REQUEST FOR PROPOSAL (RFP)
FOR PROCUREMENT OF COMPREHENSIVE ENDPOINT SECURITY SOLUTION FOR STATE BANK GROUP

CORRIGENDUM Dated 08-Oct-2021

To RFP

Ref no. SBI/GITC/Platform Engineering-I/2021/2022/792 Dated: 16-Sep-2021

Deputy General Manager
IT-Platform Engineering-I Department,
State bank of India Global IT Centre,
Gr Floor 'A'- Wing, Plot no 8/9/10,
Sector -11, CBD Belapur
Navi Mumbai- 400614

Corrigendum Dated 08-Oct-2021
RFP no. SBI/GITC/Platform Engineering-I/2021/2022/792 Dated: 16-Sep-2021
for PROCUREMENT OF COMPREHENSIVE ENDPOINT SECURITY SOLUTION FOR STATE BANK GROUP

Sl no.	RFP Page No	RFP Clause No.	Existing Clause	Revised Clause
1	67	11	Solution must have following features and should be able to manage from central management console: Full Disk Encryption (Drive Encryption-FDE) File and Folder Encryption (FFE) Removable Media Encryption (RME) Solution should allow management and configuration of the encryption product features preferably within a single console.	Clause Removed.
2	72	35	Solution should be able to perform Cognitive Threat Analysis for Endpoints for inspecting web proxy logs to uncover issues such as memory-only malware and infections that may live in a web browser only.	Solution should be able to perform Threat Analysis of Endpoints for inspecting to uncover issues such as file less malware prevention and web browser base attacks prevention.
3	75	54	Solution should provide Digital Identity Protection (protecting personal information from being leaked through cookies, temporary internet files, etc.)	Solution should provide Digital Identity Protection (protecting personal information from being leaked such as cookies, temporary internet files, etc.)
4	77	67	Solution should integrate with Hypervisors like VMware ESXi without the need to install agents on the guest VMs and all other Hypervisors available in market and use by corporates/industry.	Solution should integrate with Hypervisors like VMware ESXi with/without the need to install agents on the guest VMs and all other Hypervisors available in market and use by corporates/industry.
5	100	167	The solution shall have the capability to inspect and block attacks that happen over SSL.Solution should support SSL orchestration features and provide all latest features/ technologies.	The solution shall have the capability to inspect and block attacks that happen over SSL.Solution should support SSL.
6	108	206	The solution should support forwarding of alerts through SNMP and E Mail.	The solution should support forwarding of alerts through E-Mail.

7	70	25	Solution must identify and block/alert on lateral movement (SMB relay, pass the hash) and provide Network traffic monitoring, Deception via fake nodes, Deception via fake user accounts, Deception via fake network connections	Solution must identify and block/alert on lateral movement (SMB relay, pass the hash) and provide Network traffic monitoring originating from endpoints.
8	69	22	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List • Threats related to virtual infrastructure like hyper jacking, guest VM escape etc.	The Solution should be able to perform the following correlations (but not limited to) based on analysis rules mapped to various threat categories and provided with criticality information. The various threat categories to be covered include: • Vulnerability based. • Statistical based. • Historical based. • Heuristics based. • Behavior based on source entity, applications etc. • Information Leak. • Unauthorized Access. • Denial of Service. • Service Unavailable. • Phishing attack • Pattern based rules • Profiling • Whitelist/ Blacklist/ Reference List • Applicable to Virtual environment endpoints. (Threats related to virtual infrastructure like hyper jacking, guest VM escape etc.)
9	79	81	Solution should support Investigation and ensure threat containment by complete incident playback with continuous recording of endpoint activity, view specific endpoint processes	Solution should support Investigation and ensure threat containment by complete and continuous incident logging of endpoint activity, view specific endpoint processes
10	89	120	Solution must have a Vulnerability Protection feature and does not only give visibility, but Rules should also be able to do Virtual patching of the vulnerabilities using Deep Packet Inspection and should have CVE ID mapping to the rules.	ESS solution should be capable to protect the endpoints from OS related vulnerabilities by automated virtual patching/scripting/tool base protection of the endpoints in absence of patch/fix release by OS vendor

