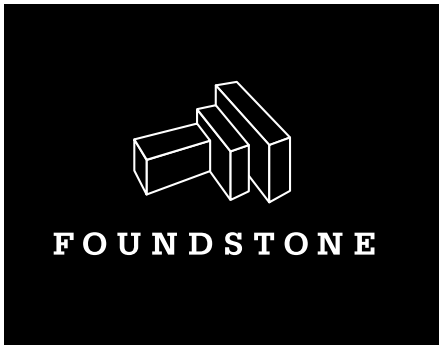


MANAGED SECURITY SERVICES

Managed Security Services:
The Future of Vulnerability Assessments

Vulnerability Assessments are a critical component of every complete security strategy. Vulnerability assessments are performed for two primary reasons: to identify exposures and validate existing security measures. To adequately identify exposures, vulnerability assessments require talented security professionals and specialized software, both of which are scarce resources in today's technology marketplace. To validate existing security measures, vulnerability assessments obtain credibility when performed by objective, independent third parties. For these reasons, vulnerability assessments are strong candidates for outsourcing to Managed Security Services (MSS) firms. This paper is not intended to make the decision of when to use managed security services; rather it is meant to raise awareness of the issues that should be considered when making that decision.

Introduction

Managed Security Services (MSS) are a fairly new concept in the security industry. In a nutshell, managed security services are another way of describing outsourcing. By far, the most commonly outsourced security service is firewall management. However, many components of security are candidates for outsourcing: intrusion detection system (IDS) monitoring, policy creation, and vulnerability assessments.

As with the outsourcing of any business function, the ultimate decision is based on whether or not a trusted partner can do the job better, cheaper, and faster. To answer this question for vulnerability assessments, we'll examine how vulnerability assessments are currently performed, and then discuss evolving roles for vulnerability assessments. We will introduce a new and potentially revolutionary concept in network security: Intrusion Prevention.

Old School Vulnerability Assessments

Vulnerability assessments are widely recognized as a crucial component of network security. Vulnerability assessments are performed to determine the actual security posture of an environment—can a malicious attacker affect the confidentiality, availability, or integrity of information? This question is answered by vulnerability assessments in a proactive manner—identifying vulnerabilities in your network before hackers do, allowing you to correct the problems before they are exploited. Since networks change often, vulnerability assessments should be performed periodically, either by internal audit teams or by external consulting organizations.

There are just over 4,000 Certified Information Systems Security Professionals (CISSPs) worldwide, and even fewer engineers qualified to perform vulnerability assessments.

Vulnerability assessments are difficult to perform. To identify security weaknesses, the assessment team must accurately and comprehensively discover, enumerate, and assess complex, heterogeneous networks. The team must have current, broad, and deep technical expertise in a myriad of technologies. Let's examine what it takes to perform vulnerability assessments in more detail:

People and Technology

A meaningful vulnerability assessment is one that simulates the capabilities of knowledgeable malicious attackers. Simulating these capabilities in a controlled and trusted environment requires specialized knowledge and tools, both of which are extremely sparse and expensive in today's IT environment. In fact, there are just over 4,000 Certified Information Systems Security Professionals (CISSPs) worldwide, and even fewer engineers qualified to perform these esoteric vulnerability assessments.

The shortage of qualified personnel is compounded by the fact that security is alarmingly dynamic—the knowledge and software that adequately tested your network last week is now obsolete due to newly discovered vulnerabilities. Maintaining technical currency in vulnerability testing, much less bleeding edge technical know-how requires a multidisciplinary team well versed in the countless hardware and software combinations used in today's networks. Additionally, the team must monitor the myriad of mailing lists, news groups, and web sites devoted to security vulnerabilities. Few organizations can afford to dedicate the necessary resources to accomplish these tasks.

For all but the largest organizations, attracting and retaining a qualified team is all but impossible. Maintaining current software and assessment techniques is similarly difficult due to meager resources. Which explains why so many organizations currently use third party consultants and software to assist with vulnerability assessments, a trend that is growing everyday as networks and assessment technology grows more complex.

Security is alarmingly dynamic—the knowledge and software that adequately tested your network last week is now obsolete due to newly discovered vulnerabilities.

External Regulatory Pressure

When corporations file their taxes and income statements, an independent third party is required by law to audit the accounting process. Why does the government impose this invasive requirement? An independent third party provides independent oversight, assuring shareholders and customers of the company's actual financial status.

Government and other regulatory agencies are now defining similar guidelines for security audits. A variety of regulations are in effect and more are proposed which require an independent third party for assessments. Examples from the health care industry come from the Health Insurance Portability and Accountability Act (HIPAA, 1986); from the financial industry we have Office of the Comptroller of the Currency (OCC) guidelines, and more widespread regulations in the form of the Gramm, Leach, Bliley (GLB) Act.

