

RFP Reference: UHS/IT/TENDER/041/2026

1st October 2026

RFP Closing Date: 22nd October 2026

No.	Description
1	Security Information and Event Management (SIEM) Solution

University Hospital Sharjah. (UHS) Management has decided to invite vendors for a Request for Proposal (RFP). You, as a vendor are requested to participate in the RFP process by submitting your offer to provide the services as described in this document.

The RFP should comply with the following terms & conditions:

1. The proposal shall be clear, informative & include as per the requirement described in the RFP.
2. The financial offer should be on your company letterhead containing the authorized signatory and must be sent to the attention of the Director of Finance, **University Hospital Sharjah, PO Box 72772, Sharjah in a sealed document.**
3. The price quoted is as mentioned in the technical requirement listed below (RFP) to UHS.
4. All deliveries should be made for the ordered quantity in full, without partial shipments, to our Main Warehouse, located in UHS vicinity or as specified on the Purchase Order/ Contract. Failure to comply with the agreed delivery schedule or any shortfall in quantity may result in penalties or contract termination, as per the Purchase Agreement Terms and Conditions.
5. As a part of the RFP document, the Vendors are requested to provide their valid Trade License, Name, and Designation of the Managing Director/General Manager/Sr. Manager having the authority to bind their company for the business relationship. Also, the vendors are required to provide licenses, certificate confirming that the vendor is legalized to operate the proposed business activity. As well as the following documents:
 - a) Valid Trade License
 - b) Updated Company Profile
 - c) Tax Registration Certificate (TRN)
 - d) Full Company Address & Contact Details
 - e) Memorandum of Association (MOA) and Power of Attorney (POA) for authorized signatory (if applicable)
 - f) An official Authorization Letter/Agency Certificate, confirming the vendor's legal authorization to supply the specified items on behalf of the manufacturer or principal company.
 - g) Any additional approvals or compliance documents mandated by government authorities for the supply of the specified equipment.
 - h) Non-Liability Letter and Legal Clearance Confirmation.
 - i) Insurance Policies (General Liability, Professional Indemnity, etc.).

- j) Declaration of No Ongoing Legal Disputes.
 - k) Vendor Code of Conduct Acknowledgment.
6. Standard payment terms are 90 days from the date of completion of delivery of supplies/ services or as specifically agreed in purchase contract/ agreement.
 7. Any delays or non-conformance may result in the termination of Services agreement and/or imposition of penalty for delayed services as per the Services Agreement terms and conditions. **A performance bond may be required to ensure commitment to the agreed timelines and quality standards.**
 8. The proposed services shall be evaluated & approved by UHS's before confirmation. Once the agreement is signed off, the services will have to correspond to the required services with specific time-frame, and as originally proposed, agreed and any deviations shall be considered a breach of service contract/agreement.
 9. The specified brand and manufacturer must remain unchanged throughout the contract period unless otherwise approved by UHS in writing.
 10. UHS will be constantly evaluating the compliance of Contract/Agreement Terms and consistency in performance of the services throughout the duration of the agreement.
 11. Vendors are required to submit regular progress reports at agreed intervals detailing progress, challenges, and actions to address any delays or issues. Should Vendors not meet the requirements of UHS, UHS reserves the right to terminate the agreement if the vendor is not able to rectify during the time allotted by UHS's representative.
 12. Vendor Contact details (landline, mobile, emails) of the authorized representatives should be mentioned.
 13. **Tenders should be submitted in two sealed envelopes and submitted to the Administration Office Finance Department- UHS:**
 - a. **The Technical Specification details (PLEASE DO NOT INDICATE ANY FINANCIAL VALUE IN THIS).** If requested for additional clarifications and details these need to be submitted to **(Administration Office Finance Department- UHS).**
 - i. The offer should must conform to the RFP Document as per the attachment.
 - ii. The offer shall be submitted (hard copy and soft copy saved in USB).
 - iii. Reference Project/Hospital where similar work was performed.
 - b. **The Financial Offer** addressed to UHS's Director of Finance, with **tender reference.**

All above documents should be submitted before the tender expiry date, all documents submitted after the expiry date will not be accepted.
 14. UHS shall have no obligation to accept any tender proposal submitted by any vendor. UHS may at its sole discretion and without providing any reason, accept or reject any or all

proposals, in whole or in part. Such rejection shall not give rise to any claim, liability, or cause of action of any kind by the vendor against UHS.

