Definitive Guide™
to
Continuous Network Monitoring

Reduce Risk and Ensure Compliance with Powerful Security Analytics and Reporting

Steve Piper, CISSP

Compliments of:

tenable network security

FOREWORD BY:

Ron Gula

About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View, which provides the most comprehensive and integrated view of network health, and Nessus, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world's largest corporations, not-for-profit organizations, and public sector agencies, including the entire U.S. Department of Defense. For more information, please visit tenable.com.

Definitive Guide™
to
Continuous Network Monitoring

Steve Piper, CISSP
Foreword by Ron Gula

CYBEREDGE
PRESS

Definitive Guide™ to Continuous Network Monitoring

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9888233-8-9 (paperback); ISBN: 978-0-9888233-9-6 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from Tenable: Narayan Makaram, Ron Gula, Steve Hall, Aarij Khan, Jeff Man, Jennifer Collis, Manish Patel, Ted Gary, Diane Garey

Table of Contents

Foreword

After nearly two decades in the information security business, I've found the single best analogy for continuous network monitoring that resonates with non-security professionals: Fitbit. Many of us have learned through Fitbit that we're not sleeping enough, exercising enough, or eating correctly. It's the same scenario with continuous network monitoring, although instead of tracking your personal health, it monitors your organization's security posture. IT teams deploying continuous network monitoring for the first time often find they are not remediating their vulnerabilities as fast as they thought, are not monitoring their users as thoroughly as they believed, and are spending precious resources working on the wrong risk reduction programs.

Regardless of industry sector, every executive needs some form of assurance that the organization's cyber assets are protected. Every company that leverages networks, mobility, cloud, and virtualization is subject to the threat of network attacks and the demands of regulatory compliance. Many of Tenable's customers deploy our continuous network monitoring solutions as a peer to their business systems. Our solutions help provide assurance that the IT organization is not adding new types of cyber risks, so executives can be confident the business is operating safely over the Internet.

We've recently introduced Tenable Critical Cyber Controls. These controls allow an organization to discover all of its assets, confirm they're secured, and determine if they're monitored for abuse. Critical Cyber Controls re-emphasize the core themes from more-complex standards and frameworks while providing you the capability to continuously measure effectiveness of security controls and enabling you to communicate results to an audience broader than just IT experts.

Lastly, vulnerability management is not dead; it was just looking at half of the problem. Most vulnerability management programs feel successful if they reduce the number of critical vulnerabilities or the time it takes to deliver patches. But I've never encountered a vulnerability management program

that achieved zero vulnerabilities or real-time patching. We all know that because of these limitations, firewalls, anti-malware, intrusion detection, and many other cyber defenses are needed.

Continuous network monitoring allows your organization to take an automated, holistic approach to monitoring your security state and activity — discover all assets, identify all vulnerabilities, monitor networks in real time for threats, gather contextual analytics, and provide assurance that mitigating controls are in place. Without this end-to-end view of your entire security program, you and your executive team won't have the right data to fix security issues fast enough to make a difference.

This book provides you with an excellent foundation for building a continuous network monitoring program in your organization. It describes why so many enterprises are abandoning their legacy periodic monitoring mentalities in favor of new methods for continuously identifying risks, mitigating threats, and ensuring regulatory compliance — from cloud to core.

Continuous network monitoring is game-changing technology. And I'm proud that Tenable is leading the charge.

Ron Gula
Co-founder, CEO and CTO
Tenable Network Security

Introduction

Today's enterprise networks are in a perpetual state of flux. The use of mobile devices to access corporate data is skyrocketing. More IT services are being delivered via the cloud than ever before. And users are constantly subscribing to SaaS-based applications, including file sharing applications like Box, Dropbox, and Google Drive, without IT's consent.

Meanwhile, hardly a day goes by without reports of a major data breach appearing in the trade rags or some high-profile cyberattack being featured on the evening news. But why? Are the bad guys really getting smarter? Or are our existing defenses becoming outdated? Perhaps it's a bit of both.

Innovations in continuous network monitoring are giving savvy IT security teams a leg up in mitigating risks associated with advanced threats. Unlike legacy vulnerability management systems that rely on active scanning, continuous network monitoring provides real-time visibility into mobile devices, virtual platforms, cloud applications, and network infrastructure — including their inherent security risks.

If you and your colleagues are tasked with reducing network security risks while maintaining compliance with industry or government regulations, then this book is for you.

