SERVICE DESCRIPTION

Managed Vulnerability Scanning

Overview

Trustwave's Managed Vulnerability Scanning (MVS) service (**"Service"**) provides Client with vulnerability scanning solutions to identify vulnerabilities and misconfigurations in Client's environment.

Trustwave will provide and manage all aspects of the vulnerability scanner (**"Scanner"**), which includes maintaining the Scanner and scheduling and running vulnerability scans. Trustwave may also use Client's vulnerability scanner, depending on whether it is supported by Trustwave, in a manner agreed by Trustwave and Client.

The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Form between Trustwave and Client.

Core Service Features

The Service includes the following core features:

Initial Vulnerability Workshop

Trustwave will conduct a collaborative workshop to identify Client's areas of concern and understand Client's security maturity.

Client Obligations

For Trustwave to provide the Service, Client will:

- Provide contact details for and access to Client stakeholders and escalation points and remain available for communication from Trustwave;
- Attend the workshop and provide logistics support for booking meetings and arranging access to required personnel;
- Coordinate with Trustwave to discuss concerns and perceived threats, objectives, and delivery expectations;
- Provide Trustwave with access to systems with appropriate credentials, as reasonably requested by Trustwave; and
- Provide Trustwave with any documentation Trustwave may reasonably request to perform the Service.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Establish engagement roles and responsibilities for stakeholders;
- Deliver and facilitate the initial workshop at a date and time agreed between Trustwave and Client;

- Coordinate with Client to discuss concerns and perceived threats, objectives, and delivery expectations;
- Review current state information and documentation provided by Client; and
- Develop a report giving details on the workshop and outcomes.

Environment Scanning – Discovery, Network, Application, and Database

Trustwave will scan and rescan for vulnerabilities with a full suite of scanning capabilities dependent on the assets and targets within scope:

Discovery Scanning

Trustwave will identify the active assets within Client's environment.

Network Scanning

Trustwave will seek to identify network vulnerabilities and generate insights into where Client's network may be exposed to threats from within and outside the firewall:

- Internal scanning provides a hacker's view of vulnerabilities inside the network behind the firewall.
- External scanning offers insights into what vulnerabilities may be exposed to the outside. External scanning is conducted against internet-facing assets.

The scope of network scanning is based on Client's number of IPs and network segments, as indicated by Client and agreed with Trustwave.

Application Scanning

Trustwave will seek to identify vulnerabilities across Client's applications prior to deployment and/or in production to mitigate risks to Client's sensitive data. Additionally, Trustwave will employ stack ranking to prioritize time spent on significant threats.

The scope of application scanning is based on Client's number of applications, as indicated by Client and agreed with Trustwave.

Database Scanning

Trustwave will seek to identify misconfigurations, identification and access control issues, missing patches, and other vulnerabilities that could lead to unauthorized modification of data held within Client's databases.

The scope of database scanning is based on Client's number of databases and database segments, as indicated by Client and agreed with Trustwave.

Client Obligations

For Trustwave to provide the Service, Client will:

- Coordinate with Trustwave to define assets and targets; and
- Provide Trustwave with support during the scanning process, as required.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Coordinate with Client to define all assets and targets to be scanned within Client's environment;
- Work with Client to identify compliance requirements to determine appropriate scanning policies that may be applicable to Client's security objectives;

- Conduct discovery and vulnerability scans of the in-scope assets and targets (i.e., discovery scanning, network scanning, application scanning, database scanning); and
- Notify Client of any assets or targets that the Scanner is unable to scan and provide supporting information to Client.

Scan Frequency

Trustwave will conduct vulnerability scans of the in-scope assets and targets on either a one-time, quarterly, monthly, or weekly basis. The scan frequency will be indicated in a SOW or Order Form between Trustwave and Client.

Client Obligations

For Trustwave to provide the Service, Client will:

- Coordinate with Trustwave to develop and implement schedules that set forth the frequency at which the Scanner scans the in-scope assets and targets; and
- Coordinate with Trustwave to determine whether the Scanner may run in Client’s maintenance windows and set up the parameters for such schedules.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Develop and implement schedules that set forth the frequency at which the Scanner scans the in-scope assets and targets; and
- Determine whether the Scanner may run in Client’s maintenance windows and set up the parameters for such schedules.

Scanner Management

Trustwave will provide the Scanner to deliver the Service, including maintenance and monitoring of the Scanner:

Virtual Appliance

Trustwave will provide Client with a virtual remote appliance (**“Virtual Appliance”**) for internal scanning purposes and ensure Client is using the latest version of the Virtual Appliance.

Software Updates

Trustwave will apply updates and security patches to the Scanner. Trustwave will work with Client to schedule security updates during Client’s maintenance windows.

Health Monitoring

Trustwave will inform Client regarding issues experienced with the Scanner and remediate issues in a timely manner.