External regulatory pressure is beginning to force many organizations to use a third party, or Managed Service Provider, for regular vulnerability assessments. However, the most compelling reason to use a Managed Service Provider may very well be due to a fundamental shift in the way vulnerability assessments are perceived and executed.

Intrusion Prevention

Current vulnerability assessments provide a snapshot in time of an organization's security posture. They show vulnerabilities that exist at the time the assessment was performed. Changing networks, new functionality,

and newly discovered vulnerabilities render the results of any one vulnerability assessment out of date in little time.

The large time gap between assessments represents a significant exposure. What if vulnerability assessments could be performed regularly, even continuously? Vulnerabilities would be discovered before a hacker has the opportunity to do so. The advantages of this service represent a fundamental shift in the current state of security. Rather than intrusion detection, this ongoing service is what we call Intrusion Prevention.

Consider the example of physical security for your home. An alarm monitoring company such as ADT alerts you after an intruder has penetrated your home through known weaknesses, i.e. the door or window. This is intrusion detection. Of course it is valuable to know when your defenses have been compromised, but wouldn't you rather know about your security weaknesses before you are compromised?

If vulnerability assessments are constantly updated with the latest attack signatures, and occur continuously, there is virtually no window of opportunity for a malicious hacker to compromise your network.

What if ADT sent a technician to your house every week to make sure your doors and windows were locked? What if that technician came by every day? Every hour? This may not be feasible in the physical security world, but it is exactly the capability that is now available through managed vulnerability assessment services. Just as intrusion detection systems monitor for hackers using known attack patterns, vulnerability assessments test your network for those same known attack patterns. If vulnerability assessments are constantly updated with the latest attack signatures, and occur continuously, there is virtually no window of opportunity for a malicious hacker to compromise your network.

Query any seasoned IT auditor or security professional about security controls and they will explain the three types: Preventive, Detective, and Corrective. Preventive controls stop the security issue or vulnerability from happening. Detective controls identify the occurrence of problems. Corrective controls remedy known problems. Preventive controls are obviously the most desired, as they end up costing less in terms of exposure and resources. Continuous managed vulnerability assessments are a preventive control.

While Intrusion Prevention is a powerful and revolutionary security concept, it is non-trivial to implement. Continuous execution of vulnerability assessments requires significant manpower, software, and infrastructure. Maintaining a current database of attack signatures requires extensive and ongoing research and development. For these reasons, managed security services can deliver vulnerability assessments in a manner far superior to the capabilities provided in-house by most organizations.

Intrusion Prevention Process

Intrusion Prevention services center around the Security Operations Center (SOC). To maximize the effectiveness of this service, the assessment process is as follows:

Step 1: Network Identification and Enumeration

The SOC identifies all live hosts and services within a given network range. Each host and service is enumerated to determine attributes such as name, operating system, application versions, patch level, etc. A topology map *(shown on page 6)* is created which shows the entire target infrastructure.

Step 2: Vulnerability Scanning

The SOC next scans all live hosts for known vulnerabilities. The vulnerability assessment engine is both current and comprehensive, testing for the most recent vulnerabilities.

Step 3: Report Generation

Secure, automated reports deliver the results in a comprehensive and comprehendible fashion. The reports include the detailed attributes of the network, as well as identified vulnerabilities and associated countermeasures. The MSS firm provides human feedback to interpret and analyze the results.

