MEGHNA BANK

together we sail

**Tender Schedule**

**Of**

**Supplying, Installing, and Commissioning of a Security Information and Event Management (SIEM) solution For Meghna Bank PLC.**

**Date: 11-05-2026**

Tender Ref: MGBPLC/PROC/RFQ/Y26/6820

Version: 1.0

Meghna Bank PLC. IT Division, Head Office, Dhaka

## Table of Contents

## 1.0 Introduction & Overview

This Request for Proposal (RFP) is issued by Meghna Bank PLC (MGBPLC) to invite proposals from qualified and experienced bidders for the design, deployment, integration, and ongoing technical support of a Security Information and Event Management (SIEM) software solution. In response to the evolving cyber threat landscape, the Bank seeks to enhance its cybersecurity posture through a centralized and scalable SIEM platform. The proposed solution is expected to provide comprehensive visibility across the Bank's IT environment, enabling real-time log correlation, proactive threat detection, and structured incident response support.

1.1 Strategic Alignment:

The SIEM platform shall serve as the core technological engine for the Bank's security monitoring framework, facilitating advanced forensic analysis and ensuring strict alignment with regulatory requirements, including Bangladesh Bank ICT Security Guidelines, ISO/IEC 27001, SWIFT CSP, and PCI DSS v4.0. To maintain architectural consistency, the solution will be deployed on the Bank's internal virtualization infrastructure. While the Bank provides the underlying hardware environment and the personnel for daily operations, the selected bidder will be responsible for the complete software delivery, technical integration, and specialized knowledge transfer.

1.2 Legal Disclaimer:

This RFP is issued solely for the purpose of vendor evaluation and does not constitute a binding commitment. Any engagement resulting from this process will be subject to a formal contractual agreement and final approvals by the management of Meghna Bank PLC.

## 2.0 Important BID Details

| | |
|---|---|
| RFP Reference No. | Tender Ref: MGBPLC/PROC/RFQ/Y26/6820 |
| RFP Issue Date | May 11, 2026 |
| Last date for submitting Queries by the vendor | May 20, 2026 |
| Proposal Submission Deadline | May 24, 2026, 2.00 PM |

* Any bid received by the Bank after the deadline for submission of bids will be rejected and/or returned unopened to the Vendor, if so desired.

**RFP and Inquiry Response to:** For any clarifications, please communicate with the following Bank's Official:
Name: Mr. Nazir Ahammed,
Contact: +8801719406118

Email: ahammed.nazir@meghnabank.com.bd.

Meghna Bank PLC. will attempt to respond to all reasonable queries received in the specified manner but will not answer queries received after the specified date. Meghna Bank PLC. may, at its discretion, seek additional information from any respondent after the RFP closes, and such information will form part of the respondent's response.

**Tender Preparation:** Tenders must be submitted in two-envelope system i.e., one Technical Proposal & one Financial Proposal mentioning Technical/Financial Proposal on the top of each envelope. These two proposals will be submitted together in a third envelope. All the envelopes should be sealed & signed.

**Submitted to:**

The Chairman, Procurement committee, Meghan Bank PLC.,
Address: Suvastu Imam Square (Level-7), 65 Gulshan Avenue,
Gulshan-1, Dhaka 1212, Bangladesh.

## 3.0 Organizational Background

Meghna Bank PLC (MGBPLC) is a fourth-generation scheduled commercial bank in Bangladesh, providing a comprehensive suite of financial products and services through its extensive branch network, digital platforms, and technology-driven delivery channels.

The Bank operates a sophisticated and evolving IT landscape anchored by its Core Banking Systems (CBS), Internet Banking, Mobile Financial Services (MFS), and SWIFT infrastructure. This ecosystem extends across a diverse range of critical enterprise applications, peripheral banking systems, and digital touchpoints, all supported by a modern infrastructure foundation featuring Software-Defined Networking (SDN) across Primary Data Center (DC) and Disaster Recovery (DR) sites, built upon a Hyperconverged Infrastructure (HCI) architecture.

In line with its commitment to digitalization and interconnectivity, the Bank prioritizes the security, availability, and integrity of its enterprise-wide assets. As part of an ongoing initiative to strengthen cybersecurity resilience, Meghna Bank PLC continues to adopt advanced security technologies and frameworks that strictly align with national regulatory requirements and international security standards.

## 4.0 Objective of the RFP

The primary objective of this RFP is to identify and engage a technically proficient partner for the end-to-end implementation of a comprehensive Security Information and Event Management (SIEM) software solution at Meghna Bank PLC (MGBPLC).

**The proposed engagement is designed to achieve the following strategic outcomes:**

- Enterprise-Wide Visibility: Consolidate security telemetry from the Bank's diverse IT ecosystem into a single, high-fidelity monitoring plane.

- Advanced Threat Detection: Deploy intelligent correlation and analytics capabilities to identify complex security events in real-time.
- Operational Efficiency: Empower the Bank's internal security team with structured automation and response workflows to reduce the Mean Time to Detect (MTTD) and Respond (MTTR).
- Regulatory Excellence: Automate audit-ready logging and reporting frameworks to satisfy the requirements of Bangladesh Bank, SWIFT CSP, and other international standards.
- Technical Self-Sufficiency: Ensure a successful knowledge transfer that allows the Bank to maintain and evolve the platform independently of external operational support.

## 5.0 Purpose

The purpose of this initiative is to deploy a robust technology stack that enables the Bank's internal security team to maintain a 24x7 proactive defense posture.

**The project focuses on achieving the following functional milestones:**

- Unified Monitoring: Deployment of a centralized platform for automated log collection and high-speed correlation across all critical IT layers.
- Incident Lifecycle Management: Establishment of automated workflows for detection, integrated ticketing, and rapid response orchestration.
- Audit & Compliance Readiness: Provision of customized dashboards and reporting templates aligned with Bangladesh Bank, SWIFT CSP, and PCI DSS v4.0 requirements.
- Advanced Security Intelligence: Integration of User & Entity Behavior Analytics (UEBA), File Integrity Monitoring (FIM), and Threat Intelligence to identify sophisticated threats, while leveraging SOAR-based automation to streamline remediation.

## 6.0 Scope of Project Delivery

The scope of this engagement includes the design, supply, implementation, integration, and technical support of an enterprise-grade SIEM platform. The solution shall be deployed on the Bank's internal virtualization infrastructure to provide centralized monitoring and incident response capabilities across Primary (DC) and Disaster Recovery (DR) sites.

6.1 SIEM Platform Implementation & Integration:

The selected bidder is responsible for the technical operationalization of the platform and the delivery of all required software components:

a) **Software Supply & Deployment:** Supply of all necessary software licenses, subscriptions, followed by end-to-end installation within the Bank's virtual environment.
b) **High Availability:** Configuration across DC and DR sites with automated synchronization and seamless failover mechanisms.
c) **Source Integration:** The bidder shall perform the end-to-end integration of all critical log sources across the Bank's infrastructure, including Core Banking

Systems (CBS), IB, MFS, SWIFT, SDN, servers, network devices, security layers, and endpoints. (A detailed list of specific assets and log sources is provided in Section 9.2 of this RFP).

**d) Data Normalization:** Configuration of real-time ingestion, parsing, and normalization for all integrated data streams.

**e) Use Case Development:** Design and tuning of detection rules and executive dashboards aligned with the Bank's specific risk profile.

