شركة الحوسبة الصحية

Electronic Health Solutions

REQUEST FOR PROPOSAL

RFP-EHS-PROC-18-2024 On-premises Workloads Hardening and Cyber Resilience with ATP Solution

RFP Reference Number: RFP-EHS-PROC-18-2024

Table of Contents

Transmittal Letter

Date: 22-DEC-2024

Dear Sir / Madam,

Electronic Health Solutions “EHS” is in the process of tendering “**RFP-EHS-PROC-18-2024**” for **On-premises Workloads Hardening and Cyber Resilience with ATP Solution For Hakeem Air Gapped environment.**

Interested companies are encouraged to submit their technical and financial proposals as per the details provided in this RFP. EHS appreciates your timely and accurate response, meanwhile, shall you have any questions please do not hesitate to contact us.

Procurement Department

Tel: +962 6 580 0461 | Ext. 3050, 3071, 3074 & 3067

Email: procurement@ehs.com.jo

Yours sincerely,

Electronic Health Solution

Confidentiality Statement

This Request for Proposal (RFP) contains information proprietary to Electronic Health Solutions, hereafter referred to as “EHS”. Each recipient is entrusted to maintain its confidentiality. The information contained in this RFP is provided for the sole purpose of permitting the Bidder to respond to the RFP. This information may not be reproduced in whole or in part without the expressed written permission of EHS.

The recipient shall hereby agree to keep all the information in this RFP confidential and shall not, without prior written permission of EHS, disclose this information to any person other than the employees, agents, subcontractors, and advisors who are required in the course of their duties to execute proposal preparation activities. The recipient shall undertake the responsibility that all such persons are informed of the confidential nature of the information.

No recipient of this RFP shall, without the prior consent of EHS, make any public statements to any third parties in relation to this RFP or the subsequent short-listing of any prospective implementer or the subsequent awarding of any order. Unauthorized release of information or public statements will result in immediate disqualification.

Information provided by each Bidder will be held in confidence and will be used for the sole purpose of evaluating a potential business relationship with the respective Bidder’s company.
There will be no obligation to maintain the confidentiality of any information that was known to EHS, prior to the receipt of a proposal from the Bidder, or due to becoming publicly known through no fault of EHS, or if received without obligation of confidentiality from a third party owing no obligation of confidentiality to the Bidders.

Company Abstract

Company Profile

Electronic Health Solutions (EHS) was founded in 2009 as a non-profit company. EHS is owned by the main stakeholders in health and technology sectors in the Kingdom including Ministry of Health (MoH), Ministry of Information and Communication Technology (MoICT), Royal Medical Services (RMS), King Hussein Cancer Center, King Hussein Institute for Cancer and Biotechnology, Royal Health Awareness Society and Private Hospitals Association.

Hakeem is Jordan's National Electronic Health Records (EHR) initiative by which the healthcare sector will be computerized. The program was incepted in October 2009.

The company's mandate is to implement Hakeem in public hospitals, Royal Medical Services sites, Universities Hospitals and King Hussein Cancer Center, in addition to healthcare centers including comprehensive clinics and primary clinics.

Vision, Mission, Goals, and Objectives

Vision

Transform and sustain a continuously improving healthcare system in Jordan by leveraging information technology.

Mission

Provide a secure and accessible platform that enables the storing and sharing of electronic patient health records at all healthcare facilities enrolled in Hakeem.

Objectives

EHS main objectives are the following:

1- Improve Healthcare
2- Reduce the Cost of healthcare services.
3- Provide Data for Research and Decision Making

Benefits

- Raising healthcare quality and outcomes by enhancing the accuracy of diagnoses, medication administration, and patient information management;
- Boosting health facilities' efficiency and workflow by saving time and reducing errors in information retrieval;
- Supporting research, scientific studies and, decision-making by supplying the necessary patient data, history and statistics;
- Reducing operating costs by optimizing resource utilization and, preventing lab test repetition.

1. Contact Information

Any questions regarding this RFP shall be directed to the following email address in writing:

Name:	Procurement Department
Company:	Electronic Health Solutions
Address:	King Hussein Business Park, King Abdullah the second street. 4408 Amman 11952
Telephone / Fax:	Telephone +962 (6) 5800461 EXT3050, 3071Fax +962 (6) 5800466
Email:	Procurement@ehs.com.jo

The bidder should receive a response from the procurement department, if not please call the following number +962 79 668 1595 Or Tel: +962 6 5800461 | Ext: 3050, 3071.

2. General Conditions

Upon participation, the bidder agrees to the following:

1. All costs incurred by Bidder in the preparation of this proposal shall be borne by the Bidder.

2. “EHS” will assume that all statements in writing, made by persons submitting Proposals are true, accurate, complete and, not misleading.

3. “EHS” reserves the right to cancel, at any time, this RFP partially or in its entirety. No legal liability on the part of “EHS” for payment of any kind shall arise and in no event will a cause of action lies with any bidder for the recovery of any cost incurred in connection with preparing or submitting a proposal, in response hereto all efforts initiated or undertaken by the bidder shall be done considering and accepting this fact.

4. Bidder's proposals shall be based on full compliance with the terms, conditions and, requirements of this RFP and its future clarifications and/or amendments.

5. “EHS” shall not be under any obligation to return or save either the original or any copies of any Bidder’s Proposals (technical and/or financial), and all documents submitted to “EHS”, whether originals or copies, shall be kept or disposed of by “EHS”.

