6.2.2.95 GTP of Network Threat Detection

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of Network Threat Detection			
S/N.	**Item**	**Technical Requirements**	**Bidder Response**
1	Quality	ISO 9001:2000 certification	
2	Brand	To be mentioned by the bidder	
3	Model	To be mentioned by the bidder	
4	Country of Origin	To be mentioned by the bidder	
5	Solution Requirements	The proposed solution should have network-based identity threat defenses that trap insider threat actors from deceiving, misdirecting, and isolating known and unknown human & automated attacks that have established footholds in-network using decoys of production OS, applications, and more	
6		The proposed solution should deploy fake devices, systems, and assets among the real assets to bait attackers without exposing the existing systems and assets.	
7		The proposed solution should support various operation system & service not limited to Windows, Linux, SSL VPN, HTTP, FTP, TFTP, SMNP, IPMI, ERP, POS, SQL, SMB, RDP,SSH etc.	
8		Solution should be On prem & dedicated VM based or hardware based. If VM base bidder have to submit detail requirements of hardware, OS & hypervisor.	
9	Threat Detection and Response	Solution should detect malicious outsiders and insiders seeking to escalate privileges, leverage access credentials, and make lateral movements in networks	
10		Solution should reduce the time an attacker can remain on a network, thereby decreasing a compromise and remediation cost	
11		Solution must have the ability to download the malware/threat actor engagement as PCAPs or executables dropped for further analysis	
12		Solution should analyze the captured data by several built-in engines like IPS, AV, Web Filter. Bidder should quote license if required to meet the requirement	
13		Solution must support to detect Malware & Ransomware attack and ability to alert	
14		Solution should have the ability to see how attackers are moving in the inside network, their primary targets and how they are progressing, through the IT infrastructure	
15		The proposed solution should enable security teams to early detect and respond by analyzing attacker's techniques, tools, and procedures for inside attacks prevention	
16	Monitoring, Management and Reporting	Support GUI and SSH for management access	
17		Ability to generate security incident reports in PDF format	
18		Ability to send incident alerts over email	

19		Support Role Base Admin Access	
20	Security Integrations	Solution must have the ability to integrate into SIEM technology	
21		Solution must have the ability to integrate with NGFW, NAC, SOAR for quarantine/banned IP and the ability to quarantine depending on the severity of an event	
22		Solution must provide a built-in option to integrate with any third-party tool that supports REST-API	
23	Manufacturer's part number & License	Bidder must be submitted Manufacturer Authorization (MAF)	
24		Bidder should submit BOQ of device including the details part number with license of 6 IP subnet/VLAN/Network Address.	
25	Industry Recommendation	The OEM must be a member of Cyber Threat Alliance (CTA) which is a non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field	
26		The OEM must have local employee & office in Bankgladesh to get the prompt response	
27		The proposed solution should have minimum 3 (three) install based reference in Bangladesh.	
28	Warranty & Support	Bidder should propose hardware & software for 3 (three) years OEM warranty and RMA support.	
29	**License**	**The license period shall have at least 03 years and will be calculated from the first day of system handover**	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.96 GTP of SIEM

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of SIEM		
S/N	**Technical Specification**	**Bidder's Response**
1	**Vendor Information:**	
	a. **Brand:** To be mentioned by bidder	
	b. **Model:** To be mentioned by bidder	
	c. **Country of Origin**: To be mentioned by bidder	
	d. **Country of Manufacture**: To be mentioned by bidder	
2	**Solution Acceptance:**	
	a. The solution must be an on-premise solution.	
	b. The solution must be listed as leader / challenger from 2022 to 2025 on Gartner Magic Quadrant for Security Information and Event Management (SIEM). Necessary documents should be provided.	
3	**SIEM Architecture**	
	a. All Collection components, from here on referred to as collectors/ forwarders. The proposed solution should have physical or logical separation of the collection module, logging module and analysis/ correlation module with the ability for adding more devices, locations, applications, etc.	
	b. SIEM solution provide 1500 or more real-time rule correlation across all cluster components	
	c. SIEM solution provide in memory distributed rule correlation across all cluster components	
	d. The proposed solution must support caching mode of transfer for data collection, to ensure data is being logged in the event of loss of network connectivity, and resume sending of data upon network connection.	
	e. Collectors / Forwarders compress the data before sending to the storage and correlation tier.	
4	**The SIEM storage and correlation tier**	
	a.The Bidder must propose the solution for a single-tier architecture.	
	b. The SIEM solution shall have the capability to compress logs for reducing disk space usage.	
	c. The SIEM solution shall have the capability to stored event data must be in a compressed mode and should suppot compression of 10:1 and should support upto 15:1 compression for log size more that 1000 bytes	
	e. The Data Retention Period for warm data should be 9 months and for hot data should be 3 months.	
5	**The SIEM must be able to collect additional context beyond log data from devices and this should be achieved by:**	
	a. Actively discovering the devices within the network without an agent and using standard protocols such as SNMP, WMI, SSH, Telnet, JDBC, OPSEC & JMX	
	b. Ability to monitor the status and responsiveness of services including DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH and Web — HTTP, HTTPS (Single and Multi-Step).	
	c. Once active discovery of the devices is complete the SIEM should have a built-in template that will automatically define what metrics will be collected for devices and the collection intervals.	
6	The SIEM should provide a unified analytics interface that allows the same query language to analyze both log data and performance data.	