6.2 Advanced Technical Modules:

The implementation shall include the supply and configuration of the following native capabilities:

a) SOAR: Provisioning of automated playbooks for incident enrichment and response orchestration.
b) UEBA: Deployment of behavioral analytics to identify anomalous patterns and insider threats.
c) FIM: Configuration of integrity monitoring for critical system files and sensitive configurations.
d) Threat Intelligence: Integration of automated feeds to provide real-time context for all security alerts.

6.3 Technical Training & Empowerment:
The bidder shall conduct a structured Knowledge Transfer (KT) program to enable the Bank's internal team to manage the platform independently:

a) Comprehensive Sessions: OEM-authorized, hands-on training for eight (8) designated personnel.
b) Operational Depth: Coverage of rule tuning, advanced query techniques, and SOAR playbook management.
c) Deliverables: Provision of training manuals, Standard Operating Procedures (SOPs), and OEM-recognized certification vouchers.

6.4 Software Maintenance & Technical Support:
To ensure the long-term health of the platform, the bidder shall provide:

a) Warranty & Maintenance: Three (3) years of full warranty & support, but not limited to all updates, patches, and version upgrades.
b) Service Level Agreement (SLA): The bidder shall adhere to defined SLAs for system availability and technical support response times. (Detailed SLA requirements are provided in Section 12 of this RFP).
c) Technical Assistance: 24x7 access to the bidder's and OEM's Technical Assistance Center (TAC) for system-level troubleshooting.
d) Health Reviews: Conduct formal system health checks on a quarterly basis to optimize platform performance and ingestion efficiency.



Meghna Bank PLC. IT Division Head Office, Dhaka

## 7.0 Project Implementation Approach

The implementation shall follow a structured, phased approach to ensure controlled deployment, seamless integration, operational readiness, and effective knowledge transfer of the SIEM platform with integrated SOAR capabilities.

### 7.1 Phase 1: Project Initiation & Planning

The vendor shall:
a) Conduct a project kick-off meeting with Meghna Bank PLC. stakeholders to define objectives, scope, governance structure, communication protocols, and escalation procedures.
b) Finalize system inventory, log sources, integration points, and access requirements.
c) Develop a detailed project plan outlining timeline, milestones, resource allocation, dependencies, and risk management strategy.

### 7.2 Phase 2: Solution Design & Architecture

The vendor shall:
a) Assess DC and DR environments, including infrastructure, network topology, and existing security architecture.
b) Design the SIEM architecture with integrated SOAR capabilities, including data flow, integration framework, and high availability mechanisms.
c) Document the High-Level Design (HLD) and Low-Level Design (LLD), including use cases, playbooks, and correlation logic.

### 7.3 Phase 3: Delivery & Setup

The vendor shall:
a) Delivery of required software, licenses, and integrated modules (including SIEM, SOAR, UEBA, FIM, and Threat Intelligence)
b) Install and configure SIEM components, collectors, agents, and management consoles.
c) Execute base integration for log ingestion, ensuring data normalization and parsing accuracy.

### 7.4 Phase 4: Development & Tuning

The vendor shall:
a) Configure correlation rules, UEBA models, FIM policies, threat intelligence feeds, and SOAR playbooks.
b) Design and implement automated and semi-automated response workflows using SOAR capabilities for common security use cases
c) Perform tuning and optimization to improve detection accuracy and reduce false positives.
d) Configure dashboards, reports, and alerting mechanisms for different user roles
e) Conduct end-to-end testing, including log ingestion, correlation, alerting, SOAR automation workflows, failover, and access control validation.



Meghna Bank PLC. IT Division, Head Office, Dhaka

7.5 Phase 5: Training & Operational Handover

The vendor shall:
a) Deliver structured, role-based training programs for Bank personnel covering SIEM operations, alert management, and reporting.
b) Provide training on SOC workflows, including incident triage, escalation procedures, and response processes.
c) Provide specialized training on SOAR playbook configuration, customization, and automation workflows.
d) Perform formal handover, ensuring the Bank's team is fully capable of independently operating and managing the SIEM and SOAR platform.

7.6 Phase 6: Go-Live & Stabilization

The vendor shall:
a) Initiate live operations of the SIEM platform with integrated SOAR capabilities for real-time monitoring and response.
b) Provide on-site/remote support during the "Hyper-care" period to resolve immediate post-launch issues.
c) Verify system stability and ingestion performance against the technical requirements.

7.7 Phase 7: Optimization & Handover

The vendor shall:
a) Perform final fine-tuning of detection rules and SOAR playbooks based on live traffic data.
b) Conduct a final project review and submit the formal Project Closure Report.
c) Ensure a clean handover to the Bank's internal team for independent operations.

7.8 Acceptance Criteria & Project Closure

The project shall be considered successfully completed only after the proposed SIEM solution, integrated modules, and associated components are fully implemented, tested, validated, and formally accepted by Meghna Bank PLC.
The following acceptance criteria shall be fulfilled prior to project closure and final sign-off:
a) Successful User Acceptance Testing (UAT): The bidder shall conduct UAT to demonstrate that all functional requirements—including log ingestion, correlation accuracy, alert generation, and SOAR playbooks—operate as per the agreed technical design.
b) Resilience & Failover Validation: A successful demonstration of high availability and data synchronization between the Primary DC and DR environments.
c) Documentation & SOP Submission: Delivery of all finalized technical documentation, including architecture designs, integration maps, administrative guides, and Standard Operating Procedures (SOPs).
d) Knowledge Transfer Completion: Verification that all designated Bank personnel have completed the required training sessions and received OEM-authorized materials.

Meghna Bank PLC. IT Division Head Office, Dhaka

e) Issue Resolution: All critical and high-severity technical observations identified during the testing phase must be fully remediated.
f) Formal Project Sign-Off: Submission of a concise Project Closure Report followed by formal acceptance from the authorized representatives of Meghna Bank PLC.

7.9 Implementation Schedule & Timeline

The bidder shall submit a comprehensive project schedule as part of the technical proposal, adhering to the following requirements:

Visual Roadmap: Provision of a detailed Gantt Chart (or equivalent project management tool) that clearly maps all activities against the seven phases defined in this RFP.

Inter-phase Activities: The bidder is encouraged to identify and document any parallel workstreams or activities conducted between phases (e.g., performing base configuration while finalized designs are being reviewed) to demonstrate a streamlined delivery approach.

Critical Path & Milestones: The schedule must highlight the critical path, including major milestones, task dependencies, and the expected duration for each stage from initiation to final acceptance.

Resource Dependencies: A clear indication of the timelines required for the Bank's internal team to provide technical access, infrastructure readiness, or UAT feedback.