6. This Request for Proposal doesn’t constitute an offer. “EHS” shall not be under obligation to enter into any agreement with any Bidder in connection with this RFP and responses received.

7. The Bidder’s proposals (technical and financial) shall comply with the laws and regulations of the Hashemite Kingdome of Jordan.

8. The Bidder’s proposals (technical and financial) shall be compatible with international standards and best practices.

9. As a part of the RFP response, the Bidder is requested to fill out the compliance sheet included in this RFP.

10. The bidder must include in his technical proposal a detailed Bill of Quantity “BOQ” for all proposed and priced items and services. Accordingly, this should be reflected and included in the financial offer with itemized quoted prices for all proposed items.
11. The bidder must commit to providing EHS with the same prices and terms for a period of (1) year starting from the Awarding Letter date for the purpose of Variation Orders

12. The quantities requested in this RFP are subject to increase, decrease or, cancellation as per the actual requirements in the awarding date. In case the quantities decrease the vendor is responsible to install the available materials from the EHS warehouse.

في حال أن تعذر على "المناقص الفائز بالعطاء" تنفيذ التزاماته التعاقدية و/أو أي جزء منها، بحيث يكون قد تأخر في توريد المواد و/أو الخدمات المحددة لمدة (45) يوم من التاريخ الواجب على " المناقص الفائز بالعطاء " خلاله تنفيذ التزاماته، فسيكون في هذه الحالة من حق "شركة الحوسبة الصحية" إلغاء قرار الإحالة والعلاقة التعاقدية التي تجمعهم مباشرة دون الحاجة الى اشعار و/أو انذار و/أو استصدار حكم قضائي. كما يكون من حق " شركة الحوسبة الصحية " في هذه الحالة شراء ما كان متفق عليه من مورد آخر يراه مناسبا، على أن يتحمل " المناقص الفائز بالعطاء " كافة النفقات التي قد تكبتدها " شركة الحوسبة الصحية " جرّاء ذلك الى جانب تعويض " شركة الحوسبة الصحية " عما لحقه من أضرار إثر تعذره عن تنفيذ إلتزاماته.

3. Bidder Qualifications

1. Bidder should be a Company registered under the Jordanian Ministry of Industry and Trade for more than three years or represented by a company abiding by the aforementioned condition; otherwise, any international or regional bidder must present the formal documents which prove the financial capacity of the company in addition to its commercial registration documents at the country of origin
2. Bidder should have at least three references of similar projects preferably in the health care sector and to be accepted by EHS.
3. The Bidder / Vendor shall have at least three enterprise scale live installations for similar solution. The contacts information for such projects must be provided within the bidder's technical proposal in order to be contacted by EHS as part of the technical evaluation.
4. The Bidder shall have specialized and certified engineers with relevant technical certification for at least two engineers.
5. The bidder must submit Up-To-Date official documents of registration issued from the Companies Control Department at the Jordanian Ministry of Industry and Trade.
6. The bidder must be an authorized Partner of the mother company he represents in this bid; the highest two partnership levels are only accepted. The bidder must submit an up-to-date valid official letter/certificate from the mother company as part of the bidder's qualification documents.
7. The bidder shall have at least two certified engineers according to the manufacturer's recommendations on the proposed solution; at least one of them shall be assigned to the project with EHS.
8. All proposed and supplied equipment\solutions\items\services must be original, brand new (not refurbished) and, licensed by the manufacture (mother company) to be supplied and installed for this project at EHS.
9. All proposed and supplied equipment / solution / items / appliances / hardware must be newly manufactured with manufacturer valid warranty and support duration for not less than (7) years from the date of delivery. This implies that supplied products must not be obsolete, phased out of production, out of sales, or out of support.
10. All proposed and supplied equipment\solutions\items\services must be original, brand new (not refurbished) and, licensed by the manufacturer (mother company) to be supplied and installed for this project at EHS.

11. تلتزم الشركة المحال عليها بتحديد نسبة الصيانة و الدعم الفني في العرض المالي للأجهزة المحال عليها للسنوات التي تلي فترة الصيانة المجانيةشاملة قطع الغيار و الأيدي العاملة علماً بأن هذا البند سيكون جزء من التقييم المالي للعرض المقدم

The winning bidder is obliged to determine the percentage of maintenance and technical support including spare parts and manpower for the years following the free maintenance duration. This has to be specified clearly in the financial offer for the supplied devices\solutions as per this RFP and will be part of the financial evaluation of the bid.

4. RFP Guidelines

a. RFP Issuance & Submission

Event	**Date**
1. RFP distribution to vendors	22-DEC-2024
2. Questionnaire Session	N/A
3. Proposal due date Closure Date	12-JAN-2025

b. Queries and Responses

All inquiries during the questions and answers session (Bidder Conference) if conducted must be documented., Verbal clarifications, inquiries or communication are not permitted, and only written communication is accepted.

c. RFP Acknowledgement

1. Award of the contract resulting from this RFP will be based upon the most responsive vendor whose offer will be the most advantageous to "EHS" in terms of cost, functionality, and other factors as specified elsewhere in this RFP.

2. Vendor has a period of (5) days to acknowledge and accept the awarding letter with its terms and conditions. Delay of acceptance will yield into consideration of rejection.

