RFP FOR PROCUREMENT OF ADVANCED MALWARE – EDR SOLUTION

PAKISTAN STOCK EXCHANGE LIMITED

PROPOSAL SUBMISSION DATE

August 30th, 2019

5:00 p.m.

REQUEST FOR PROPOSAL

PROPOSAL SUBMISSION ADDRESS

Pakistan Stock Exchange

Basement, PSX New Building.

WWW.PSX.COM.PK

TENDER SECTION

CONTACT INFORMATION

Chief Information Security Officer -

1. Introduction.

Pakistan Stock Exchange (PSX) intends to procure Advanced Malware - EDR solution, and for this reason publishes this RFP to invite Service Providers/ resellers to submit their technical and financial proposals in sealed envelopes for the requirements specified within Annexure 'A'.

2. The Pakistan Stock Exchange.

PSX is the premier Stock Exchange of Pakistan having its offices in Karachi, Lahore and Islamabad. PSX's mission is to provide quality and value-added services to the capital market in a secure, efficient, transparent and orderly manner, which is compatible with international standards and best practices.

3. Project Objectives.

The Primary objective of this RFP is to procure Advanced Malware - EDR solution with one-year technical support. The technical requirements are specified in Annexure 'A'.

4. Information to be submitted.

a) Content of Proposal

The proposal document must include both technical and financial proposal in separate sealed envelopes clearly marked as 'Proposal for the procurement of Advanced Malware - EDR solution'.

b) Delivery Timeframe

Proposed solution should be fully delivered within 4 weeks from the date of issuance of purchase order. Thereafter, Exchange reserves the right to deduct 5% of the total costs each month, if deemed appropriate.

c) Technical Proposal

In the Technical proposal, the service provider should include the following:

a. Company Profile
b. Team profiles, structure and number of certified professionals
c. Deliverables
d. Three verifiable client references where bidder has provided similar type of services

d) Financial Proposal

The financial proposal must include

a. Total cost estimates
b. The financials should be in the format provided as Annexure 'B'.
c. Please include all taxes, fares, fee, transportation, or any other charges.
d. PSX will not entertain any claim of taxes or any other fee after the award of contract.

Please feel free to include additional information you may consider relevant to your proposal.

e) Payment Terms

The payment terms will be as follows:

#	Project Milestone	Payment (% of proposed Cost)
1.	Project Mobilization Advance	50%
2.	Upon Delivery and Installation / Project Completion	50%

5. Vendor Pre-Qualification Criteria

In order to ensure that the services needed by PSX are provided to an acceptable standard and by a qualified vendor, it is necessary to assess all prospective vendors before they can be selected as "eligible vendor". The pre-qualification process uses a pre-established set of requirements against which prospective vendors are evaluated prior to being selected to open their financial bids. All bidders must submit the replies of following questions within the technical proposal:

a. The vendor shall be the renowned IT / Security firm from Pakistan/International Origin OR their authorized business partner with established office in Karachi, Pakistan. The vendor should provide copies of valid Registration Certificates including Service Tax, Sales Tax, Central Excise, etc.
b. Vendor must have at least 5 Years of experience in supporting and implementing similar category solutions i.e. Endpoint Security.
c. The Company should be profit making for at least last three years.
d. Required technical strength and product specific certifications of the vendor's staff must be available. Vendor should share the profiles of the engineers and their experience details.
e. List of 3 (Three) major customers should include public and private sector companies and the vendor should have experience of delivering or implementing product/services to mission critical environments of different enterprises or organizations. Vendor can share its project references of local and international projects in which similar type of services are provided.

6. Proposal Evaluation Criteria

The evaluation will be carried out in two stages as indicated below:

A. Technical Evaluation

The Procurement Committee (PC) will evaluate the technical proposal submitted by the vendor in order to determine the vendors who have fulfill the prequalification criteria.

The PC may call the vendor to seek any clarification (if required). The objective of the PC will be to screen proposals received and evaluate the same for eligibility and establish that:

i. The vendor is technically and financially stable and will be able to cope with the exigencies of the project.

ii. The vendor has made an informed choice while quoting, considering technical understanding of the specification, skills and estimates.

iii. The vendor is technically competent and has the expertise needed for project execution and has presented proof of competence in specific areas.

iv. The vendor has the capacity to deliver the project in time.

v. The vendor has submitted all required information/documents sought as part of RFP response.

vi. The compliance of the technical proposal to the requirements.

B. Commercial Evaluation

The PC will carry out the commercial evaluation of the bids of those vendors who have been found eligible for the said project. The decision of PC will be binding on all concerned and cannot be challenged in any forum.

7. Proposal Scoring Criteria

Each technical proposal will be evaluated against a set of pre-determined criteria to assess the degree to which it meets that criterion. Compliance with requirements will be assessed as a point score based on a scale such as:

0 = No response or Failed to need the criteria
1 = Meet the criteria
2 = Exceeds the criteria

All prequalification criteria have equal weightage. The bidders shall be considered as eligible if the score against the prequalification criteria is at least six.