Chapters at a Glance

Chapter 1, "Surveying the New IT Landscape," sets the stage for why continuous network monitoring is critical by reviewing computing trends and describing why legacy periodic monitoring practices fall short.

Chapter 2, "Understanding Continuous Network Monitoring," details four common motivations for acquiring a continuous network monitoring platform.

Chapter 3, "Exploring Key Features and Functions," reviews basic and advanced capabilities of leading continuous network monitoring solutions.

Chapter 4, "Achieving and Sustaining Regulatory Compliance," describes how continuous network monitoring can help enterprises maintain ongoing regulatory compliance.

Chapter 5, "Integrating with Your Existing Infrastructure," details the value of, and methodology for, integrating continuous network monitoring systems into your existing network and security infrastructure.

Chapter 6, "Scaling for Tomorrow's Network," will help you ensure that your continuous network monitoring solution meets your needs now and well into the future.

Chapter 7, "Getting Started," provides 10 steps to get your continuous network monitoring investment up and running.

Chapter 8, "Selecting the Right Solution," provides guidance on what to look for — and what to avoid — when evaluating continuous network monitoring solutions.

Glossary provides handy definitions for key terminology (appearing in *italics*) used throughout this book.

Helpful Icons

Tips provide practical advice that you can apply in your own organization.

When you see this icon, take note as the related content contains key information that you won't want to forget.

Proceed with caution because if you don't it may prove costly to you and your organization.

Content associated with this icon is more technical in nature and is intended for IT practitioners.

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Surveying the New IT Landscape

In this chapter

- Review recent trends affecting the way security professionals defend their networks
- Understand why periodic monitoring fails to mitigate threats
- Define continuous network monitoring and review its common use cases

The information technology (IT) landscape has evolved considerably over the last half-decade. The rise in workforce mobility, the proliferation of cloud computing, and a surge in advanced cyberthreats are just a few of the trends facing today's IT security professionals.

Before exploring the merits of continuous network monitoring — the core focus of this book — it's important to quickly review recent macro-level shifts in the IT landscape that have caused "old school" network monitoring practices to fail when used to mitigate today's advanced threats.

The Rise in Workforce Mobility

Perhaps the most impactful trend facing IT security professionals is the dramatic rise in workforce mobility — fueled, in part, by corporate adoption of of *bring-your-own-device* (BYOD) policies (see "The risks and rewards of BYOD" sidebar for more information).

The risks and rewards of BYOD

Implementation of company-approved BYOD policies is both a blessing and a curse. From a positive perspective, BYOD improves employee productivity as workers can access company applications and data from virtually anywhere — even while standing in line at the supermarket. It also improves job satisfaction as employees gain newfound freedom to work using devices that are most familiar to them.

However, BYOD comes with significant trade-offs. Often employee-owned laptops, tablets, and smartphones lack even the most basic endpoint protections. These devices are rarely kept up-to-date with OS and application security patches and often don't conform to company policies regarding security configurations.

Make no mistake: BYOD is here to stay. According to IT security researcher, CyberEdge Group, nearly one-third of enterprises have already adopted BYOD policies, with another third planning to implement BYOD within the next year.

A decade ago, laptop (notebook) sales surpassed desktop sales. According to IT research firm, Gartner, tablet sales are forecasted to surpass PC sales (laptops and desktops combined) for the first time in 2015!

A mobile workforce means transient endpoint devices. When endpoint devices are constantly connecting and disconnecting from the corporate network, monitoring them for vulnerabilities and security misconfigurations is a headache at best. And when personally owned devices are used to connect to corporate applications and data, mitigating security risks becomes a nightmare.

Shifting Data Silos

Modern network design has evolved from aggregating corporate applications and data into a centralized datacenter into hosting applications and their associated data in data silos whose access is limited to office workers and remote/mobile workers who must connect to them. As depicted in Figure 1-1, three common types of data silos are:

- ☑ On-premises applications
- ☑ Infrastructure-as-a-service (IaaS)
- ☑ Software-as-a-service (SaaS)