3. EHS" reserves the right to:

   a) Accept other than the lowest-priced offer.
   b) Award a contract on the basis of initial offers received, without discussions or requests for best and final offers.
   c) Award the RFP contract on a partial basis (i.e. not all requirements requested from a single vendor.)
   d) Not declare the name of the winning bidder, and awarding details.

d. Proposal Format Requirements

1. The financial and technical proposals must be submitted separately. Each proposal must be sent in a separate (PDF) electronic file (PDF). (**If the proposal file document size is bigger than 9 Megabyte (MB), you may send the document through a secured file hosting service and an internet-based computer file transfer service company such as Dropbox, WeTransfer, etc.**)
2. The proposals must be sent to the Procurement Department email namely; (Procurement@ehs.com.jo). A password divided into (3) portions and not to be less than (9) nine digits must be set on the financial offer.
3. The passwords must be sent through a text message (SMS) to relevant mobile numbers which will be cellular mobile numbers that will be provided to the bidders at a later stage.
4. Pricing must be per site with a breakdown itemized pricing for each item, component, product and services included in the submitted Financial Proposal.
5. The Financial Proposal must specify clearly the compliance with the (5) five years' warranty duration required in the Technical Specification section.

6. The bidder shall submit only one financial proposal file. The financial proposal must include all of the products or solution options proposed in the Technical Proposal. The financial proposal must be in a format that is easy to read and understand and in compliance and consistent with the pricing and terms and conditions mentioned in this RFP document. The financial proposal must be in English.

The financial proposal must be signed by an authorized representative of the bidder.

If the bidder submits more than one financial proposal file, or if the financial proposal does not include all of the products or solution options proposed in the Technical Proposal, the bidder's proposal may not be considered.

7. The bidder must submit a cover letter in a PDF format as a separate document from the Technical and the Financial Proposal. The cover letter must include the following information:
   - The tender reference number.
   - The name of the bidder.
   - The contact information for the bidder.
   - A list of the product(s) and\or solution(s) names that are being proposed, along with the corresponding product and/or solution code.
   - A listing of the proposed product(s)\ solution(s)\service(s) along with their relevant brief description.

The aforementioned information must be filled in the following "Table Template" **(ملخص للمنتجات والخدمات والحلول المعروضة)** and must be consistent and in a total match with the relative names and descriptions included in the financial and technical proposals. The list of product and/or solution names must match those included in the Technical and Financial Proposal. If the bidder does not submit a cover letter, or if the list of product and/or solution names do not match those included in the Technical and Financial Proposal, the bidder's proposal may not be considered.

Table Template (ملخص للمنتجات والخدمات والحلول المعروضة)

The following table template can be used to list the product and\or solution names that are being proposed:

Option	Product\Solution\Services Name	Product\Solution\Services Description
Option (1)	**Product 1**	
Option (2)	**Solution 1**	
Option (3)	**Solution 2 & Product 2**	

5. RFP Terms & Conditions

a. Evaluation Criteria

1. "EHS" will evaluate each response. Responses will be evaluated on many criteria deemed to be in EHS's best interest, including but not limited to, technical offering, price, warranty, delivery duration, Bidder certification, accreditation, schedule, bidder's capabilities, compliance with bonding, and any other factors that "EHS" determine. The order of these factors does not denote relative importance.
2. "EHS" reserves the right to consider other relevant factors as it deems appropriate in order to obtain the best value.
3. This RFP does not commit "EHS" to select any firm, enter into any agreement, pay any costs incurred in preparing a response or procure or contract for any services or supplies. "EHS" reserves the right to request additional information from the bidders whose response meets "EHS" needs and business objectives without requesting such information from all respondents.

b. Rejection of Proposals

"EHS" reserves the right to reject any or all offers and discontinue this RFP process without obligation or liability to any potential Vendor.

c. Proposal Costs and Expenses

No legal liability on the part of "EHS" for payment of any kind shall arise and in no event will a cause of action lies with any bidder for the recovery of any cost incurred in connection with preparing or submitting a proposal. In response hereto all efforts initiated or undertaken by the bidder shall be done considering and accepting this fact.

d. Bid, Performance, Advance payment, and Warranty Bonds

1. Unconditional Bid Bond valid for (3) three months with an amount of (JoD 5,400.00) Five Thousand Four Hundred Jordanian Dinar to be renewed automatically must be submitted by every participating bidder.

2. Advance payment LG, is to be submitted against any required advanced payment.

3. Unconditional Performance Bond for (10%) of the total amount of the awarded value shall be submitted by the winning bidder and within (5) working days from the date of the award. The Performance bond must remain valid for the total duration of the implementation of the project and until the delivered solution is finally received and accepted by EHS. This Performance Bond will be replaced by the Maintenance LG after items delivered installed and finally accepted duly. The Maintenance Bond will remain valid until the end of the warranty duration. In case the winning bidder fails to submit the performance bond, EHS reserves the right to cancel the contract and liquidate the bid bond without reverting to the bidder.

e. Penalties

In the event, the bidder fails to deliver according to the agreed time (for either the initial agreed delivery date or any of the subsequent delivery dates). The Bidder must pay EHS a delay penalty of (1%) of the total contract amount for each week of delay. The maximum penalty for delays shall not exceed (10%) of the total contract value. The payment or deduction of such penalty shall not relieve the winning bidder from its obligations to complete the services or from any other obligations and liabilities under this bid.

f. Payment Terms

1- Payment terms:

20% Advance Payment against "Advance Payment LG"
20% upon items delivery
20% upon installation or implementation
40% on final EHS acceptance.