15. Submission of a tender proposal shall not create an agreement, legal or other relationship between the vendor and UHS. No vendor shall acquire any rights, interests, or claims against UHS by submitting a proposal, participating in the tender process or relying on any communications related to the tender.
16. In the event UHS accepts a tender proposal of a vendor, the parties agree any such tender award will be subject to a Services Agreement and separate agreement outlining the specific terms and conditions of the project and services agreed.
17. All costs, expenses or losses incurred by the vendor in connection with the preparation, submission or presentation of its proposal shall be borne solely by the vendor. UHS shall have no liability, under any circumstances to reimburse, compensate or indemnify the vendor whether in part or in whole for such costs or expenses.
18. The vendors acknowledge and agree that they have not relied on any statement, representation, warranty, or promise made by UHS, whether oral or written, in preparing their tender proposal and all decisions and judgements regarding the submission of their proposal are made at their own discretion and risk.
19. UHS may at any time without liability, amend, suspend, or withdraw the tender invitation in whole or in part. UHS may also request additional information, clarifications or documents from any vendor and may reject any proposal that is incomplete, unclear or does not comply with the tender requirements as outlined in this document.
20. Quality, Price, and service are combined parameters for tender evaluation. Once a vendor has been selected, a negotiation period will follow to allow both parties to review the agreement terms thoroughly. This will ensure that all deliverables, KPIs, and expectations are clearly outlined before the final agreement is signed.
21. Vendors must submit a risk management plan, identifying potential risks to the project, such as security and confidentiality breaches, system failures, and disruptions to delivery schedules. Vendors should outline how they intend to address these risks, including their disaster recovery and business continuity plans.
22. Vendors are encouraged to adhere to ethical practices and sustainability standards in their operations. This includes providing energy-efficient equipment and adopting environmentally friendly practices in their supply chain and delivery.
23. The Vendor, its employees, its subsidiaries, and everyone who has a direct or indirect relationship with implementing and securing the works and Services included within the scope of this tender, shall be obligated to inform UHS and disclose in writing any case of conflict of interest or any private interest that has arisen, will arise, or may arise. For any transaction related to the activities of UHS, in accordance with UHS policies.
24. The vendor, its employees, and subsidiaries shall be obligated to maintain confidentiality of any data, drawings, documents, or information related to the tender - written or oral. Vendors must ensure that any data shared is protected by encryption standards and secure transfer protocols. Additionally, vendors are required to notify UHS of any data breaches immediately. Compliance with relevant data privacy regulations (e.g., GDPR, UAE Data Protection Law) is mandatory. This includes all dealings, affairs, or secrets related to UHS they may have encountered during the tender process. Vendors shall not be allowed to disclose any information related to the tender through any media outlet without obtaining prior written approval from UHS.
25. The copyright, rights and ownership of any documents, materials and information submitted by UHS within this tender is owned by UHS, and accordingly, these documents and materials

may not be copied, in whole or in part, or reproduced, distributed, made available to any third party, or used without obtaining prior written approval from UHS. If the vendor develops any custom software or systems for UHS as part of this tender, UHS will retain ownership of the intellectual property or have clear licensing terms for its continued use. All documents submitted by the UHS in connection with the request for proposals shall be returned upon request without any copies being retained by the bidder or any other person.

26. The vendors shall indemnify, defend and hold harmless UHS, its officers, employees and agents from and against any and all claims, liabilities, losses, damage costs, or expenses arising out of or in connection with:
 - a. the vendors participation in the tender process
 - b. any errors, omissions, misrepresentations or inaccuracies in the proposal
 - c. any breach of the vendors' obligations under this tender invitation
27. To the maximum extent permitted by law, UHS expressly excludes any liability for:
 - a. Any direct, indirect, incidental, consequential or special losses
 - b. Loss of profits, revenue, goodwill or business opportunities
 - c. Any claims by third parties arising from a vendor's proposal
 - d. Any loss or damage caused by errors, omissions or delays in the tender process
28. This tender invitation and all matters relating to it shall be governed by any construed in accordance with the laws of the United Arab Emirates. The competent courts of Sharjah, United Arab Emirates shall have exclusive jurisdiction over any disputes arising from or in connection with this tender.
29. This document and clauses therein constitute the entire understanding between UHS and any vendor regarding liability, proposal submission, and the tender process. No other communication, agreement or understanding, whether oral or written shall be deemed to modify, supersede, or expand these clauses.

University Hospital Sharjah

REQUEST FOR PROPOSAL (RFP)

Security Information and Event Management (SIEM) Solution

1. Introduction and Objective

UHS invites qualified vendors to submit proposals for the supply, implementation, configuration, integration, and principal vendor support of an enterprise Security Information and Event Management (SIEM) solution. The objective is to establish centralized security monitoring and log management to improve visibility, detect and investigate threats, support incident response, and meet applicable audit and regulatory requirements.

