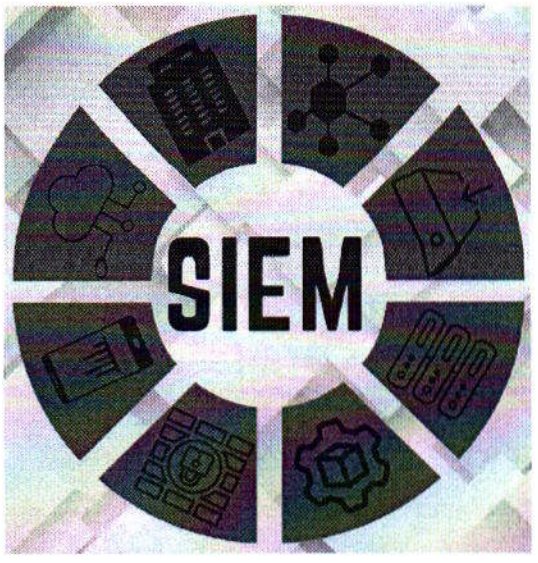

for

Supplying, Installing, and Commissioning of a Security Information and Event Management (SIEM) System and Establishment of an On-Premises/Hybrid Security Operations Center (SOC).

Premier Bank
service first

Last Date of Bid Submission	April 22, 2026
Bid Opening Date & Time	April 26, 2026

The Premier Bank PLC.
IT Security & Governance Division,
Information Technology Division
5th floor, IQBAL CENTRE, 42, Kemal Ataturk Avenue, Banani, Dhaka-1213
Web: https://thepremierbankplc.com

1 EXECUTIVE SUMMARY

This Request for Proposal (RFP) is issued by The Premier Bank PLC. to invite proposals from qualified vendors for the design, supply, deployment, integration, and ongoing support of a complete Security Information and Event Management (SIEM) solution, along with the establishment of an on-premises/hybrid Managed Security Operations Center (SOC) operated through a hybrid model.

In today's evolving cyber threat landscape, The Premier Bank PLC. seeks to enhance its cybersecurity posture through a robust SIEM platform and a fully operational SOC. The solution must provide real-time log collection, advanced threat detection, incident response, forensic investigation, and regulatory compliance support, in alignment with Bangladesh Bank guidelines and international standards such as ISO/IEC 27001.

The scope includes:

a. Implementation of a scalable and feature-rich SIEM system for centralized log management, event correlation, threat analytics, and incident alerting;
b. Establishment of a Managed SOC within the Bank's premises, which will be operated by the selected vendor's skilled security professionals with active involvement from The Premier Bank PLC's own security personnel;
c. Integration with the Bank's IT infrastructure across both Data Center (DC) and Disaster Recovery (DR) sites, covering core banking systems, network devices, endpoints, servers, applications, and cloud services as required;
d. SOAR (Security Orchestration, Automation, and Response), UEBA (User and Entity Behavior Analytics), Threat Intelligence Feeds to enhance the capabilities of the security environment.

The selected vendor will be responsible for:

a) Supplying all necessary hardware, software licenses, and related components;
b) Deploying and configuring the SIEM and SOC infrastructure;
c) Staffing the SOC with qualified security analysts and engineers for next six (6) months after completion of the work.
d) Facilitating seamless knowledge transfer and training for bank personnel to enable parallel operations and skill development;
e) Providing continuous monitoring, incident handling, system maintenance, and upgrade support throughout the contract period.

This RFP initiative reflects The Premier Bank PLC's commitment to establishing a resilient and proactive cybersecurity ecosystem. The Bank aims to ensure rapid threat detection and response, maintain data integrity, and comply with evolving regulatory requirements.

Vendors with a proven track record in delivering on-premises/hybrid Managed SOCs and enterprise-grade SIEM deployments—preferably in the financial services domain—are encouraged to participate. Proposals will be evaluated based on solution fit, technical capabilities, service methodology, team qualifications, and commercial terms.

With a future-focused mindset, The Premier Bank PLC continues to evolve, delivering excellence and shaping the banking experience of tomorrow.

AT A GLANCE
Corporate (Head) Office: Iqbal Centre, 42, Kemal Ataturk Avenue,
Banani, Dhaka-1213.
Branches & Sub-Branches across the country: 136 & 67
Agent outlet: 214
Number of Employees: more than 2800

2 BACKGROUND

2.1 About PBPLC

The Premier Bank PLC is a leading commercial bank in Bangladesh, committed to delivering secure, efficient, and technology-driven banking services across its nationwide branch network and digital platforms. As part of its continuous transformation and in line with regulatory expectations from Bangladesh Bank, the Bank is placing increased emphasis on fortifying its cybersecurity infrastructure and operational readiness.

In recent years, the cybersecurity threat landscape has evolved rapidly, with increasing occurrences of sophisticated attacks targeting financial institutions. Threat actors now employ advanced tactics such as ransomware, zero-day vulnerabilities, APTs (Advanced Persistent Threats), and social engineering campaigns. These developments have highlighted the urgent need for centralized visibility, automated threat detection, and swift response mechanisms across the Bank's entire IT ecosystem.

The Premier Bank PLC. currently operates a diversified technology environment that includes core banking systems, web-based services, data centers, communication infrastructure, and cloud-enabled platforms. To ensure continuous protection, accountability, and auditability, the Bank has taken the strategic decision to deploy an advanced Security Information and Event Management (SIEM) system along with a dedicated, on-premises/hybrid Managed Security Operations Center (SOC).

3 SCOPE OF WORK

3.1 SIEM Solution Delivery

The vendor shall:

a) Supply and implement an SIEM solution (appliance-based or software-based) that meets the Bank's current and future log collection and correlation needs.
b) Deploy the SIEM solution at the Bank's Primary Data Center (DC) and Disaster Recovery (DR)site.
c) Integrate the SIEM with various log sources including (but not limited to):
   - Firewalls, Routers, Switches
   - Windows and Linux Servers
   - Core Banking System (CBS)
   - Web Applications and Email Systems
   - Endpoint Protection and Antivirus Solutions
   - Cloud Infrastructure (if applicable)
d) Configure real-time log collection, normalization, correlation, and alert generation.
e) Develop and tune use cases, correlation rules, and dashboards based on common threats and the Bank's operational context.
f) Provide central dashboards and role-based access for security monitoring and reporting.

g) Ensure log retention as per regulatory guidelines (minimum 6 months online, 1 year's archive).

3.2 On-Premises/Hybrid SOC

The vendor shall:

a) Deploy and hand over a fully operational SOC at the Bank's premises, equipped with all required hardware, software, consoles, monitoring systems, and workspace.
b) Provide the complete SOC solution, while the SOC will be fully operated and managed by The Premier Bank PLC's internal team.
c) Implement a ticketing/workflow system for logging and tracking incidents, alerts, and responses.
d) Enable reporting capabilities to support daily, weekly, and monthly reports on security alerts, incidents, health checks, and trends.
e) Provide tools and functionalities to support log correlation, incident validation, triage, threat intelligence analysis, and root cause investigation.
f) Ensure the solution supports structured incident escalation and response activities, to be executed by the Bank's internal team.
g) Provide a secure and auditable SOC framework, including documentation templates for action rules, runbooks, and escalation matrices, for the Bank to maintain and operate.

3.3 Advanced Capabilities

The vendor must integrate the following components to strengthen the security ecosystem:

a) SOAR (Security Orchestration, Automation and Response) for automating repetitive incident handling tasks.
b) UEBA (User & Entity Behavior Analytics) for detecting insider threats and anomalous behavior.
c) Threat Intelligence Feeds to enhance correlation and threat enrichment.
d) Integration with SIEM-supported APIs and third-party tools to enable future extensibility.

3.4 Training & Knowledge Transfer

The vendor shall:

a) Provide hands-on training to Bank personnel for SIEM usage, dashboarding, rule creation, basic incident handling, and reporting.
b) Conduct SOC process orientation sessions, including incident triage, escalation, and post-incident review.
c) Deliver complete documentation, including:
    - System architecture
    - User and administrative manuals
    - Configuration guides
    - SOPs and action rules for incident handling

3.5 Support & Maintenance

The vendor shall:

a) Provide a minimum 3-year warranty for the software with full support, including updates, patches, and health monitoring, along with an additional 2-year AMC for post-warranty hardware support.

b) Maintain system performance SLAs for uptime, alert processing, and incident response.
c) Provide 24x7 support through onsite personnel and/or remote escalation channels.

4 DEPLOYMENT PHASES & METHODOLOGY

This project will follow a structured, phased implementation approach to ensure seamless delivery, knowledge transfer, and operational readiness:

4.1 Phase 1: Project Initiation & Planning

a) Kick-off Workshop: Conduct an onboarding meeting with stakeholders from The Premier Bank PLC. and the vendor team to define objective es, success criteria, communication protocols, and escalation procedures.
b) Scope Definition: Finalize the detailed inventory of systems, log sources, stakeholders, and access requirements.
c) Project Plan Development: Prepare a comprehensive plan outlining milestone, resource allocation, risk management, dependencies, and timelines.