## 8.0 Functional Requirement

The proposed solution must be an enterprise-grade SIEM platform with natively integrated modules for SOAR, UEBA, and FIM. All components must be accessible via a unified management console.

| Requirement | Description |
|---|---|
| **Log Collection** | The solution shall support real-time log collection using both agent-based and agentless methods from network devices, servers, endpoints, applications, databases, and cloud environments. |
| **Log Ingestion & Processing** | The solution shall ingest, index, and process structured and unstructured log data without data loss. It shall support schema-less ingestion and ensure that changes in log formats do not result in dropped events. Unparsed logs shall remain searchable and usable for correlation and analytics |
| **Log Normalization** | The solution shall automatically normalize logs from heterogeneous sources into a unified and searchable format. |
| **Event Correlation** | The solution shall provide rule-based, behavior-based, and context-aware correlation to detect complex attack patterns, anomalies, and multi-stage attacks. |
| **Machine Learning & Advanced Analytics** | The solution shall include natively embedded machine learning capabilities for anomaly detection, behavioral analytics, and threat prediction. It shall support both pre- |



Meghna Bank PLC. IT Division Head Office, Dhaka

| | |
|---|---|
| | built models and the ability to create, train, and deploy custom models without requiring separate infrastructure. |
| **Generative AI & Intelligent Assistance** | The solution shall feature an integrated Generative AI assistant to provide natural language querying, automated incident summarization, and guided investigation. It shall be capable of translating complex queries into plain language, explaining the logic behind specific alerts, and suggesting remediation steps based on internal playbooks and global threat intelligence. |
| **MITRE ATT&CK & Kill Chain Mapping** | The solution shall provide out-of-the-box mapping to the MITRE ATT&CK framework and or Cyber Kill Chain, including identification of detection coverage gaps and guidance on required data sources. |
| **Alerting & Notification** | The solution shall support configurable alerts with severity levels, thresholds, and multi-channel notifications (e.g., email, SMS, dashboards, APIs). |
| **Dashboards & Visualization** | The solution shall provide real-time, customizable dashboards for SOC analysts, management, and auditors, with drill-down, filtering, and role-based views. |
| **Search, Investigation & Forensics** | The solution shall provide advanced search, query, and investigation capabilities to support threat hunting, incident analysis, and forensic investigations across real-time and historical data. |
| **Log Retention & Archiving** | The solution shall support configurable log retention and archival policies in compliance with regulatory requirements (minimum 3 months online and 1 year archived) |
| **Data Integrity & Log Protection** | The solution shall ensure integrity and protection of logs and audit trails through encryption, hashing, and tamper detection mechanisms to prevent unauthorized modification or deletion. |
| **Time Synchronization & Localization** | The solution shall support accurate time synchronization and time zone alignment across all log sources to ensure consistency in event correlation, forensic analysis, and regulatory reporting. |
| **Access Control (RBAC)** | The solution shall support granular role-based access control (RBAC), including segregation of duties and full audit logging of user activities. |
| **Case Management or Ticketing** | The solution shall include an integrated case management system to create, assign, track, and manage security incidents throughout their lifecycle, ensuring traceability, accountability, and audit readiness. |
| **SOAR (Integrated Automation & Response)** | The solution shall include natively integrated or tightly coupled SOAR capabilities within the SIEM platform. It shall support automated and semi-automated response using playbooks and workflows. All response actions shall be executed through SIEM-integrated connectors and APIs, ensuring centralized control. |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | |
|---|---|
| **Threat Intelligence Integration** | The solution shall support integration with internal and external threat intelligence feeds (e.g., STIX/TAXII), enabling enrichment, prioritization, and improved detection accuracy. |
| **UEBA (User & Entity Behavior Analytics)** | The solution shall provide behavioral analytics capabilities to detect insider threats, account compromise, privilege misuse, and anomalous user or entity behavior |
| **FIM (File Integrity Monitoring)** | The solution shall include File Integrity Monitoring capabilities to detect, alert, and report unauthorized or suspicious changes to critical files, configurations, registries, and sensitive data. It shall support real-time monitoring, baseline comparison, and compliance reporting. |
| **Asset & Identity Contextualization** | The solution shall support enrichment of events with asset and identity context, enabling correlation of activities across users, systems, and network entities for improved visibility and investigation. |
| **System Health & Performance Monitoring** | The solution shall provide monitoring of platform health, including log ingestion rates, agent status, log source availability, and overall system performance. |
| **Compliance Reporting** | The solution shall provide pre-built and customizable compliance reports aligned with regulatory and industry standards such as Bangladesh Bank guidelines, PCI DSS, and ISO/IEC 27001. |
| **High Availability** | The solution shall support a highly available architecture with redundancy across components to ensure uninterrupted log collection, processing, and analysis. |
| **RTO/RPO** | The solution shall support near-zero Recovery Time Objective (RTO) and Recovery Point Objective (RPO) through native clustering and data replication across nodes and sites, without reliance on third-party technologies. |
| **Disaster Recovery Support** | The solution shall support synchronization between DC and DR sites with automated or manual failover capabilities to ensure continuity of operations. |
| **Platform Maintainability** | The solution shall support regular updates, patches, and version upgrades with minimal disruption to operations. |

The bidder must provide a Compliance Matrix as part of the technical proposal. For every requirement listed above, the bidder shall specify whether the feature is 'Standard/Out-of-the-Box,' 'Requires Customization,' or 'Third-Party.' The Bank reserves the right to request a Proof of Concept or a live technical demonstration to verify the operationally of any stated functional capability before final selection.

## 9.0 Log Source Coverage & Sizing Requirements

To ensure appropriate sizing, performance, and scalability of the proposed SIEM solution, Meghna Bank PLC. provides indicative estimates of log sources, system coverage, and expected event volume.

Bidders are required to propose a solution architecture that can efficiently handle the specified workload with adequate headroom for future growth.

9.1 Solution Expectations

The proposed solution shall:
a) Support the estimated workload based on either **Events Per Second (EPS) or daily log volume (GB/day) or equivalent any other licensing criteria**, depending on the vendor's licensing and architectural model, without performance degradation.
b) Provide scalability to accommodate future growth in log sources, EPS, and/or data volume.
c) Ensure no data loss during peak ingestion periods and burst traffic conditions.
d) Support burst handling capability beyond average EPS or log ingestion rates.
e) Maintain consistent performance for correlation, search, alerting, and reporting under peak load conditions.
f) Support integration with all identified systems without architectural limitations or restrictive licensing constraints.

9.2 Indicative Log Source Coverage (Not Limited)

| System Type | Examples of Integrations |
|---|---|
| Network Devices | Firewalls, core routers, core switches, Load Balancer, WAF |
| Operating Systems | Windows Server, Linux (RHEL, Ubuntu, CentOS, Oracle Linux or any other Custom OS) |
| Applications | Banking Application or any other custom Application |
| Databases | Oracle, Microsoft SQL Server, MySQL, MS SQL |
| Security Tools | XDR, Web Proxy, Microsoft Exchange, EOP |
| Cloud Platforms | Private Cloud(VMware-VCF), Public Cloud |
| Directory Services | Microsoft Active Directory |

9.3 Estimated Infrastructure & Log Sources

| SL. | Item Description | Quantity |
|---|---|---|
| 1 | Windows Severs | 100 |
| 2 | Linux Severs | 50 |
| 3 | Next Generation Firewall | 26 |
| 4 | SDN Devices | 25 |
| 5 | SDWAN Devices | 15 |
| 6 | Web Application Server | 50 |
| 7 | Database Server | 10 |
| 8 | Application | 50 |
| 9 | Endpoint Protection(XDR) | 02 |
| 10 | Email security(EOP) | 01 |
| 11 | Other IP enables Device | 05 |



Meghna Bank PLC. IT Division, Head Office, Dhaka

9.4 Sizing & Licensing Baseline

| Parameter | Baseline Estimate |
|---|---|
| Licensing for SIEM | 3000 EPS or 100 GB Data per day Volume or Equivalent. There should not be limitations on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. |
| Log Retention (Online) | Minimum 3 months (hot storage) |
| Log Archiving (Offline) | 1 year (Worm/archive storage) |
| SOAR User License | Min 2 |
| UEBA | 100 |
| FIM | 100 |
| Threat Intel Service | 1 |

