Trustwave®

SERVICE DESCRIPTION

Managed Vulnerability Scanning

Overview

Trustwave's Managed Vulnerability Scanning service ("**Service**") manages all aspects of the vulnerability scanner ("**Scanner**") provided by Client or Trustwave, which includes setting up, scheduling, running scans, reviewing results, and sharing agreed reports to achieve the Client's security goals. The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Service Features

The Service includes the following features:

Scanning Tool Management

Scheduling

Trustwave will assist Client in developing and implementing schedules that set forth the frequency at which the Scanner scans the Client's environment. Trustwave will also assist Client in determining whether the Scanner may run in a maintenance window and set up the parameters for such schedules.

Coverage

Trustwave will define all external assets or internal network segments ("System Targets") to ensure they are within the appropriate scanning schedule. Additionally, Trustwave will notify Client of any System Targets the Scanner is unable to scan and provide any supporting information to Client.

Platform Maintenance

Trustwave will only apply upgrades and security patches supplied by the Scanner vendor. Trustwave will work with Client to schedule any security patches, hotfixes, and policy updates during Client's maintenance windows.

Virtual Appliance

If Client selects an internal vulnerability scanning, Trustwave may provide Client with a virtual remote appliance called VRPT ("Virtual Appliance") and ensure the client is using the latest version of the virtual appliance.

Client may opt to provide their own Virtual Appliance and makes sure that the appliance is updated.

Reporting

Trustwave will generate and deliver all reports to Client using the tool that was agreed upon during the SOW process.

Report format and templates available will be dependent on capability of the reporting tool chosen by the Client.

Health Monitoring

Trustwave will monitor scanning start and completion times and inform Client if the Scanner is unreachable. Trustwave will collect and report to Client any errors displayed by the Scanner. If any issues arise that Trustwave determines are outside of the Scanner, Trustwave will notify Client and provide any supporting information to enable Client to remediate appropriately.

Continuous Improvement

The fluidity of modern business means that to deliver to the business needs a program of continuous improvement needs to be adopted. This is delivered via:

- Identify and help deliver on areas of improvement with the report we are providing
- Assist in prioritizing vulnerabilities
- Review scanning schedules and approach
- License usage and review
- User entitlement reviews

Optional Add-On Services

Trustwave will provide the following add-on services for an additional charge:

Fine-tuning False-Positive

Trustwave will review all findings generated from the Scanner and remove any false positives that can be removed by product functionality available, as determined by Trustwave. Trustwave may present certain findings to Client for additional review if such findings are not reasonably determined to be false positives, and Client will review and make such determinations instead.

On-Demand Scans

Client may request on-demand vulnerability scans as new threats emerge in Client's network environment or when Client deploys new assets. Client may request additional on-demand scans, but Trustwave does not guarantee the availability of such scans. Factors including but not limited to resources' availability, tool limitation, and project scope will be put into consideration.

Threat Vulnerability Manager (Advisor)

Trustwave will provide Client a single point of contact who will guide the Client through vulnerability process, provide context to vulnerability reports, and customize details of the scanner to the environment.

The Threat and Vulnerability Manager (TVM) may assist in using the Scanner to its fullest potential, including taking advantage of unused features, provide detailed information about vulnerabilities, remediation progress, and share best practices.

This single point of contact will make exchanging information between Trustwave and the client more efficient and increase the client's effectiveness in remediating vulnerabilities. Along with providing detailed information about vulnerabilities and remediation options, the SpiderLabs TVM can share best practices with the client. TVM would then provide:

- Key point of contact between CLIENT and the Trustwave Team
- Review of discovery scans
- Review of vulnerability scans
- Prioritization of vulnerabilities
- Remediation advice
- Access to SpiderLabs Security Advisories

Obligations

Client Obligations

For Trustwave to provide the Service, Client will

- License a scanner from a Trustwave-approved scanning vendor
- Provide Trustwave with appropriate access to its Scanner and scanning environment
- Remediate any errors, bugs, or other such issues within the client environment

Trustwave Obligations

As part of the Service, Trustwave will

- Meet Client's scanning requirements as detailed in a SOW or Order Confirmation
- Gather information needed to resolve any issues with the Scanner

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 Statement of Work or Order Confirmation between Trustwave and Client.