11	89	121	Solution should have deep packet inspection, Integrity monitoring, Log inspection and correlation capability to identify content that may harm the application layer, Filters forbidden network traffic and ensures allowed traffic through stateful inspection	Solution should have deep packet scrutiny, Integrity monitoring, Log scrutiny and correlation capability to identify content that may harm the application layer, Filters forbidden network traffic and ensures allowed traffic through stateful investigation.
12	98	157	Solution must have central repository of threat intelligence - powered with 3T+ threat queries, more than 60 B threats per day, sensors, and multiple sources of threat information and same should be available as update for SBI.	Solution must have central repository of threat intelligence - powered with 01 trillion+ threat queries and more than 10 Billion threats per day, sensors, and multiple sources of threat information and same should be available as update for SBI.
13	100	163	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (E.g., Selecting rules, Configuring policies, updating policies, etc...)	Solution should provide ability to automatic/script base/tool base rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (E.g., Selecting rules, Configuring policies, updating policies, etc.)
14	100	165	Solution should provide recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.	Solution should provide recommendation for automatic/script base/tool base removal of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.
15	104	186	Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events. Solution should be capable of providing application Server Security Requirement such as • Deep Packet Inspection (HIPS/HIDS). • Anti-Malware/ransomware. • Integrity monitoring. • Log inspection.	Solution should have a Log scrutiny which provides the ability to collect and analyze operating system, databases and applications logs for security events. Solution should be capable of providing application Server Security Requirement such as • Deep Packet Inspection (HIPS/HIDS). • Anti-Malware/ransomware. • Integrity monitoring. • Log scrutiny.
16	105	187	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow

			allow creation of custom log inspection rules as well.	creation of custom log scrutiny rules as well.
17	105	188	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/un-assignment of rules when not required.	Solution must have an option of automatic recommendation of rules for log analysis as per the Server OS and can be scheduled for automatic/script/tool base assignment/un-assignment of rules when not required.
18	105	190	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.	Log scrutiny rules should allow setting of severity levels to reduce unwanted event triggering.
19	90	123	Solution should have multiple types of rules i.e., Vulnerability, exploit and smart rules.	Solution should have multiple types of rules i.e., Vulnerability, exploit and general rules.
20	91	131	Solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT, Imaging, Prt Scrn key, Wireless Nic	Solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT, Imaging, Prt Scrn key, and Wireless Nic for endpoints (Desktops). If required Bank will implement for servers also.
21	67	9	The solution to support disk encryption features for the endpoints.	Clause Removed.
22	152	PAYMENT SCHEDULE:	*License Cost* 1. Product Delivery, Signing of SLA --10% of License Cost 2. On successful security clearance from Information Security Department of the Bank for production rollout of ESS solution.--15% of License Cost 3. First Year Payment in Arrears --15% of License Cost 4. Second Year Payment in Arrears --15% of License Cost 5. Third Year Payment in Arrears --15% of License Cost 6. Fourth First Year Payment in Arrears--15% of License Cost 7. Fifth Year Payment in Arrears--15% of License Cost	License Cost 1. Product Delivery, Signing of SLA --10% of License Cost 2. On successful security clearance from Information Security Department of the Bank for production rollout of ESS solution.--15% of License Cost 3. First Year Payment in Advance --15% of License Cost 4. Second Year Payment in Advance --15% of License Cost 5. Third Year Payment in Advance --15% of License Cost 6. Fourth First Year Payment in Advance--15% of License Cost 7. Fifth Year Payment in Advance--15% of License Cost

23	70	27	Solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files) • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Locking a local user account or a domain user. • Zeroing user password. • Blocking telecommunications based on destination (domain address or IP address). • Disconnection of network cards. • Change of IP address. • Capability of editing a HOST file. • Renewed operation of an end station and/or a server. • Include Damage Cleanup Service functionality which addresses changes to the Windows registry and other similar malicious alterations.	Solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint and provide the capability such as • Capability of running a coordinated command (such as CMD interface). • Running script or a file from a network location or mapping a drive. • Shutting down an endpoint and/or a server. • Isolation of an endpoint/ server from the network and should support for virtualized infrastructure as well. • Deletion of a file (including active run files). • Put file into quarantine (including active run files). • Kill a process. • Remove malicious files, roll back and repair other changes or - can create remediation instructions that can be made available for other tools to implement. • Kill a malicious process immediately after tracing it. • Removal and/or deletion of a service/scheduled task. • Blocking telecommunications based on destination (domain address or IP address). • Disconnection of network cards. • Capability of editing a HOST file. • Renewed operation of an end station and/or a server. • Include Damage Cleanup Service functionality which addresses changes to the Windows registry and other similar malicious alterations.
24	110	(C) Application Change Controls (ACC) Features		Bank requirement is to implement all ACC features/functionality on desktops and ACC limited/critical feature/functionality on Servers.

25	117	(D) File Integrity Monitoring features.		Presently, Bank requires FIM module for servers only. Bank may implement the FIM on endpoints other than servers, if required. All cost included in Project cost. No extra cost will be paid during contract period.

********** End of Document**********