7	Analytics must support nested queries where a user can use a query to filter the results of the previous query.	
8	The system should be able to drop events on the Collectors that are not relevant or not needed. This should not impact any licensing.	
9	Both raw, parsed and enriched data must be passed to the SIEM Cluster from the Collectors. Separate event database should not be used for raw data and parsed data.	
10	Processing of event data should be performed by parsers at receipt time of the event.	
11	All parsers should be able to be modified and customized.	
12	Custom parsers should be able to be created and defined in the GUI without CLI access.	
13	Devices shall be monitored without agents via SSH, telnet WMI, JMX and Power Shell.	
14	Ability to collect Windows events via WMI and agent	
15	The SIEM should provide role based access to restrict access to the data and also restrict access to the GUI.	
16	**Ability to integrate Threat Intelligence (TI) feeds:**	
	a. Integration via REST API with different supported data format (CSV, Custom, STIX)	
	b. Support for STIX/TAXII	
	c. Support for but not limited to IP Addresses, Domains, Hashes, URLs, Malware Process Names	
	d. Ability to correlate TI data in real-time, in memory against event data.	
	e. Ability to correlate TI data against historic event data.	
17	Ability to collect network device configuration, identify changes and provide side-by-side comparison.	
18	Proposed solution should offer separate dashboard for PCI/ DSS reporting.	
19	**Notification and Incident Management**	
	a. Policy-based incident notification framework.	
	b. API-based integration to external ticketing systems — Jira/ Service Now/ Sales force/ Zen desk/ The Hive/ Connect Wise/ Remedy.	
20	**Solution shall have Built-in ticketing/case management system or the vendor shall propose one that has the below minimum capabilities:**	
	i. Ability to define an escalation policy that sends an email to management when thresholds reached.	
	ii. Ability to add PDF and PNG to tickets.	
	iii. Ability to assign tickets to other operators.	
	iv. Timeline view to capture activities on a Case and on related incidents.	
	v. Provides Mean Time To Resolution metric	
21	The proposed solution shall integrates Security Orchestration, Automation, and Response (SOAR) capabilities natively into the SIEM platform from day one. Bidder should quote necessary license if required.	
22	The proposed solution shall support automated workflows across the incident lifecycle, including investigation, enrichment, remediation, and attack response.	
23	The proposed solution should provides a library of pre-built playbooks for common use cases like incident investigation and threat hunting and playbooks should be triggered automatically by events, on a schedule, or manually by an analyst.	
24	The proposed solution should enables the creation of custom playbooks to fit specific security needs and workflows.	
25	**Powerful and Scalable Analytics**	
	a. The proposed solution must be able to search events in real-time and must support sophisticated statistical/ summary analysis by pipelining advanced search commands together in a single search/ using logical operator such as AND, OR, NOT and parenthesis.	

	b. Schedule reports and deliver results via email	
	i. Ability to export reports in CSV and PDF	
	c. Search events across the entire organization, or down to a physical or logical reporting domain	
	d. Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any report or rule	
	e. Correlation Rules should be mapped to MITTRE (https://attack.mitre.org/matrices/enterprise/) categories and the Incidents view must include a dashboard mapping devices, incidents and their MITTRE category.	
	f. Able to automatically correlate user to location and IP address:	
	i. Provide ability to report and search on user to IP address to location. Location may be physical switch port, Mac address or VPN.	
	ii. Enrich events where no user context is provided based on IP address.	
26	The SIEM solution should be able to integrate with Generative AI such as OpenAI/ChatGPT 4.0 platforms should support to responds to the Securiy Operations Center queries with include the product specific health, latest known vulnerabilites, high severity incidents, most frequent incidents, top risky users and top risky devices based on the incidents.	
27	The SIEM solution should be able to integrate with Generative AI such as OpenAI/ChatGPT 4.0 platforms should create the reports using the aggregation queries and Raw messages query	
28	Solution shall have capability to perform an automated response should an incident occur	
29	Policy based archiving of data to another location such as an NFS mount. Data must be able to be restored via the GUI for analytics searches.	
30	Solution shall include File integrity monitoring capabilities as integrated or separate solution to be integrated with SIEM, wherein deletion or modification of any critical file needs to be monitored and alerted	
31	SIEM should have the capability to discover OT/IOT devices and provide a list of them	
32	The vendor shall provide Threat Intel along with the SIEM as integrated.	
33	**Parser and Connector support for Device/Endpoint/Application**	
	Ability to monitor the status and responsiveness of services including DNS, FTP/SCP, Generic TCP/UDP, ICMP, JDBC, LDAP, SMTP, IMAP4, POP3, POP3S, SMTP, SSH and Web — HTTP, HTTPS (Single and Multi-Step).	
	i) Configuration management Database must store	
	ii) Version/Firmware/OS installed on the device	
	iii) Device serial number	
	iv) Interfaces configured on the device along with	
	1. Interface name	
	2. IP and subnet	
	3. Interface status (enabled, disabled)	
	4. Any security levels configured on the device	
	5. The interface speed	
	6. The interface speed and name should be editable	
	v) Processes running on the device or operating system	
	SIEM Should provide 300+ devices/Endpoints/Applications support and provide the option to add customized devices	
	Devices should automatically be populated within Groups in the Configuration Management DataBase, for example Windows Server Group, Firewall Group as a result of the discover process	
	Once active discovery of the devices is complete the SIEM should have a built-in template that will automatically define what metrics will be collected for devices and the collection intervals.	

