Trustwave®

SERVICE DESCRIPTION

Managed Security Testing

Version 2.0
September 2020

Table of Contents

Service Description Overview

Trustwave Managed Security Testing (MST) service is a subscription based managed vulnerability scanning and penetration testing service. MST helps identify vulnerabilities and findings that can lead to data compromise in Networks, Applications, and Databases, which helps organizations measure and manage risk. The MST service consists of:

- Reconnaissance, which is the information gathering and discovery process to understand the Client's Target System(s) and the scope of the required scanning and/or testing of those systems.
- Scanning & Testing helps identify potential vulnerabilities or weak configurations of the Client's Target System(s), the confirmation and evaluation of those vulnerabilities and the attempted exploitation of, and extraction of data from the Clients Target System(s).
- Reporting is the provision of results of Scanning & Testing and, where relevant, tests, as a completed report available through the Trustwave Fusion platform.

Basic Features of Service

The Managed Security Testing Service (MST) includes the following basic service features:

- Tracking of provisioning progress; MST portal account subscription; client target system enrolment; change management and support requests creation and response; and Reporting.

Virtual Appliance

Supply of virtual appliance for use in the Client's Target System(s) to perform testing on internal client systems.

Reconnaissance

During this phase and depending on the scope of the Client's MST service, the associated application architectural information is assessed and/or a port scan of the Client's network is completed.

Scanning & Testing

- Vulnerability Assessment
  - Compliance scanning and basic hygiene checks; or
  - Best practice scanning of specified checks in addition to basic hygiene checks with actionable findings for remediation.
- Penetration Testing
  - Basic – simulation of a basic attack executed by an attacker of limited sophistication with minimal skill, typically using freely available automated attack tools;
  - Opportunistic – simulation of an opportunistic attack executed by a skilled attacker that does not spend an extensive amount of time executing highly sophisticated

attacks, typically seeking easy targets using a mix of automated tools and manual exploitation;

- Targeted - simulation of a targeted attack executed by a skilled and patient attacker expending a significant effort trying to compromise a specific organization's systems and includes Credentialed and Uncredentialed Testing;
- Advanced - simulation of an advanced attack executed by a highly motivated, well-funded and sophisticated attacker, who will exhaust all options for compromise before relenting and includes Credentialed and Uncredentialed Testing.

Reporting

Predefined scan and test result reports are available through the Trustwave Fusion platform. Depending on the scope of the Client's MST service, the Client also has visibility of penetration test results during the testing process through the Trustwave Fusion platform.

Provisioning and Implementation

- The provisioning team is the Client's first point of interaction with Trustwave after the contract is executed. This team is responsible for working with the Client to implement the MST service. Please see the Trustwave Provisioning Guide for additional details on the service implementation.
- The MST service is deemed to be delivered and operational when Client has access to the Trustwave Fusion platform to subscribe for the service; schedule scans and tests; and view reports.

Service introductions and information gathering

Trustwave provisioning, assurance and delivery teams are assigned to implement and facilitate the successful configuration of the Client's MST service, which includes the following actions:

- Send an introduction email to the Client providing guidance on how to provide the necessary Client contact information prior to a remote kick-off meeting.
- Notify the Client that they have access to the MST service and the Trustwave Fusion platform; and remotely create an account for, and establish the Client within, the Trustwave Fusion platform.

Client environment assessment

Trustwave provisioning will work with the Client to verify that Client's environment can communicate with Trustwave Platform; and there is an active secure connection between the Trustwave Platform and the Client's environment.

MST Portal Account

The Client leverages the Fusion portal to exercise the services provided. The client can do the following from within the Fusion Portal.

- Subscribe for the relevant MST package(s);

- View the Subscription Funds based on the number of MST packages purchased by the Client.
- The Client's MST portal account will be debited with each enrolment of an individual Client's Target System.

Trustwave Responsibilities

- Create a Client account in the Trustwave Fusion platform and Verify that the Client has access to the Trustwave Fusion platform.
- Provide applicable user guides, introduce and review the Client's usage and understanding of the Trustwave Fusion platform and implement the applicable support process and procedures.

Client Responsibilities

- Respond to requests from the provisioning team when establishing contact and collecting the Client user information.

Read and confirm the Client's understanding of all provided user guides and documentation.

Vulnerability Assessment

Client's Target System enrolment

The Trustwave Security Operations Center (SOC) works with the Client to help ensure completeness of the Client enrollment information for each scheduled scan or test event including

- enrollment of the Client's Target System(s);
  - with the correct installation and configuration of any Virtual Appliance in the Clients Target System(s) environment.
  - complete the scheduling of the number of scans and/or tests available under the purchased MST package(s).

Trustwave Responsibilities

- Establish and maintain contact with the Client and navigate the Client through the enrollment process.
- Request and collect Client enrollment information.
- Supply the Virtual Appliance for use in the Client's Target System(s).
- Provide support to the Client to ensure the correct installation and configuration of the Virtual Appliance.
- Provide and maintain a secure connection between the Client's Target System(s) and the Trustwave Platform.
- Provide and maintain a vulnerability database and relevant software version upgrades and security policy updates, inclusive of changes to existing vulnerability and threat

signatures and new vulnerability and threat signatures, to the Trustwave scanners and Trustwave Platform.

- Provide security experts to conduct the managed scanning and penetration testing on the enrolled Client's Target System(s).
- Provide remote support to the Client to ensure the correct installation and configuration of the Virtual Appliance.
- Provide remote support in response to any issues arising during scanning or testing of the enrolled Client's Target System(s). Verify that Client's Target System(s) are visible to the Trustwave Platform;
- Client's Subscription Funds are correctly debited on enrollment of a specific MST Package(s).

Client Responsibilities

- Enrol the Client's Target System(s).
- Install Virtual Appliance.
- Schedule the purchased scans and or penetration test during the package period, through the Trustwave Fusion platform.
- Make available an onsite resource during the time(s) scheduled for scanning or testing of the Client's Target System(s).
- Maintain the Client's Target System(s) as stable as possible (i.e. no configuration changes or new systems added to the network segmentation) during the time(s) scheduled for scanning or testing.
- Provide appropriate credentialed access to Trustwave and to the Client's Target System(s).
- The Client acknowledges that:
  - relevant IP address ranges identify the Client's Target System(s) on which the managed security scanning and/or testing is to be completed and is used to calculate the amount to be debited from the Client's Subscription Funds;

Reporting

Report functions

The MST service includes the following available reporting features through the Trustwave Fusion platform:

- Online reporting and metrics: vulnerability assessment data (including risk, remediation status, and data compromised) and access to historical test results for trend analysis.
- Pre-defined fields: generation of executive summary, summary recommendations, test methodology and findings.
- Custom Reporting: Users selected fields, sorted by risk, finding status, project(s), selected fields or individual tests.

- Common Vulnerability Scoring System (CVSSv2) Values: CVSS is a standard method for risk ranking and prioritizing security vulnerabilities.
- Multi-format Reports: Export report data in PDF, Excel, XML, CSV and HTML.

Report timeline targets

- Trustwave will use best efforts, but does not warrant availability of the relevant reports, within the following timelines from completion of the relevant scan or test:
  - Managed scanning: within 10 Business Days
  - Penetration Testing- Tier 1 Basic and Tier 2 Opportunistic: within 10 Business Days
  - Penetration Testing- Tier 3 Targeted and Tier 4 Advanced: within 15 Business Days.
- All timelines are subject to the Client:
  - Accurately specifying the Client's enrolment information; and
  - Correctly installing and configuring the virtual appliance within the Client's Target System(s).

Service Category Packages

Single Network Penetration Test Package

- One (1) x opportunistic internal or external network test.