In case the winning bidder fails to comply with the "Advance Payment LG" term set for the first payment, hence, the winning bidders will be entitled to receive (40%) of the total contract value after the fulfillment of the delivery and initial receiving conditions "إستلام توريدي" set forth in this RFP.

2- Payment currency shall be in Jordanian Dinar (USD and Euro exchange rate will be calculated at the currencies exchange rate issued by Central Bank of Jordan at the payment date).

g. Terms of Delivery

- Delivery, Installation, and implementation must be within (8-12) Weeks from the date of issuance of the purchase order. Final acceptance is required by EHS, and penalties for delays will be imposed as per the condition specified in clause (5.e) of this RFP.
- Any bidder who fails to meet the above named durations for delivery and implementation **may be considered dis-qualified**.
- Weight: The duration of delivery and implementation of projects will be given a high weighting value in the evaluation criteria. Accordingly, the weighting value for the bidder with the shortest proposed duration will receive the highest score.

h. Offer Expiry Date

The validity of the Proposal shall be no less than (90) days unless clearly mentioned differently.
The prices must remain fixed and valid for (90) days from the date of the invitation for bid closing date and shall be clearly stated in the technical and commercial bids.

6. Financial Compliance Sheet

#	Description	Comply (Yes/No)	Reference in the proposal
1	The bidder shall comply with all points included in the general conditions section		
2	The bidder shall comply with all points included in the bidder qualifications section		
3	The bidder shall comply with all points included in the RFP guideline section		
4	The bidder shall comply with all points included in the RFP terms and conditions section		

7. RFP Objectives

The purpose of this Request for Proposal (RFP) is to solicit submissions from qualified vendors for the design, supply, installation, configuration, testing, and deployment of an enterprise-grade security solution for Hakeem program data centers. This solution will be implemented across data centers, delivering comprehensive protection and seamless integration with critical healthcare systems.

The ideal solution will ensure robust security, high availability, scalability, and resilience for data centers servers, meeting the stringent requirements of the healthcare environment. The goal is to establish secure, protect all production servers.

Scope and Requirements: The chosen vendor will provide a fully integrated solution, including:

- All necessary hardware and software components
- Design, installation, and configuration services across all data centers
- Rigorous testing and validation to confirm optimal performance and reliability

Strategic Importance: This initiative is central to the operational continuity and security of the Hakeem program, supporting mission-critical healthcare applications. We seek proposals that combine advanced technical capability with competitive commercial terms.

8. Business Requirements

From a business perspective, On-premises Workloads Hardening and Cyber Resilience with ATP on Air Gapped environment, solution must be delivered as a robust, enterprise-grade turnkey solution meticulously tailored to align with EHS requirements and uphold industry standards. This imperative encompasses a comprehensive approach addressing the following key points:

1. **Comprehensive Security and Threat Protection**

   Protection from network, application, and web-based threats, including DDoS, intrusion, malware, and zero-day attacks. Ability to enforce policies to guard sensitive data.

2. **Performance and Scalability**

   Ability to handle high volumes of data traffic with minimal latency, scalable as data demands grow in enterprise and data center networks.

3. **Compliance and Reporting**

   Meet regulatory requirements (e.g., GDPR, HIPAA) and provide reporting tools for audit trails, threat monitoring, and incident response.

4. **Ease of Integration and Interoperability**

   Seamless integration with existing IT infrastructure, identity management, and third-party monitoring tools to streamline operations.

9. Technical Proposal Submittals

The Submittals within technical proposal:

1. **Technical Compliance Sheets:** Provide detailed compliance matrices for all requirements listed in the RFP, showing the proposed solution's adherence to specifications.
2. **Data Sheets for All Items:** Include manufacturer data sheets for each component in the solution, detailing technical specifications, capabilities, and certifications.
3. **Project Implementation Plan**: High-level timeline and methodology for project phases, including milestones, resource allocation, and estimated timelines for deployment and testing.
4. **Acceptance Test Procedure (ATP) Document**: Outline the criteria and procedures for system acceptance testing, detailing performance, security, and reliability metrics to be met.
5. **Service Level Agreement (SLA)**: Detailed SLA specifying response times, resolution times, support tiers, and escalation processes for ongoing support.
6. **Project Team Details**: Information on project personnel, including roles, relevant certifications, and experience with similar implementations.
7. **Detailed Bill of Quantities (BOQ)**: List of all items with specifications, quantities, durations, and any necessary installation materials or licenses.
8. **End-of-Sale/End-of-Life Information**: Documentation on the support lifecycle, end-of-sale, and end-of-life timelines for each proposed solution component, including replacement strategies.
9. **Warranty and Support Coverage**: Clearly defined warranty terms for all hardware and software components, including post-deployment maintenance options.