4.2 Phase 2: Solution Design & Architecture

a) Site Survey & Assessment: Assess the Bank's DC and DR infrastructure, network topology, security devices, and data flow architecture.
b) Solution Design: Develop detailed SIEM architecture diagrams, network integration plans, and redundancy design.
c) Use Case & Rule Definition: Define and document use cases, detection rules, dashboards, alerts, and escalation workflows tailored to the Bank's environment.

4.3 Phase 3: Procurement & Setup

a) Hardware & Software Procurement: Coordinate with the Bank to procure required SIEM appliances, licensing.
b) Installation & Configuration: Install SIEM components, SOC consoles, network connectivity, and logging agents.
c) Integration of Log Sources: Connect all systems (firewalls, servers, endpoints, core banking, etc.) to the SIEM, ensuring secure and reliable log flow to the SOC.

4.4 Phase 4: Implementation & Tuning

a) Correlation Rule Development: Configure initial detection rules and thresholds; conduct iterative tuning to reduce false positives.
b) Dashboard Development: Build dashboards, reporting templates, and alert visualizations for different user roles (SOC analysts, management, auditors).
c) Testing & Validation: Perform end-to-end testing of log ingestion, correlation, alerting, reporting, failover, and user access controls.

4.5 Phase 5: SOC Activation & Training

a) SOC Commissioning: Set up the SOC within the Bank premises and deploy all mentioned necessary SOC infrastructure, tools, and systems.
b) Operational Handover: Fully hand over the SOC solution to The Premier Bank PLC, enabling the Bank's internal team to operate and manage all SOC functions independently.

c) Training: Conduct comprehensive, hands-on training programs to fully prepare Bank personnel as per training requirements, ensuring they are proficient in SIEM operations, alert management, dashboard usage, incident triage, escalation workflows, and SOC best practices—so that the SOC is fully capable and staffed with trained resources at the time operations begin.

4.6 Phase 6: Operational Stabilization & Go-Live

a) Live Monitoring Commencement: Initiate 24×7 SOC operations by the Bank's trained SOC team, with the vendor providing necessary technical support, fine-tuning, and configuration optimization during the initial activation period to ensure full operational stabilization.
b) SLA Monitoring: Begin tracking KPIs for alert handling time, incident response, system uptime, and SLA compliance.

4.7 Phase 7: Continuous Service & Optimization

a) Ongoing Optimization: Periodically refine detection rules, use cases, dashboards, and integrations to adapt to emerging threats and operational feedback.
b) Threat Intelligence Updates: Incorporate new threat feeds and update content regularly.
c) Incident Post-Mortem & Reporting: Provide structured reports of significant incidents, root cause analysis, and recommended preventive controls
d) Knowledge Transfer & Capacity Building: Sustain training programs for internal staff to continuously enhance their SOC capabilities, ensuring they become progressively more skilled and operationally ready over time.

Methodology & Governance

a) Project Governance: Establish a project oversight framework where the vendor provides structured progress updates, technical inputs, and risk advisories, while The Premier Bank PLC independently governs all decisions, approvals, and escalations related to project execution.
b) Agile-Informed Approach: Although the project will follow defined milestones, the vendor shall use iterative development cycles—particularly for SIEM use cases, correlation rules, dashboards, and tuning—to refine outputs based on Bank feedback and ensure the SOC is fully optimized for internal operation.
c) Quality Assurance: The vendor must implement strict quality assurance measures for every deliverable, including testing, validation, and performance checks, while final acceptance testing and sign-off will be performed solely by The Premier Bank PLC.
d) Documentation: The vendor shall provide complete, detailed documentation covering architecture, configurations, SOPs, runbooks, incident action rules, and user manuals to fully enable the Bank's internal team to operate and maintain the SOC independently.

5 FUNCTIONAL & TECHNICAL REQUIREMENTS

The proposed solution must fulfill the following functional and technical criteria, ensuring seamless security monitoring, log analysis, incident response, and regulatory compliance for The Premier Bank PLC.

5.1 SIEM Functional Requirements:

Requirement	Description
Log Collection	Real-time, agent-based and agentless collection, parsing,

	normalization and indexing of logs from various systems (network devices, servers, applications, cloud).
Log Ingestion	The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.
Log Normalization	Automatic normalization of logs from heterogeneous sources to a unified format.
Event Correlation	Customizable rule-based and behavior-based correlation engine to detect patterns and anomalies.
Big Data Analytics Capability	Solution must include Next Gen SIEM, Security Analytics, Security Big Data Lake (SBDL) with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM & Security Big Data Lake (SBDL).
Next-Gen SIEM with ML	Machine learning should be embedded across the platform (SIEM & SBDL). It should empower every user in the SOC with Machine Learning models (ML) i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and should be able to integrate various ML frameworks.
Machine Learning Capability	The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.
MITRE ATTACK & Kill Chain	The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques.
RTO/RPO	The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.
Alerting & Notification	Configurable alerts with severity levels, thresholds, and multi-channel notification (email, SMS, dashboard).
Dashboards & Visualization	Intuitive, real-time dashboards for SOC analysts and management with customizable widgets.
Search & Forensics	Powerful search tools for investigation, threat hunting, and forensic analysis over historical data.
Threat Intelligence Integration	Support for integration with internal and external threat intelligence feeds.
Log Retention & Archiving	Online log retention for minimum 6 months; archiving capability for at least 1 years, in compliance with Bangladesh Bank regulations.
Multi-Tenancy/Role-Based Access	Granular access control to restrict users based on roles and responsibilities.
SOAR	Workflow automation for incident response with fully automated and semi-automated response capabilities using Action Rules and Incident Management features.
UEBA	Behavioral analytics to detect insider threats, privilege misuse,

	and account compromise.
High Availability	Redundant architecture to ensure high availability of log ingestion, storage, and analysis.
RTO/RPO	The proposed solution must support the data replication natively without relying on other third-party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR.
Disaster Recovery Support	Synchronization of SIEM functionality between DC and DR sites with failover readiness.

5.2 SOC Functional Requirements

Requirement	Description
24x7 Monitoring	Continuous monitoring of security events, alerts, and incidents by the Bank's internal SOC team, supported by vendor-provided tools, configurations, and technical optimizations to ensure effective operational performance.
Incident Triage & Escalation	Classification, validation, prioritization, and escalation of incidents based on severity and impact.
Vulnerability Monitoring Support (via SIEM Feeds)	Integration with vulnerability scanners and mapping vulnerabilities to real-time threats.
Asset & Identity Visibility	Ensuring assets, identities, and network topology are accurately reflected in the SIEM for effective monitoring.
Threat Hunting	Periodic proactive threat hunting using SIEM data and threat intelligence.
Ticketing System	The solution should have a built-in ticketing mechanism to raise, manage, track, and close cases, ensuring end-to-end case management and traceability.
Reporting & Metrics	Daily, weekly, and monthly reports on SOC activity, incidents, health status, and trends.
KPI/KRI Tracking	Operational efficiency metrics (MTTA, MTTR, false positives, rule effectiveness).
Playbooks &action rules	Automated response capabilities for handling alerts and mitigating common attack types and system anomalies.
SOC Health & Performance Monitoring	Continuous monitoring of SIEM ingestion rates, agent health, log source availability, and system performance.
Patch and Version Management for SOC Tools	Ensuring SIEM platform, agents, connectors, and databases stay updated and secure.
Knowledge Base	Maintain a secure, evolving repository of incident records, signatures, TTPs, and response strategies.
Audit Readiness	Capable of generating audit-compliant reports with time-stamped logs and investigation trails.
Compliance Reporting Templates	Pre-built reporting formats aligned with Bangladesh Bank, PCI-DSS, ISO 27001, etc.

Compliance Alignment	Adherence to Bangladesh Bank security guidelines, ISO/IEC 27001, and other relevant standards.
Security Awareness Input Loop	SOC findings feeding into the Bank's awareness and training programs.
Continuous Improvement Process	Periodic reviews of SOC posture, rule performance, threat landscape, and adaptation cycles.

5.3 Integration Requirements (Not Limited)

System Type	Examples to be Integrated
Network Devices	Firewalls, core routers, core switches, Load Balancer, WAF
Operating Systems	Windows Server, Linux (RHEL, Ubuntu, CentOS), Unix
Applications	Core Banking System (CBS), Internet Banking, ATM, POS, SMS Gateway, CMS, Agent Banking Solution (ABS), SWIFT, Remittance
Databases	Oracle, Microsoft SQL Server, MySQL, PostgreSQL
Security Tools	Antivirus, Endpoint Detection & Response (EDR), Web Proxy, Email Gateway
Cloud Platforms	Microsoft Azure, AWS (if applicable)
Directory Services	Microsoft Active Directory, LDAP

5.4 Technical & Performance Requirements

Parameter	Requirement
Event Per Second (EPS) Capacity	4000-6000 EPS or 100-150 GB Data Volume per day 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 Sources	Minimum support for 100+ active log sources across multiple systems.
Search Latency	Historical log queries should respond within acceptable limits (<10 seconds for 30-day window).
Uptime	≥99.95% availability for SOC and SIEM platform, excluding planned maintenance.
Security Hardening	All components must follow OS and application hardening standards (e.g., CIS benchmarks).
Data Integrity	Tamper-proof logs and audit trails with hash verification and encryption.
Localization	Time zone and compliance support for Bangladesh-specific regulatory reporting.