Step 4: Alerting

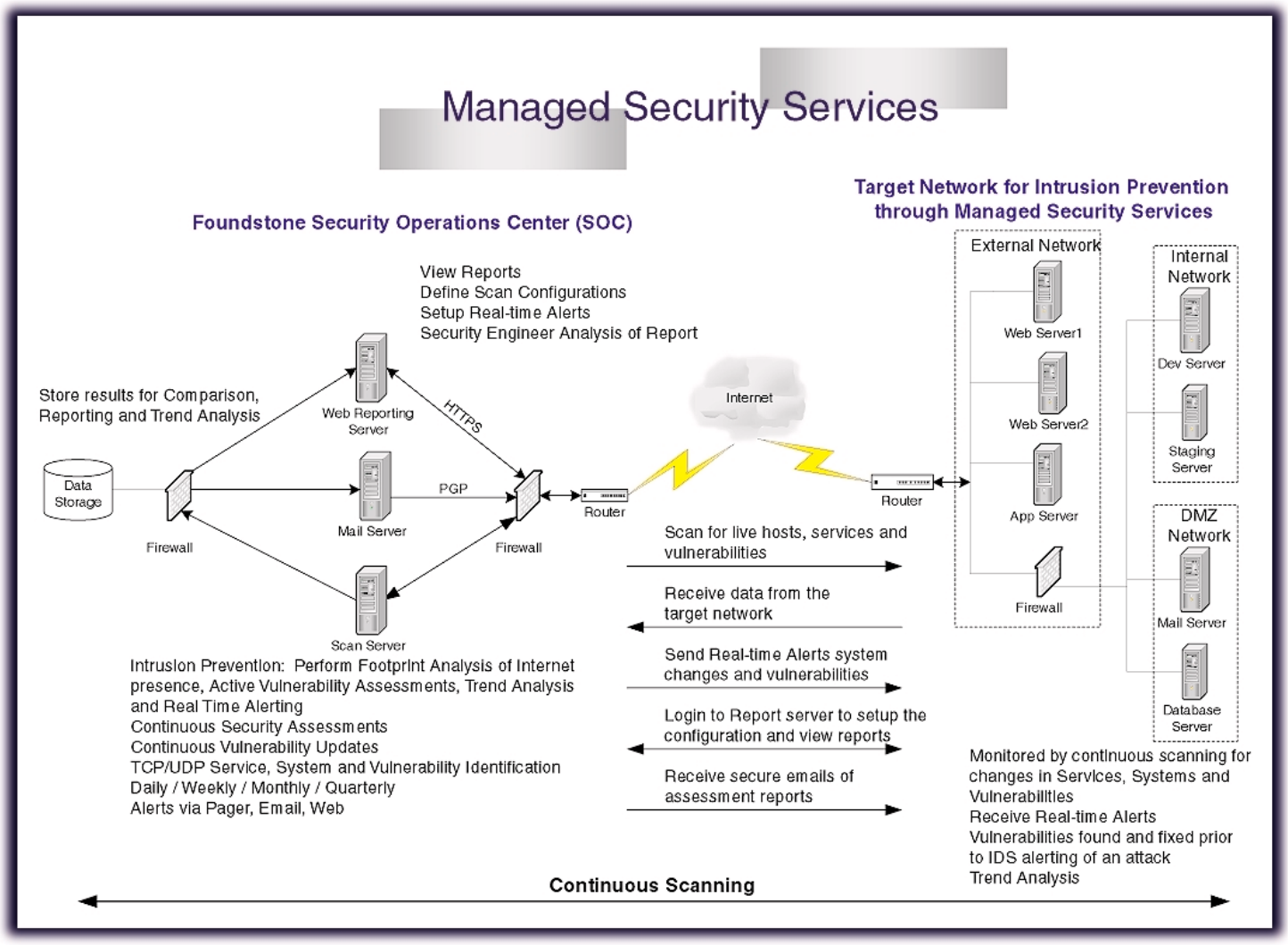
While incremental reports provide the primary mechanism for delivering results, reporting a high-risk vulnerability should not be delayed until the next report is generated. Real time reporting of newly discovered vulnerabilities should be available via web, pager, or email.

Step 5: Trend Analysis

One of the key values of the managed vulnerability assessment service is trend analysis—viewing the changes in your network over time. Changing hosts, services, and vulnerabilities are immediately available in the incremental reports.

Step 6: Continuous Analysis

The service is continuous, so that the network is constantly rediscovered and analyzed. This drastically reduces the time interval between the introduction and discovery of vulnerabilities.

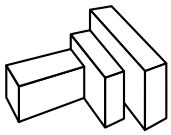


This topology map shows the infrastructure of the Managed Security Service.

Why Consider Managed Vulnerability Assessment Services?

We've touched upon what it takes to successfully execute vulnerability assessments—personnel and technology. The resources required in obtaining, retaining, and maintaining the people and technology are far beyond what most organizations can afford. Managed vulnerability assessment services provide an independent assessment unavailable from internal sources—independence that is increasingly required by external regulation. Finally, the dramatic shift to Intrusion Prevention via continuous vulnerability assessments requires a combination of infrastructure, technology, and personnel of a magnitude available in very few organizations. The required combination of resources is nearly impossible to achieve without dozens of engineers and technicians coupled with the requisite technologies devoted to vulnerability assessment.

A Managed Security Services firm dedicated to vulnerability assessments is able to assemble the resources necessary to execute continuous, current, and comprehensive assessments, achieving economies of scale that clearly show managed services to be "better, faster, and cheaper."



FOUNDSTONE

Foundstone, Inc.
2 Venture Street, Suite 100 • Irvine, CA 92618
1 877 91 FOUND • tel 949-450-5999 • fax 949-450-5995
www.foundstone.com