10. Solution Technical Specification

11.4 Technical Specification for Server Security

#	Description	Comply	Note
1.	The proposed solution security technologies should be delivered in a single agent		
2.	The proposed solution security technologies should be delivered fully on-prem		
3.	The proposed solution should have all of the following deployment options; Physical, Virtual, VDI, Agentless, Cloud, Container		
4.	The proposed solution should be capable to deliver all Gartner's security recommendation for servers' workload		
5.	The proposed solution should defeat all malware threat lifecycle stages. This includes; Entry Point Protection, Pre-Execution Protection, Runtime Protection, and Exit-Point Protection		
6.	The proposed solution should have Antimalware protection to defeat known malwares		
7.	The proposed solution should have File and Web URL Reputation protection		
8.	The proposed solution should have Machine Learning malware protection to defeat unknown and emerged malwares		
9.	The proposed solution should have Behaviour Analysis to monitor runtime processes and detect suspicious or malicious activities		
10.	The proposed solution should natively support samples submission to a custom sandbox solution to detect advanced and targeted malwares		
11.	The proposed solution should have Application Control to whitelist applications or block unwanted and unknown applications		
12.	The proposed solution should have Integrity Monitoring to monitor and report any unauthorized system's changes, and hardening violations		
13.	The proposed solution should have Log Inspection to identify and alert for intrusions and advanced malware attacks and report what is happening on the systems		

14.	The proposed solution should have Host-Based Intrusion Prevention System (HIPS) to detect and block network-based attacks such as lateral movements		
15.	The proposed solution should have Virtual Patching to automatically detect and shield unpatched or zero-day vulnerabilities on the servers		
16.	The proposed solution should have detailed Dashboarding features with a wide range of widgets to represent the security posture and status of the servers		
17.	The proposed solution should support SIEM integration		
18.	The proposed solution should streamline and accelerate achieving Compliance requirements such as; GDRP, PCI DSS, HIPAA, etc		
19.	The proposed solution should support a connected threat defense to receive in real-time the emerging threat information and Indicator of Compromise (IOCs)		
20.	The proposed solution should support wide range of platforms includes Windows, Linux, and legacy Operating Systems: Windows Server 2003 SP1 or SP2,Windows Server 2003 R2 SP2 (32-bit and 64-bit) ,Windows Server 2008 (32-bit and 64-bit),Windows Server 2008 R2,Windows Server 2012 (64-bit),Windows Server 2016 (LTSC, version 1607) (64-bit), Windows Server 2019 (LTSC, version 1809),Windows Server 2022 (LTSC, version 21H2) (64-bit),Ubuntu 10.04,Ubuntu 12.04,Ubuntu 14.04,Ubuntu 16.04,SUSE Linux Enterprise Server 11, SUSE Linux Enterprise Server 12 (PowerPC little-endian),SUSE Linux Enterprise Server 15,SUSE Linux Enterprise Server 15,Red Hat OpenShift supported versions,Red Hat Enterprise Linux Workstation 7,Red Hat Enterprise Linux 8		
21.	The proposed solution's vendor should be the market leader in vulnerability disclosure. The vendor should prove its capability to discover zero-day vulnerabilities and build security controls to protect servers from the relevent exploits		
22.	The proposed solution's vendor should have one of the biggest Cloud Threat Intelligence in the world and Market-Leading threat research centers		

11.4 Technical Specification for Sandbox

#	Description	Comply	Note
1.	The proposed solution should support classifing password-protected files based on ICAP pre-scan results		
2.	The proposed solution should support sandboxing HTTP/HTTPs and FTP/FTPs URLs		
3.	The proposed solution should support native integration with SOC Platform to enable collaborative security analytics in a hybrid environment. Update the Threat Intelligence and share it with other connected security solutions		
4.	The proposed solution should allow to filter sample submission based on MITRE ATT&CK Tactics, MITRE ATT&CK Techniques, and Malware Notable Characteristics		
5.	The proposed solution should allow to filter sample submission based on MITRE ATT&CK Tactics, MITRE ATT&CK Techniques, and Malware Notable Characteristics The proposed solution should allow to filter sample submission based on MITRE ATT&CK Tactics, MITRE ATT&CK Techniques, and Malware Notable Characteristics		
6.	The Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.		
7.	The Proposed Solution should be a dedicated hardware appliance series solutions should have models which support the following redundant features: Power Supply & Hard Disks		
8.	The Proposed Solution Should have support (.jar) for enhanced Predictive Machine Learning integration		
9.	The Proposed Solution Should have YARA rule detection for all file types		
10.	The Proposed Solution Should have URL extraction from RTF files for analysis by Web Reputation Services		
11.	The Proposed Solution Should provides increased protection and detection by supporting up to 100 file password entries for analyzing password protected files		
12.	The Proposed Solution Should support file SHA-256 for user-defined suspicious objects (STIX, sync from on-prem threat intelligence orchestrator)		

13.	The Proposed sandbox system should provide the following: 1. Predictive Machine Learning support for VBS file type 2. URL analysis results in Suspicious Objects table 3. Coin Miner as a new threat category and threat type 4. New file types (slk and iqy) for sandbox analysis		
14.	The Proposed Solution should have the analysis of file and URL samples received from integrated ICAP clients.		
15.	The Proposed Solution should integrates with a integrates with a Microsoft Active Directory server to allow Microsoft Active Directory user accounts to be added as system access users.		
16.	The Proposed Solution should integrate with central management software to add the following features: 1. Single Sign On 2. On-demand synchronization of suspicious objects in sandbox with the central management software.		
17.	The Proposed Solution should have inclusion of events performed by central management software users in the sandbox audit log		
18.	The Proposed Solution Should have submission of Portable Executable files with all their dependencies in one archive file		
19.	The Proposed Solution Should have Addition of screenshots to the sandbox report		
20.	The Proposed Solution Should have extraction of URLs from office files for submission to web reputation security scanning		
21.	The Proposed Solution should support reanalysis of samples which sandbox has already processed. Reanalysis ignores any cached data to ensure that the new analysis is not affected by previous results.		
22.	The Proposed Solution should have the capability to export submissions to a CSV file.		
23.	The Proposed Solution should have support adding the average sandbox Processing Time Widget, which shows the average processing time used by sandbox.		
24.	The Proposed Solution should have support addition of the following events: 1. System event logs 2. Alert event logs		
25.	The Proposed Solution have for Structured Threat Information eXpression (STIX) files to perform the following functions: 1. Use of user-defined match list for detection 2. Export via the WebService API for 3rd party		