6 DEVICE COVERAGE & EPS/DATA VOLUME ESTIMATION

The vendor is required to size the proposed SIEM solution appropriately based on the projected number of devices, systems, and applications from which logs will be collected, while ensuring scalability for future expansion. The sizing should be based on Events Per Second (EPS)/Data Volume or Asset based.

The following table presents a baseline estimate of log sources currently in operation at The Premier Bank PLC. The actual count may vary and will be finalized during the implementation phase after a joint discovery and log profiling assessment.

6.1 Estimated Device Coverage (Not Limited)

1	No. of Windows Severs	100
2	No. of Linux Severs	20
3	No. of ESXI Severs	10
4	No. of Security & Network Devices (if SDN formation, minimum requirement of **30–40 devices** should be considered)	40
5	Web Server	20
6	Database Server	15
7	Application	20
8	Anti-virus / Anti-malware	02
9	Email security/ Anti-SPAM Filter	02
10	Web Access Security / Proxy	05

6.2 EPS & Log Volume Estimation (Not Limited)

Licensing for SIEM and UEBA	4000-6000 EPS or 100-150 GB Data per day Volume 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 6 months (hot storage)
Log Archiving (Offline)	1 year (cold/archive storage)
SOAR User License	Min 2 or more

Bidder will follow detail technical specification for Software and Hardware requirement.

6.3 Vendor Responsibilities

The selected vendor shall:

- Conduct an initial discovery and sizing workshop with The Premier Bank PLC. to confirm final EPS requirements.
- Size the SIEM and storage components to handle the estimated peak EPS with room for 30% future growth.
- Ensure scalable architecture for both compute and storage (e.g., modular or cluster-based growth).
- Implement appropriate data compression and retention policies to optimize storage use while maintaining compliance.
- Recommend high-availability and DR synchronization strategies that ensure log integrity and availability.

7 SERVICE LEVEL REQUIREMENTS

To ensure continuous protection, visibility, and operational excellence, the selected vendor must commit to defined Service Level Agreements (SLAs) covering availability, responsiveness, system performance, incident handling, and support delivery. These SLAs will form a key part of the contractual obligations.

7.1 System Uptime and Availability

Component	Minimum Uptime Requirement
SIEM Platform (Production)	≥ 99.95% uptime per calendar month
SOC Facility (On-Premises/hybrid)	24x7x365 operational readiness
DR Synchronization (SIEM)	≥ 98% sync availability between DC and DR

7.2 Incident Response Time (Based on Severity)

Severity Level	Definition	Response Time	Resolution Time
Critical (P1)	Security breach, malware outbreak, major system compromise	≤ 15 minutes	≤ 2 hours
High (P2)	Active attack attempt, unauthorized access, service degradation	≤ 30 minutes	≤ 4 hours
Medium (P3)	Suspicious activity, policy violation, abnormal behavior	≤ 1 hour	≤ 8 hours
Low (P4)	Informational alerts, false positives, audit support	≤ 4 hours	≤ 24 hours

7.3 Support and Helpdesk

Service	Requirement
Support Hours	24×7×365 coverage (onsite and remote)
Support Channels	Onsite, Phone, Email, Web Portal
Escalation Matrix	Must be shared with defined response levels
Ticketing Support	The ticketing and case management must be implemented, operated, and maintained by the Bank Officials affiliated with the vendor.
Service Review	Monthly SLA and performance review with The Premier Bank PLC

7.4 Reporting & Documentation SLA

Report Type	Frequency	Delivery Method
Daily SOC Activity Report	Daily	Email / SMS/ Portal
Weekly Incident Summary	Weekly	PDF / Dashboard
Monthly Security Posture Report	Monthly	Presentation & Report
Quarterly SLA Review Report	Quarterly	In-person Meeting
Log Archiving Status	Monthly	Archival dashboard/report
Threat Intelligence Updates	As Released / Weekly	Integrated into SIEM / Reported

7.5 Penalty for SLA Violation

In case of SLA breaches (e.g., excessive downtime, delayed incident handling), The Premier Bank PLC. reserves the right to impose penalties as outlined in the commercial contract. Typical penalty clauses may include:

- Service Credit deductions from AMC fees or monthly bills.
- Escalation to higher management and re-negotiation of operational control.
- Termination clauses in case of repeated non-compliance.

7.6 Additional SLA Commitments

- SLA Adherence Guarantee must be signed and submitted with the proposal.
- The vendor shall maintain a knowledge base of all known issues, incident types, response actions, and remediation logs.
- The SOC must be audit-ready, with documentation available on request for regulatory reviews and internal/external audits.

8 IMPLEMENTATION & KNOWLEDGE TRANSFER

The selected vendor will be responsible for the end-to-end implementation of the SIEM solution and the establishment of an on-premises/hybrid SOC at The Premier Bank PLC, ensuring a smooth transition into full internal operations. The vendor must equip the Bank's internal team with all required skills, tools, configurations, and documentation so that the SOC can be independently operated and maintained by Bank personnel after implementation.

8.1 Implementation Responsibilities

The vendor shall:

- Assign a dedicated Project Manager to oversee the planning, coordination, and execution of all implementation activities.
- Establish the required SIEM infrastructure (hardware/software) at both the Bank's Data Center (DC) and Disaster Recovery (DR) site.
- Set up and configure the SOC environment, including analyst consoles, dashboards, ticketing systems, monitoring tools within Bank premises.
- Integrate all relevant log sources from network, systems, applications, and security platforms.
- Develop and deploy use cases, correlation rules, alert thresholds, and response workflows tailored to the Bank's risk profile.
- Conduct system performance testing, security testing, and user acceptance testing (UAT) prior to go-live.
- Document the baseline configuration, tuning adjustments, escalation paths, and technical runbooks.

8.2 Knowledge Transfer Plan

The vendor must deliver a structured Knowledge Transfer Program to ensure operational handover, cross-team collaboration, and skill development for The Premier Bank PLC's IT/security staff.
This includes:

Knowledge Area	Delivery Method	Target Audience
SIEM Administration (GUI, Rules, Dashboards, Log Source Onboarding)	Hands-on+ Administrator Manuals	SIEM Admins, SOC L2/L3
SOC Role-Based Operations (Level 1, Level 2, Level 3 Duties & Responsibilities)	Structured Training Tracks + Practical Exercises	SOCs L1, SOC L2, SOC L3 Teams
Alert Monitoring & Initial Triage (SOC Level 1 Readiness)	Hands-on Exercises + Step-by-Step Playbooks	SOC L1 Analysts

Advanced Investigation, Correlation Analysis & Threat Hunting (SOC Level 2/3 Readiness)	Scenario-Based Labs + Use-Case Walkthroughs	SOC L2 & L3 Analysts
SOC Processes (Triage, Escalation, Playbooks, Action Rules)	Workshops + Real Incident Simulations	SOC L1/L2/L3 & Security Team
Use Case Development & Rule Tuning	Scenario-Based Training + Practical Labs	SIEM Admins, SOC L2/L3
Reporting & Dashboards (Operational, Executive, Compliance)	Live Demo + Reporting Guide	Risk, Audit, IT Infra, SOC Leads
Threat Intelligence Interpretation & Usage in SIEM	Use-Case-Based Sessions	SOC L2/L3 Analysts
Incident Response Workflow & Coordination	Live Walk-Through + Simulation	SOC Analysts, IT Security Team, Bank Staff
DR, Failover & HA Operations for SIEM/SOC	Simulation + Technical Documentation	DR/BCP Team, SIEM Admins
Compliance & Audit Reporting (Including Bangladesh Bank & ISO 27001 Requirements)	Sample Walkthrough + Templates	Compliance, Internal Audit, SOC Leads
SOC Operations Management (Shift Schedules, SLA, KPI/KRI Tracking)	Workshop + Templates	SOC Managers / Supervisors
Knowledge Base Development (TTPs, Signatures, Incident Records)	Hands-on Sessions	SOC L2/L3, SIEM Admins
Full SOC Center Readiness Program	End-to-End Operational Simulation ("Go-Live Drill")	Entire SOC Team (L1–L3), Security, IT Infrastructure

8.3 Documentation Deliverables

The vendor shall provide the following documentation in both digital and printed form:

- SIEM Solution Architecture & Deployment Plan
- List of Configured Use Cases & Correlation Rules
- SOC Operational Workflows & Escalation Matrix
- Ticketing & Reporting Framework
- User Manuals (Admin, Analyst, Manager)
- Log Source Onboarding Guide
- Log Retention & Archiving Policies
- SOPs for Incident Handling, Daily Operations, Reporting
- Final Acceptance Test (FAT) Plan & Results

8.4 Handover and Sign-Off

- Upon successful completion of implementation and knowledge transfer, a formal sign-off process will be initiated, including:
  - Validation of all technical configurations and integrations
  - Acceptance of documentation and training completion
  - Verification of system performance and SLA readiness
- The vendor must provide a post-implementation support plan, including the contact matrix and escalation points.

