Trustwave®

Managed Security Testing

SERVICE DESCRIPTION

This document will describe the various scanning and testing aspects of Trustwave Managed Security Testing (MST) to help you decide what level of scanning or penetration testing is right for your needs.

Overview

Trustwave Managed Security Testing (MST) identifies vulnerabilities in networks, applications and databases to identify where and how data could be compromised to help IT teams measure and manage risk.

MST blends vulnerability scanning and penetration testing into a complete vulnerability assessment and security testing service. Different assets are valued differently and have different risks associated with them. A low value asset may only require scanning to identify potential threats. A mission-critical asset, however, needs deeper testing to determine the ramifications of the actual exploitation of its vulnerabilities. MST fulfills each of those needs and also illustrates how the chaining together of multiple vulnerabilities across multiple assets may clear an attacker's path to the compromise of systems and data.

With MST, users can enroll targets in, schedule and review and manage the results of scanning and penetration testing of the following types:

- Scanning
- Applications
- Databases
- External network infrastructure
- Internal network infrastructure
- Penetration Testing
- Applications
- External network infrastructure
- Internal network infrastructure

Scanning

MST provides flexible scanning options based on your needs. Depending on the expertise of your resources, users can choose to schedule and manage scans and interpret results themselves (self-service scanning) or have Trustwave SpiderLabs experts do it for them (managed scanning).

Self-Service Scanning

Users of self-service scanning can schedule, configure and run scans themselves. Upon completion of a scan, the user receives a list of raw results from our scanning tools that they interpret on their own.

Managed Scanning

Managed scanning consists of Trustwave SpiderLabs experts validating and interpreting scan results for the user. Upon completion of a scan, the user receives a report of validated results.

	Self-Service Scanning	Managed Scanning
Scheduling:	User	User
Configuration:	User	User
Scan kick-off:	User	User
False-positive filtering:	User	Trustwave SpiderLabs
Validation of results:	User	Trustwave SpiderLabs
Interpretation of results:	User	Trustwave SpiderLabs

Levels and Types of Scanning

Application Scanning

Service	Number of Tests	Description
Self-Service Compliance Scan Enrollment	Four (4) Application Compliance scans —unlimited scanning available	Cloud-based application scanning that will perform the minimum required checks to meet compliance requirements. The client will setup, configure and manage the scans and review and manage the results on their own.
Self-Service Best Practices Scan Enrollment	Four (4) Application Best Practices scans —unlimited scanning available	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will setup, configure and manage the scans and review and manage the results on their own.
Managed Compliance Review Scan Enrollment	Four (4) Managed Application Compliance Review Scans	Cloud-based managed application scanning that will perform the minimum required checks to meet compliance requirements. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.
Managed Best Practices Assessment Scan Enrollment	Four (4) Managed Application Best Practices Assessment Scans	Cloud-based application scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.

Database Scanning

Service	Number of Tests	Description
Managed Compliance Review Scan Enrollment	Four (4) Managed Database Assessment Scans	Cloud-based managed database scanning that will perform the minimum required checks to meet compliance requirements. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.
Managed Best Practices Assessment Scan Enrollment (Tier 0)	Four (4) Managed Database Best Practices Assessment Scans	Cloud-based database scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.

Internal or External Network Scanning

Service	Number of Tests	Description
Managed Best Practices Assessment Scan Enrollment (Tier 0)	Four (4) Managed Network Best Practices Assessment Scans	Cloud-based network scanning that will fulfill compliance requirements but extend beyond to run a set of vulnerability checks designed to address a broader array of security concerns to assist organizations in protecting their information systems. The client will enroll the target and schedule the scan, and Trustwave SpiderLabs experts will configure and execute the scans and review and manage the results in order to provide a report of validated findings.

Non-MST, Licensed Scanning Options

Trustwave delivers MST scanning via the cloud. For licensed options, see product and service descriptions for Trustwave AppDetectivePRO or DbProtect for databases and for Trustwave App Scanner Enterprise. Licensed options are not available for internal vulnerability scanning or external vulnerability scanning for networks.