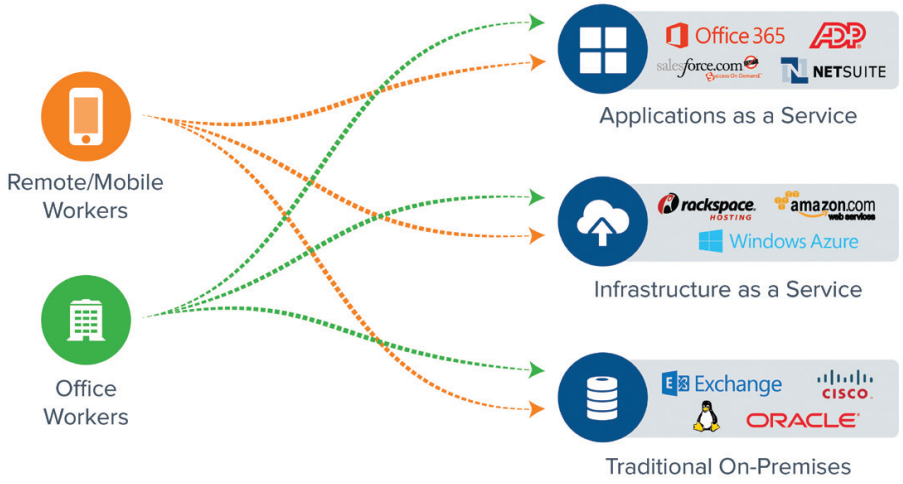

Figure 1-1: Relation between types of users and types of data silos.

On-premises applications

The first and most common data silo today is on-premises applications. This entails hosting applications on bare metal or virtualized servers located within an on-site datacenter. The configurations of these servers rarely change. They are guarded by traditional perimeter- and host-based defenses.

Infrastructure-as-a-service (IaaS)

The next data silo, IaaS, is more difficult to protect with periodic monitoring defenses. IT organizations install and configure operating systems and applications on servers hosted by IaaS service providers, complemented by storage and networking capabilities also maintained by the providers. The challenges are two-fold — the rapid provisioning of new systems and the inability to monitor the service provider's supporting infrastructure.

Software-as-a-Service (SaaS)

The final data silo, SaaS, raises new concerns for IT security professionals. First, IT may not be notified when employees access new SaaS-based applications (a phenomenon known as *shadow IT*) hosted and maintained by service providers. This makes it difficult for IT to maintain the confidentiality and integrity of corporate data — especially when file sharing applications like Dropbox and Box are used. And second, SaaS-based applications are sometimes affected by their own

inherent vulnerabilities and security misconfigurations, placing organizational data at risk.

Knowing what you're defending in large, geographically dispersed enterprises is often half the battle. As you'll soon discover, continuous network monitoring is ideally suited for discovering network assets, from cloud to core.

Evolving Cyberthreat Tactics

Another significant change in the IT landscape over the last half-decade has been the growing sophistication of cyberthreats. Long gone are the days of hacking for kicks. Today's cyber "bad guys" are highly motivated, well funded, and more dangerous than ever.

Faces of today's cybercriminals

Today's cybercriminals can be grouped into four different categories:

- ☑ **Cyberthief** – Individual motivated by financial gain, who may steal banks of credit card numbers or intellectual property that are sold to the highest bidder.
- ☑ **Nation state threat actor** – Individual employed by a government to commit cyberattacks against foreign commercial and/or government entities for political gain. China is often accused of employing nation state threat actors, but now North Korea has joined the club (see "North Korea attacks Hollywood… allegedly" sidebar) with its alleged attack against Sony Pictures.
- ☑ **Hacktivist** – Individual who commits cyberattacks against entities operating in opposition to his or her beliefs regarding free speech, human rights, or political issues of the day.
- ☑ **Insider threat** – Disgruntled employee or contractor who steals confidential data and/or disrupts IT systems from inside the organization.

North Korea attacks Hollywood... allegedly

Until recently, China was seen as the poster child for employing nation state threat actors. Its alleged attacks against Google, Northrop Grumman, Symantec, Yahoo, Dow Chemical, and Adobe Systems – and the U.S. government, of course — have all compounded this perception.

But in November 2014, North Korea stole the headlines with its alleged cyberattack against Sony Pictures in retaliation for a movie titled *The Interview* — a comedy depicting two American journalists recruited by the CIA to assassinate North Korea's leader, Kim Jong-un.

This alleged cyberattack underscores that not all international cyber espionage is motivated by national defense or financial gain. Sometimes it's perpetrated in response to a world leader's temper tantrum.

Surveying advanced threat tactics

Cyberthreats and the means by which they're delivered have grown in sophistication. The following is a list of advanced threat tactics employed by today's cybercriminals:

Consult the Glossary for definitions of these tactics.

