Tender Reference: UHS/IT/TENDER/028 /2024
Tender Issue Date: 1st October.2024
Tender Expiry Date: 31st October 2024 - Extended

Subject: IT Infrastructure Monitoring & Security Project

Dear Valued Vendors,

The management of **University Hospital Sharjah (UHS)** has decided to invite vendors to participate in the tender process for the project detailed above. You are cordially invited to submit your proposals to supply one or more of the items outlined in the attached documents.

The Tenderer is expected to adhere to the following terms and conditions:

1. The specifications of the proposed services and materials must be comprehensive and informative, clearly detailing the Brand, Origin, Unit of measurement, Quantity, Duration, Delivery Method, and Period. Vendors are also required to provide performance criteria, compatibility with UHS's existing IT infrastructure, mandatory warranties or support services, and any necessary certifications, such as ISO standards for quality and cybersecurity.

2. The quoted price should align with the technical requirements in the attached document. This must be addressed to University Hospital Sharjah.

3. The financial offer must be submitted on your company's official letterhead, signed by an authorized representative, and delivered in a sealed envelope to the attention of the Director of Finance, **University Hospital Sharjah, PO Box 72772, Sharjah, in a sealed document**. The financial offer must include a clear cost breakdown by item (equipment, support, training, maintenance), as well as details of any potential additional charges that may arise during the project. UHS requests fixed pricing terms throughout the duration of the contract.

4. All deliveries should be made in full for the ordered quantity to our Main Warehouse, located in the UHS vicinity, or as specified on the Purchase Order/Contract.

5. As a part of the Tender document, the Vendors are requested to provide their valid Trade License, Name, and Designation of the Managing Director/General Manager/Sr. Manager has the authority to bind their company for the business relationship. Also, the authorization letter/Agency certificate is required to confirm that the vendor is legalized to supply the items on behalf of the manufacturer/principal company. Additionally, vendors must submit proof of compliance with relevant local regulations, including VAT registration and applicable certifications in IT security and data protection, such as ISO/IEC 27001, as well as the following documents:

    a) Updated company license/ MOA/ POA for the signatory (if any)

    b) Company profile

    c) Tax registration certificate

d) Full company address

e) Non-conflict of interest declaration letter and disclosure of any COI

f) Any other documents/approval required by the government authorities to supply the same equipment

6. Payment terms are standard at 90 days from the date of full delivery of the ordered items unless otherwise agreed upon in writing with UHS's Materials Management Department.

7. Any delays, short supplies, or non-conformance may result in the termination of the Purchase contract and/or imposition of a penalty for delayed supplies as per the Purchase Agreement terms and conditions. UHS may impose penalties up to 10% of the total contract value for delayed deliveries or non-compliance with agreed deliverables. **A performance bond may be required to ensure commitment to the agreed timelines and quality standards**.

8. All proposed items should be evaluated & approved by UHS's technical team prior to confirmation. After the agreement, the supplies must adhere to the same quality, specifications, and sources as originally agreed upon. Any deviation will be deemed non-compliant.

9. The brand/manufacturer mentioned should be maintained during the Supply contract period.

10. Any defective products should immediately be replaced with new ones or rectified, as and when notified, within a maximum period of one month from the date of notification.

11. UHS will constantly evaluate the compliance of contracted terms, consistency in supplies, and progress of work throughout the duration of the project. 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 contract if the vendor is not able to rectify it during the time allotted by UHS's representative. Purchase Contact details (landline, mobile, emails) of the authorized representatives should be mentioned.

12. **Tenders should be submitted in two sealed envelopes and submitted to the Materials Department UHS:**

    a. **The Technical Specification details (PLEASE DO NOT INDICATE ANY FINANCIAL VALUE IN THIS).** Vendors must submit a detailed work plan, including key milestones, timelines, resource allocation, and project phases. If additional clarifications and details are requested, these need to be submitted to **(the Materials Department- UHS).** Vendors must also provide information about the key personnel who will manage the project and their qualifications. Vendors are also required to submit references and a performance history of previous projects similar in scope, particularly in the healthcare sector, and show their post-implementation support plans, detailing how they will manage maintenance, upgrades, and ongoing support after the project's completion.

        i. The technical offer should conform to the attached indicative specification.

ii. Technical offer (hard copy and soft copy).
iii. Reference project where similar work was performed.

b. **The Financial Offer** addressed to UHS's Director of Finance, with **tender reference**.

