Trustwave®

SERVICE DESCRIPTION

Managed Security Testing

Overview

Trustwave's Managed Security Testing (MST) service ("**Service**") provides bundled penetration testing and managed scanning through the Trustwave Fusion platform. The Service assists Client in identifying vulnerabilities and findings in its environment to better measure and manage risk.

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

Provisioning and Implementation

During provisioning and implementation, Trustwave will introduce Client to the Service, collect relevant information, assess Client's environment in order to securely connect to it, and provision Client's Trustwave Fusion platform account to enable Client to enroll in the Service. Trustwave's Provisioning Guide, provided during this phase, includes additional details.

Trustwave works with the Client to help ensure completeness of Client enrollment information for each scheduled scan or test, including (i) enrolling Client's Target System(s) with correct installation and configuration of any Virtual Appliance in the Clients Target System(s) environment, and (ii) completing scheduling of the number of scans or tests available under the purchased MST package(s).

Virtual Appliance

If Client selects an internal network penetration test, Trustwave will provide Client with a virtual penetration test (VRPT) appliance ("**Virtual Appliance**").

Reconnaissance

Reconnaissance includes passive methods such as researching available information and scanning Client's network, prior to performing actual scans or tests. Performing reconnaissance in a systematic manner enables a pen tester to discover potential security liabilities that an attacker may exploit. Furthermore, it helps to determine an organization's online profile, including network architecture, operating systems, applications, and users.

Reporting

Predefined scan and test result reports are available through the Trustwave Fusion platform. Depending on the scope and the package selected, as further described below, the Client also has visibility of penetration test or managed scanning results during the testing process through the Trustwave Fusion platform.

Client may generate any of the following reporting types within 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 (CVSS) 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.

Client Obligations

For Trustwave to provide these features of the Service, Client will:

- Enroll the Client's Target System(s)
- Install the Virtual Appliance if scheduling internal penetration testing
- Schedule penetration tests or managed scans through Trustwave Fusion platform
- Make available an onsite resource during scheduled test times
- Keep Client's Target System(s) as stable as possible (i.e., no configuration changes or new systems added to the network segmentation) during the scheduled test times
- Provide appropriate credentialed access to Trustwave and to the Client's Target System(s)
- Provide relevant IP address ranges for the Client's Target System(s) on which the penetration testing or managed security scanning is to be completed
- Respond to Trustwave's requests to establish contact and collect user information
- Read and confirm its understanding of all provided user guides and documentation

Trustwave Obligations

For these features, Trustwave will:

- Create Client's account and verify Client's access within and to the Trustwave Fusion platform
- Provide Client applicable user guides, introduce and review Client's usage and understanding of the Trustwave Fusion platform, and implement any applicable support processes and procedures
- Establish and maintain contact with Client and assist with the enrollment process
- Request and collect Client enrollment information
- Supply the Virtual Appliance for use in 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 Fusion 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 Fusion platform
- Provide security experts to conduct penetration testing or managed scanning on the enrolled Client's Target System(s)
- Provide remote support to the Client to ensure 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 in the Trustwave Fusion platform and that Fees debited are correct

Service Packages – Overview

The Service comprises of the following packages and test tiers. Client may elect any number of package or test combinations based on the amount of Fees allocated in the SOW or Order Confirmation. Trustwave will perform the applicable test or scan following Reconnaissance as scheduled in the Trustwave Fusion platform.

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 (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 (includes Credentialed and Uncredentialed Testing).

Managed Scanning

- Scanning and basic hygiene checks for vulnerability assessment; or
- Best practice scanning of specified checks in addition to basic hygiene checks with actionable findings for remediation.

Network Penetration Test Package

- Single Penetration Test – includes one (1) x opportunistic internal or external network penetration test
- Tier 1 Basic Tests (1+1) – includes
  - One (1) x managed network best practice maintenance tests; and
  - One (1) x basic internal or external network penetration test
- Tier 1 Basic Tests (1+0) – includes
  - Zero (0) x managed network best practice maintenance tests; and
  - One (1) x basic internal or external network penetration test
- Tier 1 Basic Tests (1+4) – includes
  - Four (4) x managed network best practice maintenance tests; and
  - One (1) x basic internal or external network penetration test
- Tier 2 Opportunistic Test (1+1) – includes
  - One (1) x managed network best practice maintenance tests; and
  - One (1) x opportunistic internal or external network penetration test
- Tier 2 Opportunistic Test (1+0) - includes
  - Zero (0) x managed network best practice maintenance tests; and
  - One (1) x opportunistic internal or external network penetration test
- Tier 2 Opportunistic Test (4+1) - includes
  - Four (4) x managed network best practice maintenance tests; and
  - One (1) x opportunistic internal or external network penetration test
- Tier 3 Targeted Test (1+1) – includes
  - One (1) x managed network best practice maintenance tests; and
  - One (1) x targeted internal or external network penetration test, Uncredentialed Testing only
- Tier 3 Targeted Test (1+0) 0 includes
  - Zero (0) x managed network best practice maintenance tests; and