Reference checks - certain requirements, such as those that pertain to previous experience in required areas of expertise, may be evaluated further though reference checks. If deemed necessary, PC may designate an official who conduct reference checks, the results of which will be provided to members of PC. Once reference checks are completed, PC will review their initial scoring of vendor responses in the context of reference responses.

Further Pakistan Stock Exchange Limited reserves the right to:

I. Reject any or all offers and discontinue this documented process without obligation or liability;
II. Accept other than the lowest bid;
III. Award a contract on the basis of initial offers received, without discussions or requests for best and final Offer;

IV. The decision of PSX will be binding on all concerned and cannot be challenged in any forum.

8. General Terms & Conditions.

a. The price must be quoted in Pakistan Rupees **(PKR).**

b. Penalty will be imposed (Fortnightly One percent of the total amount) in case of supplier didn't supply the equipment in the given time frame.

c. PSX reserves the right to accept or reject proposal of any vendor without explaining or assigning a reason thereof thereby incurring no liability to the affected firm or firms or any obligation to inform the affected firm or firms.

d. A prospective bidder requiring any clarification of the RFP shall notify the PSX in writing well before the submission deadlines.

e. At any time prior to the deadline for submission of bids, PSX may amend the RFP, whether at its own initiative or in response to a clarification requested by a prospective bidder. Prospective bidders shall be informed of changes in the same manner as PSX used for distributing the original RFP. In the case of the amendment to the RFP, the PSX may if it deems necessary & solely at its discretion, extend the deadlines for submission of bids.

f. Terms & Conditions submitted by the vendor will only be valid and applicable, if agreed by PSX.

g. PSX will deduct taxes, duties etc. At the rates prescribed under the applicable laws of Pakistan.

h. Vendors who are insolvent or have filed for bankruptcy are prohibited from participation in the proposal process.

i. The ownership of all data, technical documentation, etc. rendered as a result of this RFP shall be the solely property of PSX. All information pertaining to PSX obtained by the bidder as a result of participation in this project is confidential and must not be disclosed without written authorisation from PSX.

9. Validity of Proposals.

The proposal shall remain open and valid for a period of at least 60 days from the date of submission.

10. Withdrawals and Modification of Proposals.

Proposals may be modified or withdrawn in writing, prior to the proposal closing time specified herein. Proposals may not be modified or withdrawn after that time.

11. PSX Contact Information.

For further details and enquiries, please contact:

Department: Information Security Office

Email : iso@psx.com.pk

Address: Basement, PSX New Building, Stock Exchange Building
Stock Exchange Road, Karachi

Annexure 'A'

S.NO	Description	Yes / No
	General Requirements	
1	The proposed solution must provide complete advanced protection for endpoints with on premise sandbox integration to protect against known and unknown or targeted threats.	
2	The proposed solution must provide EDR capability for in-depth investigation and optionally the quoted vendor must have MDR service in place for future consideration.	
3	The proposed solution must be leader in Gartner and Forrester for EPP and must have strong standing in NSS Labs' AEP and BDS testing.	
4	The endpoint security solution alongside traditional signature based technology must also have behavior monitoring and machine learning features in order to protect against new threats.	
	Endpoint Security Requirements	
5	The proposed solution must have signature based detection alongside advanced machine learning that can machine learn in both file and process analysis and combine it with other techniques to reduce false positives like Certified Good File database.	
6	The solution must have technologies to detect, stop and restore encrypted files from ransomware and must be able to terminate memory resident virus processes.	
7	The proposed solution must have kernel-based technology to catch C&C callbacks that are not browser based and must include Intrusion Prevention System (IPS) with rules that show severity of vulnerability with CVEs being protected, where applicable.	
8	The proposed solution must include behavior monitoring feature to detect suspicious malware activities being performed on endpoint including those conducted via files-less malware and in addition should be able to detect or prevent host file modification, system file modification and system process modification.	
9	The proposed solution should be able to detect and prevent unknown or targeted threats via integration with sandbox – where unknown files can be analyzed dynamically and signatures pushed to proposed endpoint security solution.	
10	The proposed solution should provide application lock-down feature and device control feature to block access to network drives, CD/DVD and USB storage devices. The solution should also be capable to block auto-run function on USB drives.	
11	The proposed solution should be able to provide application lockdown feature via applying both blacklisting and whitelisting.	
12	The proposed should provide application control feature that can block gray software like key loggers, P2P, packet analyzer, password crackers and proxy anonymizer applications without the need to specify these applications manually – the proposed solution should have its own database.	
13	The proposed solution should provide performance impact as little as possible on the endpoints during update and during full system scanning. The proposed solution should provide digital signature cache and should not scan files added to digital scan cache and similarly should provide scan cache that stores file information that has not changed since last scan and	