All the above documents should be submitted before the tender expiry date; all documents submitted after the expiration date will not be accepted.

13. UHS reserves the right to accept/reject the tenders without assigning any reason thereof.
    a. The tender will be awarded project-wise as per the Purchase contract.

14. Quality, Price, and sale services are combined parameters for tender evaluation. Once a vendor has been selected, a negotiation period will follow to allow both parties to review the contract terms thoroughly. This will ensure that all deliverables, KPIs, and expectations are clearly outlined before the final agreement is signed.
15. Vendors must submit a risk management plan, identifying potential risks to the project, such as security 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.
16. 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.
17. The Vendor, its employees, its subsidiaries, and everyone who has a direct or indirect relationship with implementing and securing the works and purchases 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. Any transaction related to UHS activities must be in accordance with UHS policies.
18. 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.
19. The copyright of any documents and materials 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.

For University Hospital Sharjah
Materials Department

Tender Technical Requirements:

IT Infrastructure Monitoring & Security Project

1. **NDR (Network Detection and Response)**

- The solution must deliver continuous, real-time visibility into network traffic and activities, including the ability to capture and analyse network packets.
- Real-time analytics and detection mechanisms that ensure immediate identification of anomalies, threats, and performance issues without significant delay.
- The solution must have the capability to perform granular classification of network traffic, including application type, communication protocol, and user identity.
- The solution must leverage advanced machine learning algorithms or statistical techniques to detect deviations from established baselines of normal network behaviour and identify patterns that may indicate potential security threats
- The solution must support comprehensive packet analysis by inspecting and decoding network packets' payloads beyond the basic header information. This includes performing content-based analysis, protocol-specific inspection, and extracting detailed application-layer data to identify, classify, and respond to potential threats or anomalies within the network traffic.
- The solution must provide robust analysis capabilities for a wide range of network protocols, including but not limited to TCP/IP, HTTP/HTTPS, DNS, SMTP, and FTP. This includes decoding, interpreting, and monitoring header and payload information for each protocol, enabling detailed traffic analysis, anomaly detection, and threat identification across various communication layers and protocols.
- The system must be able to automatically segment or isolate affected devices or users based on the severity of the threat detected without manual intervention
- The system should allow administrators to configure containment policies at a granular level, defining which types of assets (e.g., workstations, servers, IoT devices) can be isolated and under what conditions
- Incident containment must be executed in real-time, with minimal latency, to prevent the spread of threats.
- Every containment action must be logged in detail, providing an audit trail for post-incident analysis.
- Administrators should be able to define customizable response playbooks that specify actions the system takes when detecting specific threat patterns.
- Ability to define and customize alert thresholds and criteria based on specific network conditions and threats. The system must support various types of alerts, including different severity levels and categories, to differentiate and prioritize incidents based on their criticality and impact.
- The solution must feature intuitive, user-friendly dashboards and management interfaces that facilitate efficient navigation and operation.
- The solution must provide Real-time and Historical reports for the period of 1 year.
- The interface should offer extensive customization options, allowing users to tailor views, layouts, and report formats according to their specific needs and preferences.
- The solution must include a comprehensive set of out-of-the-box reporting functionalities that provide standard reports on key metrics and activities.

- Users should have the capability to design and generate custom reports and dashboards, enabling tailored data analysis and visualization based on unique organizational requirements.
- The solution should provide configurable alert notification methods, such as email, SMS to ensure timely delivery of critical alerts.
- The ideal solution is virtual appliance-based and on-premise.

2. EDR (Endpoint Detection and Response)

- The solution, including both agent and management components, must demonstrate robust security against insider and external threats, ensuring secure design, deployment, and operation.
- Must use behaviour analysis, leveraging real-time cross-machine correlations and enriched endpoint data to accurately identify threats.
- The solution should integrate advanced techniques such as machine learning (pre-execution and runtime), vulnerability protection, and behaviour analysis to enhance automated detection, response, and application control.
- The solution must provide robust ransomware protection, including detecting, preventing, and responding to ransomware attacks and offering file recovery options to restore data after an attack.
- Must support continuous data collection, analytics, and centralized reporting, managed from a single console with support for threat hunting and predefined automated incident responses.
- The agent must maintain communication and reporting capabilities even when disconnected from the corporate network and must not degrade endpoint performance, including in virtualized environments (VDI).
- Deployment must be smooth, without requiring multiple reboots or interruptions, and must include a lightweight agent with minimal performance impact.
- The solution must support USB device management (block or restrict read/write/execute) and provide host-based firewall capabilities for Windows and macOS.
- The solution must integrate with external threat intelligence feeds to enhance detection capabilities
- Must integrate with any SIEM/SOC/SOAR solutions for streamlined security information management.
- Must ensure full threat detection and prevention even in offline mode without requiring network connectivity.
- Must use real-time techniques, including signature-based and behavioural analysis, to detect malware within files and provide reputation-based file protection to block suspicious applications.
- Must support application whitelisting, management of exceptions, and allow or block unsigned applications based on hash for minimizing false positives.
- Dashboards should provide actionable incident investigation and resolution elements, including continuous hunting for threats and adversarial activity.
- Must continuously record telemetry for investigation, detect server exploitation (e.g., web shells, SQL injections), and track social engineering attacks, privilege escalation, registry changes, and inbound network processes.