	Performance metrics collected via polling and not relying on device generated logs, should include: i. Interface utilisation, errors, sent and received bytes ii. CPU iii. Memory iv. Disk v. Process utilisation	
34	The vendor shall propose User and Entity Behavior Analytics (UEBA) capability as integrated or standalone solution	
35	**The UEBA solution shall be able to:**	
	i. Monitor User, Process & File activity on user machines	
	ii. Collect information from Network Devices, Active Directory & log sources for user activity	
	iii. Record User account activity	
	iv. Monitor and alert USB device activity in user's machine	
	v. Provide visibility on remote worker or traveling user machines	
	vi. Log data ex filtration activity like file upload and file transfer to USB devices	
	vii. Alert General anomalous user behavior based on base lining of historical user activity	
	viii. Solution shall be able to detect and alert on browser upload and downloads	
	ix. Capability to detect and alert cloud upload of data	
	x. Detect applications like TOR, Gaming Applications etc.	
	xi. Detect uncommon VPN Clients installed in the system	
	xii. UEBA shall be able to gather logs when an user system is off the corporate network (off-net)	
36	Solution shall have Threat Hunting Capability based on Machine Learning	
37	The solution shall have AI based capabilities to predict Risk based on data collected from network, user systems, vulnerability scanners etc.	
38	**License, Warranty/RMA and TAC support**	
	a. The proposed hardware based solution should be size for 3000 EPS or 100 GB/Day at all layers from day one.	
	b. The SIEM platform of the offered solution should be supplied for supporting minimum one threat intelligence (TI) license from day one and support external threat intelligence sources	
	c. The solution must have 50 agent based FIM and 50 agent based UEBA license from Day 1.	
	d. Bidder must offer necessary software, hardware, licenses & subscriptions for three years without any additional costs.	
	f. Bidder must have minimum 3 (Three) SIEM deployment experience of the proposed solution in Bangladesh.	
	g. The OEM must have local employee & office in Bankgladesh to get the prompt response	
	h. Bidder must submit BOQ of proposed solution including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 3 years with support, patch, software update & upgrade.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer

6.2.2.97 GTP of Macbook

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Tender Technical Specification for Macbook			
Sl.No.	**Item**	**Required Specifications**	**Bidder's Response**
1	Brand	Any internationally reputed brand operating in recognized continental markets for decades.	
2	Model	To be mentioned by tenderer.	
3	Country of Origin	To be mentioned by the bidder	
4	Country of Manufacture	To be mentioned by tenderer.	
5	Processor	M4 chip with 10-core CPU, 10-core GPU, 16-core Neural Engine / Intel Core Ultra 9 / AMD Ryzen 9 AI or equivalent with equal or superior benchmarks.	
6	Memory (RAM)	Minimum 16GB Unified Memory / 16GB LPDDR5x RAM ,configurable up to 32GB.	
7	Storage	Minimum 512GB SSD	
8	Display	Minimum 15 inch Liquid Retina / IPS/OLED , Brightness: Minimum 500 nits	
9	Graphics	Integrated 10-core GPU or GPU with superior benchmarks.	
10	Audio	Speaker system with force-cancelling woofers & Spatial Audio /Dolby Atmos and subwoofers.	
11	Camera	Minimum HD Camera	
12	Microphones	Three-mic array with directional beamforming / Studio-quality AI noise-suppressed microphone array.	
13	Keyboard	Standard Keyboard	
14	Pointing Device	Standard Touchpad	
15	Wireless	Minimum Wi-Fi 6, Bluetooth 5 or higher.	
16	Wired Networking	Dedicated Ethernet port or included USB4/Thunderbolt docking station with Ethernet.	
17	Ports	USB-A, Thunderbolt 4 (USB-C), 3.5mm jack, USB 4 with PD & DP,	
18	Battery	Minimum 12 hours real-world usage	
19	Operating System	Latest stable OS installed with official license	
21	Software	Essential built-in apps	
22	Warranty	3 years international warranty	
23	Support	3 years technical support	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer