SERVICE DESCRIPTION

Managed 3rd Party Vulnerability Scanning

Service Outline

Description

Trustwave Managed Vulnerability Scanning Services (MVSS) will allow organizations to utilize the Vulnerability Scanner that they have already invested in to provide actionable reports that will enable key security resources to focus on organization's priorities. The Trustwave SpiderLabs Vulnerability Management Services (SVMS) team will use its extensive knowledge base to maintain Client's Vulnerability Scanner to assist in achieving Client's vulnerability management and application security goals.

SVMS will maintain Client's security scanning scanner's schedule(s) to help ensure completion, coverage, and reporting. Client's security process will define how SVMS implements and configures the scanner's policy(s)/check(s) along with patches, updates, and upgrades.

Features

Trustwave MVSS will provide the following services for approved Vulnerability Scanner.

- Scan maintenance
    - Scheduling and coverage
    - Policy
    - Validation
- On-demand scans
    - Zero-day/new application scans
    - Remediation validation scans
- Reporting
- Vulnerability scanner maintenance
    - Upgrades
    - Patches/updates
    - Health monitoring

Service Operations

Scan Maintenance

Scheduling

The remediation process followed by Client will define the vulnerability scanning schedule. Clients may have a mix of scan schedules as long they have processes in place to utilize the results within their vulnerability or development lifecycles. Should the Vulnerability Scanner allow it, SVMS will set the scan schedule (or schedules) to run in a maintenance window. SVMS will advise Client of the scanner's ability to complete the scan(s) within the maintenance window.

Coverage

SVMS define all the scan targets and ensure that all are within the appropriate scan schedule. SVMS will notify Client of any targets that the scanner is unable to scan and provide any information available to Client as to why that target could not be scanned.

Policy

SVMS will define Client's policy(ies) to ensure that only applicable checks are enabled. SVMS will create as many policies as needed to ensure that the scan(s) can complete in a reasonable timeframe and remove any results that do not apply to Client's technologies or security posture.

Validation

Trustwave will monitor scans as they start and complete. SVMS will provide a report (if available within the scanner) on which targets the scanner was unable to scan and why. Should any scans result in error, SVMS will investigate and notify Client.

On-Demand Scans

Zero-Day/New Application Scan

As new threats emerge or Client releases a new web/mobile application, Client may request an on-demand vulnerability/application scan. Client is guaranteed two on-demand scans per quarter. Clients can request additional ad-hoc scans but Trustwave cannot guarantee performance of such scans.

Remediation Scan

A remediation scan is a scheduled scan to test for previously known vulnerabilities. Clients are guaranteed one remediation scan per completed scan. Clients can request additional remediation scans but Trustwave cannot guarantee performance of such scans.

Reporting

Scan Results

SVMS seeks to make all scan results without validation available to Client within one (1) business day. Variables within the scanner or Client's environment might make this timeframe impossible.

Reporting

SVMS will generate all reports for Client using the default report templates in Client's vulnerability scanner. SVMS will not edit reports except in the event that a reported vulnerability makes the report unreadable or makes it impossible to distribute the report because of its size or other factors.

Scan Platform Maintenance

Upgrades and Patches

SVMS will only apply upgrades and patches supplied by the vendor of the selected scanner. All security patches/hotfixes and policy updates will be scheduled and applied during Client's maintenance windows. SVMS will plan and implement upgrades and major releases a maximum of twice a year. Client will also be responsible for any OS upgrades and patching, and or upgrading agents on endpoints.

Health Monitoring

Trustwave will provide health monitoring for the vulnerability scanner. If the vulnerability scanning device is unreachable by Trustwave, SVMS will inform Client. SVMS will monitor scan start and completion. If the issue is outside of the scanner, SVMS will notify Client and provide information for remediation. Errors displayed by scanner will be collected and reported to Client for remediation.

Troubleshooting

Client is solely responsible for remediation of any errors, bugs or other such issues that occur within the scanner. Trustwave will assist in replacing and gathering any information needed to resolve the issue.

Optional Services

False-Positive Remediation

SVMS will review all findings generated from the scanning scanner. SVMS will escalate findings that need further evidence beyond what the scanner identified. SVMS will also remove findings that are proven to be incorrect (false positives) Any finding that does not have significant evidence or cannot be proven incorrectmay be de-escalated but presented to Client for further information or review.

SpiderLabs Vulnerability Advisor

The SpiderLabs Vulnerability Advisor will be available as a single point of contact to guide Client through the vulnerability/application remediation process, provide context to vulnerability/application reports, and customize the details of the scanner to Client's environment. This single point of contact will make exchanging information between Trustwave and Client more efficient and increase Client's effectiveness in remediating vulnerabilities. Along with providing detailed information about vulnerabilities and remediation options, the SpiderLabs Vulnerability Advisor can share best practices with Client. While SVMS will tune the policy to Client's environment, the SpiderLabs Vulnerability Advisor will work to help Client use their scanner to its fullest potential, including taking advantage of unused features or functionality.

Responsibilities and Assumptions

Client

- Have a valid license and support contract from vendor
- Has sole discretion to remediate what and when for the scanner but understand that it will invalidate any guarantees by Trustwave
- Remediate any failed scanner login attempts to target(s)

Definitions

Target(s):

- Vulnerability Scanner: An Ip-addressable asset that is responsive to remote requests by the vulnerability scanner.
- Database Scanner: An Ip-addressable asset that is responsive to remote requests that the database scanner identifies as a database.
- Application Scanner: A web "Application," for purposes of Trustwave scanning, is a unique set of code that has a business function, usually with a starting URL accessing a normal entry point, hosted from one server with one IP address to access it. It has one "hostname," (e.g., store.mycorp.com). "store.mycorp.com" and "news.mycorp.com" are different hostnames and are therefore considered different Applications. Disjoint, unrelated websites that happen to be hosted from the same server are not considered part of one "Application."