9 PROJECT TIMELINE & DELIVERABLES

The implementation of the SIEM solution and the establishment of the on-premises/hybrid SOC at The Premier Bank PLC. will be carried out in a phased approach within a clearly defined timeline. The vendor must submit a detailed project plan covering major milestones, dependencies, deliverables, and resource allocation required for successful deployment. After implementation, the SOC will be fully operated and managed by the Bank's internal team; therefore, the vendor must ensure all systems, configurations, documentation, and training are completed to enable full operational readiness.

The following table presents a suggested high-level timeline, and vendors may propose an optimized timeline based on their implementation methodology and resource availability, subject to approval by The Premier Bank PLC.

9.1 Suggested Project Timeline

Phase	Activity	Duration	Responsible Party
Phase 1	Project Kickoff & Planning	Week 1	Vendor & Bank
Phase 2	Site Readiness Assessment & Final Sizing	Week 2	Vendor
Phase 3	Delivery of Hardware & Licenses	Weeks 3–11	Vendor
Phase 4	SIEM & SOC Infrastructure Setup	Weeks 11–13	Vendor
Phase 5	Log Source Integration & Use Case Development	Weeks 13–16	Vendor
Phase 6	Design, configure, and implement SOAR workflows and automated playbooks for security incident detection, response, and remediation.	Weeks 16-22	Vendor
Phase 7	System Testing, Tuning & Optimization	Weeks 22–23	Vendor & Bank
Phase 7	Knowledge Transfer & Documentation Delivery	Weeks 23–24	Vendor
Phase 8	Go-Live & Operational Handover	Week 24	Vendor & Bank
Phase 9	Stabilization & Post-Go-Live Support	Week 25 onwards (as per AMC)	Vendor

9.2 Key Deliverables

The vendor is expected to deliver the following items as part of the engagement:

Infrastructure & Software

- SIEM software (licensed) and/or appliances as per requirement
- SOC infrastructure: consoles, dashboards, ticketing system, etc.
- DR setup and failover mechanism

9.3 Configuration & Integration

- Integrated log sources with real-time monitoring
- Developed correlation rules, use cases, alert profiles
- Configured dashboards for multiple user levels

9.4 Training & Documentation

- End-user and administrator training sessions

- Knowledge transfer workshops
- Complete technical and user documentation (soft and hard copies)

9.5 Reports & Reviews

- Weekly progress reports during implementation
- UAT report and Final Acceptance Test (FAT) report
- Incident handling SOPs, escalation matrices, Playbooks
- Final project closure report and sign-off documentation

9.6 Support Setup

- Post-Go-Live stabilization support plan
- Contact list and escalation matrix for 24×7 support
- SLA monitoring dashboard and reporting templates

10 TERMS & CONDITIONS

Following are the Terms & Conditions applicable for this tender:

10.1 General Requirements

- The tender shall be filled in with permanent ink and shall not contain any stipulation, erasures or strike-over; corrections or revisions may be made by neatly marking through the figures or words and writing the correction above.
- The person signing the tender shall legibly initiate all revisions. Any overwriting, or omission in quoting rate for any item will disqualify the tender.
- The bidders should quote the unit price & total cost both in figures and words and there should not be any cutting/erasing/overwriting. The Offer must be made in BDT (Bangladeshi Taka).
- Tenders containing wrong information, illegible words, figures or names will be liable for rejection.
- Project Plan with timeline.
- If the service provider is foreign, authentication documents/agreements with the local partner must be included.
- Client list with contact details.
- Technical specifications at technical proposal and financial detail at financial proposal.
- Organization strength and relevant experience.
- Any other things required for technical and financial proposal.
- A Non-Disclosure Agreement (NDA) will be signed between supplier and The PREMIER BANK PLC. for the implementation the project.
- The Bidders must sign and seal every page of the tender.
- Post Audit support including remediation.
- The Bidder must provide the validity for the offered products/service for 90 days from the date of opening of financial offer.
- THE PREMIER BANK PLC. reserves the right to ask for any modification, amendment, adjustment and/or alteration of the proposal submitted by a participant and in such case, the participant may be required to submit the proposal again.
- THE PREMIER BANK PLC. may seek clarification of Technical and/or financial proposals from the respective participant for proper examination and evaluation of the proposals. The

request for clarification by THE PREMIER BANK PLC. and the response from the participants shall be in writing or by E-mail.

- The bidder must provide requested information in their proposal mentioned in the tender document and provide their confirmation on the acceptance of requested deliverables.
- All communications and documentation shall be submitted in English.
- The bidder must submit the offer in a sealed envelope containing the full name and address of the bidder. The forwarding letter should include the name, address, and telephone number of the authorized contact person.
- Tender documents must be presented on the bidder's official letterhead and duly signed by the authorized signatory.
- All pages of the tender document—including technical proposals, financial proposals, annexures, and submitted offers—must be signed and sealed by the authorized signatory.

10.2 Project Governance & Compliance

- The Bank and its regulators shall have full audit rights over the SOC, SIEM systems, configurations, logs, reports, and incident records.
- The proposed solution must comply with Bangladesh Bank guidelines, ISO/IEC 27001, and all applicable local and international regulatory standards.
- Repeated failure to meet SLA requirements may result in penalties or termination of the contract.
- During implementation, a dedicated project team must be assigned, including a Project Manager serving as the Single Point of Contact (SPOC).

10.3 Contract & Payment Terms

- A formal agreement will be executed between The Premier Bank PLC and the selected vendor, outlining commercial, technical, legal, and operational terms.
- Payments will be made on an annual basis, contingent upon satisfactory delivery, performance, and acceptance by the Bank. Final payment terms will be determined during contract negotiations.
- The tender amount shall include VAT & Tax as per applicable rules.

10.4 Performance & Warranty

- The vendor must provide a 3-year offer (software) and a 2-year AMC (hardware) as per the prescribed format.
- All supplied hardware must carry a minimum 3-years replacement warranty. Vendors must separately propose post-warranty Annual Maintenance Contract (AMC) terms for 2-years.

10.5 Intellectual Property & Licensing

- All software licenses must be genuine, verifiable, and clearly identified as perpetual or subscription based.
- All documentation, scripts, use cases, action rules, and configurations developed for the Bank shall remain the sole intellectual property of The Premier Bank PLC.

10.6 Termination Clauses

- The Bank reserves the right to immediately terminate the contract in cases of:

- Breach of confidentiality
- Repeated SLA failures
- Regulatory non-compliance
- Fraud or misrepresentation

❖ The Bank may terminate the contract with 60 day's prior written notice without penalty, subject to payment for completed work.

10.7 Evaluation & Acceptance

❖ The Bank may seek any clarification necessary for proper evaluation of technical and financial proposals.
❖ Submission of requested information in full is mandatory for evaluation.
❖ The lowest financial bid shall not automatically receive preferential consideration.
❖ The Premier Bank PLC. reserves the right to accept or reject any proposal, in whole or in part, without assigning any reason and is not obliged to select the lowest bidder.

11 PREPARATION OF THE TENDER

The Offer will consist of a two-envelope system: one for the "Technical Offer" and another for the "Financial Offer." Both envelopes should be sealed and placed in a larger envelope. The Tender Name must be clearly marked on the outer envelope.

I. Format and signing of bid

The bidder shall prepare one original and one copy both for the technical and the financial proposals in separate envelop, clearly marking each one as:

- **TECHNICAL OFFER**
- **FINANCIAL OFFER**

In the event of discrepancy between the original and its copy, the original shall prevail. All the envelopes will contain the full name and address of the participant company.

The originals and all copies must be signed by a person, or persons duly authorized to sign on behalf of the bidder. All pages of the bid where entries or amendments have been made shall be initialed by the person or persons signing the bid.

The bid shall contain no alterations, omissions or additions.

➢ **Technical Offer**

The Technical Offer must provide comprehensive information on the bidder's capability to **implement, configure, integrate, and support a Security Information and Event Management (SIEM) solution**, along with Managed SOC services.

Bidder(s) may need to submit supporting documents if required by the Bank to evaluate the offer.

❖ The Heading should be marked as "**Technical Proposal for Supplying, Installing, and Commissioning of a Security Information and Event Management (SIEM) System and Establishment of an On-Premises/hybrid Security Operations Center (SOC).**"
❖ The Tender document should be submitted along with a company letterhead pad mentioning participation in the tender process duly signed by the authorized signatory.

- ❖ Company profile.
- ❖ Technical Approach and Methodology. Including:
  1. SIEM deployment architecture
  2. Log source onboarding methodology
  3. Use-case development and correlation strategy
  4. Incident alerting, escalation, and reporting process
  5. Integration with security controls and infrastructure
- ❖ Implementation Work Plan, including timelines for deployment, configuration, tuning, stabilization, and handover.
- ❖ All related documents as per the Eligibility Criteria.