- Must provide incident response capabilities, isolating infected endpoints while maintaining communication for investigation and automating actions based on specific conditions (e.g., endpoint isolation, notifications via email, SMS).
- Must offer scheduled, customizable dashboards and reports for continuous monitoring and auditing.
- Must support granular control over security policies by excluding specific files, folders, behaviours, and telemetry from designated applications to reduce false positives.
- Must allow remote execution of commands from the management console, including support for custom scripts (e.g., PowerShell, Zsh, Bash) across Windows, macOS, and Linux, even when endpoints are off-corporate network or network-contained

3. PAM (Privilege Access Management)

- The solution must provide secure and controlled access to external users, ensuring they can only access specific internal resources based on predefined permissions and time-limited sessions.
- Must enforce granular role-based access control, ensuring only authorized users have access to specific systems or resources based on least-privilege principles and predefined roles.
- The solution must provide approval-based authorization workflows, requiring managerial or peer approval before granting access to privileged accounts or resources, ensuring accountability and control over privileged actions.
- The solution must support real-time monitoring, recording, and auditing of privileged sessions, including remote desktop and SSH. Capture privileged account events for compliance audits.
- Should provide Just-In-Time (JIT) access, allowing temporary access to privileged accounts with automatic revocation once tasks are completed.
- Analyse unusual privileged activity that might be harmful to your organization
- Must enforce multi-factor authentication (MFA) for all privileged access attempts, adding an extra layer of security beyond basic login credentials.
- The solution must offer comprehensive audit logging of privileged activities and generate reports.
- Must allow session recording and playback for privileged sessions, providing forensic analysis and tracking for security investigations.
- The solution must support secure, automated management of credentials for applications, services, and scripts, eliminating the need for hard-coded credentials.
- Must integrate with SIEM/SOC/SOAR platforms, providing real-time logs, alerts, and events related to privileged access for continuous monitoring and incident response.

4. SIEM/SOAR/SOC

- The solution must provide integrated SIEM, SOC and SOAR capabilities, offering centralized incident detection, response, and automation
- The solution must provide a centralized platform for monitoring, detecting, and responding to security threats across the organization’s entire IT infrastructure

- The solution must offer real-time threat detection and alerting, leveraging advanced analytics, machine learning, and threat intelligence to detect anomalies, unusual patterns, and known attack vectors.
- Must integrate with multiple data sources (firewalls, endpoints, servers, network devices) to gather comprehensive security information and enable correlation of events across the environment.
- The solution must support log collection, aggregation, and analysis from all network devices, endpoints, applications, and cloud services in real-time, with the ability to store logs for compliance and forensic analysis.
- The solution must include Security Information and Event Management (SIEM) capabilities to perform deep event correlation, prioritization, and risk scoring of security events, providing context to alerts and incidents.
- Should have a wide database of playbook-driven incident response features, allowing security analysts to define automated response actions for various types of incidents, including containment, eradication, and recovery workflows.
- Provides customizable playbooks that guide incident response steps based on predefined processes, ensuring consistency in handling security events.
- The solution must provide real-time dashboards and customizable reporting for continuous monitoring and high-level overviews, including drill-down capabilities for detailed incident investigation.
- The solution must support integration with external threat intelligence feeds, allowing it to leverage up-to-date threat indicators and provide actionable insights on emerging threats.
- Must offer behavioural analytics to detect advanced threats, such as insider attacks, by analysing deviations in user and entity behaviours.
- The solution should include automated threat-hunting capabilities, enabling proactive searches for hidden or sophisticated threats that may have bypassed traditional security controls.
- The solution must provide threat visualization tools, enabling security teams to map and visualize attacks through frameworks like MITRE ATT&CK, allowing them to understand the tactics and techniques used by adversaries.
- Must include SOAR capabilities, allowing the orchestration of incident response workflows across various security tools, automating tasks such as blocking IPs, quarantining endpoints, and notifying teams.
- The solution must offer endpoint visibility and control, allowing SOC analysts to remotely investigate and contain incidents on compromised devices.
- Must provide the ability to generate compliance reports and audits on security events and incidents to meet regulatory and governance requirements.
- Must offer customizable data retention policies for logs and security events to meet both compliance requirements and long-term forensic investigation needs.
- The solution must support integration with threat intelligence platforms, firewalls, EDR solutions, and other security tools to provide a unified security infrastructure.
- The solution must include ransomware detection and mitigation capabilities, providing automated responses to isolate infected systems and prevent lateral movement across the network.

