MANAGED SECURITY TESTING SERVICE DESCRIPTION

Overview

IT teams that urgently need to investigate a particular security issue don't have time to wait for a slow budgetary approval process. Trustwave Managed Security Testing (MST) helps IT teams get the right vulnerability scan or penetration test at the right time minus the bureaucratic inefficiencies. With MST's flexible model, businesses purchase annual credits to consume as needed on any kind of network, application or database scan or penetration test.

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. The product blends vulnerability scanning and penetration testing into a complete vulnerability assessment and security testing service. Different assets are of different value 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. IT teams can take the context-rich results to then fix the right vulnerabilities first and make the most impact on their organization's security posture in the shortest amount of time.

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

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

Subscriptions & Enrollments: How They Work

1. **A subscription consists of an MST account in the TrustKeeper portal and an account balance**
   a. The balance is loaded into the MST account based on the signed Statement Of Work (SOW).
   b. This sum of money is the MST subscription's initial account balance
   c. The SOW will specify the subscription term

2. **As needed, the user enrolls targets for scanning or penetration testing**
   a. A target includes one of the following: an application, database, or external or internal network segment
   b. An enrollment lasts for 12 months and is the time during which scans or tests of the target can take place
   c. A subscription may consist of multiple enrollments, and an enrollment may extend beyond the subscription term

3. **As part of the enrollment process, the user selects an appropriate level of scanning or penetration testing**
   a. **Levels of scanning** (managed and self-service options are available)
      i. *Compliance*—Minimum required to support fulfillment of compliance requirements for vulnerability scanning
      ii. *Best Practices*—Supports the fulfillment of compliance requirements for vulnerability scanning and extends beyond to address a broader array of security concerns

   b. **Levels of penetration testing**
      i. The four levels of testing include varying degrees of testing modeled after increasingly sophisticated threats
         - Basic threat test (tier one) modeled after an attacker of limited sophistication with minimal skills
         - Opportunistic threat test (tier two) modeled after a skilled but impatient attacker
         - Targeted threat test (tier three) modeled after a skilled and patient attacker
         - Advanced threat test (tier four) modeled after a highly motivated, sophisticated, well-funded attacker

4. **Once the user enrolls the target, the associated price will be deducted from the customer's MST account**

5. **The customer then schedules scans and/or tests of the target as needed during the 12-month enrollment period**
   a. A scanning enrollment typically consists of four scans (unlimited scanning is also available)
   b. A basic-, opportunistic-, target-, or advanced-threat (tiers one-through-four) penetration testing enrollment consists of four managed best practices scans and the associated penetration test

Levels and Types of Vulnerability 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.

Levels and Types of 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.

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 an attacker of limited sophistication with minimal skills. This class of attacker (often referred to as "script kiddies") typically use 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.*

Internal or External 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 an attacker of limited sophistication with minimal skills. This class of attacker (often referred to as "script kiddies") typically use 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.

About Trustwave

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations--ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers--manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit https://www.trustwave.com.