Technical evaluation matrix is given below:

Sl.	Technical evaluation	Marks
1	The OEM/Bidder must have at least two (2) years of proven experience with SIEM, SOAR, UEBA, Threat Intelligence, SOC, or Security Analytics solutions in banks or governments, or financial institutions or MNC and the proposed SIEM solution should preferably be listed in the Gartner Magic Quadrant for SIEM for at least one of the last two consecutive years.	15
2	The OEM and Bidder must have completed at least one (01) successful SIEM or SOC implementation project/work order within Bangladesh (documentary evidence required both). Preference will be given to experience with banks, government organizations, financial institutions, or multinational companies (MNCs). **Evaluation Criteria:** • Each qualifying implementation in **banks, government organizations, financial institutions, or MNCs** will be awarded **2.5 points**.	10
3	Availability of 24/7 SOC operations, incident investigation (onsite/remote), and dedicated cybersecurity support teams	5
4	A single OEM–integrated security stack is required, with SIEM, SOAR, UEBA, and Threat Intelligence provided by the same OEM to ensure seamless integration, unified workflows, and centralized management.	5
5	The OEM/Bidder must have certified engineers (e.g. CISSP, CISM, CISA, CEH, or equivalent) for solution deployment, configuration, and support. Copies of certificates must be submitted with the proposal. Additionally, certified resources specific to the offered product will be given preference during evaluation.	10
6	The Bidder must hold a **valid ISO/IEC 27001:2022 certification**, demonstrating adherence to international information security management standards. The proposed solution must comply with **Bangladesh Bank ICT Security Guidelines**, **ISO/IEC 27001**, **PCI-DSS** (where applicable), and other relevant regulatory and information security standards.	10
7	The OEM/Bidder should have valid **SOC 2 Type I & Type II** certifications, covering security, availability, and confidentiality controls.	5
8	Completeness, clarity, technical soundness, scalability, architecture maturity, and reporting capabilities of the proposed SIEM solution	5
9	The bidder must have prior experience in cybersecurity-related projects and maintain a registered local office.	5
	Total marks	**70**

➢ Financial Offer

The financial offer shall contain the following:

- ❖ The bidder must submit a 3-year (software) proposal along with a 2-year AMC (hardware), following the prescribed format.
- ❖ The Heading should be marked as "**Financial Proposal for Supplying, Installing, and Commissioning of a Security Information and Event Management (SIEM) System and Establishment of an On-Premises/hybrid Security Operations Center (SOC).**"
- ❖ Submission of declaration regarding bidder(s) has the legal capacity to enter the contract under the applicable law of Bangladesh and bidder(s) shall not be barred as per law of the land that may subject to legal proceedings of any kind.
- ❖ "The last 03 (three) years' financial reports were audited by a reputed audit firm of Bangladesh.
- ❖ "Company Name, Local address, Contact numbers and date of establishment of the firm, Trade license, Certificate of Incorporation, TIN certificate, up-to-date Income Tax Clearance certificate, BIN certificate etc.
- ❖ Self-declaration of not being blacklisted anywhere.
- ❖ Rates and total cost of all items in BDT as per schedule of Items.
- ❖ In case any discrepancy is found between the amount mentioned in the figure and the words, the amount mentioned in the words will prevail.
- ❖ Only arithmetic errors will be corrected by the Bank after opening of the Financial Offer and the final calculated result will be considered as a financial offer by the bidder. Once the financial offer is opened, no inclusion or exclusion in any form will be governed.
- ❖ Any claim for enhancement of rate shall not be entertained during the period of contractor or during an extended period of Contract, if any, for any price escalation or any other reason whatsoever.
- ❖ If there are any ambiguities between the quoted rate and amount due to computation mistake, the quoted rate shall be considered as valid, and the total amount shall be corrected accordingly.
- ❖ The first 3(three) bidders scoring highest in the technical & financial section (70%+30%=100%) will be considered for evaluation.

II. Sealing and marking of bid

a. The bidders shall seal the original bids and each copy of the bids in envelope, duly marking as mentioned earlier.
b. The envelopes shall be addressed at the following address:

Mohammed Fazlur Rahman
FVP & Head of GSD (CC)
The Premier Bank PLC
Head Office, 5th floor,
IQBAL CENTRE, 42 Kemal Ataturk Avenue,
Banani, Dhaka-1213
Cell no: +880 1713083010

c. If the envelope is not sealed and marked as above, the Bank will assume no responsibility for the misplacement or premature opening of the bid.

III. **Deadline of bid**

Bids must be received by Bank at the address specified above by **April 22, 2026 at 5 PM.**

IV. **Technical Clarification**

For any Technical clarification the following addresses can be contacted:

Abu Md. Sabbir Hassan Chowdhury
EVP & CITO, IT Division
The Premier Bank PLC
Head Office, 10th floor,
IQBAL CENTRE, 42 Kemal Ataturk Avenue,
Banani, Dhaka-1213
Cell no: +880 1730325143
&
Kh. Golam Sarwar
SAVP & Head, IT Security & Governance Division
The Premier Bank PLC
Head Office, 6th floor,
IQBAL CENTRE, 42 Kemal Ataturk Avenue,
Banani, Dhaka-1213
Cell No: +880 1313046588

V. **Award of Contract**

The Bank will award the contract to the successful bidder. After successful negotiations, the Bank will notify the successful bidder that his/her bid has been accepted. The notification of award will constitute the formation of the contract.

11.1 Minimum Eligibility Criteria

Criteria	Requirement
Company Registration	Must be a registered company in Bangladesh or have an authorized local partner if foreign.
Gartner Magic Quadrant Position	The OEM/Bidder must have at least two (2) years of proven experience with SIEM, SOAR, UEBA, Threat Intelligence, SOC, or Security Analytics solutions in banks or governments, or financial institutions or MNC and the proposed SIEM solution should preferably be listed in the Gartner Magic Quadrant for SIEM for at least one of the last two consecutive years.
Cybersecurity Related Experience & Registered Office	Must have prior experience in cybersecurity-related projects and maintain a registered local office.
Relevant Experience	Minimum 1 successful implementations/WO of SIEM and/or SOC projects, preferably in the banks or governments, or financial institutions or MNC.
SOC Capability	Proven experience in setting up on-premises/hybrid SOCs.
Single OEM Integrated Security Stack	SIEM, SOAR, UEBA, and Threat Intelligence components must be from the same OEM (native modules or OEM-provided solutions) to ensure smooth integration, unified workflows, and centralized management.
Technical Expertise	Certified technical staff in SIEM platforms, incident handling, cybersecurity, and system integration. Threat intel
Financial Soundness	Audited financial statements for the last 3 years, demonstrating solvency and operational capacity.

OEM Authorization	If proposing a third-party SIEM solution, must submit a valid OEM authorization letter or partnership certificate.
Support Capability	Ability to provide 24×7 support, on-site personnel, and remote escalation channels.
Compliance Familiarity	Knowledge of Bangladesh Bank IT security guidelines, ISO/IEC 27001, PCI-DSS and other relevant standards.

11.2 Mandatory Submission Documents

- Company Profile
- List of Relevant Projects (with client references)
- Proposed SIEM & SOC Architecture
- Implementation Methodology & Project Plan
- Resumes of Key Team Members
- Hardware & Software Bill of Materials (BoM)
- Signed SLA Template & Compliance Matrix
- Financial Proposal (in separate envelope)
- Valid Trade License, BIN, TIN, and VAT Registration
- OEM Authorization Letter (if applicable)
- Declaration of No Blacklisting or Litigation

12 FINANCIAL PROPOSAL FORMAT

Bidders must submit a detailed financial proposal in a separate sealed envelope clearly marked as "Financial Proposal for SIEM & On-Premises/hybrid Managed SOC – The Premier Bank PLC".

The proposal should clearly itemize all costs associated with the supply, implementation, and ongoing support of the solution. All prices should be quoted in BDT (Bangladeshi Taka), exclusive and inclusive of VAT and applicable taxes, in line with the local tax regulations.

12.1 Cost Breakdown Template

Bidders are required to submit their financials in the following structure:

A. One-Time Costs

Item Description	Quantity	Unit Price (BDT)	Total Price (BDT)
SIEM-UEBA-SOAR Software Licenses	Lot (100-150 GB/Day)	-	-
Servers (DC 2 and DR 1)	3	-	-
Storage	2	-	-
One-Time Implementation, Integration & Configuration Services	-	-	-
Training & Knowledge Transfer	Lot	-	-
Total One-Time Cost (A)			**BDT XXX৳**

B. Recurring Costs (Annual)

Service	Year 4 (BDT)	Year 5 (BDT)	Total (BDT)
AMC Cost after 3 Years	-	-	-
Total Recurring Cost (B)			BDT XXX৳

C. Total Cost Summary

[redacted]	[redacted]
Total One-Time Cost (A)	BDT XXX৳
Total Recurring Cost over 5 Years (B)	BDT XXX৳
Grand Total (A + B)	BDT XXX৳

12.2 Additional Financial Notes

- Clearly mention the validity period of the proposal (minimum 90 days preferred).
- Include payment milestone proposals tied to deliverables (e.g., advance, post-implementation, post-go-live).
- Specify warranty period and AMC cost beyond the initial 5 years.
- Include any licensing limitations (e.g., EPS cap, number of log sources, storage size).
- No hidden charges will be accepted post-contract award.