    - One (1) x targeted internal or external network penetration test, Uncredentialed Testing only

- Tier 3 Targeted Test (4+1) - includes
    - Four (4) x managed network best practice maintenance tests; and
    - One (1) x targeted internal or external network penetration test, Uncredentialed Testing only
- Tier 4 Advanced Test (1+1) – includes
    - One (1) x managed network best practice maintenance tests; and
    - One (1) x advanced internal or external network penetration test, Uncredentialed Testing only
- Tier 4 Advanced Test (1+0) - includes
    - Zero (0) x managed network best practice maintenance tests; and
    - One (1) x advanced internal or external network penetration test, Uncredentialed Testing only
- Tier 4 Advanced Test (4+1) – includes
    - Four (4) x managed network best practice maintenance tests; and
    - One (1) x advanced internal or external network penetration test, Uncredentialed Testing only

Application Penetration Test Package

- Single Penetration Test – includes one (1) x opportunistic internal or external application penetration test
- Tier 1 Basic Test (1+1) – includes
    - One (1) x managed application best practice maintenance tests; and
    - One (1) x basic application test
- Tier 1 Basic Test (1+0) – includes
    - Zero (0) x managed application best practice maintenance tests; and
    - One (1) x basic application test
- Tier 1 Basic Test (4+1) – includes
    - Four (4) x managed application best practice maintenance tests; and
    - One (1) x basic application test
- Tier 2 Opportunistic Test (1+1) – includes
    - One (1) x managed application best practice maintenance tests; and
    - One (1) x opportunistic application test
- Tier 2 Opportunistic Test (1+0) – includes
    - Zero (0) x managed application best practice maintenance tests; and
    - One (1) x opportunistic application test
- Tier 2 Opportunistic Test (4+1) – includes
    - Four (4) x managed application best practice maintenance tests; and
    - One (1) x opportunistic application test
- Tier 3 Targeted Test (1+1) – includes
    - One (1) x managed application best practice maintenance tests; and
    - One (1) x targeted application test
- Tier 3 Targeted Test (1+0) – incudes
    - Zero (0) x managed application best practice maintenance tests; and
    - One (1) x targeted application test
- Tier 3 Targeted Test (4+1) – includes
    - Four (4) x managed application best practice maintenance tests; and
    - One (1) x targeted application test
- Tier 4 Advanced Test (1+1) – includes
    - One (1) x managed application best practice maintenance tests; and

    - One (1) x advanced application test
- Tier 4 Advanced Test (1+0) – includes
    - Zero (0) x managed application best practice maintenance tests; and
    - One (1) x advanced application test
- Tier 4 Advanced Test (4+1) – includes
    - Four (4) x managed application best practice maintenance tests; and
    - One (1) x advanced application test

Managed Scanning Package

- Managed Best Practice Network Scanning – includes
    - Managed network best practice vulnerability assessment scans
    - Offered at four frequencies: one-time, quarterly, monthly, weekly

Service Packages - Detail

The Service includes the following penetration testing and managed scanning best practices depending on the package selected:

Managed Network Scanning

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

Network Scanning	
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	

Managed Application 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

Managed Database Scanning

Database Scanning		Best Practice
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

Penetration Testing

External Network Penetration Testing	Basic (Tier 1)	Opportunistic (Tier 2)	Targeted (Tier 3)	Advanced (Tier 4)
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 Penetration Testing	Basic (Tier 1)	Opportunistic (Tier 2)	Targeted (Tier 3)	Advanced (Tier 4)
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 Penetration Testing	Basic (Tier 1)	Opportunistic (Tier 2)	Targeted (Tier 3)	Advanced (Tier 4)
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 authorization 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

Core Trustwave Features

The Service includes the following core features which are standard to many of Trustwave services:

Trustwave Fusion Platform

The Trustwave Fusion platform is Trustwave's proprietary cloud-based cybersecurity platform. Client will be automatically enrolled in the Trustwave Fusion platform as a part of the Service. Client will have access to the following on the Trustwave Fusion platform:

- Vulnerability findings, and support tickets
- Client's reports and dashboards

- Request methods for change support and management
- Multiple methods for Client to securely communicate with Trustwave and the ability to upload documentation, security policies, and more

Definitions

- 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.
- A "**Client Target System**" is one or more Client-owned applications, networks, or databases.
- "**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.
- A "**Database**" is a database management system providing the ability to access, manipulate, and update the data contained within.
- 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**" assesses and asset without authenticating with the asset.

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.