- ☑ *Customized malware*
- ☑ *Spear phishing & whaling*
- ☑ *Drive-by download*
- ☑ *Search engine poisoning*
- ☑ *Watering hole attack*
- ☑ *Zero-day attack*

Why Periodic Monitoring Fails

The reason why periodic monitoring fails is simple. It's because your network — including all hosts, operating systems, applications, and data — is constantly in flux. Not just day-to-day, but minute-by-minute. Defending a static environment is challenging enough. Defending a constantly changing environment is nearly an exercise in futility.

Information security researcher, CyberEdge Group, recently surveyed 814 IT security professionals in North America and Europe to gauge their frequency of performing full-network active vulnerability scans. The results (see Figure 1-2) are shocking! Only 15 percent of those surveyed are scanning more frequently than once per month.

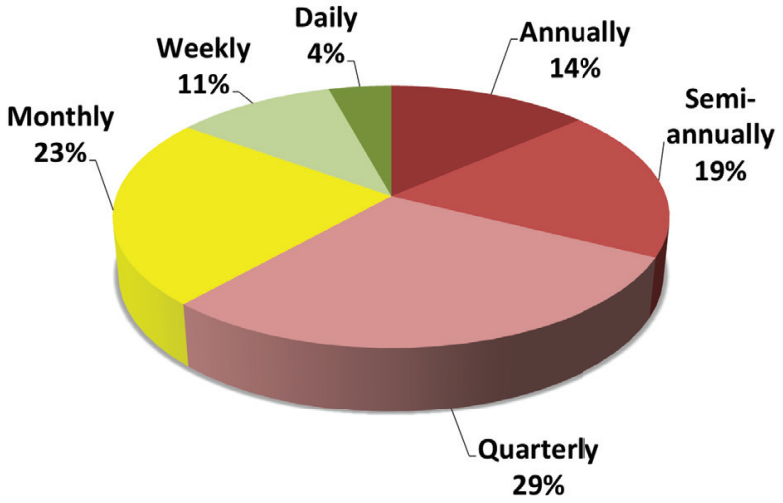

Figure 1-2: Surveyed frequency of full-network active vulnerability scans.
Source: 2015 Cyberthreat Defense Report, CyberEdge Group

The Need for Continuous Network Monitoring

The concept of continuous monitoring in the context of information security is defined by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-137 as "maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions." Although NIST's publication was written in support of the Federal Information Security Management Act (FISMA), the benefits of continuous monitoring apply equally to both commercial and government computer networks.

Today, *continuous network monitoring* has become the benchmark for mitigating internal and external cyberthreats and reducing a network's attack surface. As you'll discover in the next chapter, continuous network monitoring has many use cases.

Chapter 2

Understanding Continuous Network Monitoring

In this chapter

- Reduce your network's attack surface and eliminate blind spots
- Optimize your network defenses while reducing security risks
- Ensure compliance with internal policies and external regulations

Chapter 1 sets the stage for this book by briefly explaining why periodic monitoring fails and why continuous network monitoring is so important. This chapter explores specific use cases for implementing a continuous network monitoring architecture, including:

- ☑ Reducing your attack surface
- ☑ Eliminating network blind spots
- ☑ Optimizing network defenses
- ☑ Ensuring compliance

Continuous network monitoring can't be achieved with point products. Rather, it requires a highly integrated solution designed to continuously audit your entire security program. In addition to vulnerability management, the optimal solution should provide, security configuration assessments, malware defenses, network activity monitoring, event monitoring, and more.

Reducing Your Attack Surface

Reducing system *vulnerabilities* and security misconfigurations on IT assets across your network — also known as reducing your network's *attack surface* — is arguably the most significant benefit of continuous network monitoring. You see, without exploiting weaknesses in your network, your cyber adversaries can't succeed!

Identifying and patching vulnerabilities

More than 68,000 operating system and application vulnerabilities have been assigned *CVE* identifiers within NIST's National Vulnerability Database, including nearly 8,000 from 2014. Of course, the severity of vulnerabilities varies, as depicted by their respective *CVSS* scores assigned by NIST. Any vulnerability with a CVSS score of 7.0 or higher (on a 0.0 to 10.0 scale) is considered "High" and should be patched as quickly as possible.

To research vulnerabilities listed in the National Vulnerability Database, connect to http://nvd.nist.gov.

Even if your organization is diligent about patching system vulnerabilities, it's still important to verify those patches on an ongoing basis. Sometimes systems are "rolled back" to prior configuration states for a variety of reasons, or new virtualized systems are deployed without recent patches.

