Terms of Reference (ToR) for establishing subscription based service to the Vulnerability Management Platform by Qualys

Introduction

The purpose of this Terms of Reference (ToR) is to obtain offers to provide the Organization for Security and Cooperation in Europe (OSCE) with vulnerability assessment and management solution and support services based on Qualys platform for a 5-year period.

The successful Vendor is expected to deliver the necessary products and licenses and provide maintenance and operational support on an as-needed basis during the duration of the Contract.

Background

The Organization for Security and Co-operation in Europe (OSCE) is the world's largest security-oriented intergovernmental organization with its Secretariat located in Vienna, Austria. For the detailed information about the work of the OSCE and its presence, please visit www.osce.org

The Organisation operates distributed information systems architecture, with servers primarily concentrated at the Organisation's Secretariat offices in Vienna, Austria, and distributed infrastructure and local application servers in several locations across Europe and Central Asia. The locations are connected to the OSCE Secretariat in Vienna, Austria through Virtual Private Network (VPN) connections, but each of them also has its own internet connection protected by firewalls and other security appliances.

In order to assess the security posture of the assets on the internal and externally facing networks, the OSCE has deployed a Vulnerability Assessment and Management System based on Qualys platform in 2016 (the established Contract expire at the end of September 2018). The solution was extended to cover all internal hosts on the network in 2017. Currently the OSCE has the following Qualys modules and licenses:

- Qualys Vulnerability Management – Enterprise – Public Sector – for 8,000 internal and 96 external IPs:
    - Scheduled and on demand security scans;
    - Unlimited user accounts;
    - Unlimited network discovery maps;
    - Executive-level & detailed technical reports;
    - Qualys PCI is bundled for External IPs only at no added cost;
    - 24x7 email and telephone Customer Support.
- Qualys Virtual Scanner – 6 appliances;
- Qualys Cloud Agents – 5,500 agents.

Solution Requirements

The Information and Communications Technology Services (ICT) of the OSCE Secretariat is interested to obtain a solution that must fulfil the following mandatory requirements:

1. A cloud-hosted vulnerability assessment and management platform based on Qualys Enterprise version that provides the ability to assess security vulnerabilities for 8,000 internal hosts (including 5,500 with Cloud Agent) and 96 external IPs;
2. Virtual scanner appliances on VMWare platform (6 appliances, support for vSphere 6.0 – 6.7 mandatory);
3. Cloud Agents for all endpoints and servers on internal network (at least 5,500 hosts);
4. Unified View of asset and vulnerability data from network and agent-based scans, without duplication of assets;
5. Must support a variety of reports, including of the following:
    a. High Severity Vulnerability/Risk report;
    b. Time series trend reporting for vulnerabilities with asset pools;
    c. Aggregate recommended remediation tasks;
    d. Remediation timelines and time to remediation for vulnerabilities at the per-host and aggregate levels (e.g., average remediation times for category X vulnerabilities);
    e. Compliance reporting on meeting remediation target deadlines per asset location and asset group;
    f. Per scan ad-hoc reporting;
    g. Per host ad-hoc reporting;
    h. Per network ad-hoc reporting;
    i. Per platform (e.g., Windows, Linux, Cisco, etc.) vulnerability reporting;
    j. Customisable reporting mechanisms other than the above.
6. Platform data export and import for custom reporting and data input (e.g., approved asset inventory) to/from the OSCE internal MS-SQL database, via API;
7. Capability to local IT staff across the Organisation to manage their own scanning, asset management and reporting requirements;
8. Vulnerability assessment and reporting with differentiated levels of risk per vulnerability and recommended remediation targets per vulnerability based on criticality of asset and severity of vulnerability;
9. Assignment of vulnerability remediation tasks to asset pool owners with remediation deadlines based on criticality of asset and severity of vulnerability;
10. Must support unlimited number of users;
11. Must support differentiated user roles by privilege level, asset pool and device access;
12. Authenticated network scans for databases, network devices and non-endpoint devices (e.g. printers, scanners, IoT devices, etc.);
13. Must support two factor token integration for user authentication (use of RSA token is preferred as this is already available at OSCE);
14. Must support authenticated/encrypted report delivery;
15. Upgrade protection including signature updates, patches and upgrades to major releases as well;
16. Remote and on-site support, training and maintenance services on an as-requested basis for configuration, changes, reports and operational issues.

The platform is intended to be used for the next 5 years, paid on a per year base. The OSCE is expecting to establish a new Contract in Q3 of 2018.
A yearly increase or decrease of licensed volume must be possible to adjust to actual consumption.