RFP for vulnerability management product: cloud

Required features & functions

|  |  |  |
| --- | --- | --- |
|  | **Service/function:** | **Description:** |
| **1** | **Attack vector coverage:** | |
| 1.1 | Network and systems | Scanning of all types of systems connected via TCP/IP. Support scanning of local and public systems and computers, cloud infrastructure, OT/SCADA, and IoT. |
| 1.2 | Web applications | Web application scanning (scanning of websites). |
| 1.3 | API | Scanning of Rest APIs. |
| **2** | **Deployment & administration:** | |
| 2.1 | On-premise | The service should be installed as a virtual appliance in the customer’s local environment. No data should be communicated outside the organization’s network. |
| 2.2 | Web-based control panel | One single web-based interface for all products and functions. |
| 2.3 | Orchestration | Possibility to let different sub-departments have access to designated systems and data, at the same time as there is a central login for the central IT function. |
| 2.4 | Multiple control panels with permissions | Possibility to set up multiple control panels with restricted permissions while providing centralized access. |
| **3** | **Scans:** | |
| 3.1 | Unlimited amount of scans | Unlimited number of scheduled scans and on-demand scans. |
| 3.2 | Unlimited number of scan nodes | Scan using an unlimited number of scan nodes that allows scanning of different parts of the network simultaneously. |
| 3.3 | Scan the entire IT environment | Scan segmented and geographically separated networks etc. |
| 3.4 | Attack Surface Management (ASM) | Scan publicly facing attack vectors to detect and minimize the attack surface. |
| 3.5 | Scheduling | Schedule scans and reports. |
| 5.9 | Blackout window | Possibility of predefining time windows when scans are paused automatically. |
| **4** | **Scan functions:** | |
| 4.1 | CIS Benchmark for system hardening | Certified for CIS Benchmark policy scanning for system hardening for all common systems. |
| 4.2 | PCI DSS ASV scanning and ASV certified | The network scan engine should be certified by PCI DSS for ASV (Approved Scanning Vendor). |
| **5** | **Functions:** | |
| 5.1 | Platform API | Platform API for integrations. |
| 5.2 | Ready-made integrations | Ready-made integrations with systems for notifications. ticketing, SIEM, and CMDB. |
| 5.3 | Administration of vulnerabilities | A central tool with vulnerability data with the ability to prioritize, filter, ignore, and sort vulnerabilities. |
| 5.4 | Customizable reports | Customizable reports to control report type, selection, and scope. |
| 5.5 | Compliance reports | Reports for GDPR, NIS/NIS2, ISO 27001, and PCI DSS. |
| 5.6 | Monitoring of changes | Monitoring of changes, such as new vulnerabilities, opened/closed ports, and new/dead hosts. |
| 5.7 | Remediation | Policy-based remediation (ticketing system). Ability to sort, filter, and structure tickets and set due dates for cases. |
| 5.8 | SAML 2.0 Single Sign-on (SSO) | Support for federated login using SAML 2.0. |
| **6** | **Unification:** | |
| 6.1 | Unified asset, vulnerability, and unified risk score | Unified asset and vulnerability management for all attack vectors to be able to prioritize risk efficiently. |
| **8** | **General:** | |
| 8.1 | Help to create continuity routines and processes | Carried out by specialists within vulnerability assessment. |
| 8.2 | IPv6 support | The service is fully IPv6 compatible. |
| **9** | **Security:** | |
| 9.1 | Users | An unlimited number of users and collaboration opportunities between users. |
| 9.2 | Two-factor authentication | Policy-based two-factor authentication. |
| 9.3 | Network restricted access | Restrictions to login to the web interface based on IP networks. Possibility to select that if the user does not come from a known network, two-factor authentication is automatically activated. |
| 9.4 | RBAC | Role-Based Access Control (RBAC) to restrict access. |
| **11** | **Support** | |
| 11.1 | Support and training | Support and training carried out by specialists within vulnerability assessment. |

Amounts for quote

|  |  |  |
| --- | --- | --- |
|  | **Product:** | **Amount:** |
| **12** | **Technical:** | |
| 12.1 | Network scanning | [amount of active IP addresses] |
| 12.2 | Web application scanning | [amount of web apps] |
| 12.3 | API Scanning | [amount of APIs] |