The proposed solution shall provide centralized log collection, normalization, correlation, analytics, alerting, investigation, reporting, retention, and administration for the organization's IT and security environment.

2. Scope of Work

- Supply and licensing/subscription of the proposed SIEM platform. Required information for the sizing will be provided during the product evaluation.
- Solution assessment, architecture, sizing, installation, configuration, and commissioning.
- Integration of agreed infrastructure, security, application, and cloud log sources.
- Configuration of security use cases, correlation rules, dashboards, alerts, and reports.
- Log retention, archival, search, and integrity controls.
- Testing, tuning, User Acceptance Testing (UAT), documentation, knowledge transfer, and administrator training.
- Technical support, maintenance, software updates, upgrades, and escalation support.

3. Technical Requirements

3.1 Log Collection and Management

- Collect logs centrally using agent-based and/or agentless methods and support standard methods such as Syslog, Windows Event Collection, APIs, database/file connectors, and other supported native connectors.
- Normalize and parse logs from different sources; support real-time and scheduled collection and alert on collector/log-source failure.
- Maintain confidentiality, integrity, and secure transmission of logs; prevent unauthorized modification or deletion.
- Provide high-performance search, filtering, drill-down, compression, archival, and configurable online/offline retention.
- Support scalable ingestion and clearly state licensed capacity in EPS and/or GB per day.

3.2 Integration Requirements

The solution shall support integration, where technically applicable, with the following environment. Any connector or functionality requiring an additional license shall be clearly identified.

- Microsoft Active Directory, Windows Servers, Exchange, Microsoft 365, and related Microsoft services.
- Firewalls, VPN, routers, switches, wireless infrastructure, and other network/security devices.
- Endpoint security/EDR, antivirus, PAM, NAC, vulnerability management, and other cybersecurity solutions.
- VMware/virtualization, Linux servers, databases (MSSQL, SAP HANA, IRIS), web/application servers, storage, and backup systems.

- PACS and other critical healthcare systems where standard integration methods are available.
- External systems through APIs, Syslog, webhooks, or other supported standard interfaces.

4. Security Monitoring, Detection and Threat Intelligence

The SIEM shall provide real-time monitoring, correlation, prioritization, and alerting. It should support creation and customization of use cases and rules by UHS administrators without vendor dependency for routine changes.

At minimum, the solution should support detection/use cases for:

- Brute-force attacks, repeated failed logins, suspicious authentication, impossible/abnormal logins, account compromise, and unauthorized access attempts.
- Privileged account misuse, creation/modification of privileged accounts, administrative changes, and security policy violations.
- Malware/ransomware activity, endpoint security alerts, suspicious PowerShell/command-line activity, and disabled security controls/logging.
- Communication with known malicious IPs/domains, firewall/VPN anomalies, unusual network activity, and potential data-exfiltration indicators.
- Changes to critical systems and modification/deletion of security or audit logs.

Threat Intelligence: The solution should integrate with multiple threat-intelligence sources, correlate indicators such as malicious IPs, domains, URLs, and hashes with internal events, and allow customer-provided feeds. Detection content should support mapping to the MITRE ATT&CK framework where applicable.

5. Incident Investigation and Alerting

- Centralized security operations console with real-time alerts, severity classification, prioritization, event correlation, and incident timelines.
- User/host investigation, historical search, drill-down from incidents to original events, and related-event context.
- Incident assignment, status tracking, analyst notes/comments, and email notifications.
- Integration capability with ticketing or incident-management platforms.
- Capabilities for duplicate-alert suppression, tuning, and reduction of false positives.

6. Dashboards, Reporting and Compliance

The solution shall provide customizable dashboards and scheduled/on-demand reports for security incidents, alert severity, authentication, privileged activity, firewall/VPN events, endpoint/EDR alerts, attack sources/targets, trends, and log-source health. Reports should be exportable to commonly used formats such as PDF, CSV, and Excel and support internal audit, cybersecurity assessment, and applicable regulatory/compliance requirements.

7. Access Control and Platform Security

- Role-Based Access Control (RBAC), Active Directory integration, and Multi-Factor Authentication capability.
- Separation of administrator/analyst privileges and complete audit trail of administrative/configuration activities.
- Encryption of data in transit and protection/encryption of sensitive stored information.
- Secure communication between collectors, log sources, and SIEM components.

8. Architecture, Availability and Sizing

The vendor shall propose an architecture suitable for the current environment and future growth and shall clearly identify all components, server/VM requirements, CPU, memory, storage, network requirements, collectors, high availability, disaster recovery options, and scalability limits. The proposal shall state whether the solution is on-premises, cloud, and where organizational log data will be stored and processed.