	are not scanned again. The solution should provide the ability to define the storage period for both these caches.	
14	The proposed solution must additionally provide ability to do full disk encryption and file / folder encryption alongside content based data leakage prevention feature which must block sensitive information being sent via USB, web and email.	
15	The proposed solution must detect data-stealing malware and mitigate risky behavior, must support user justification option when violating the content policies, must provide a way to find and locate sensitive information on endpoints, must restrict printing of sensitive information, must restrict print-screen and must support content control on HTTP, HTTPS, FTP and SMB protocols.	
Endpoint Detection & Response (EDR) Requirements		
16	The proposed solution must have EDR capability that allows monitoring, recording, and performing of both current and historical security investigations and should help in assessing the extent of damage.	
17	The proposed solution should allow PSX the ability to drill down on an interactive process tree that illustrates the full chain of attack in order to identify how the detection was able to arrive, what changes were made, and how it was spread by analyzing activities performed by objects and processes.	
18	The proposed solution must have the ability to provide immediate response in order to terminate processes and isolate users and isolate whole system and also have the ability to use current findings to sweep more endpoints.	
19	The proposed solution must allow administrator to sweep endpoints with multiple search parameters. Sweeping must be available on parameters such as, communication being done, file hashes, registry based activity, user activity, and running processes. The proposed solution must also support industry standard OpenIOC and YARA rules.	
20	The proposed solution should help incident responder by performing steps in incident response lifecycle on endpoints such as Triage and Containment.	
Sandbox Requirements		
21	The proposed sandbox should be on premise with the ability to analyze files / malware without any unnecessary waiting / delay.	
22	The proposed solution must have the ability to create customized sandbox images for virtual execution based on PSX environment in order to effectively detect targeted attacks.	
23	The proposed solution must not be detectable by malware in order to avoid evasion. The solution must be able to detect when system sleep functions are used by malware to evade detection and must be able to accelerate the time to force the malware into execution. The solution must be able to simulate end user actions in order to force the execution of malware that rely on triggers from and end user, like a mouse click.	
24	The solution must be able to utilize both live and fake internet connection to better understand the malware analyzed. It must also be able to utilize a separate network interface for the live communication and not the management interface.	
25	The proposed solution should support the following Windows operating systems for sandbox: Windows 7, Windows 8/8.1, Windows 10, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016 at minimum.	

Email Security Requirements		
26	The proposed solution must include spam filtering engine, IP reputation/RBL feature, SPF, DKIM and DMARC feature and should provide marketing/graymail filter.	
27	The proposed solution must be able to detect known and unknown or targeted attacks with sandbox analysis.	
28	The proposed solution must include machine learning feature to detect malware and must have URL reputation feature to detect phishing or malware based URLs. Additionally, the solution must be able to analyze URLs in sandbox as well and provide complete report on any suspicious objects identified. Also, should provide URL time of click protection.	
29	The proposed solution must utilize multiple detection engines and sandbox simulation to investigate file attachments. Supported file types must include a wide range of executables, Microsoft Office, PDF, web content, and compressed files. Sandbox environment must detonate files, including password-protected archives and document files, and URLs to test for malicious behavior.	
30	The proposed solution should be able to detect social engineering attacks by analyzing several parts of email transmission including email header, subject line, body, attachments and SMTP protocol information.	
31	The proposed solution must be able to detect fraud/business email compromise attacks and it should be possible to select specific high-profile users to detect possible fraud/business email compromise attack to them.	
32	The proposed solution must be able to detect threats hidden in password protected files and password protected archives and should be able to detect threats masqueraded in shortened URLs.	
33	The proposed solution should be able to take action on the suspicious email messages like block and quarantine, delete and should have the capability to whitelist certain email messages to pass through to the recipient. The solution should also be capable to strip suspicious attachments, redirect suspicious links to blocking or warning pages and tag the email subject with a customized string. The solution should notify recipients when a policy rule is matched and must be able to send copies of malicious detected email messages to archive servers.	
34	The proposed solution should be able to effectively block content that is specified as inappropriate from reaching recipients by analyzing both the message content and attachments. The proposed solution should also be able to prevent sensitive content being sent outside by analyzing message content and attachments.	
35	The proposed solution should provide End-User Quarantine feature to improve spam management. Messages that are determined to be spam should be available for users to review, delete or approve for delivery. The solution should be able to automatically send digest notifications to end-users.	

- Please include all applicable taxes in your quoted price.
- PSX will not entertain any claim of taxes or any other fee after the award of contract.

Annexure 'B'

Deployment, Support and Training of Advanced Malware – EDR Solution			
Product	**Description**	**Qty.**	**Price in PKR**
Advanced Malware – EDR Solution	Endpoint Detection & Response (License)	200-300	
	Sandbox (License)	1	
	Implementation, Configuration and Support (1 Year)	-	
	Product training including Foundation, Administration, and Configuration (Foreign training, travel, and accommodation costs)	2	
Advanced Malware – EDR Solution & Email Security Solution (Bundled)	Endpoint Detection & Response (License)	200-300	
	Sandbox (License)	1	
	Email Security (License)	1	
	Implementation, Configuration and Support (1 Year)	-	
	Product training including Foundation, Administration, and Configuration (Foreign training, travel, and accommodation costs)	2	
All Taxes, Fares, Fees etc. with Breakup			
Total Amount			