Contact Details at The Premier Bank PLC.:

For any clarification, the following addresses can be contacted:

Name of contact at The Premier Bank PLC.	
Name	
Address	
Mobile	
Phone/Fax	
E-mail	
Name	
Address	
Mobile	
Phone/Fax	
E-mail	
Secondary Contact Persons	
Name	
Address	
Mobile	
Phone/Fax	
E-mail	

Contact Details of (Vendor Name):

For any clarification the following addresses can be contacted:

Point of Contact at (Vendor Name)	
Name	
Address	
Mobile	
Phone/Fax	
E-mail	
Technical Support	
Name	
Address	
Mobile	
Phone/Fax	
E-mail	

13 PAYMENT SCHEDULE:

Progress payments subject to certification by the Employer that the Services have been rendered satisfactorily, pursuant to the deliverables. Payments shall be made according to the following schedule:

- All Prices are included VAT and TAX (AIT).
- 5-year Subscriptions while payment would be made on yearly basis in advance.
- All payment made by Bangladesh Currency.

13.1 Payment Terms

The total payment will be given according to the following slabs:

Tenure	Payment Percentage	Milestone
1	50%	After Successful delivery of Hardware and Software
2	30%	After completion of the full SIEM deployment and go-live, a Performance Guarantee (PG) equivalent to 15% of the total contract value shall be retained as security money for the entire warranty period.
3	20%	Payment shall be released upon successful completion of the full SOAR deployment and formal go-live, subject to acceptance by the client.

14 TECHNICAL SPECIFICATION

14.1 General Requirement

Sl.	Parameters	Specification and Standards
1	**Deployment**	One (01) SOC Solution (SIEM+SOAR+UEBA+TIP) For DC and One (01) for DR
2		Solution must be deployed **on-prem/hybrid**
3	**NIC**	Minimum dual 10 Gbps
4	**System Sizing**	**The Bidder must clearly** specify the complete hardware infrastructure requirements, including the number of Physical Servers and/or Virtual Machines for both the **Primary Data Center (DC) and the Disaster Recovery (DR) site.**
5		Detailed specifications must include CPU configuration, RAM capacity, storage type, usable storage size, RAID/redundancy configuration, and any virtualization or platform dependencies. The proposed sizing must be properly calculated based on the bank's estimated daily log volume, Events Per Second (EPS), log retention policy, regulatory compliance requirements, and projected future growth to ensure adequate performance, scalability, high availability, and business continuity.
6		
7		To ensure the proper functioning of the solution, the vendor must provide all required hardware, software, and any other necessary components and support for minimum **05 (three) years.**
8	**Archival Storage**	The proposed SIEM solution shall support archiving of indexed

		data to secondary or long-term storage systems without loss of integrity or accessibility
9		Archival shall allow retrieval and re-indexing of historical data for future investigations and compliance needs.
10		The archival retention shall be definable **as 365 days.**
11		Archived data shall be stored in a compressed and searchable format supported by the SIEM for quick restoration.
12	**Bidder's Skill**	The bidder must guarantee that a minimum of two (02) team members possess valid and up-to-date OEM certifications relevant to the solution being deployed. Proof of such certifications must be submitted as part of the proposal.
13	**Local Training (SIEM+UEBA+TIP)**	Trainer should have professional certification and Experience to provide hands on Training **covering monitoring and day to day operation.**
14		Bidder will arrange all logistic and other support.
15		Bidder will provide training material and course completion certificate to the participants.
16		Duration: **3 days**
17		Persons: **10 persons**
18	**Local Training (SOAR)**	Bidder will arrange all logistic and other support.
19		Trainer should have professional certification and Experience to provide **hands on Training covering installation, configuration, administration, in-depth of all functionality and day to day operation.**
20		Duration: **2 days**
21		Persons: **10 persons**

14.2 Next Gen Security Information and Event Management

1	**Brand**	To be mentioned by bidder
2	**Model**	To be mentioned by bidder
3	**Country of Origin**	To be mentioned by bidder
4	**Recognition**	The proposed SIEM solution should preferably be listed in Gartner's Magic Quadrant
5	**Key Features**	The proposed solution must include Next Gen SIEM, Security Analytics, Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM, UEBA.
6		The proposed solution should be sized for 100-150 GB daily data ingestion 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.
7		To virtually segregate different types of data, proposed solution should support unlimited virtual storage groups or indexes. Each index/ virtual storage group should be used for searching specific data and retention period should be configurable as per indexes.

8		The proposed solution must support the data replication natively without relying on other third-party replication technologies on the operating system or storage level with near zero RPO and RTO. Like big data platforms solution should also allow admin to decide on replication factor within DC and replication factor for DR. DR should always be active and should be updated with artifacts for any incident analyst is working on.
9		The proposed solution should provide a test/dev license as part of the solution. It should also provide a tool in-built or integrable, that allows to create test bed environment which can help to simulate blue team and red team attacks to test use cases, train analysts etc.
10		The proposed solution should be able to receive, ingest and index structured or unstructured data without schema or normalization and no events should be dropped if log source changes the format of log data. Unparsed events should be usable for co-relation and machine learning models.
11		Machine learning should be embedded across the platform (SIEM & UEBA). It should empower every user in the SOC with ML.
12		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 180 days and 365 days of archival. Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re-ingesting security analyst would save storage cost and identify and pinpoint attack intime.
13		The proposed solution should have Out of The Box support for identifying data gap for deploying MITRE ATTACK & Kill Chain use cases. It should help to check data availability and guide on data sources are required to implement MITRE ATTACK Technique & Sub techniques.
14		UEBA should perform identity resolution to find the real-time association between endpoints, IP addresses, host names, endpoint location, and users, and maintain these associations over time.
15		Log Filtering – Not all logs are needed for the compliance requirements faced by organization, or for forensic purposes. Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.
16	**General Specifications**	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.
17		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.
18		The proposed solution must have a user-friendly interface to convert statistical results to dashboards with a single click. The Dashboard should be accessible from the endpoints as & when required.

19		The Proposed solution must offer all the below built-in threat detection techniques out of the box: - Detect Web Application Threats. - Detect APT Threats - Integrate with any Honeypot/Deception solutions - Integrate with any NBAD tools - Detect threats indicated by advisories - Give visibility of endpoints also by integrating with EDR, Antivirus etc. for endpoint analytics.
20		The proposed solution must provide an interface that allows the same query string to be configured as an alert, report or a dashboard panel. Same query string should also be capable of being used for SBDL & SIEM.
21		OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.
22		The proposed solution must be scalable and have a distributed architecture with native replication of data across DC & DR. DR should be active all the time to ensure continuous security monitoring. The dual forwarding feature should be configurable as per bank requirements and capability for enabling & disabling should be available depending on the device, IP address, and other related parameters.
23		The proposed solution must support single site or multiple site clustering allowing data to be replicated across the peer's nodes and across multiple sites with near zero RTO & RPO.
24		The proposed solution must support a configurable replication factor of N where it can tolerate the failure of N-1 peer nodes or should handle failure of a node in the solution.
25		The proposed solution must be software based allowing flexible deployment models and architecture.
26	**Supported Data Sources**	The proposed solution must be able to support both real-time and on-demand access to data sources from files, network ports, database connections, custom APIs and interfaced incl. text, XML, JSON and other evolving format.
27		The proposed solution must be able to read data input from the following log file formats: a. Archived Log Files (Single line, Multi-line, and Complex XML and JSON Structure) b. Windows Events Logs c. Standard Log Files from applications such as Web (HTTP) servers, FTP servers, Email (SMTP/Exchange) servers, DNS servers, DHCP servers, Active Directory servers, etc.

28		The proposed solution must be able to accept the following indicative live data streams feeding through the network: a. Syslog Messages b. Security Alerts c. JSON streaming over HTTP/HTTPS
29		The proposed solution must support the decoding of the following indicative network protocols from log data or picking the meta data from network traffic: HTTP, FTP, DNS, MySQL, SMTP, SNMP, SMB, TCP, UDP,NFS, Oracle (TNS), LDAP/AD, PostgreSQL, Sybase/SQL Server (TDS), IMAP, POP3, RADIUS, IRC, SIP, DHCP, AMQP, DIAMETER, MAPI
30		The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.
31	**Index, Search, Filter, Analyze and Investigate**	The proposed solution must be able to index all data from any application, server or network device including logs, configurations, messages, traps and alerts, metrics and performance data without any custom adapters for specific formats so that the analyst can have end to end visibility of the ecosystem. Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.
32		The proposed solution must be able to build an unstructured index or store data in its original format without any rigid schema.
33		The proposed solution's licensing should be based on post filtering of events. If log events are filtered, then they should not be counted in license.
34		Proposed solution should forward data to multiple destinations apart from its own SIEM processing/data storage layer. Log collector should be able to forward data to multiple destinations.
35		The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events.
36	**Monitor, Alert and Reporting Functions**	The proposed solution must be able to run any search on a schedule and set alerting conditions based on thresholds and deltas in the number and distribution of results across a time range or days like a histogram visualization.
37		The proposed solution must be able to execute automated corrective or follow-on actions via scripted alerts.

