Synoptek® {

Vulnerability Management

Service Definition

Table of Contents

1 INTRODUCTION

This Service Definition is subject to the terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Vulnerability Management (the "Service").

This Service Definition reflects Synoptek's standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any particular standard herein to reflect its current best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERINGS – VULNERABILITY MANAGEMENT

As electronic commerce, online business-to-business operations, and global connectivity have become vital components of a successful business strategy, enterprises have adopted security processes and practices to protect information assets. Most companies work diligently to maintain an efficient, effective security policy, implementing the latest products and services to prevent fraud, vandalism, sabotage, and denial of service attacks. However, many enterprises overlook a key ingredient of a successful security policy: They do not test the network and security systems to ensure that they are working as expected. Vulnerability Management is a vital component of a comprehensive security program. The intent of Vulnerability Management is to identify opportunities for prevention of data loss or endangerment through the exercise of scanning a networked environment and analyzing the results.

Key Features and Benefits

1. Proactive Security Solution
2. Supports Compliance
3. Identifies Exposures
4. Quarterly Tests and Reports
5. Quick Deployment
6. Elevates Infrastructure Hygiene
7. Improves Security Posture

Vulnerability Management – using tools to scan the networked environment for vulnerabilities and processes to remediate found vulnerabilities – helps refine an enterprise's security policy, identify vulnerabilities and ensure that the security implementation provides the protection that the enterprise requires and expects. Vulnerability Management helps enterprises uncover system security weaknesses that can lead to data or equipment being compromised or destroyed by exploits (Further attacks on a network, usually through the exploitation of system vulnerabilities), malware, denial of service attacks and other intrusions. Vulnerability Management also expose vulnerabilities introduced by patches or other updates.

3 SOLUTION PURPOSE

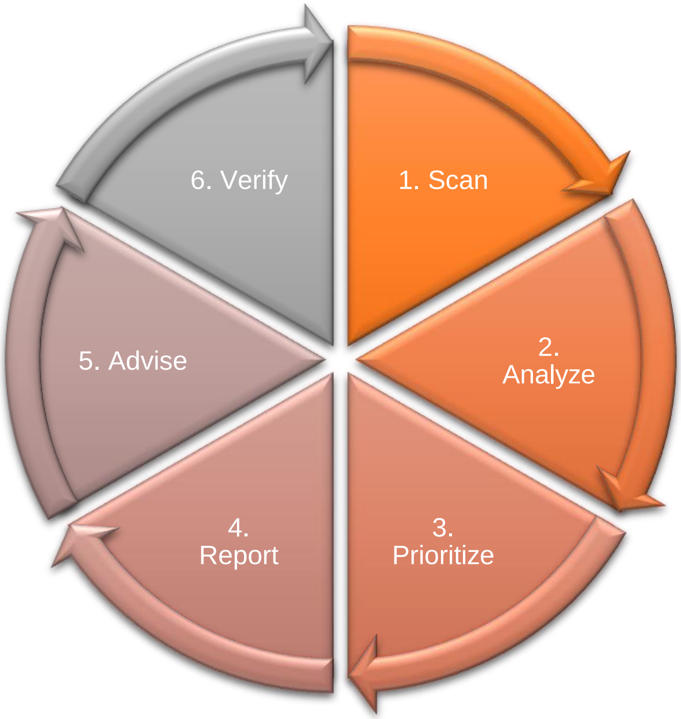
Software and hardware complexity grows at an exponential rate. Through this process of evolution, vulnerabilities are often introduced, unexpectedly and unintentionally in upgrades, updates, and patches. Synoptek's Vulnerability Management Service is focused on swift identification of new and existing vulnerabilities that make their way into your technological ecosystem and assisting in removing them before they can be exploited by threat actors.

4 HOW IT WORKS

Synoptek's Vulnerability Management Service provides a multi-pronged approach to Vulnerability Management. First, Synoptek leverages proven methodologies and tools to detect vulnerabilities in your organization's network. Second, Synoptek analyzes and makes risk-based recommendations that address the found vulnerabilities. Lastly, Synoptek will advise on vulnerability remediation, performing re-scans when necessary to ensure that the proper patch has been applied, no new vulnerabilities have been introduced and that your organization's threat surface continues to shrink.

5 WHAT'S INCLUDED

By subscribing devices to Synoptek's Vulnerability Management Service, you receive the following:



a) **Quarterly Vulnerability Scans.** Synoptek will scan, on a quarterly basis, the subscribed devices in your environment. These devices can be anything from switches, routers, and firewalls to servers, mobile devices, desktops, and laptops;

b) **Scan Results Analysis.** Upon scan completion, Synoptek's expert security analysts will begin analyzing the results from the scan.

c) **Risk-Based Prioritization.** Using vulnerability research and industry tools, Synoptek's analysts will prioritize the findings using a risk-based approach, looking for the vulnerabilities with the greatest criticality, residing on the assets with the greatest organizational value, that requires the swiftest remediation, following industry best practices. The focus of the analysts will be on high-severity vulnerabilities. Definitions of what constitutes high-severity are available at the end of this document.

d) **Actionable Reporting.** Each quarter you will receive a detailed report that contains the following data as identified by the vulnerability assessment:

1) **Executive summary**
2) **Hosts scanned**
3) **Vulnerability count by host**
4) **Vulnerability count by criticality**
5) **Missing patch details**
6) **Top 5 common vulnerabilities**
7) **Raw data**

e) **Compliance**. Synoptek's Vulnerability Management Service support your organization's compliance needs; from PCI to HIPAA, we have you covered. Synoptek's Vulnerability Management Service provide a Certified Approved Scanning Vendor (ASV) solution.