	integrationHave option allow sessions with untrusted certificates		
26.	The Proposed Solution should enable user to configure debug log level setting for ease in troubleshooting.		
27.	The Proposed Solution should include enhanced active update with the following features: 1. Several new ActiveUpdate components 2. Option to rollback ActiveUpdate components 3. Frequency of ActiveUpdate update check increased from every 24 hours to every 15 minutes		
28.	The Proposed Solution should provide the option to specify optional command line arguments for PE samples received from integrated products, manual submissions, and support tools.		
29.	The Proposed Solution should have support proxy configuration in the custom sandbox image.		
30.	The Proposed Solution should provide increased protection by improving its detection capabilities:		
31.	The Proposed Solution should support all the following Windows operating systems in its custom sandbox virtual machines : CentOS 7.8, Redhat 7.9,8.3		
32.	Support Microsoft Office 2016 and 2019 application for Office file analysis in sandbox images		
33.	New file types (Microsoft Publisher 2016, Microsoft Windows Command Script file, Microsoft Windows Batch file, and Scalable Vector Graphics) for file submission filters		
34.	Extract files in archive files with multiple compression layers		
35.	The Proposed Solution should have support enhanced submission screen that includes the following features: 1. Improved Advanced filter to provide more search options 2. A separate Unsuccessful tab to display all samples which were not successfully analyzed		
36.	The Proposed Solution should provide users with the option of automatically inline migrating the settings from previous version.		
37.	The Proposed Solution should be a centralized, open, scalable sandboxing analysis platform that provides on-premise, on-demand analysis of file and URL samples.		
38.	The Proposed Solution should have out-of-the-box integration with security products such as Messaging Security, Web Security, Microsoft Exchange Email Server Security, IBM Domino Email Server Security,		

	Network/Web/Files Advanced Threat Protection, Email Advanced Threat Protection, Endpoint security and Datacenter servers security		
39.	The Proposed Solution should have support sending SNMP trap messages to notify administrators about events that require attention, and listens to SNMP manager requests for system information, status updates, and configuration.		
40.	The Proposed Solution should have advanced sandbox analysis to extend the value of security products such as endpoint protection, web and email gateways, network security.		
41.	The Proposed Solution should use extensive detection and anti-evasion techniques, detect ransomware, advanced malware, zero- day exploits, command and control (C&C) and multi-stage downloads resulting from malicious payloads or URLs on Windows, non Windows and Mac OS systems.		
42.	The Proposed Solution should provide on-premise custom sandboxing : supports environments that precisely match target desktop software configurations (Operating systems and applications) resulting in more accurate detections and fewer false positives.		
43.	The Proposed Solution should have full customization of the sandbox by the IT administrator without Vendor intervention.		
44.	The Proposed Solution should have automated sandbox creation tool		
45.	The Proposed Solution must be able to run multiple Micro Tasks in a single VM (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution)		
46.	The Proposed Solution Should provide detection for windows, non-windows and mobile devices malwares.		
47.	The Proposed Solution should have flexible deployment that can be deployed as a standalone sandbox or alongside a larger connected threat defense deployment to add additional sandbox capacity. It should be scalable to have up to 60 sandboxes in a single appliance, and multiple appliances can be clustered for high availability or configured for a hot or cold backup.		

48.	The Proposed Solution should have advanced detection methods such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. It should also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.		
49.	The Proposed Solution should have URL analysis by performing sandbox analysis of URLs contained in emails or manually submitted samples.		
50.	The Proposed Solution should detect ransomware script emulation, zero-day exploits, targeted and password-protected malware commonly associated with ransomware. Is also should use information or known threats to discover ransomware through pattern and reputation based analysis. The custom sandbox can detect mass file modifications, encryption behavior, and modifications to backup and restore		
51.	The Proposed Solution should have support the following file types which includes a wide range of executable, Microsoft Office (2003,2007,2010,2013, both 32 & 64bit), PDF, web content, and compressed files using multiple detection engines and sandboxing. Custom policies can be defined by file type. EXE, DLL (CPL, BHO included), LNK, SWF, PDF, RTF, DOC, PPT, XLS, DOCX, PPTX, XLSX, OFFICEX, JTD, HWP, ZIP, JAR, URL, JAVA_CLASS_APPLET, JAVA_JAR_APPLET, JAVA_JAR_APPLICATION, GUL, VBS, ps1, hta, wsf, slk, iqy , ELF , .sh		
52.	The Proposed Solution should support files greater than 15 MB		
53.	The Proposed Solution should provide an open Web Services Interface API that enables any product or process to submit samples and obtain detailed results in a timely manner		
54.	The Proposed Solution Should support analysis of at least 45,000 samples/day		
55.	The Proposed Solution Should share IOC detection intelligence automatically with its own solutions and third-party security products.		