38		The proposed solution must support viewing of the same log data in different formats or should support multiple schema views during search time or report building time without redundant storage or re-indexing so that complex report or user defined reports can be built.
39		The proposed solution must be able to support sophisticated statistical and summary analysis by pipelining advanced search commands together in a single search.
40		The proposed solution must be able to support mathematics functions to perform calculations on field values, examples Converting bytes to kilobytes, mega-bytes, absolute value functions, highest integers, standard deviation, command length etc. Finding the time duration between time stamp values. These functionalities should be available as a search, report, alert or dashboard etc. so that analyst can build any kind of report required.
41		The proposed solution must be able to support predictive analytics to predict future values of single or multi-valued fields. This will help security analytics to predict the attack patters or specific attacks using multiple fields in the alerts or logs. Indicative Use Case: Predicting Malware spread based on previous malware attack patterns.
42		The proposed solution must possess built-in function for Predictive Analysis: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results Indicative Use Case: If the system performance is degraded or Memory/CPU utilization is high then Analyst can know from single console weather this is due to a DDOS Attack or Malware outbreak or due to some IT issue. This helps to reduce the false positive and improve response time.
43		The proposed solution must come with pre-packaged alerting capability, flexible service-based hosts grouping, and easy management of many data sources, and provide analytics ability to quickly identify performance and capacity bottlenecks and outliers in Unix and Linux environment. It should quickly compare resources and capacity utilization across many hosts Indicative Use case: Visibility of services running on servers are also critical to monitor. These could be impacted due to any security incident. Overall performance of the system may get impacted etc. Hence if a SOC analyst has all this view from central platform, then this helps to reduce the time to identify and fix any issue.

44		The proposed solution should provide dashboards for insight into resource consumption of desired systems, service availability status of critical services, integration with NMS tools for network status visibility, security alerts, risky users & entities, anomalies and outliers across all the data etc. from a single dashboard. Indicative Use Case: To have a single view of entire bank by integrating with NMS and other tools giving the security posture & IT posture status to track issues and fix them immediately.
45		The proposed solution must possess built-in feature for anomaly detection: a. Uses historical data as a baseline to forecast future patterns, thresholds and tolerances b. Ability to identify the future needs of critical system resources, no prior knowledge in predictive modeling algorithms required to use this functionality, and the ability to easily interpret and customize the results
46		The proposed solution should give visualization of operational health of the Windows, Linux & Unix environment through a single dashboard customizable to service-groupings in your environment Indicative Use Case: To have a Single dashboard which can help analyst to identify the real cause of performance degradation which could be due to a security issue or due to any other IT issue.
47		The proposed solution report or table must be able to be embedded in third-party business applications incl. Email, SharePoint, WordPress, Wiki, WhatsApp etc.
48	**Machine Learning**	The proposed solution must provide GUI that can easily help to build, built-in or custom machine learning models using the pre-defined sequence and should be able to integrate with a collection of NLP and classical machine learning libraries, generic machine learning tools like tensor flow, pytorch, R, Python, Scala etc.
49		The proposed solution machine learning capabilities must include API access, role-based access controls for machine learning models.
50		The proposed solution machine learning capabilities must allow addition of custom machine learning algorithms from popular open-source libraries like NL, Python etc.
51		The proposed solution should natively have ML capabilities and should not have separate engine/compute requirements for running ML models.
52	**Search and Reporting**	Reports can be scheduled in a dynamic fashion with schedule windowing and prioritization to improve run priority of high value scheduled reports and manage concurrently running reports to meet the requirements of completing reports under 24 hours. The report should be parameterized, and the user should be able to scale the parameter as needed. And out of box aging analysis of incident should be available.

53		The solution must provide drill down functionality that is user defined, allowing users to drill down into another report, dashboard, raw events or passing URL parameters to any third-party website. The Report should be scalable IP-wise, device-wise, user-wise, data-wise, location-wise based on requirement between any two dates.
54		The product internal logs must be ingested within the product for ease of troubleshooting and investigation and those logs do not consume the product license. investigation and those logs do not consume the product license. The SIEM platform should be able to ingest logs, events, Metrics and Traces.
55		The solution must provide granular license utilization down to devices, log sources and data store or additional lookups of devices to agencies by the minute and the retention of granularity can be extended to the project requirement.
56		The solution must provide the same search language for search, investigate, alert, report and visualize license utilization. A proper error handling screen should be available.
57		The solution's reports should run fast on large data sets. Proposed solution should use next generation functionalities like creating set of data from the main index or data store. This will avoid running the queries on large index or full index and faster response for searching and reporting.
58	**Fields, Schema and Log Parsing**	The solution must support viewing data in different formats or schemas without re-ingesting, re-indexing, redundant storage. Historical data also should be viewed as per new format or schema without re-ingesting or without additional storage utilization. Indicative Use Case: Referencing old data for predictive analytics, proactive monitoring etc. By not re-indexing and re- ingesting security analyst would save storage cost and identify and pinpoint attack in time.
59		The solution must allow the adding/modifying/removing of log parsers without impacting log collection from the web interface.
60		The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface.
61		Old data should be parsed with new parser without re-ingesting or re-indexing the data.
62	**Security Analytics Platform**	The proposed solution must provide the following capabilities as a Security Analytics Platform: a. One single syntax that can be used universally for search queries, alerts, reports or dashboards, SIEM, SBDL. b. Incident management technique to facilitate incident tracking, investigation, pivoting and closure c. Risk management technique to apply risk scores to any asset or user based on relative importance or value to the business d. Threat intelligence technique that automatically collect, aggregate, deduplicate indicators of compromise from threat feeds

63		The proposed solution must be fully integrated with the log platform without the need to duplicate the collected raw logs.
64		The solution should be able to assign risk score with Scoring for various identified entities like user & assets should be possible based on the threats or correlations that particular host, username, entity, location has contributed. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.
65		The proposed solution must be able to assign any arbitrary risk score based on self-defined query based on any correlated events, statistical analysis, threat indicator match. Indicative Use Case: Risk Score of User or Entity in the organization is calculated to reduce false positives and identify critical incidents by assigning the risk score of each and every subsequent offence and calculating the overall risk score based on the offenses by each entity or user.
66		The proposed solution must be able to retrieve from any threat feeds without restriction, retrieve threats in various ASCII/UTF- 8 file formats like text, csv, xml. Must be able to automatically parse IOC from STIX and Open IOC formats. Must be able to support multiple transport mechanisms such as TCP or Trusted Automated exchange of Indicator Information (TAXII).
67		The proposed solution must be able to support the following indicative list: - **Network:** HTTP Referrer, User Agent, Cookie, Header, Data, URL, IP, Domain - **Endpoint:** File Hash, Name, Extension, Path and Size, Registry Hive, Path, Key Name, Value Name, Value Type, Value Text, Value Data, Process Name, Arguments, Handle Name, Handle Type, Service Name, Description - **Certificate:** Certificate Alias, Serial, Issuer, Subject, Start Time, End Time, Version, Handshake Type, Public key Algorithm, Signature Algorithm - **Email:** Email Address, Subject Body
68		Beside event matching signature use cases, the proposed solution must have the following analytical capabilities to address anomalies and behavioral based use cases.
69		Basic Statistical analysis that can be applied to any fields like calculating the length of command line arguments, HTTP user agent string, sub domains, URLs, standard deviation of count of events over time
70		The proposed solutions should use Using distance formula to detect geographically improbable access
71		The proposed solutions should use randomness to measure domain names that can be potentially from malware domain generated algorithms. Indicative Use Case: Detect DGA using randomness. Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of

		domain names hence above methodologies are required in proposed solution to detect such attacks
72		The proposed solution should use statistic functions or techniques like percentile or standard deviation to detect unusual activities that can be applied to insider or fraudulent use cases. Other analysis: Find common or rare events using cluster or most commonly and widely used means clustering method Find percentage of times two fields exist in the same events correlating all the fields. Indicative Use Case: Analyst should be able to see an overview of the co-occurrence of fields in data. It should give the percentage of times that the two fields exist in the same events. This will help analyst to see the relationship among all the fields in a set of results
73		The proposed solution should find relationship between pairs of fields by change in randomness in pair of fields. Indicative Use Case: This helps to predict the value of another field by knowing the value of one field.
74		The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT&CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per bank requirements.
75		The proposed solution should also guide administrator on data sources required to implement detection technique from the same console (ATTACK MITRE, CIS, NIST, Kill Chain etc.)
76	**Incident Response**	The proposed solution must provide investigation auditing capability to enable analysts to easily: Track searches and activities Review activities at any point Select and place into timeline for temporal analysis Help remember searches, steps taken, provide annotation support
77		The solution must be able to provide a built-in facility to centralize incident analysis of entities in one location.