9.5 Vendor Responsibilities for Sizing, Architecture & Pricing

The selected vendor shall:
a) Conduct an initial **discovery and sizing workshop** with Meghna Bank PLC. to validate log sources, estimated workload, and integration requirements.
b) Size the proposed solution based on either **Events Per Second (EPS) or daily log volume (GB/day)**, depending on the vendor's licensing model, and clearly state the adopted methodology.
c) Ensure the solution is designed to handle the estimated workload with a **minimum 30% headroom** to accommodate future growth in EPS, log volume, and system onboarding.
d) Propose a **scalable and modular architecture** (e.g., distributed or cluster-based) that supports seamless expansion of compute, storage, and processing capacity without major redesign.
e) Design and implement efficient **data management mechanisms**, including compression, indexing, and retention optimization, while ensuring compliance with regulatory requirements.
f) Recommend and implement appropriate **High Availability (HA) and Disaster Recovery (DR)** strategies, ensuring data integrity, synchronization between DC and DR, and continuous availability of logs and analytics.
g) Clearly document the **sizing methodology and assumptions**, including EPS calculation (if applicable), log volume estimation, storage sizing, retention calculation, and growth projections.

## 10.0 Technical Requirement .

The proposed solution shall meet the technical specifications required for secure, scalable, and high-performance deployment within Meghna Bank PLC.'s IT environment, covering both Data Center (DC) and Disaster Recovery (DR) sites.



Meghna Bank PLC. IT Division, Head Office, Dhaka

Detailed technical requirements, including architecture, performance parameters, integration capabilities, and infrastructure specifications, are provided in **Annexure–A (Technical Compliance Sheet)**.

Bidders are required to review all technical requirements outlined in the Annexure and submit a **completed Technical Compliance Sheet**, clearly indicating compliance against each requirement. Any deviations, exceptions, or additional remarks must be explicitly stated.

Non-submission or incomplete submission of the Technical Compliance Sheet may result in disqualification from the evaluation process.

## 11.0 Technical Enablement

The bidder shall provide a comprehensive training program to ensure the Bank's internal team is equipped to independently operate and optimize the SIEM platform and its integrated modules.

### 11.1 Training Standards & Requirements

- **Target Audience:** The program shall be tailored for eight (8) designated personnel, covering both administration and security operations.
- **Certification & Materials:** The bidder shall provide **eight (8) OEM-authorized certification vouchers** and a complete set of **official OEM training manuals** (hard or soft copy) for all participants.
- **Instructor Qualification:** Training must be delivered by **OEM-certified trainers** or authorized partners to ensure technical accuracy.
- **Hands-on Methodology:** Sessions must be lab-based, allowing participants to perform real-world tasks of the proposed solution.
- **Location & Hosting:** To ensure effective knowledge transfer, the bidder shall arrange for training sessions and all associate facilities. This includes providing a fully equipped training facility and a dedicated hands-on lab environment where the Bank's team can engage with the solution's features in a practical, uninterrupted setting.

### 11.2 Specialized Training Tracks

The training program must cover the following core areas:

| Track | Coverage Area |
|---|---|
| Platform Administration | System architecture, user management (RBAC), health monitoring, backup/restore procedures, and software update/patch management. |
| Data Ingestion | Onboarding new log sources, configuring collectors/agents, troubleshooting parsing issues, and managing storage/retention policies. |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | |
|---|---|
| SOC Operations | Real-time monitoring, triage, incident lifecycle management, and advanced forensic query techniques. |
| Detection Engineering | Creating/tuning correlation rules and mapping detections to the MITRE ATT&CK framework. |
| Automation & SOAR | Configuring integrated SOAR playbooks and automated response workflows. |
| Advanced Analytics | UEBA behavioral models, ML-based anomaly detection, and identity context enrichment. |
| Compliance | Generating regulatory reports (Bangladesh Bank, PCI DSS, ISO 27001) and managing threat intelligence feeds. |

## 12.0 Service Level Agreement (SLA) & Support

The bidder shall provide a comprehensive support framework to ensure the 24/7 availability, stability, and continuous evolution of the SIEM platform and its integrated modules.

12.1 Service Availability & Performance

The solution must meet the following performance benchmarks during the contract tenure:

| Report Type | Frequency | Delivery Method |
|---|---|---|
| **System Availability** | **≥ 99.9% Uptime** (Excluding planned maintenance) | Monthly |
| **Log Ingestion Delay** | **< 3 Minutes** from source generation to SIEM visibility | Real-time |
| **UI/Search Response** | **95% of standard queries** must return results in < 30 seconds | Continuous |

12.2 Technical Support & Incident Response

The bidder shall provide a **24x7x365** technical support model. Response times are defined as the interval between the Bank reporting an issue and a qualified engineer commencing active troubleshooting.

| Severity Level | Definition | Response Time | Report Time |
|---|---|---|---|
| Critical (P1) | Complete system outage; Data ingestion halt; Console inaccessible, major system compromise | ≤30 Minutes | ≤ 4 Hours |



Meghna Bank PLC. ★ Division, Head Office, Dhaka

| | | | |
|---|---|---|---|
| High (P2) | Major module failure (e.g., SOAR down); HA failover issues., unauthorized access, service degradation | ≤ 1 Hour | ≤ 8 Hours |
| Medium (P3) | Partial impact; Single log source error; Reporting failure., policy violation, abnormal behavior | ≤ 4 Hours | ≤ 24 Hours |
| Low (P4) | Informational alerts, false positives, audit support, General inquiries; Minor UI glitches; Feature requests. | ≤ 8 Hours | ≤3–5 Business Days |

- **On-Site Requirement:** For P1 and P2 incidents, the bidder must provide on-site technical assistance within **2 hours** if remote troubleshooting does not provide a verified workaround.

12.3 Lifecycle Management: Updates, Changes, & Modifications

The bidder is responsible for the platform's technical integrity through proactive Lifecycle management at no additional cost to the Bank:

- **Updates & Patches:** Provision and implementation of all updates, hotfixes, and security patches within **72 hours** of release.
- **Version Changes (Upgrades):** Execution of at least one major version upgrade per year (if released by OEM), including pre-upgrade compatibility testing and post-upgrade validation.
- **Modifications:** Technical assistance for configuration modifications, including adjusting correlation logic, modifying RBAC user levels, or updating storage retention policies to meet evolving needs.

12.4 Platform Migration Support

The bidder shall provide end-to-end technical support for platform-related migrations:

- **Internal Migration:** Support for the migration of SIEM components between different infrastructure segments (e.g., between Data Centers or transition to Hybrid/Public Cloud environments).
- **Data Integrity:** Ensuring full data continuity and integrity during backend database migrations or hardware refreshes.
- **Exit Transition:** Upon contract termination, the bidder shall facilitate the migration of configurations and logs to a format accessible by the Bank to ensure zero data loss.

12.5 Operational Assistance & Continuous Growth

The vendor shall act as a technical partner for the SOC's maturity:



Meghna Bank PLC. Division, Head Office Dhaka

- **Log Source Integration:** Support for the integration of additional log sources and security tools as requested by the Bank to enhance visibility (subject to feasibility and mutually agreed scope).
- **Content Engineering:** Assistance in fine-tuning correlation rules, developing new SOC dashboards, and optimizing SOAR playbooks to reduce false positives.
- **Audit & Compliance Support:** Technical walkthroughs and evidence gathering during regulatory reviews (e.g., Bangladesh Bank ICT Guidelines, PCI DSS).