The vendor shall specify expected EPS and/or GB/day capacity, supported log-source count, storage sizing assumptions, compression ratio, online/searchable retention, archive retention, annual growth assumptions, and any licensing impact associated with increasing ingestion or retention.

9. Implementation Requirements

1. Project kickoff and existing-environment assessment.
2. Solution design, architecture, sizing, installation, and configuration.
3. Integration and validation of agreed log sources.
4. Configuration of agreed security use cases, dashboards, alerts, reports, and notifications.
5. Tuning, testing, UAT, production handover, and implementation completion report.
6. Administrator training, knowledge transfer, and delivery of technical/operational documentation.

The vendor shall submit an implementation plan including key milestones, responsibilities, prerequisites, dependencies, and expected project duration.

10. Documentation and Training

The successful vendor shall provide solution architecture, installation/configuration details, integrated log-source inventory, SIEM administration guide, configured use-case list, backup/recovery procedures, and operational troubleshooting documentation. Authorized virtual classroom administrator training interactive, live, instructor-led sessions (or) pre-recorded material and knowledge transfer shall be included for the UHS IT/Security team.

11. Support and Maintenance

- Clearly state support period, service hours, and 24x7 support availability for critical incidents.
- Provide SLA/response targets for Critical, High, Medium, and Low severity incidents and define escalation procedures.
- Include software updates, upgrades, security patches, and applicable principal/manufacture support.
- Clearly state remote and onsite support availability and local UAE support capability.

12. Licensing and Commercial Requirements

The vendor shall clearly explain whether licensing is based on EPS, GB/day ingestion, devices/log sources, users, nodes/workloads, storage capacity, or a combination. The proposal shall include sufficient capacity for the current environment with future growth and identify any additional licenses for connectors, collectors, APIs, reporting, threat intelligence, analytics, storage, or other mandatory functionality.

The commercial proposal shall separately identify SIEM licenses/subscription, required hardware (if applicable), implementation/professional services, integration, training, support/maintenance, optional components, annual renewal/subscription costs, additional ingestion/storage costs, and third-party licenses. The complete solution shall be priced without hidden mandatory components.

13. Vendor Response / Compliance Summary

Requirement	Vendor Response
Architecture & Sizing – Servers/VMs, CPU, RAM, storage, collectors, and network requirements	
Licensing Model – EPS, GB/day, devices, log sources, users, storage, or other parameters	
Log Collection Capacity – Supported EPS and/or GB of logs per day	
Log Sources & Integration – Windows, AD, Linux, firewalls, switches, routers, VPN, EDR, NAC, PAM, databases, VMware, and applications	
Agent / Agentless Collection – Syslog, Windows Events, APIs, SNMP, database connectors, etc.	
Real-Time Monitoring & Correlation – Real-time monitoring, normalization, correlation, and alerting	
Security Use Cases – Predefined and customizable use cases and correlation rules	
Threat Detection – Brute-force, compromised accounts, malware, ransomware, privileged misuse, and suspicious activities	
Threat Intelligence – Integration with threat intelligence feeds	
MITRE ATT&CK – Mapping of alerts and detections to MITRE ATT&CK	
Incident Investigation – Timeline, drill-down, historical search, user/host identification, and incident tracking	
Alert Management – Severity-based prioritization, notifications, duplicate suppression, and false-positive tuning	
Dashboards & Reporting – Customizable dashboards, scheduled reports, and export options	
Log Retention – Online/searchable and archived log retention	
Log Integrity – Protection against unauthorized modification or deletion of logs	
Access Control – RBAC, Active Directory integration, and MFA support	
Encryption – Encryption of data in transit and at rest	
High Availability – HA capability and architecture	
Scalability – Support future growth in log sources, EPS/GB per day, users, and retention	
Health Monitoring – Monitoring of collectors, log sources, ingestion, storage, and SIEM components	
Support & SLA – 24x7 critical support, SLA, escalation, and local UAE support	
Software Updates & Support – Upgrades, updates, patches, and vendor/principal support	
Additional Components / Cost – Any additional licenses, hardware, storage, connectors, modules, or third-party costs	

14. Evaluation Criteria

Proposals will be evaluated based on technical compliance, security monitoring/detection capabilities, integration coverage, scalability/performance, administration and reporting, implementation methodology, support capability, licensing flexibility, vendor/principal experience, and total cost of ownership. UHS may request technical demonstrations, a Proof of Concept (POC), clarifications, or additional information before final selection.