78		The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.
79		The proposed solution should have integration with major commercially available tools OOTB for triggering actions or integration with all commercially available SOAR for initiating action to be taken.
80	**Bidder's Skill**	The bidder should have at least 2 (Two) Certified resources on the proposed solution.
81	**License, Warranty/RMA and TAC support**	Bidder must offer necessary license & subscriptions for three years
82		Bidder should provide minimum 5 (Five) years warranty for proposed solution including support, patch, software update & upgrade.
83		Bidder must submit the required performance document or manufacturer authorization form or compliance reference document for the proposed solution.

14.3 User and Entity Behavior Analytics

Item No	Item or Related Service	Technical Specification and Standards
1	**Brand**	To be mentioned by bidder
2	**Model**	To be mentioned by bidder
3	**Country of Origin**	To be mentioned by bidder
4	**Key Features**	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modelling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning and other statistical analysis techniques. The bidder must provide licenses for all specified assets from Day 1 of implementation.
5		Proposed solution should use behavior modelling, peer-group analysis, and machine learning to uncover hidden threats in our environment. It should automatically detect anomalous behavior from users, devices, and applications, combining those patterns into specific, actionable threats.
6		The proposed UEBA solution should perform identity resolution to find the real-time association between IP addresses, host names, endpoints, endpoints location and users, and maintain these associations over time.
7		Investigate and respond to detected threats using a streamlined threat review workflow that provides visibility into anomalous activity and supporting evidence. Should increases the effectiveness of our security analysts by helping them focus on threats and malicious activities with kill chain and geographical visualizations.
8		Proposed solution should detect threats by normalizing device and domain names, and associate all accounts identified in our HR data with a single human user.

9		The proposed solution should use unsupervised machine learning algorithms to analyze the data for activity deviating from normal behavior.
10		The proposed solution should have threat detection technique and models to distil anomalies down to a real handful threat. A single violation might not represent a legitimate threat in our environment. Over time, however, a series of violations should tell a story about a threat that must be investigated. Threat detection models should stitch together anomalies to provide an end-to-end story about a high-fidelity threat.
11		Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields.
12		The proposed solution should have anomaly detection models to analyze the data in UBEA and create anomalies or violations based on a variety of factors.
13		The proposed solution should be able to create new anomaly detection models or clone existing models from the GUI.
14		The above categories typically should correspond to stages of the kill chain and make it possible for the threat logic to place anomalies into the correct sections of the chain.
15		The proposed solution should find deviations from typical behavior or detection of interesting patterns like beaconing.
16		The proposed solution should detect threats using graph-based threats, which are computed based on groups of similar anomalies rather than anomalies grouped by user or device. Example graph-based threats are public-facing website attack or fraudulent website activity.
17		The proposed solution should detect threats like Lateral Movement and Data Ex-filtration. These should collect data about anomalies and users or devices to determine the likelihood of a threat.

14.4 Security orchestration, automation and response (SOAR)

Item No.	Item of Related Service	Technical Specification and Standards
1	**Brand**	To be mentioned by bidder
2	**Model**	To be mentioned by bidder
3	**Country of Origin**	To be mentioned by bidder
4	**License & Subscription**	The proposed SIEM solution should be integrated with SOAR & UEBA solution seamlessly. Bidder should offer min 2 or more Users License for SOAR effect after 6 months.
5		Bidder must offer necessary license & subscriptions for three years
6	**Key Features**	The proposed solution must have an orchestrator ability to direct and oversee all activities from beginning to end.

7		The proposed solution orchestrator must be able to ingest security data from any source and in any format. Example: Email based alerts SIEM based alerts
8		The proposed solution orchestrator must be able to poll data sources or pull data into the platform.
9		The proposed solution orchestrator must be able to interpret the data and make it usable by the platform. Example: extracting indicators from emails IP Address Domains File Hashes
10		The ability to extract indicators from various files attachments such as PDFs, emails, or raw text. Example: txt .eml like Outlook Email Messages pdf docx csv html
11		The proposed solution orchestrator must be able to initiate automation upon creation of new events with artifacts or existing events with new artifacts without human intervention.
12		The proposed solution orchestrator must be able to dispatch automation tasks from its queue at the appropriate and optimal time, passing them to the automation engine for execution.
13		The proposed solution orchestrator must be able to introduce human supervision if necessary, pausing the automation engine for an approval by asset owner is needed to execute a security action on a target.
14		The proposed solution orchestrator must ensure output data from one action is properly parsed, so that future actions can make use of it.
15		Consistent, Standardized naming conventions for actions. Normalized action names in a Virtualization/Abstraction layer allows easy transition across API action calls and/or products
16		The proposed solution built-in visual automation editor must enable users to construct comprehensive and sophisticated playbooks to fully validate, investigate and resolve incident using drag and drop capabilities visually without needing the expert ability to code.
17		The proposed solution built-in visual automation editor must be able to represent code using blocks and blocks can be connected in a one-to-one, one-to-many and many-to-one fasion to dictate an order of execution.
18		The proposed solution built-in visual automation editor must be able to provide an interface where testing and debug can take place allowing transition from edit mode to test mode seamless.
19		The proposed solution must provide an open and extensible interface for new integrations to connect the platform to any of the thousands of point products available in the security market

		today.
20		The proposed solution must provide easy transition in and out of other security technologies without negatively impacting automated playbooks.
21		The proposed solution must provide users with the framework and open control of integrating with other technologies without relying on the solution provider for development work.
22		The proposed solution must standardize on one language like Python for developing integrations with other technologies for custom actions and custom handling of playbooks confined in a block while retaining the original visual playbook editor functionality for the entire playbook.
23		The ability to run multiple playbooks and actions while retaining the data in the containers/events/cases.
24		The proposed solution should have customizable playbooks designed as per SOC Analyst requirements.
25		Retaining the data of all multiple runs of playbooks ensure the retention of key artifacts especially with dynamic information like reputation information.
26		The proposed solution must have documented REST API access that allows full control over the platform.
27		The proposed solution must have ability to label the nature of the event.
28		The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.
29		The proposed solution must be able to extract and store attachments from ingested emails.
30		The proposed solution must have the ability to mark artifacts as evidence.
31		The proposed solution must be able to provide an indicator view to quickly pivot investigation of an indicator to past incident occurrences.
32		The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.
33		The proposed solution must provide fine grained role-based access into actions and assets, so users can be granted with investigative actions and not containment actions.
34		The proposed solution should have an out of the box guidance by offering suggestions to help investigate, contain, eradicate, and recover from a security event, allowing newer analyst to take and validate choices of more experienced analysts.
35		The proposed solution must have an activity log of actions taken (automated and manual), results returned by actions, chat and comment history in each event.
36		The proposed solution must provide central management of incidents and administrative functions from a single web-based user interface.

37		The proposed solution must provide multi-tenancy support allowing multiple departments or business units to use the same solution with appropriate segregations/separations.

14.5 Technical Specification for Threat Intelligence Platform (TIP)

SL	Parameter		Technical Specification/Standard
1	In -Built Threat Intelligence with SIEM and SOAR	Threat Intelligence Integration	The proposed SIEM solution must support ingestion and integration of multiple threat intelligence feeds, including commercial, open-source, and organization-specific feeds.
2			The solution should support threat intelligence formats such as STIX (Structured Threat Information Expression), TAXII (Trusted Automated exchange of Indicator Information), JSON, CSV, and XML
3			The SIEM shall allow real-time correlation of ingested logs with threat intelligence indicators.
4		Indicators of Compromise (IOC) Management	The system must support ingestion, storage, and search of various IOC types, including IP addresses, domains, URLs, file hashes, email addresses, and registry keys.
5			IOC (Indicator of Compromise) data must be searchable, filterable, and taggable for efficient investigation.
6		Automated Threat Correlation	The solution must automatically match and alert on security events that correspond to threat intelligence IOCs.
7			It shall support risk scoring based on severity and confidence levels of matched IOCs.
8		Custom Threat Intelligence Feeds	The solution shall allow administrators to create, import, and manage custom threat intelligence lists and rules.
9			The solution must support manual IOC input through the user interface or API.
10		Threat Intelligence Sharing	The system should support exporting relevant threat intelligence data in standardized formats for sharing with trusted partners and regulatory bodies.
11			It must comply with information sharing standards such as STIX/TAXII.
12		Automated Updates	The solution must be capable of automatically updating threat intelligence data on a configurable schedule.
13			The system must provide alerting in case of feed update failures.

14		**Integration with Security Ecosystem**	The solution must allow integration of threat intelligence with firewalls, intrusion detection/prevention systems, EDR, and SOAR platforms for automated response.
15			The threat intelligence module must support REST APIs for integration with third-party systems.
16		**Visualization and Reporting**	The system must provide dashboards and visualizations to show IOC matches, trends, and top threats.
17			The solution must generate scheduled and on-demand reports of threat intelligence activity.

2/4/26
Muhammad Saddam Khaleed
SAVP, IT Security & Governance Division

2/4/26
Kh. Golam Sarwar
SAVP & Head of
IT Security & Governance Division

02/04/26
Md. Naquibul Islam
SEVP & CRO (CC)