Managed Network Package

- Tier 0 Managed Best Practice Scanning – includes
  - managed network best practice vulnerability assessment scans
  - offered at four frequencies: one-time, quarterly, monthly, weekly
- Tier 1 Basic Test – includes
  - 4 x managed network best practice vulnerability assessment scans; and
  - One (1) x basic internal or external network test
- Tier 2 Opportunistic Test – includes
  - 4 x managed network best practice vulnerability assessment scans; and
  - One (1) x opportunistic internal or external network test.
- Tier 3 Targeted Test – includes
  - 4 x managed network best practice vulnerability assessment scans; and
  - One (1) x targeted internal or external network test, Uncredentialed Testing only.
- Tier 4 Advanced Test – includes
  - 4 x managed network best practice vulnerability assessment scans; and
  - One (1) x advanced internal or external network test, Uncredentialed Testing only.

Single Application Penetration Test Package

- One (1) x opportunistic application test.

Managed Application Package

- Tier 0 Managed Best Practice Scanning – includes
  - Managed application best practice vulnerability assessment scans
  - Offered at four frequencies: one-time, quarterly, monthly, weekly
- Tier 1 Basic Test – includes
  - 4 x managed application best practice vulnerability assessment scans; and
  - One (1) x basic application test.
- Tier 2 Opportunistic Test – includes
  - 4 x managed application best practice vulnerability assessment scans; and
  - One (1) x opportunistic application test.
- Tier 3 Targeted Test – includes
  - 4 x managed application best practice vulnerability assessment scans; and
  - One (1) x targeted application test.
- Tier 4 Advanced Test – includes
  - 4 x managed application best practice vulnerability assessment scans; and
  - One (1) x advanced application test.

Managed Database Package

- Managed best practice scanning – consists of
- Managed database best practice vulnerability assessment scans
- Offered at four frequencies: one-time, quarterly, monthly, weekly

MST Service Scans and Tests

The MST service vulnerability assessment includes the following scanning and penetration testing security categories depending on the MST package selected:

Network Scanning and Testing

Network Scanning Best Practice

Network Scanning (Best Practice)	
Host discovery and OS Fingerprinting	• Windows • Linux and other Unix variants • Routers, firewalls and other networking

Network Scanning (Best Practice)	
	appliances • User profile settings – advanced • Advanced password analysis
Common service discovery and fingerprinting	• Application servers • Authentication providers • Backdoors and remote access services • Backup applications • Database servers • Active Directory, LDAP • DNS • Mail servers & SMTP • NFS, NetBIOS and CIFS • NTP • Point of Sale (POS) applications • Remote Procedure Call • Routing protocols • SNMP • Telnet, TFTP, SSH • VPNs • Web applications (common) • Web servers
Missing vulnerability patches	
'Out of Support' services and Operating Systems (OS)	
Known vulnerability detection – CVE and vendor disclosed	
Insecure application/OS configurations	
WebApp vulnerabilities	
Scan interference	
Built-in accounts and default/blank passwords	
SSL/TLS insecure configuration, certificates and weak encryption	
Unencrypted communications	

External Network Managed Testing

External Network Managed Testing	Basic	Opportunistic	Targeted	Advanced
Most exploitable vulnerability	x	x	x	x
Any exploitable vulnerability		x	x	x
Vertical escalation		x	x	x
Horizontal escalation		x	x	x
Video evidence		x	x	x
Attack chains			x	x
Escalation to adjacent systems			x	x
Limited Phishing			x	x
Post-Test debrief			x	x
Client side attacks				x
Social engineering				x
Custom protocol attacks				x
Escalation to internal network				x

Internal Network Testing

Internal Network Managed Testing	Basic	Opportunistic	Targeted	Advanced
Most exploitable vulnerability	x	x	x	x
Layer 2 Testing (Broadcast, ARP)	x	x	x	x
Vertical escalation	x	x	x	x
Segmentation testing	x	x	x	x
Any exploitable vulnerability		x	x	x

Horizontal escalation		x	x	x
Video evidence		x	x	x
Attack chains		x	x	x
Data exfiltration testing		x	x	x
Enterprise escalation			x	x
Testing from client subnets			x	x
Horizontal escalation (Enterprise)			x	x
Any exploitable vulnerability (Enterprise)			x	x
Post test debrief			x	x
Client side / browser attacks				x
Advanced protocol attacks				x
Password analysis				x