12.6 Escalation Matrix

The bidder must provide a clear escalation path for unresolved issues:

- **Level 1:** Support Engineer (Immediate)
- **Level 2:** Technical Lead / Project Manager (After 2 Hours for P1/P2)
- **Level 3:** Support Engineer from OEM (After 4 Hours for P1/P2)

## 13.0 Bidder Eligibility & Tender Preparation

This section outlines the mandatory qualifications and the specific structure required for a valid proposal submission. Bidders must follow these instructions strictly.

13.1 Minimum Eligibility Criteria

Bidders should have meet the following mandatory requirement. If bidder has deviated in any of the terms, then it should be explicitly mentioned in the response of bidder.

| Category | Minimum Eligibility Requirement |
|---|---|
| **Legal Registration** | The bidder must be a legally registered entity in Bangladesh(RJSC) with a valid Trade License, TIN, and VAT/BIN registration. |
| **No Blacklisting** | The bidder must not be blacklisted or debarred by any government authority, regulatory body, financial institution, or international organization. A signed **Self-Declaration** must be provided. |
| **Contractual Capacity** | The bidder shall confirm that it has the full legal capacity to enter into a binding contract under the laws of Bangladesh. |
| **OEM Authorization** | For foreign OEM products, the bidder must submit a valid **Manufacturer Authorization Form (MAF)** specifically for this tender to ensure legitimate support and licensing. |
| **Experience** | Minimum of **two (2) years** of proven experience in cybersecurity projects, preferably having **one (1) successful implementation** of a SIEM/SOC project in the Banking/FSI sector. |
| **Product Maturity** | The proposed SIEM solution should preferably be listed in the **Gartner Magic Quadrant** for SIEM for at least one of the last two (2) consecutive years. |

| | |
|---|---|
| **Local Support** | The bidder must maintain a **registered local office** in Bangladesh with 24x7 support capability and OEM-certified engineers available for on-site assistance. |
| **Financial Soundness** | Submission of **Audited Financial Statements** for the last two (2) years demonstrating solvency and the operational capacity to manage the project. |

13.2 Bid Submission process

Proposals must be submitted using a two-envelope system. The 'Technical Proposal' and 'Financial Proposal' must be sealed in separate envelopes, both clearly marked with their respective contents. These two sealed envelopes must then be enclosed together within a single, larger outer envelope, which must also be sealed and clearly labeled with the tender reference and bidder's information.

- **Envelope 1: Technical Proposal** (Must NOT contain any pricing information).
- **Envelope 2: Financial Proposal** (Sealed separately).

13.3 Technical Proposal Requirements (Envelope 1)

The Technical Proposal shall be comprehensive and organized as follows:

➢ **Solution & Architecture**

- Detailed solution overview and architecture diagram (HLD/LLD).
- Deployment model (On-premises) including High Availability and Disaster Recovery design.
- Details of integrated modules: UEBA, FIM, Threat Intelligence, and SOAR.

➢ **Compliance & Functional Capability**

- **Section 8 Compliance:** A point-by-point compliance matrix against the Functional Requirements.
- **Section 10 Compliance:** A point-by-point compliance matrix against the Technical Specifications.
- **Technical Compliance Sheet:** Completed Annexure with status (Compliant / Partially Compliant / Non-Compliant) and remarks for any deviations.

➢ **Implementation & Project Plan**

- Detailed implementation methodology aligned with Section 7 (Deployment Phases).
- Project timeline (Gantt Chart) with milestones and resource deployment plan.
- Approach for log source onboarding and SOAR playbook design.

➢ **Vendor Profile & Experience**

- Company profile and organizational structure.
- At least 2–3 relevant project references with client details (BFSI sector preferred).
- Proposed project team structure
- CVs of key personnel with relevant OEM certifications.

➢ **Declarations & Administrative Documents**

- Valid Trade License, TIN, and VAT/BIN.
- Forwarding Letter (including Declaration of No Blacklisting and No Conflict of Interest).
- Confidentiality and Non-Disclosure Undertaking (NDA).
- Deviation statement (if any); if none, "No Deviation" must be stated.

13.4 Financial Proposal Requirements (Envelope 2)

The Financial Proposal must be submitted separately and shall include:

**A. Commercial Breakdown**

- Itemized cost for the SIEM platform and integrated modules (UEBA, FIM, Threat Intelligence, SOAR).
- Implementation, training, and support services costs.

**B. Licensing & Scalability**

- Clearly defined licensing model (EPS or GB/Day).
- Bidders must provide unit pricing for future expansion (EPS, log volume, or storage). Specifically, a fixed price for a 10 GB/Day (or equivalent EPS) increment must be provided in a separate sheet and remain valid for the contract duration.

**C. Commercial Declarations**

- Proposal validity (minimum 90 days).
- Currency in BDT; all prices must clearly mention applicable Tax and VAT.

13.5 General Submission Instructions

- All documents must be signed, stamped, and properly indexed.
- Proposals must be submitted in hard copy format.
- Incomplete or improperly submitted proposals may be rejected without further evaluation.



Meghna Bank PLC. IT Division, Head Office, Dhaka

## 14.0 Commercial Proposal & Pricing Structure

Bidders are required to submit a detailed and itemized commercial proposal. The proposal must be transparent, ensuring that no hidden costs exist for the core SIEM platform and other modules (SOAR, UEBA, FIM, and Threat Intelligence).

### 14.1 Commercial Pricing Table

To ensure a fair evaluation, the bidder must provide the cost breakdown in the following tabular format:

| Scope | Unit | Quantity | Unit Price | Total Price(BDT) |
|---|---|---|---|---|
| SIEM Platform License (**Sized for 3000 EPS / 100 GB Day**) | License | 1 | | |
| UEBA Subscription License | License | 100 | | |
| FIM user License | License | 100 | | |
| SOAR | License | 2 User | | |
| Threat Intel (IOC Service) | Service | 1 | | |
| Implementation, Integration & Configuration Services | Job | 1 | | |
| Training & Knowledge Transfer | Sessions | 1 | | |
| **Total Cost excluding Tax and VAT (BDT)** | | | | |
| **TAX** | | | | |
| **VAT** | | | | |
| **Total Cost including Tax and VAT(BDT)** | | | | |

- Expansion Price in a Separate Sheet.

| Component | Expansion Unit | Fixed Unit Price |
|---|---|---|
| **Incremental Log Volume** | **10Gb/Day** | |
| **Incremental Log EPS** | **500 EPS** | |



Meghna Bank PLC. IT Division, Head Office Dhaka

14.2 Licensing Model & Transparency

The bidder must clearly define the technical boundaries of the proposed license:

- **Licensing Metric:** Explicitly state if the license is based on **EPS** (Events Per Second) or **Log Volume** (GB/Day). Bidders are encouraged to offer licensing based on **Log Volume (GB/Day)** or a volume-based model to accommodate the Bank's diverse log ingestion requirements.
- **Limitations:** The bidder must confirm that there are **no limitations** on the number of log sources (Nodes/IPs) or SOC users.
- **Storage:** Clearly state if the license limits the database storage capacity or if it is unlimited based on hardware availability.

