دولة الكـــــويت

المؤسسة العامة للرعاية السكنية

REQUEST FOR PROPOSAL

كراسة المواصفات الفنية الخاصة بمناقصة

أعمال توريد وتركيب وتشغيل وصيانة أجهزة تجميع وتحليل الثغرات الأمنية لشبكة المؤسسة العامة للرعاية السكنية

2023

Contents

1. Introduction

1.1 Current Environment

Public Authority for Housing Welfare is a Government Organization serving the needs of the Kuwaiti Citizens in the areas of Housing and Welfare. The Head Office is located in South Surra.

Public Authority for Housing Welfare (PAHW) is planning to monitor and collect all the network devices, security devices logs to enhance its security level and protect PAHW network. Bidders are required to comply with all requirements and conditions.

1.2 Project Purpose

The aim of this project is to protect PAHW network, assets, and information by Network Detection and Response (NDR) solutions. These solutions are critical components in cybersecurity infrastructure, especially for PAHW organization, which manages sensitive data and requires consistent network performance. This will enhance the security for PAHW network by identifying and eliminating the threats that could attack the organization on a network-level.

Investing in an NDR solution fundamentally enhances PAHW's ability to protect its assets, ensure continuous operation, comply with regulations, and safeguard its reputation in an era where cybersecurity threats are continually evolving and expanding. This technology is pivotal in developing a mature, responsive, and robust cybersecurity posture that can defend against both current and emerging threats.

The bidder should be responsible for delivering, installing, implementing, and supporting a comprehensive NDR solution. The successful bidder will be responsible for ensuring the complete implementation of the project with PAHW IT team.

2. Scope of Work

The proposed NDR solution should monitor network traffic and user behavior, detects and responds to anomalous and malicious activities using advanced analytics, ensures compliance with relevant regulations, and proactively safeguards operational continuity by significantly minimizing the impact of cybersecurity threats on PAHW.

The NDR solution should have the following features:

- An On-Premises solution ensuring data remains confined to the customer's network.
- Integration with all PAHW's current network and security fabric.

- Proprietary, high-capacity malware scanning, leveraging Artificial Neural Networks (ANN)1, aimed at identifying file-based assaults, encompassing more than 20 malware attack scenarios.
- Minimize the timeframe for malware detection and investigation from minutes down to seconds.
- Accurately identify intrusions from all directions: North/South/East/West
- Recognize botnets and weak ciphers within the network.
- Emulate the strategies of seasoned security analysts in identifying outbreaks, anomalies, and root causes of malware infiltrations.
- Implement on-site learning to diminish false positives by examining organization-specific traffic and adapting to newly camouflaged threats.
- Provide Detections and Device Enrichment Netflow Ingestion and AD Integration

At the time of installation, vendor must do the necessary configuration to integrate different network components required to be managed by the proposed solution. For further plans in the future, the bidder is responsible for adding or removing any integrated system within the proposed solution.

3. General Requirements

The bidding company should meet the following requirements and qualifications. Failure to do so will disqualify the bidder and his bid will be rejected.

- Bidder must be registered with Central Agency of Information Technology (CAIT). (Valid Proof must be submitted)
- Bidder must be an authorized **partner** for all the proposed devices (Valid proof must be submitted).
- The bidder should have **Gold partnership or higher for the proposed NDR solution and delivered devices**; the partnership certificate should be submitted in the bidder proposal (Valid proof must be submitted).
- The bidder should agree on a monthly site visit to check the hardware appliances and NDR solution.
- Bidder must provide regular support as well as NDR and ANN engine updates & baseline.
- The bidder has to present its credentials in terms of staff qualifications as follows and failure to comply with the below shall result in disqualification of the Bidder offer:
    - At least 2 Engineers with certifications of the proposed solution for implementing the project. All proposed staff shall be under **Bidder sponsorship during tender submission (civil id for each engineer has to be attached in the proposal).**
    - The bidder must have a dedicated project management team to do the installation, implementation, integration and testing. Different services team to do the

maintenance during warranty period. Organization chart must be submitted as evidence.
    - Bidder must submit list of project and support teams showing each member skills, certificates, and description for his contribution in the project. CVs, civil IDs, and Certificates of all the staff must be submitted with the tender submission.
    - The bidder must have dedicated project management team to do the implementation, and different services team to do the maintenance during warranty-period.
    - Bidder must have qualified staffs that are capable of Support and Maintenance of proposed solution.
- Bidder must supply a warranty throughout the period of the contract of all the required hardware and NDR software solution.
- Bidder should submit Help Desk/Call Center Details including level of escalation and staff details.
- All Hardware and solution installation, implementation, and configuration should be qualified engineers from the bidder.
- Bidder should provide support letter confirming that bidder will offer vendor support and warranty for proposed solution.
- The bidder must submit along with his submission complete details on the support services including Support Coverage, Escalation Procedures and SLA.
- The project must be accomplished and maintained by the bidder. **Third parties are prohibited during all the project phases.**
- Handing over the project will be subject to inspection; testing and acceptance of all items by PAHW technical staff.
- Training and knowledge transfer to PAHW engineers will also be the responsibility of the bidding company during the support period.

4. Technical Requirements

The NDR solution should provide a scale out distributed architecture with the following characteristics:

- Systems requirements
    1. Supports 2 factor for administrative log-in.
    2. Supports LDAP/RADIUS remote admins.
    3. Supports RBAC for administrative access.
    4. Solution must be able to run on an air-gapped environment.