11. Scope of Work

The scope for delivering the On-premises Workloads Hardening and Cyber Resilience with ATP Solution for Hakeem Air Gapped environment shall include the following:

1. Project Kickoff:
    (1) Hold an initial meeting to align project objectives and timelines.
    (2) Define roles and responsibilities.
    (3) Develop a Project implementation plan and project schedule. The supplier shall assign a qualified technical project manager to manage the project and to ensure the controls and successful delivery.

2. Solution Components Delivery
    (1) The delivery of all the solution components to EHS Warehouse and the sites based on EHS requirements and policies, including moving the materials to and within the sites.

3. Pre-Implementation Assessment:
    (1) Perform preparatory site visits and related activities to ensure the best deployment.
    (2) Conduct an assessment of the existing IT infrastructure and security polices applied on the current security systems at the data center.
    (3) Identify specific requirements and constraints.

4. Solution Design:
    (1) Develop a detailed solution design based on the provided business requirements.
    (2) Include architecture diagrams, component specifications, and integration points.
    (3) Conduct technical workshops with EHS technical team to develop the solution architecture, HLD, and LLD. The entire project's documentation must be approved by EHS.
    (4) The solution design must be validated by the vendor.

5. Solution Setup and Installation:

(1) Deploy necessary hardware and software components.
(2) Configure solution's equipment.
(3) Follow EHS instructions in labeling all equipment and put a description in the network devices configuration.
(4) Patching the copper and fiber patch cords cables inside the cabinets.
(5) Provide any extra materials or/and services required to deliver a complete turnkey solution.

6. Integration and Compatibility:
   (1) Ensure seamless integration with existing enterprise systems and network devices where needed.
   (2) Verify compatibility with sites' infrastructure.

7. Configuration and Optimization:
   (1) Configure solution components based on EHS requirements.
   (2) Optimize performance for scalability and efficiency.
   (3) Optimize, refine, and migrate the network circuits and current security polices in place to the new solution.

8. Security Measures:
   (1) Set up access controls and authentication mechanisms according to EHS policies

9. Testing and Validation:
   (1) Conduct thorough testing of implemented solution.
   (2) Validate high availability and disaster recovery through simulated scenarios.
   (3) Perform Acceptance Test Procedure (onsite) and any corrective action to collect EHS acceptance.

10. User Training:
    (1) Develop training materials for IT administration staff.

(2) Provide training sessions to ensure proper utilization of the data protection solution.

11. Documentation:
    (1) Document the implemented solution comprehensively.
    (2) Include configuration guides, operational manuals, and troubleshooting procedures.

12. Monitoring and Alerting:
    (1) Set up monitoring tools to track the health and performance of the data protection system.
    (2) Configure alerting mechanisms for immediate issue detection.

13. Knowledge Transfer:
    (1) Transfer knowledge to the IT team for ongoing system management.
    (2) Provide guidance on routine maintenance tasks.

14. Post-Implementation Support:
    (1) Offer post-implementation support to address any issues or concerns.
    (2) Conduct periodic reviews to ensure optimal system performance.

12. Bill of Quantities

The below is the BOQ for the solution included in the below table, each component sizing and license requirement is based on the below details within this section. **The bidders must provide the exact quantities included in the below table:**

Item	Location	Description	Qty
1.	Hakeem Datacenters	Server Security	500 Licenses
2.	Hakeem Datacenters	Sandbox	1

13. Warranty and Support

1. The bidder shall offer minimum of (5) years (8/5) manufacturer warranty and support service with next business day hardware replacement at minimum. Vendor's support contract number / ID shall be provided to EHS.
2. The bidder shall offer minimum of (5) years (24/7) local maintenance and support service; Maintenance and support service shall cover all supplied components and services.
3. The Warranty and support services starting date is the date of the EHS's final acceptations of the completed scope of work.
4. During the warranty period, the supplier shall provide all required spare parts free of charge.
5. The warranty period covers support on site.
6. The bidder shall provide the support approach in the form of a signed and stamped SLA, including the escalation matrix, support contacts, and response time.
7. Perform preventive maintenance for the delivered solution based on four yearly visits during the warranty and support period.

14. License

1. Provide all the software and hardware licenses of any/all features that require purchasing a specific license to enable and use from day one. Further, describe how licenses are to be validated or enforced.
2. The bidder shall provide the required licenses to cover all the required capacity according to section "17 Bill of Quantity" from day one without under sizing.
3. All the licenses required for the solution must be perpetual licenses or for five years.
4. The vendor shall provide how solution licensing is deployed.
5. The supplier shall provide EHS the required licenses in the name of EHS to access and use the Software supplied through this RFP.
6. The bidder shall provide the system behavior after the subscription period expire.

15. End-of-Life and End-of-Sale Conditions

1. The equipment quoted by the bidder should not be declared as End of Life (EOL) or End of Sale (EOS) by the manufacturer, at the time of bidding. The bidder shall provide the information for End of Life (EOL) and End of Sale (EOS) for all the provided items in the BOQ.
2. The bidder must provide a 5-year lifetime letter of the solution from the vendor.

16. Product origin

1. The mother company shall be from the USA, Europe, or Japan.

17. Service Level Agreement

SLA Scope
The scope of this SLA agreement covers the provided solution for On-premises Workloads Hardening and Cyber Resilience with ATP Solution for Hakeem Air Gapped environment including all hardware and software components. On-site labor and parts must also be included.