Client Obligations

For Trustwave to provide the Service, Client will:

- Coordinate with Trustwave to schedule security patches, hotfixes, and policy updates during Client’s maintenance windows; and
- Review notifications and error reports provided by Trustwave pertaining to the Scanner.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Deploy a Virtual Appliance for Client for internal scanning purposes;
- Apply upgrades and security patches to the Scanner;
- Coordinate with Client to schedule security patches, hotfixes, and policy updates during Client's maintenance windows;
- Collect and report to Client any errors displayed by the Scanner; and
- Remediate issues pertaining to the Scanner in a timely manner.

Vulnerability Reporting

Trustwave will provide Client with reporting following vulnerability scans, aligning to the scan frequency or otherwise agreed cadence between Trustwave and Client. This reporting will set out the findings and vulnerabilities identified during the vulnerability scans. Trustwave may also provide Client-specific vulnerability reporting, as reasonably requested by Client and agreed between Trustwave and Client.

Client Obligations

For Trustwave to provide the Service, Client will:

- Review Trustwave's vulnerability reports and attend review sessions conducted by Trustwave; and
- Support the identification of appropriate owners for Trustwave's findings and recommendations.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Present vulnerability reports to Client for review and feedback; and
- Confirm delivery of key activities and reports.

Vulnerability Advisor

Trustwave will provide Client with a vulnerability point of contact throughout the Service. This point of contact will guide Client through the vulnerability scanning process, provide context to vulnerability reports, and make exchanging information with Trustwave more efficient, increasing Client's effectiveness in remediating vulnerabilities.

Client Obligations

For Trustwave to provide the Service, Client will:

- Coordinate with Trustwave through the vulnerability scanning process; and
- Escalate concerns to Trustwave for resolution.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Act as the point of contact between Trustwave and Client;
- Guide Client through the vulnerability scanning process; and
- Review discovery and vulnerability scans and provide context to vulnerability reporting.

Additional Service Features (Elite Package)

The Service comes in either the Standard or Elite package. Where Client purchases the Elite package, the Service will include the following additional features:

On-Demand Scans

Trustwave will conduct on-demand vulnerability scans of the in-scope assets and targets as requested by Client, such as when new threats emerge in Client's environment or when Client deploys new assets. The Elite package includes three (3) on-demand scans over the course of the Service. For these on-demand scans, Trustwave will commence the scan within one (1) business day of Client's notification that an on-demand scan be conducted.

Client Obligations

For Trustwave to provide the Service, Client will:

- Notify Trustwave when there is a need to conduct an on-demand scan of the in-scope assets and targets; and
- Provide Trustwave with support during the scanning process, as required.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Conduct a vulnerability scan of the in-scope assets and targets within one (1) business day of Client notification that an on-demand scan be conducted.

Verification of Critical Vulnerabilities

Trustwave will manually review critical vulnerabilities identified by the Scanner and seek to remove duplicates and false positives where identified.

Client Obligations

For Trustwave to provide the Service, Client will:

- Review findings provided by Trustwave for additional review and make determinations on whether they are false positives.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Review critical vulnerabilities identified by the Scanner and present potential duplicates and false positives to Client for additional review; and
- Remove identified duplicates and false positives from vulnerability reporting.

Cyber Advisor

Trustwave will provide Client with an advisory point of contact throughout the Service. The advisory point of contact will be focused on strategic remediation advice, including roadmap development and regular cadence trend analysis.

Client Obligations

For Trustwave to provide the Service, Client will:

- Coordinate with Trustwave on vulnerability prioritization; and
- Coordinate with Trustwave on developing the roadmap for remediating identified vulnerabilities.

Trustwave Obligations

As part of providing the Service, Trustwave will:

- Support Client with vulnerability prioritization;
- Outline cybersecurity best practices for Client to consider; and
- Develop a roadmap for remediating identified vulnerabilities.

Service Packages

Client will select either the Standard or Elite package, which will be indicated in a SOW or Order Form between Trustwave and Client:

	Standard	Elite
Initial Vulnerability Workshop	Included	Included
Discovery Scanning	Included	Included
Network Scanning	Included	Included
Application Scanning	Included	Included
Database Scanning	Included	Included
Virtual Appliance	Included	Included
Software Updates	Included	Included
Health Monitoring	Included	Included
Vulnerability Reporting	Included	Included
Vulnerability Advisor	Included	Included
Verification of Critical Vulnerabilities	Not Included	Included
Cyber Advisor	Not Included	Included
On-Demand Scans	Not Included	3 per Year
Scan Frequency	One-Time, Quarterly, Monthly, or Weekly	One-Time, Quarterly, Monthly, or Weekly

Client may elect to conduct vulnerability scanning on a one-time, quarterly, monthly, or weekly basis in either the Standard or Elite package, with pricing based on the package, scan frequency, and in-scope assets and targets.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave's Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable SOW or Order Form between Trustwave and Client.