- Must offer AI-driven insights and recommendations to improve the efficiency and effectiveness of SOC operations, providing automated suggestions for incident response and mitigation.

5. IT Infrastructure and Service monitoring

- The solution must deliver real-time monitoring and alerting for the entire network and server infrastructure, ensuring continuous visibility into performance and availability.
- Must monitor key metrics for network devices, including port status, bandwidth usage, CPU load, and memory utilization, providing insights into device health and resource consumption.
- The solution should monitor key server metrics such as CPU, memory, disk I/O, and network bandwidth and services, covering both physical and virtual servers
- The solution must track storage utilization on all monitored servers, including total capacity, used space, available space, and trends over time, alerting on storage nearing capacity to prevent performance degradation or data loss.
- It must track the performance and availability of critical applications, including web servers, databases, and business services, monitoring metrics like response time, error rates.
- Solution should monitor VMWare infrastructure.
- Must monitor and track the health of Exchange Server components, including mailboxes, databases, queues, transport services, and storage availability.
- Monitor and alerting on Database expensive queries, Blocking, Deadlock process, Transaction log growth and others.
- The solution should provide customizable threshold-based alerts for critical events, such as high resource utilization, service failures, or application downtime, with notifications delivered via email, SMS
- Must support monitoring across different operating systems, including Windows, Linux, Unix.
- Support both agent-based and agentless monitoring for flexibility in various environments.
- Provide long-term data retention for performance logs, ensuring historical data is available for compliance audits or performance investigations.
- Monitor backup processes and alert on job failures.
- Offer customizable dashboards to provide real-time insights into application performance, along with detailed historical reporting for trend analysis and performance optimization.

6. **Audit**

6.1) AD Audit

- Audit User management activities, such as Adding, Removing, changing permissions, changing password, together information about who did what, when and where.
- Monitor the additions and removals of users from distributed and security groups.

- Keep track of all alteration made to the group policy settings such as adjustments to domain level rules like password and account lockout policies, as well as the old and new values for each policy.
- Receive alerts when permissions were changed in AD at several levels, Such as domain, OU, Group, container and user.
- Identify unwanted configuration changes, such as site level modifications, FSMO role changes, and custom characteristics added to the schema.
- Get information on who is logged in, from where, since when, and more, as well as a comprehensive login audit trail for any user.
- Observer all user login behaviour, including interactive, remote, local, network logins, to obtain security insights.
- Monitor unsuccessful login attempts according to user name, IP Address, Login time, And more variables.
- Track PC Start up and shutdown times, active hours, shutdown types, and more with the comprehensive reports.
- Audit and report on each account lockout, including important information about the system, User's login history and the lockout time.
- Audit and report on reoccurring account lockout by examining a variety of windows components, such as services, apps, and schedule tasks.
- Monitor the user accounts that get locked out frequently overtime to see which employees are most impacted, and discover information about the reason behind their lockout.
- Audit and report on user password set and reset attempts.

6.2) Database Audit

- The system must audit activities based on user roles and individual user actions.
- It should log specific transactions such as select, update, delete, and create for designated users.
- Administrative operations at the instance level must be tracked.
- Inactive accounts should be monitored through regular auditing.
- User login and logout events must be recorded.
- Failed login attempts should be captured for security monitoring
- Monitor modification are made to the tables, views, Procedures, Triggers, Schema and other structural elements of the database. Report on who made a change, when it was done, and where it came from with the use of clear graphical reports.
- Get real time email or SMS notification on any modifications at the database level.
- Identify the source, When, and who of the functional queries that are executed.