Application Managed Scanning

Application Scanning	Best Practice
Database injection flaws	x
Database errors	x
Integer overflow	x
Non-SSL password	x
SSL checks	x
Application exception	x
Cross-Site Scripting (XSS)	x
Directory browsing	x
Cross-Site Request Forgery (CSRF)	x
Cookie vulnerabilities	x
Session ID in URL	x

Windows/Unix command injection	x
Windows/Unix relative path	x
Password autocomplete	x
Credit card disclosure	x
Basic authentication over HTTP	x
Private IP disclosure	x
Rom –based XSS	x
Open redirect	x
Remove file inclusion	x
Insecure CORS headers	x
Cross frame scripting	x

Application Testing

Application Testing	Basic	Opportunistic	Targeted	Advanced
Manual injection testing	x	x	x	x
Manual session management testing	x	x	x	x
Manual account policy review	x	x	x	x
Manual information disclosure testing	x	x	x	x
Manual data protection testing	x	x	x	x
Manual authentication testing		x	x	x
Manual authorisation testing		x	x	x
Manual testing for simple logic flaws		x	x	x
Video evidence		x	x	x
Manual testing for complex logic flaws			x	x

Manual testing for cryptographic weaknesses			x	x
Manual bounds checking testing			x	x
Manual application resource handling checking			x	x
Post-test debrief			x	x
Exhaustive testing				x
Manual testing for all input areas				x

Database Scanning

Database Scanning		Best Practices
User and password controls	Default passwords	x
	Default accounts	x
	User profile settings – basic	x
	User profile settings – advanced	x
	Advanced password analysis	x
Access controls	Permissions granted to DBA	x
	Permissions granted to public	x
	Advanced security role permission grants	x
Application integrity	Patch level	x
	Known vulnerabilities	x
OS integrity	File permissions	x
	Service account permissions	x

CautionsDefinitions

- **Application**. An "**Application**" is a non-web-based or a web-based application. A non-web-based application is defined as a single piece of software running on a specific piece of hardware. The application may communicate with many infrastructure components (middleware, databases, etc). A Web-based application may be distributed across multiple servers; similarly, multiple applications may run on a single website. A single web-based application is defined to include only one login page, a unified "look and feel", a single session tracking mechanism, and a consistent programming language or application framework.

- **Client Target System**. A "**Client Target System**" is a collection of one or more application, network, or database, owned by the Trustwave Client.

- **Credentialed Testing**. "**Credentialed Testing**" includes authenticating with an asset to be able to test it as a user on the asset providing greater and more accurate information.

- **Database**. A '**Database**" is defined as a database management system providing the ability to access, manipulate, and update the data contained within.

- **Network**. A "**Network**" is a "logical class C" network segment of IP addresses accessed from a single point of origination. A "logical class C" is a block of 256 IP addresses. Networks smaller than 256 contiguous IP addresses may be combined to make one logical class C, provided they are accessed from the same point of origination. For example, three network segments of 64 IP addresses each can be combined under one logical class C. Tests are scoped against complete network segments (including routers, network addresses, broadcast addresses, etc.) accessed from a single location (single switch port for internal tests). Potentially unused IP addresses are still considered part of the scope since network penetration testing is performed against at least an entire network segment, and not isolated devices.

- **Uncredentialed Testing. "Uncredentialed Testing"** assesses and asset without authenticating with the asset.

Client Acknowledgement

Due to the continuously evolving nature of MST services, Trustwave hereby reserves the right to make any changes to this Service Description and the services offered as part of MST at any time. Trustwave will update Clients that are subscribed to the MST services of any changes to the MST services and this Service Description as soon as reasonably practicable after the implementation of any such changes. Client acknowledges that such changes are necessary for the continued effectiveness of the MST services and that such changes will go into effect at a minimum of thirty (30) days after receiving written notice from Trustwave. Any changes made to the MST services will not serve as a breach of any agreement with the Client unless such change leads to a material impairment of the services.