1) As a requirement of the Payment Card Industry Data Security Standard (PCI-DSS), external quarterly vulnerability scanning must be performed by an ASV. (See PCI-DSS; Requirement 11.2).
2) As a requirement of the Health Insurance Portability and Accountability Act (HIPAA), 45CFR§164.308(a)(1)(ii)(A) and 45CFR§164.308(a)(1)(ii)(B), a covered entity must conduct an accurate and thorough assessment of the potential risks and vulnerabilities that may impact or otherwise affect Confidentiality, Integrity or Availability (CIA) of electronic protected health information held by the covered entity and implement security measures to sufficiently reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).

6 SERVICE LIMITATIONS

Synoptek's Vulnerability Management Service is an excellent addition to any organization's strategy of defense in depth. This Service is not a comprehensive solution for preventing all threats, attacks or variations of malware that may be leveraged against your organization. As a result, it should be expected that this Service alone cannot guarantee that your end-users and end-devices will be defended from all threats or other attacks and is best used in conjunction with other security tools, solutions, and resources.

Vulnerability Management (and by extension, assessments and/or scans) is not the same as Penetration Testing. Vulnerability assessments are often conducted in an automated fashion, checking for flaws originating from various development or configuration errors. Unlike a vulnerability assessment, penetration tests simulate an attack from either internal or external threat actors; Penetration Testing centers on controlled exploitation. The aim of a vulnerability assessment is to identify vulnerabilities that may exist within an in-scope system. The aim of a penetration test is to validate the existence of vulnerabilities through the use of controlled exploitation. Penetration testing includes vulnerability scans, but also goes beyond just the scan itself and may also include the exploitation of security processes and procedures, not just technical weaknesses.

Vulnerability Management will only be performed on subscribed devices. Subscribed devices are the specific named devices that you identify at the time of your initial purchase of this Service, or in subsequent change orders.

High-Severity vulnerabilities are categorized as either a severity-four or a severity-five, on a five-point scale (five being the most critical type of vulnerability). For purposes of this document and Synoptek's Vulnerability Management Service, high-severity is synonymous with high-risk.

- Synoptek's Vulnerability Management Service provide actionable insight related to resident vulnerabilities within your organization.
- Synoptek's Vulnerability Management Service include project management oversight for remediation of found vulnerabilities, with the purpose of providing remediation advisory.
  Synoptek Vulnerability Management Service do not include actual remediation. Vulnerability remediation services are sold separately by Synoptek.

7 INSTALLATION AND CONFIGURATION REQUIREMENTS

Synoptek’s Vulnerability Management Service is deployed in a variety of ways, depending on the types of scan required and performed.

External Scanning: Also known as a perimeter scan, is handled by our cloud scanner and does not require any special permissions or installation. An external scan can be scheduled and initiated very quickly. The only requirement for an external scan is a valid target – often this includes the hostname and/or IP address of the intended target.

Internal Scanning: Is handled a bit differently than an external scan. With an internal scan, Synoptek leverages light-weight agents to reside on and scan devices without the need for credentialed access. These light-weight agents can be and are installed on a variety of platforms, the requirements (Fig. 1) of which are outlined below. For internal scans where a device would not support the installation of an agent, a Network Scanner must be installed and the resources for such a scanner be provisioned. The hardware (Fig. 2) and software (Fig. 3) requirements for the Network Scanner are also outlined below.

Agent Software Requirements	
Linux • Fedora 20 and 21 (x86-64) • Debian 6 and 7 (i386 and x86-64) • Red Hat ES 5/6/7 / CentOS 5/6/7 / Oracle Linux 5/6/7 (i386 and x86-64) • Ubuntu 10.04, 12.04, and 14.04 (i386 and x86-64) **Mac OSX** • Mac OSX 10.8-10.11 (x86-64) **Windows** • Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2 (x86-64) • Windows 7 and 8 (i386 and x86-64)	
Network Scanner Hardware Requirements	**Network Scanner Software Requirements**
Processor: Intel, 2 Dual-core **Processor Speed: 2 GHz** **RAM: 8GB** **Disk Space: 40GB** Virtual Machines The solution can be installed on a Virtual Machine that meets the same requirements specified. If your virtual machine is using Network Address Translation (NAT) to reach the network, many vulnerability checks, host enumeration, and operating system identification will be negatively affected.	**Linux** • Debian 6 and 7 / Kali Linux 1.x (i386 and x86-64) • Fedora 20 and 21 (i386 and x86-64) • FreeBSD 10 (x86-64) • Red Hat ES 5/6/7 / CentOS 5/6/7 / Oracle Linux 5/6/7 (i386 and x86-64) • SUSE 10 (x86-64) and 11 (i386 and x86-64) • Ubuntu (i386 and x86-64) **Mac OSX** • Mac OSX 10.8-10.11 (x86-64) **Windows** • Windows Server 2008/R2 • Windows Server 2012/R2 (x86-64)