14.3 Future Scalability & On-Demand Expansion

To accommodate the Bank's growth, the bidder must provide a fixed unit price for future expansion:

- **Incremental Slab Pricing:** The bidder shall provide a fixed price for an additional **10 GB/Day** (or equivalent EPS) license increment.
- **Price Guarantee:** The unit price for this expansion shall remain valid for **three (3) years** from the date of contract signing.
- **Architectural Impact:** The solution must support this scalability seamlessly without requiring a replacement of the core architecture.

14.4 Proposal Validity & Currency

- **Validity:** The commercial proposal shall remain valid for a minimum of **90 days** from the submission deadline.
- **Currency:** All prices must be quoted in **Bangladeshi Taka (BDT)**.
- **Taxation:** Prices must be inclusive of all applicable Taxes and VAT as per prevailing law of land.

14.5 Payment Milestones

Payment shall be released based on the following project milestones:

1. **20% of Work Order Value:** After Acceptance of Work Order.
2. **40% of Work Order Value:** Upon Successful delivery, implementation, integration of agreed log sources, and UAT (User Acceptance Test) sign-off, Training and Knowledge Transfer.
3. **20% of Work Order Value:** Beginning of 2nd Year from the date of UAT Sign off.
4. **20% of Work Order Value:** Beginning of 3rd Year from the date of UAT Sign off.



Meghna Bank PLC. IT Division, Head Office Dhaka

## 15.0 Evaluation Criteria & Selection Process

The Bank will employ a Quality and Cost Based Selection (QCBS) methodology. Proposals will be evaluated based on their ability to meet the Bank's technical requirements and provide the best commercial and financial value over a three-year period.

- **Technical Evaluation Weightage:** 60%
- **Financial Evaluation Weightage:** 40%

15.1 Preliminary Screening

Before the scoring process, all bids will be screened against the **Minimum Eligibility Criteria (Section 13.1)**. Bidders who do not meet all mandatory legal, financial, and OEM authorization requirements will be disqualified and will not proceed to the Technical Evaluation.

15.2 Technical Evaluation Matrix (Total: 60 Marks)

Technically qualified bids will be scored out of 60 based on the following matrix.

| SL No. | Technical Evaluation | Actionable | Marks |
|---|---|---|---|
| 1 | Solution Architecture & Technical Soundness | Completeness of HLD/LLD, HA/DR design, scalability of the proposed architecture, and reporting efficiency. | 15 |
| 2 | Core Functional & Advanced Capabilities | Compliance with Section 8 (SIEM) and Section 10 (UEBA, FIM, SOAR). Native integration of the security | 15 |
| 3 | OEM Market Recognition | Leader or Challenger position in the Gartner Magic Quadrant for SIEM (last 2 years). | 5 |
| 4 | Local Implementation Experience | Proven track record with at least (2-3) successful SIEM/SOC deployments in Bangladesh (preferably BFSI/Government). | 10 |
| 5 | Resource Expertise & Certifications | Assigned team must hold OEM-specific certs plus professional certs (CISSP, CISM, CISA, or CEH). | 5 |
| 6 | Performance, Scalability & Sizing | Handling EPS/log volume, future scalability, and architecture efficiency | 5 |
| 10 | Project Methodology & Timeline | Clarity of the deployment phases (Section 7), risk mitigation plan, and realistic Go-Live schedule. | 5 |
| Total | | | 60 |



Meghna Bank PLC. Head Office, Dhaka

15.3 Financial Evaluation (Total: 40 Marks)

- The **Lowest Evaluated Financial Proposal (L1)** will be awarded the maximum score of **40 marks.**
- Other proposals will receive financial scores inversely proportional to their price using the formula:

15.4 Combined Evaluation & Final Selection

The final score for each bidder will be calculated by adding the Technical Score and the Financial Score:

**Final Score = Technical Marks (Out of 60) + Financial Marks (Out of 40)**

15.5 Rights of the Bank

- **Clarifications:** The Bank reserves the right to seek clarifications or request a Live Technical Demonstration (PoC) during the evaluation.
- **Rejection:** Submission of incomplete information is grounds for disqualification.
- **Selection:** The lowest financial bid shall not automatically receive preferential consideration. Meghna Bank PLC. reserves the right to accept or reject any proposal, in whole or in part, without assigning any reason.

## 16.0 Compliance & Regulatory Standards

The proposed SIEM solution and associated services must comply with all applicable regulatory, legal, and industry standards relevant to the banking sector in Bangladesh. The solution shall act as a primary technical control for the Bank to achieve and maintain compliance through tamper-proof logging, continuous monitoring, and automated reporting.

16.1 Regulatory & Standards Alignment

The solution must provide native support, specialized detection rules, and reporting templates to satisfy the requirements of the following frameworks:

- **Bangladesh Bank ICT Security Guideline:** Specifically regarding centralized log management, 24/7 security monitoring, and incident reporting.
- **SWIFT Customer Security Programme (CSP):** Specifically, for Control 6.4 (Logging and Monitoring) to detect unauthorized access or anomalous activity within the SWIFT environment (Alliance Access, Gateway, etc.).
- **PCI DSS (Latest Version):** Specifically, for File Integrity Monitoring (FIM) and tracking access to network resources and cardholder data.
- **ISO/IEC 27001:** Specifically, for operational logging, monitoring, and audit evidence collection.



Meghna Bank PLC. ★ IT Division, Head Office, Dhaka ★

16.2 Technical Audit & Integrity Requirements

To satisfy external audit requirements, the solution shall:

- **Tamper-Proof Logging:** Maintain comprehensive audit logs of all system and user activities that are protected against unauthorized modification or deletion.
- **Audit Trails:** Provide end-to-end audit trails (who, what, where, and when) for security events, incidents, and administrative actions.
- **Data Integrity:** Ensure the confidentiality and integrity of log data at rest and in transit using industry-standard encryption (e.g., AES-256, TLS 1.2+).
- **Time Synchronization:** Ensure all logs across integrated systems are time-stamped and synchronized via a central NTP source to maintain a chronological chain of events.

16.3 Automated Compliance Reporting

The solution must simplify the audit process by providing:

- **Compliance Dashboards:** Real-time visibility into the Bank's status against Bangladesh Bank, SWIFT CSP, and PCI DSS controls.
- **Pre-built Reports:** A library of out-of-the-box (OOTB) reports designed for regulatory submissions and audit evidence.
- **Automated Scheduling:** Capability to automatically generate and distribute compliance reports to designated personnel or auditors.
- **Granular Access Control:** Support for Role-Based Access Control (RBAC), allowing auditors to view reports without having administrative access to the platform.

16.4 Data Security & Access Control

The vendor shall ensure the platform implements:

- **Segregation of Duties (SoD):** Clear separation between system administrators, security analysts, and auditors.
- **Masking & Privacy:** Capability to mask or obfuscate sensitive data within logs (such as PII or card numbers) to prevent unauthorized exposure during the monitoring process.
- **Anomaly Detection:** Identify suspicious activities such as "out-of-hours" logins or unauthorized modifications to critical configuration files across all regulated environments.

## 17.0 General Terms & Conditions

The following conditions govern the legal and operational execution of this project. These clauses, along with the technical commitments made in the proposal, will form the basis of the final Master Service Agreement (MSA).