SLA Duration
The supplier must provide maintenance and support for hardware and software for a period of five years starting the date of the EHS's final acceptations of the completed scope of work.

SLA Terms and conditions
The supplier response will be measured and monitored using EHS's Service Management tool.
During the Maintenance period, the supplier must provide the following:

- Preventive maintenance program and provide preventive maintenance scheduled visit every three months.
- Health check report after every preventive visit.
- Support methodology and escalation matrix including contacts details.
- Manufacturer support for all components.
- Maintaining spare parts to meet the "availability" target at no additional cost.
- Support, configure and resolve problems whenever needed and/or if requested by EHS.
- Commit to providing quality assurance for any major configuration changes whenever requested by EHS. Any change must be done within the EHS's Change Management process.
- Perform Firmware updates, patches, and new releases according to the manufacturer's recommendation
- Handle all support requests submitted within or outside working hours without extra charges.
- Provide the required assistance to EHS staff for any configuration modification.
- All the solution's components should be covered back-to-back by Vendor support without any exception; the supplier shall provide the approach to validate the support contract with the vendor to EHS.

Support Cases Management

EHS will set the support cases Severity level upon opening each individual support case.

Support cases covered by this agreement are to be treated by supplier according to the ITIL V4 framework incident management process and request fulfillment process, inline with the supplier provided support structure.

SLA Severity Levels and Targets

Severity Level 1: Critical
Definition:
This level represents incidents causing a critical impact to the business, resulting in severe disruption or complete unavailability of a critical system or service.
Examples:

- Complete system outage affecting all users.
- Security breach leading to unauthorized access to sensitive data.
- Data corruption or loss with significant business impact.

Response Time: Immediate response required, typically within 1 hour.
Response Time Schedule: 24/7

Severity Level 2: High
Definition:
Incidents with high impact but not immediately critical, causing significant disruption or degradation in services.
Examples:

1. Major performance degradation affecting a critical business process.
2. Service interruptions affecting a specific department or location.
3. A security vulnerability that requires urgent attention.

Response Time: Response within 2 hours.
Response Time Schedule: 24/7

Severity Level 3: Medium
Definition:
Incidents causing a moderate impact, resulting in disruption or degradation of non-critical services or affecting a limited number of users.
Examples:

- Performance issues affecting non-essential services.
- Application errors causing inconvenience but not critical to operations.
- Limited data loss with backups available for recovery.

Response Time: Response within 4 hours.
Response Time Schedule: Eight business-working hours - 5 Weekdays Excluding Holidays

Severity Level 4: Low
Definition:

Incidents causing minor impact, resulting in minimal disruption or inconvenience to users or business operations.
Examples:

- Minor performance issues with no critical impact.
- Non-urgent software or application bugs.
- Requests for information or non-urgent assistance.

Response Time: Response within one business day.
Response Time Schedule: Eight business-working hours - 5 Weekdays Excluding Holidays

During the resolution process of any problem, EHS team shall stay informed about the progress of the resolution process.

Following the completion of any service related to incident resolution (Severity Level 1 and Severity Level 2) and after closing the incident, the supplier shall provide an incident report. The Report shall include the Root Cause Analysis "RCA" and indicate the exact time at which an intervention began, the components that was serviced or replaced, the corrective measures that were taken, and the amount of time needed for the intervention since the manifestation of the problem until functionality is restored.

Response time: is the time it takes a provider to respond to an inquiry or request from a client.
SLA Availability Target and Penalties
Additional hours exceeding the allowable downtime will be subject to penalty. The minimum accepted system availability is 99.9% yearly uptime.
Throughout the execution of the SLA, vendors should not rely on system redundancy as a **permanent** resolution

Availability: the ability of an IT system to perform its agreed function as required.

The bidder will be subject to penalty if he does not meet the "response time". The following table shows all the penalties under this SLA contract. In addition, the "response time" must be met with each Severity Level.

Penalty condition	Penalty amount per hour JoD			
	Severity Level 1	Severity Level 2	Severity Level 3	Severity Level 4
Failed to achieve 99.9% availability target	400	300	0	0
Failed to achieve "response time"	400	300	100	50

18. Technical Compliance Sheet

#	Description	Comply (Yes, No)	The reference point in the Proposal
1.	**The bidder proposal shall include all the submittals mentioned in the submittal section**		
2.	**The bidder proposal shall comply all the points in the business requiems section**		
3.	**The delivered items must match the proposed technical specifications mentioned in the solution technical specifications section.**		
4.	**The bidder shall propose the quantities based on the BOQ table including part numbers as mentioned in the Bill of quantities section.**		
5.	**The bidder shall agree to all points mentioned in the scope of work section.**		
6.	**The bidder shall be committed to all technical terms and conditions mentioned in the technical term and condition section.**		
7.	**The bidder must be committed to all warranty and support points mentioned in the warranty and support section.**		
8.	**During the support and warranty period, the bidder shall be committed and meet all parameters mentioned in the service level agreement section**		
9.	**The mother company shall be from USA, Europe, or Japan.**		
10.	**The bidder must be committed to all End-of-Life and End-of-Sale Conditions that mentioned in the proposal.**		
11.	**The bidder must be committed to all requirements that mentioned in the Licenses section.**		

Electronic Health Solution