Penetration Testing

With penetration testing, MST provides different levels of testing based on your needs. Testing tiers start with basic tests designed for small environments with minimal requirements (i.e. PCI Compliance) and can expand to our most thorough advanced tests for larger and more complex environments with no constraints on the level of testing.

Levels and Types of Penetration Testing

Application Penetration Testing

Service	Number of Tests	Description
Tier 1 Basic Test Enrollment	Four (4) Managed Application Best Practices Assessment Scans One (1) Application Tier 1 Basic Test	**Managed Application Best Practices Assessment Scans** **Tier 1 Application Test: Basic Test—**This test will simulate a basic attack executed by a class of attacker (often referred to as "script kiddies") that typically uses freely available automated attack tools.
Tier 2 Opportunistic Threats Test Enrollment	Four (4) Managed Application Best Practices Assessment Scans One (1) Application Tier 2 Opportunistic Threat Test	**Managed Application Best Practices Assessment Scans** **Tier 2 Application Test: Opportunistic Threat—**This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend the time to execute highly sophisticated attacks. This type of attacker seeks easy targets ("low-hanging fruit") and will use a mix of automated tools and manual exploitation to penetrate their targets.
Tier 3 Targeted Threats Test Enrollment	Four (4) Managed Application Best Practices Assessment Scans One (1) Application Tier 3 Targeted Threat Test including uncredentialed and credentialed testing	**Managed Application Best Practices Assessment Scans** **Tier 3 Application Test: Targeted Threat—**This test will simulate a targeted attack executed by a skilled, patient attacker that has targeted a specific organization. This class of attacker will expend significant effort trying to compromise an organization's systems. To ensure thorough testing, users should enroll thick-client applications in Tier 3 or 4 testing.
Tier 4 Advanced Threats Test Enrollment	Four (4) Managed Application Best Practices Assessment Scans One (1) Application Tier 4 Advanced Threat Test including uncredentialed and credentialed testing	**Managed Application Best Practices Assessment Scans** **Tier 4 Application Test: Advanced Threat—**This test will simulate an advanced attack executed by a highly motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting. To ensure thorough testing, users should enroll thick-client applications in Tier 3 or 4 testing.

Network Penetration Testing

Service	Number of Tests	Description
Tier 1 Basic Test Enrollment	Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 1 Basic Test	**Managed Network Best Practices Assessment Scans** **Tier 1 Network Test: Basic Test—**This test will simulate a basic attack executed by a class of attacker (often referred to as "script kiddies") that typically uses freely available automated attack tools.
Tier 2 Opportunistic Threats Test Enrollment	Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 2 Opportunistic Threat Test	**Managed Network Best Practices Assessment Scans** **Tier 2 Network Test: Opportunistic Threat—**This test will build upon the basic test described above and simulate an opportunistic attack executed by a skilled attacker that does not spend an extensive amount of time executing highly sophisticated attacks. This type of attacker seeks easy targets ("low-hanging fruit") and will use a mix of automated tools and manual exploitation to penetrate their targets.
Tier 3 Targeted Threats Test Enrollment	Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 3 Targeted Threat Test including uncredentialed and credentialed testing	**Managed Network Best Practices Assessment Scans** **Tier 3 Network Test: Targeted Threat—**This test will simulate a targeted attack executed by a skilled, patient attacker that has targeted a specific organization. This class of attacker will expend significant effort trying to compromise an organization's systems.
Tier 4 Advanced Threats Test Enrollment	Four (4) Managed Network Best Practices Assessment Scans One (1) Network Tier 4 Advanced Threat Test including uncredentialed and credentialed testing	**Managed Network Best Practices Assessment Scans** **Tier 4 Network Test: Advanced Threat—**This test will simulate an advanced attack executed by a highly motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting.

Timetables for Report Deliverable

Trustwave cannot guarantee that a report will be delivered by a certain date. Upon completion of a scan or penetration test, we try to deliver reports within the following time-frames.

- Self-service scanning—within 1 business day
- 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.

Delivery time-frames can vary depending on the client completing testing pre-requisites including the proper enrollment of targets, the installation of remote appliances or virtual machines, and more.