Meghna Bank PLC. IT Division, Head Office, Dhaka

17.1 Bid Validity & Formal Response

- **Validity:** Proposals shall remain valid for a minimum period of **90 days** from the submission deadline.
- **Annexure Completion:** Bidders must complete all technical and functional annexures (Section 8, 10, and Compliance Matrix) in the prescribed format. Failure to provide a line-by-line response will result in the proposal being marked as "non-responsive."
- **Binding Response:** All "Compliant" remarks in the annexures are considered formal commitments. Any feature claimed as compliant that is found missing during implementation must be provided at no additional cost to the Bank.

17.2 Tender Security

- Bidders must submit a Bid Bond equivalent to 5% of the total offered price in the form of a Bank Guarantee or Pay Order in favor of Meghna Bank PLC. Along with the Tender documents. Any discrimination of the Bid Bond with the offer price may results disqualification of the bidder. The Validity of Bid Bond will 6 month from the date of submission.
- Successful bidder must submit 10% of the work order value as performance security in the form of Bank Guarantee/Pay order in favor of Meghna Bank PLC. for a period of 3 years i.e. project duration.

17.3 Rights of the Bank

**Meghna Bank PLC. reserves the right to:**

- Accept or reject any proposal, in whole or in part, without assigning any reason.
- Request a Best and Final Offer (BAFO) or negotiate specific technical components, sizing adjustments, and final pricing with shortlisted bidders.
- Modify, refine, add, or remove components of the Scope of Work, technical requirements, or deliverables during the evaluation phase based on operational or budgetary considerations.
- Award the contract in full or in part, defer specific modules, or exclude services based on technical suitability and budget.
- Request revised, updated, or clarified commercial quotations from bidders at any stage of the evaluation or contract finalization process.
- Negotiate future scalability, licensing expansion, and additional integrations as part of evolving business requirements.
- Bidders are required to cooperate in good faith during negotiations, providing updated architecture and implementation approaches as requested by the Bank.

17.4 Confidentiality & Data Ownership

- **Non-Disclosure Agreement (NDA):** The successful bidder must sign a formal NDA prior to the commencement of work.
- **Sole Ownership:** All logs, dashboards, automated SOAR playbooks, use cases, and reports generated during this project remain the **sole property of Meghna Bank PLC**.



Meghna Bank PLC. IT Division, Head Office, Dhaka

- **Data Privacy:** The vendor shall not retain, reuse, or disclose any Bank data. All personnel must maintain strict confidentiality regarding the Bank's infrastructure.

17.5 Audit & Regulatory Access

- Meghna Bank PLC., its internal/external auditors, and **Bangladesh Bank** regulatory authorities shall have the right to audit the solution, configurations, and logs at any stage of the project lifecycle to ensure compliance with ICT guidelines.

17.6 Termination & Exit Support

- **Termination for Cause:** The Bank may terminate the contract for breach of confidentiality, repeated SLA failures, or unethical conduct.
- **Handover:** Upon termination or project completion, the vendor must provide full knowledge transfer and handover all project artifacts, SOPs, and configurations to the Bank.

17.7 Project Execution & Governance

- The successful bidder shall commence the project within 10 (ten) working days from the issuance of the Work Order unless otherwise agreed.
- A dedicated Project Manager shall be assigned by the vendor as the Single Point of Contact (SPOC) throughout the project lifecycle.
- The vendor shall complete implementation within the agreed timeline and milestones.
- The vendor shall provide a detailed project implementation plan, including timelines, dependencies, milestones, resource allocation, and escalation procedures.
- Meghna Bank PLC. reserves the right to monitor project progress, review implementation activities, and request status updates at any stage of the project.

17.8 Governing Law & Jurisdiction

- This RFP and any resulting contract shall be governed by the **Laws of Bangladesh**. Any disputes shall be subject to the exclusive jurisdiction of the competent courts of Bangladesh.