- Branch detection capabilities

    1. Ability to detect and name botnet detections, both DNS and IP based botnet

2. Ability to profile traffic using ML and identify anomalies.
3. Ability to detect and name malicious web campaigns.
4. Ability to detect Network Intrusions
5. Ability to detect weak cipher and vulnerable protocols.
6. Ability to differentiate different malware and attack types.
7. Virtual Analyst Capabilities to offload/assist SecOps in Breach Prevention. Please detailed.
8. Ability to trace the Source of infection e.g., WannaCry.
9. Sub-second detection without running/executing file like sandbox analysis.
10. Solution must be capable of high-performance network traffic analysis, 10Gps line rate sniffer rate and at least 140K+ files per hour
11. Solution must be able to stop "patient-zero" i.e. ability to stop the first malware download (web) from host i.e. inline blocking
12. Solution must have proven detection rate via 3rd party validation such as malware strike packs from traffic generators.
13. Solution must provide MITRE ATT&CK view of attacks.
14. Solution must be able to classify different malware types (e.g., Banking Trojan) and by hosts (e.g., Host1 infected with Ransomware and Downloader)
15. Solution must detect "fileless" malware as a category. Fileless is defined as no files planted on infected hosts, purely operate in memory/CPU instructions level.
16. Solution may provide a big picture for threat analysis for forensic investigation.

- Deployment management capabilities

1. Solution can be deployed in sniffer mode without sensors.
2. Ability to integrate with NGFW for quarantine.
3. Solution has the ability to be deployed in a 'offline/airgap' (i.e. no Internet) environment.
4. Solution must have ICAP support.
5. Solution must support whitelist settings to filter trusted hosts
6. Solution must support REST API for automation, please list capabilities with API.

- Logging & reporting requirements

1. Display attack in timeline format, showing source of attack.
2. IOC export with STIX v2 format
3. Supports remote logging, please state options.

- Response integrations

1. Solution MUST have ability to integrate with NGFW and PAHW's other products for quarantine/banned IP, and ability to quarantine depending on severity of event.
2. Solution MUST support 3rd party API call upon threat detection.

- On premise hardware specifications
    1. Standalone and sensor deployment modes
    2. Total interfaces: 2x 10/100/1000 RJ45 ports, 4x 10G SFP+, 1 x RJ45 console
    3. Sniffer/Capture interfaces: 3 (3 x Fiber 10G SFP+)
    4. Storage capacity: 2 x 7.68 TB (RAID 1) total 7.68 TB (RAID 1)
    5. Include removable hard drives, redundant hot swappable, power supplies.
    6. NDR sniffer throughput :10 Gbps/ 10 Gbps (HTTP/enterprise mix) - single port sniffer 20 Gbps / 20 Gbps (HTTP/ P/ enterprise mix) - dual port sniffer.
    7. NetFlow throughput 70k per sec.
    8. Malware Analysis Throughput (files per hour) of 170K files per hour.
    9. Appliance for Network Anomalies and 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 4 x 10GbE SFP+, 2 x 1Gigabit Ethernet connection (management).
    10. Netflow support for the appliance
    11. There should be no limitation on the supported number of IPs

5. Support and Service Requirements

5.1 Hardware & NDR Solution Support:

- Bidder must provide a warranty throughout the contract period for the required hardware and NDR Solution from the date of acceptance of the installation, configuration, and testing. The date of acceptance of the devices is defined as the date that all network-related hardware devices are properly delivered, installed, configured, tested and approved as operational by PAHW team.
- The Bidder shall have a well-organized 'Help Desk' system in their office, where a support call can be placed. Immediately after placing the call, helpdesk operators shall be able to provide the Company with a ticket number. This ticket number shall be used as a reference for any future communication about that particular call.
- Bidder must provide any required hardware/software licenses per the requirements.
- Bidder has to follow PAHW hardware design for this project. Any change in the design or proposing any additional hardware will not be acceptable. PAHW Management approval is required before any change in the design.
- Bidder must agree to provide every month visit for the hardware and services components check-up (The report must be submitted after each visit).

5.2 Professional Services

- Bidder is totally responsible for the delivery of the necessary hardware and software for the project.

- The successful bidder takes full responsibility for installation, integration, configuration, testing and maintaining all delivered devices and software in accordance to PAHW scope of work.

- The bidder should be responsible for providing detailed system knowledge transfer and support during the support period.

- All the devices (hardware items) belong to PAHW should be under local partner Support (24x7).

- The Bidder should offer complete system description, brochure, and catalogue of proposed system containing full technical specifications.

- The Bidder should provide a project implementation time schedule. Bidder should provide detailed project plan with deadlines for each task.
- The bidder must propose the latest versions of required S/W and H/W at the time of bidding.
- Bidder must propose, install, test, label and warrant all components requested in this RFP.
- Bidder is totally responsible for the delivery of the necessary hardware for the project.

6 . Project Documentation & Training:

- Bidder should provide training on all the installed hardware and NDR Solution to 5 PAHW IT employees. Bidder has to train them how to run and maintain the whole solution.

- Bidder should provide documentation of how to integrate, delete, and maintain new component(s) to the proposed NDR solution data on the new appliances.

- The following documentations to be submitted to PAHW by the bidder:
  - Installation Document (Customized to PAHW)
    - The hardware and software requirements for the proposed solution.
    - Step by step instructions for building the proposed solution (screenshots are preferable with description).
    - Step by step instructions for installing, maintaining and configuring the system based on the standard configurations that come from manufacturer (unless the

PAHW request different configuration, then the configuration must reflect the requested changes). Screenshots preferable with description.

- Official vendor administration document and user document.