, data purging, and backup policies and procedures User Acceptance Testing (UAT) plan Training materials and related documentation	M	
3	The bidder must provide relevant documentation, such as SOC 2 reports, VAPT reports, and CERT-In empanelled audit reports, pertaining to their infrastructure audit processes.	M	
4	The implementation shall be carried out exclusively by the OEM at the Bank's Head Office in Chennai (onsite).	M	
5	The OEM shall be responsible for assessing and certifying the implementation, hardening, and configuration of the solution and fine tuning.	M	

6	The OEM shall generate periodic reports (daily, weekly, and monthly) on the health and performance of security devices and systems and share them with the Bank's team. In the event of any performance bottlenecks identified by either the OEM or the Bank, appropriate corrective actions and support must be provided until the issue is fully resolved.	M	
7	<u>Post-Implementation Acceptance and Go-Live Process</u> Following the implementation of the solution, the Bank will conduct an acceptance test prior to issuing the Go-Live certificate. The process shall include: 1. Evaluation by the Bank – The Bank will assess the implemented solution for compliance with specified requirements and overall functionality. 2. Non-Compliance or Deficiencies – If the solution fails to meet the required specifications or exhibits significant deviations: The Bank reserves the right to terminate the contract. Any payments made up to that point shall be recoverable from the Performance Bank Guarantee (PBG). The selected bidder shall be required to remove all deployed equipment at their own cost and risk. 3. Acceptance Testing Arrangements – The selected bidder shall be responsible for organizing and executing the acceptance testing at designated locations. The testing will be conducted in the presence of Bank officials and/or designated consultants. The implementation shall be considered complete only upon successful acceptance testing and formal issuance of the Go-Live certificate.	M	
8	The selected bidder must ensure that the project is executed in accordance with the timelines defined under the Service Level Agreement (SLA).	M	
9	The selected bidder in coordination with OEM must take all necessary precautions to prevent any damage to equipment, IT infrastructure, or existing setups during execution of the work. In the event of any damage to Bank property arising from the bidder's negligence or lack of due care, the bidder shall be held financially liable, and the cost of repairs or replacement shall be recovered from the bidder.	M	
10	<u>Roles and Responsibilities for Implementation</u> The OEM shall be responsible for all aspects of the implementation process, including: - Providing all necessary tools - Supplying appropriate testing and measurement equipment - Delivering any additional items required for successful implementation and installation.	M	

	The selected bidder shall act as a liaison between the Bank and the OEM to ensure effective coordination and execution. The bidder must ensure that the implementation is carried out in accordance with industry standards and applicable safety regulations. All required resources and equipment for safe and proper implementation shall be arranged and provided by the OEM.		
11	The OEM must demonstrate readiness for future cryptographic transitions and provide support for, or a defined and time-bound roadmap toward Post-Quantum Cryptography (PQC) standards and compliance.	D	
12	The solution shall provide MITRE ATT&CK coverage heatmaps, including views for prevention, detection, and validation coverage.	M	
	<u>Threat Simulation, Analytics, and Security Validation Capabilities</u>		
	• Threat Campaign Creation – The solution shall support the creation of threat campaigns based on industry sector, geography, threat actor profiles, malware families, and attack trends.	M	
	• Enriched Threat Libraries – Threat libraries shall include detailed metadata such as publication date, severity, targeted platforms, mapped MITRE ATT&CK techniques, and associated vulnerability references.	M	
	• Dynamic Threat Updates – The solution shall support dynamic threat collections that automatically incorporate newly released threats based on predefined criteria.	M	
	• Threat Filtering & Prioritization – The solution should enable filtering and prioritization of threats based on the organization's risk profile and business context.	M	
	• Historical Threat Intelligence – The solution should maintain historical threat intelligence data for trend analysis and forensic investigations.	M	
	• Health Monitoring & Alerts – The solution shall provide health monitoring for deployed agents, sensors, and integrations, with alerting capabilities for any failures.	M	
	• Concurrent Simulation Execution – The solution shall support simultaneous execution of multiple simulations across distributed locations and diverse attack vectors.	M	
	• Browser-Based Testing – The solution should include browser-based testing capabilities for rapid validation of selected web security controls.	M	
	• Containerized Deployment Support – The solution shall support deployment of assessment components in containerized environments, including Kubernetes, where required.	M	
	• Detailed Outcome Reporting – The solution shall provide granular pass/fail results for each simulated technique and attack stage, and continue assessment of subsequent stages wherever safely feasible, even if earlier stages are blocked.	M	

13

• Configurable Execution Controls – The solution shall support configurable execution timing, pacing, and scheduling of attack simulations.	M	
• Encrypted Exfiltration Simulation – The solution shall support simulation of encrypted data transfers across commonly used exfiltration channels.	M	
• Custom Artifact Integration – The solution shall support the import of organization-specific indicators, threat samples, and custom test artifacts for creating tailored simulations.	M	
• Predefined Threat Campaigns – The solution should provide predefined campaigns covering prevalent threats, ransomware activities, and commonly abused MITRE ATT&CK techniques.	M	
• URL Filtering Validation – The solution should support safe validation of URL filtering policies across multiple URL categories and custom-defined URL lists.	M	
• External Web Control Testing – The solution should enable controlled validation of externally exposed web security controls using non-disruptive techniques.	M	
• Detection Performance Metrics – The solution shall measure and report detection latency, alert generation time, and response visibility across integrated security controls.	M	
• Detection Outcome Visibility – The solution shall identify whether simulated activities were logged, detected, alerted, or blocked by integrated security platforms.	M	
• API-Based Integration – The solution shall support secure API-based integration with SIEM, EDR, XDR, and other monitoring platforms.	M	
• ATT&CK-Based Analytics – The solution should provide MITRE ATT&CK-based detection coverage analytics and map observed security control performance.	M	
• Evidence Export for Hunting – The solution should support export of simulation evidence and findings to facilitate threat hunting and rule optimization.	M	
• Automated Report Delivery – The solution shall support automated, scheduled delivery of both executive and technical reports.	M	
• Trend Analysis – The solution shall provide trend analysis of security effectiveness over configurable time periods.	M	
• Customizable Dashboards – The solution shall offer customizable dashboards and reporting views tailored for different stakeholder groups.	M	
• Benchmarking Capabilities – The solution should provide benchmarking of security effectiveness metrics against anonymized peer groups or industry standards, where available.	M	
• KPI-Based Remediation Tracking – The solution should include dashboards for tracking and prioritizing remediation based on key performance indicators (KPIs).	M	

• Attack Path Visualization – The solution should provide visualization of attack paths and lateral movement findings, where applicable.	M	
• REST API Support – The solution shall expose REST APIs to support automation, reporting, campaign management, and integration workflows.	M	
• Standard Format Export – The solution shall support export of findings and metrics in standard formats suitable for third-party integrations.	M	
• Role-Based Administration – The solution shall provide role-based administrative controls with granular delegation of operational and reporting permissions.	M	
• Audit Logging & Forwarding – The solution shall maintain searchable audit logs and support forwarding of audit events to centralized logging platforms.	M	
• Coverage Reporting – The solution should provide reporting on tested and untested assets, security controls, and attack surfaces.	M	