Meghna Bank PLC. IT Division, Head Office Dhaka

# ANNEXURE-A

## Technical Compliance Sheet

| Sl. | Description | Technical Specification |
|---|---|---|
| 1 | General Information: | a. **Brand:** To be mentioned by bidder |
| 2 | | b. **Model:** To be mentioned by bidder |
| 3 | | c. **Country of Origin**: USA/UK/EU/JAPAN |
| 4 | | d. Country of manufacture: To be mentioned by bidder |
| 5 | Solution Acceptance: | a. The solution must be an on-premises solution and should have the capability to deploy at Bank premise without any dependency. |
| 6 | | b. The solution must be listed on Gartner Magic Quadrant from 2022 to 2025 for Security Information and Event Management (SIEM). Necessary documents should be provided. |
| 7 | Solution Architecture | **The SIEM solution should provide a scale out distributed architecture with the following characteristics:** |
| 8 | | 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. |
| 9 | | b. 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. |
| 10 | | c. To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. |
| 11 | | d. Collectors / Forwarders compress the data before sending to the storage and correlation tier. |
| 12 | | f. SIEM solution Provide real-time, in memory distributed rule/behaviour correlation across all cluster components |
| 13 | Solution Capacity | **The SIEM storage and correlation tier now referred to as SIEM Cluster should:** |
| 14 | | a. The proposed solution must be either software solution. |
| 15 | | b.The SIEM solution should support the Active/Passive or DC/DRC deployment for the redundancy from day 1 (one). |
| 16 | | c. The SIEM Cluster should not limit how much devices are integrated. This limit should only be on how much storage is provided. |
| 17 | | d. The SIEM solution shall have the capability to compress logs for reducing disk space usage. |
| 18 | | e. The SIEM solution shall have the capability to compress logs and have a compression of minimum standards. Need to be mentioned |
| 19 | | f. Log Data Volume: 100 GB/Day or 3K EPS |
| 20 | | g. The solution must ensure that if data ingested is not parsed, then with the new parser, old data ingested should also be parsed without need to re-ingest data throughout the retention period of online 90 days and 365 days of archival |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | | |
|---|---|---|
| 21 | Solution Features | **The SIEM must be able to collect additional context beyond log data from devices and this should be achieved by:** |
| 22 | | a. Actively discovering the devices within the network without an agent and using standard protocols such as SNMP, WMI, SSH, Telnet, JDBC, OPSEC & JMX |
| 23 | | 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). |
| 24 | | 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. |
| 25 | | The SIEM should provide a unified analytics interface that allows the same query language to analyze both log data and performance data. |
| 26 | | Analytics must support nested queries where a user can use a query to filter the results of the previous query. |
| 27 | | The system should be able to drop events on the Collectors that are not relevant or not needed. This should not impact any licensing. |
| 28 | | 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. |
| 29 | | Processing of event data should be performed by parsers at receipt time of the event. |
| 30 | | All parsers should be able to be modified and customized. |
| 31 | | Custom parsers should be able to be created and defined in the GUI without CLI access. |
| 32 | | Devices shall be monitored without agents via SSH, telnet WMI, JMX and Power Shell. |
| 33 | | Ability to collect Windows events via WMI and agent |
| 34 | | The SIEM should provide role based access to restrict access to the data and also restrict access to the GUI. |
| 35 | | Ability to collect network device configuration, identify changes and provide side-by-side comparison. |
| 36 | | Proposed solution should offer separate dashboard for ISO,PCI/ DSS reporting or any other Standards or regulatory requrements. |
| 37 | | The SIEM solution integration with Generative AI platform 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 |
| 38 | | The SIEM solution integration with Generative AI platforms should create the reports using the aggregation queries and Raw messages query |
| 39 | | Solution shall have capability to perform an automated response should an incident occur |
| 40 | | 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 |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | | |
|---|---|---|
| 41 | | SIEM should have the capability to discover OT/IOT devices and provide a list of them |
| 42 | | The vendor shall provide Threat Intel along with the SIEM as integrated. |
| 43 | Threat Intel | **Ability to integrate Threat Intelligence (TI) feeds:** |
| 44 | | a. Integration via REST API with different supported data format (CSV, Custom, STIX) |
| 45 | | b. Support for STIX/TAXII |
| 46 | | c. Support for but not limited to IP Addresses, Domains, Hashes, URLs, Malware Process Names |
| 47 | | d. Ability to correlate TI data in real-time, in memory against event data. |
| 48 | | e. Ability to correlate TI data against historic event data. |
| 49 | Notification and Incident Management | a. Policy-based incident notification framework. |
| 50 | | b. API-based integration to external ticketing systems — Jira/ Service Now/ Sales force/ Zen desk/ The Hive/ Connect Wise/ Remedy. |
| 51 | | **Solution shall have Built-in ticketing/case management system or the vendor shall propose one that has the below minimum capabilities:** |
| 52 | | i. Ability to define an escalation policy that sends an email to management when thresholds reached. |
| 53 | | ii. Ability to add PDF and PNG to tickets. |
| 54 | | iii. Ability to assign tickets to other operators. |
| 55 | | iv. Timeline view to capture activities on a Case and on related incidents. |
| 56 | | v. Provides Mean Time To Resolution metric |
| 57 | Remediation | **The proposed solution shall have automated response and remediation capabilities as integrated or as a separate solution to be integrated with SIEM** |
| 58 | | a. The solution must have over built-in Response & Remediation actions for a number of different vendors such as but not limited to: Microsoft, Linux, Fortinet, Palo Alto, Infoblox, Cisco, Aruba |
| 59 | | b. The solution shall also provide for manual remediation capabilities wherever required |
| 60 | Analytics & reporting | 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. |
| 61 | | b. Schedule reports and deliver results via email |
| 62 | | i. Ability to export reports in CSV and PDF |
| 63 | | c. Search events across the entire organization, or down to a physical or logical reporting domain |
| 64 | | d. Dynamic watch lists for keeping track of critical violators — with the ability to use watch lists in any report or rule |
| 65 | | 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. |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | | |
|---|---|---|
| 66 | | f. Able to automatically correlate user to location and IP address: |
| 67 | | i. Provide ability to report and search on user to IP address to location. Location may be physical switch port, Mac address or VPN. |
| 68 | | ii. Enrich events where no user context is provided based on IP address. |
| 69 | 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). |
| 70 | | Support individual asset monitoring, configuration management, process/service monitoring, and real-time alerting for critical status or configuration changes. |
| 71 | | Alert when there is a process status change by actively monitoring using protocols as described in protocols 3.a. For example alert when a process or service stops. |
| 72 | | SIEM Should provide minimum 300+ types devices/Endpoints/Applications support and provide the option to add customized devices |
| 73 | | 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 |
| 74 | | 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. |
| 75 | | Performance metrics collected via polling and not relying on device generated logs, should include:<br>i. Interface utilisation, errors, sent and received bytes<br>ii. CPU<br>iii. Memory<br>iv. Disk<br>v. Process utilisation |
| 76 | User and Entity Behavior Analytics (UEBA) | **Bidder should quote minimum 100 UEBA license from day one and the UEBA solution shall be able to:** |
| 77 | | i. Monitor User, Process & File activity on user machines |
| 78 | | ii. Collect information from Network Devices, Active Directory & log sources for user activity |
| 79 | | iii. Record User account activity |
| 80 | | iv. Monitor and alert USB device activity in user's machine |
| 81 | | v. Provide visibility on remote worker or traveling user machines |
| 82 | | vi. Log data ex filtration activity like file upload and file transfer to USB devices |
| 83 | | vii. Alert General anomalous user behavior based on base lining of historical user activity |
| 84 | | viii. Solution shall be able to detect and alert on browser upload and downloads |
| 85 | | ix. Capability to detect and alert cloud upload of data |
| 86 | | x. Detect applications like TOR, Gaming Applications etc. |
| 87 | | xi. Detect uncommon VPN Clients installed in the system |



Meghna Bank PLC. IT Division, Head Office, Dhaka

| | | |
|---|---|---|
| 88 | | xii. UEBA shall be able to gather logs when an user system is off the corporate network (off-net) |
| 90 | Security Orchestration & Automation | The solution shall provide an automation service to execute predefined actions when security incidents are generated, reducing manual effort and improving response time. |
| 91 | | The solution shall support centralized automation policies that can be applied to multiple detection rules, avoiding rule-by-rule notification configuration |
| 92 | | Automation policies shall allow configuration by incident severity, selected rule sets, and effective time windows to control when actions are triggered. |
| 93 | | Automation policies shall support scoping to affected assets such as devices/applications and IP addresses/IP ranges, enabling targeted response actions |
| 94 | | The solution shall provide built-in notification actions including email, SMS, and webhook mechanisms with configurable recipients and templates |
| 95 | | The solution shall support automated execution of remediation scripts and/or response playbooks upon incident trigger as part of automation actions |
| 96 | | Authorized users shall be able to execute response playbooks on-demand directly from an incident view for analyst-driven response. |
| 97 | | The solution shall support invoking integration actions/policies (e.g., enrichment/lookup workflows) as part of automation to accelerate triage and decision-making. |
| 98 | | The solution shall support automatic case creation from incidents, and allow mapping to case management policies/team routing for structured incident handling. |
| 99 | | The solution shall maintain auditability by recording automation execution status and action history within incidents, and providing detailed execution logs, usage tracking, and automation audit events. |
| 100 | | Bidder Requirement: The bidder must quote two (2) SOAR users/instances along with their proposal (as part of the overall automation and orchestration capability). |
| 101 | License, Warranty/RMA and TAC support | a. The proposed solution should be sized for 100 GB daily data ingestion / 3000 sustained EPS at all layers and should be scalable without dropping or queuing of logs as per bank requirement. There should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated. |
| 102 | | b. Bidder must offer necessary software, licenses & subscriptions for three years without any additional costs. Meghna Bank Will Provide Underlying Hardware. |
| 103 | | c. Bidder can onboard OEM Implementation Team if needed for successful implementation. |
| 104 | | d. Bidder must offer 24x7 support from their security operations center located in Bangladesh. |
| 105 | | e. Bidder should provide minimum 3 (Three) years full warranty for proposed solution, but not limited to support, patch, software update & upgrade. |
| 106 | | f. Bidder Must Provide Manufacturer Form (MAF). Otherwise Submitted Proposal will be non-responsive |



Meghna Bank PLC. IT Division, Head Office, Dhaka

# ANNEXURE-B

## Designated Contact Person

**Contact Details of (Bidders Name):**

For any clarification the following addresses can be contacted:

| **Point of Contact at (Bidders Name)** | |
|---|---|
| Name | |
| Address | |
| Mobile | |
| Phone/Fax | |
| E-mail | |

# ANNEXURE-C

## Details Team Member Experience

| SL. | Name of proposed Engagement Manager/ Proposed Team Leader/ Team Members | Prof. Qualifications | Certificated/ Accreditations | IT Security Expertise in terms of Years & areas of expertise | Number of similar Assignments involved in Fintech/ Banks/NBF |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |

**[END]**



Meghna Bank PLC. IT Division, Head Office, Dhaka