6.3) File Integrity Audit

- The system should monitor changes to directories, operating systems, databases, applications, and critical business files, alerting administrators to any potentially sensitive or suspicious modifications.

- It should offer customizable alerts for unauthorized file changes, with notifications sent via email.
- Additionally, the solution must provide detailed logging and reporting of file changes, including information on who made the changes, when they occurred, and what was altered, to support auditing and forensic investigations.
- Real time Insights on all access attempts, Modifications, copy and paste operations, and deletion of files and folders.
- Monitor on unsuccessful attempts to access or alter files and folders.
- Monitor and alert sudden increases in file activity.
- Solution should support file integrity audit for Window and Linux environments.

7. Vulnerability and Patch Management

- Continually monitor endpoints for known or emerging vulnerabilities.
- Analyse the vulnerabilities risks, and generate the alerts based on the criticality.
- Identify exploit availability for every vulnerability.
- Schedule patches for windows, macOS, Linux and known third party applications. Customize every step of patching using flexible deployment policies.
- System should provide test and approved patches.
- Solution should maintain logs and provide extensive reports.
- Solution should be able to integrate with the external SIEM/SOAR/SOC solutions.

8. Password Less Authentication to the Applications:

- In order to utilize our applications, users must authenticate. Every application needs its own unique set of credentials for authentication.
- The applications listed below need independent authentications.
- Active Directory and Exchange Server
- HealthCare application
- ERP Application
- Users of the Exchange server can access the system from both their mobile devices and the official desktop/laptop computers. Mobile device email access will need to go via the perimeter firewalls.
- Instead of entering a password, we would want to have a middle-ware system manage user authentication using an RFID card, fingerprint, Face and Retina scanning with multi-factor authentication where ever is required.
- The middleware system should be able to connect to the Active Directory and applications in order to map user credentials to the appropriate RFID cards, fingerprint, Face and Retina authentication as well as to change user passwords automatically on a periodical basis.
- The user must be authenticated to the relevant system based on the authentication screen.

- The middle-ware system should be able to support and integrate the HP thin client environment and Citrix VDI for operating system login. The thin client brand should not be a limit on the system. To launch the virtual machine, we are utilizing the Citrix Workspace Client on Thin Clients.
- Require Fingerprint readers and RFID cards should be included in the proposal.
- To allow users to continue using the applications even in the event that the default login method fails, the solution should include a backup authentication strategy.
- The system needs robust security to protect from intrusions. And the solution should be free of vulnerabilities.
- Information about user credentials ought to be stored in an encrypted manner.
- Proposed solution shouldn't have any noticeable lag time in the authentication procedure.
- Solution should maintain logs and provide extensive reports.
- Solution should be able to integrate with the external SIEM/SOAR/SOC solutions.

9. Training and Support

9.1. Training

a) Vendor must provide free-of-cost certified (authorized) training from an authorized training partner for two UHS IT staff. Training should be a comprehensive administrative training and should not be basic.

9.2. Support

a) Proposal must include 24 x 7 support (Manufacturer Support) for 1 and 3 Years option.
b) Vendor should provide mandatory 3 Months support after go-live (remote or on-site support).
c) Need to specify what will be on-going maintenance cost in percentage up to the 5th year.

10. Security and Audit

The solution should not cause any security vulnerability

11. Instructions To Vendors

- Vendor must have a highest level of partnership with the proposed product.
- Vendors must address all information specified by this RFP.
- Vendor to clearly specify the structure of Licensing whether it is Subscription or Perpetual.
- It is mandatory for the Vendor to provide item-vised and with sub-total prices in Commercial Proposal.
- Technical and Financial proposals should be submitted to Director of Finance Office in separated shield envelops.
- Vendor should provide reference sites where each components/module of your proposed solution has been installed. UHS may contact these users to obtain any information on the solution and implementation. Vendors will co-ordinate with the reference sites and arrange the visit on request from UHS if required.

- Vendor is required to share the manufacturer's vision and road map to look for indicators of an advanced technology strategy (Proof documents need to be provided).
- Vendor should commit the Hardware and required software's **Delivery within 4 weeks period.**
- (Note: UHS is exempted from Sharjah customs).
- **Vendor should discuss the final technical proposal with the technical team before submission. If vendor submits the technical proposal to the finance department without discussing with IT, those proposals will be discarded from the technical evaluation.**
- Proposal should include ongoing hardware warranty, support and license subscription on annual basis up to 5th year.