Performing configuration audits

Exploiting vulnerabilities is just one method of breaching a network. Taking advantage of system security misconfigurations is another way the "bad guys" can compromise servers, desktops, laptops, and mobile devices — even network infrastructure devices.

A continuous network monitoring system can help mitigate security misconfigurations associated with hundreds of operating systems and applications. Common examples of security misconfigurations include:

- ☑ Improper file and directory permissions
- ☑ Unnecessary services enabled, such as content management and remote administration
- ☑ Default accounts with their default passwords
- ☑ Administrative or debugging functions enabled
- ☑ Misconfigured SSL certificates and encryption settings
- ☑ Use of default SSL certificates

IT security professionals often monitor for security misconfigurations associated with SANS Critical Security Controls, as they correspond to a small number of actionable controls with a high payoff. To learn more, connect to www.sans.org/critical-security-controls.

Eliminating Network Blind Spots

The second of four continuous network monitoring use cases is eliminating network blind spots. Today's cyberthreats are more sophisticated and subversive than ever. Sometimes knowing *what* you're protecting is half the battle.

Discovering unmanaged assets

Implementation of BYOD policies is causing enormous headaches for IT security professionals. How can you ensure that employee-owned devices (e.g., smartphones, tablets) used to access corporate applications and data are secure if you don't own or manage them?

Discovering unmanaged assets seems like an impossible task. The odds of inventorying and analyzing employee- and contractor-owned devices during a full-network active vulnerability scan are slim to none — especially since such scans are typically performed once per month (or quarter) during non-business hours. But as you'll discover in the next chapter, the passive network sensor component of a continuous network monitoring solution is ideally suited for discovering and evaluating such devices.

Maintaining visibility of virtual infrastructure

A key benefit of virtualization is the ability to roll out new systems with a few clicks of the mouse. Unfortunately, that blessing is also a curse — at least from a security point of view. Sometimes new virtual machines (VMs) are rolled out without having gone through a proper change management process — a problem commonly called "virtual sprawl." Such VMs may not be up-to-date with the latest patches and may contain security misconfigurations.

Leading continuous network monitoring solutions are not only suited to monitoring physical infrastructure. Key components are commonly deployed within the virtual infrastructure itself, affording IT unprecedented virtual infrastructure visibility.

Shedding light on "shadow IT"

As I mention in Chapter 1 (see "Software-as-a-Service (SaaS)" section), shadow IT causes newfound headaches for IT as users access external SaaS-based applications to share data with outside parties. Fortunately, leading continuous network monitoring solutions can detect the use of all SaaS-based-based applications, enabling IT to verify protections and compliance with internal acceptable use policies.

Optimizing Network Defenses

The third continuous network monitoring use case revolves around optimizing your existing cyberthreat defenses.

Detecting cyberthreats from within

Modern perimeter-based security defenses — such as next-generation firewalls (NGFWs) and malware analysis (sandbox) appliances — do an excellent job of detecting cyberthreats at the perimeter. Unfortunately, sometimes cyberthreats are hand-carried into the office on mobile devices used the prior evening or over the weekend — thus bypassing your perimeter defenses.

To achieve a sound defense-in-depth strategy, you must employ security solutions that continuously monitor for cyberthreats, both at the perimeter and from within the network. Leading continuous network monitoring solutions incorporate comprehensive threat intelligence, enabling the system to detect connections to external hosts with known-bad (blacklisted) IP addresses or URLs.

Analyzing suspicious activity

Over time, continuous network monitoring systems develop a "baseline" of normal network activity with regard to the volume of data transmitted by hosts and the interconnections among hosts.

For example, your laptop should never connect directly with other laptops in the office — barring unusual events, such as connecting to a local file share. Rather, your laptop typically connects to application servers, file servers, print servers, and databases. But if your laptop suddenly starts to initiate connections to other endpoints around the office, that would trigger an anomaly worth investigating, such as the spread of malware from one host to another.

Gaining contextual insight

The network and host intelligence aggregated by a continuous network monitoring solution provides a treasure trove of contextual information that can be used to prioritize security alerts and optimize network defenses.

Take an intrusion detection system (IDS), for example. An IDS is sometimes compared to a baby rattle because it constantly makes "noise" by triggering hundreds of security alerts throughout the day. Although each alert is likely caused by a legitimate threat, many threats target systems that aren't vulnerable to their attack. For example, a piece of malware designed to exploit a recent Windows vulnerability can do no harm to a Linux server or an Apple iPad. By correlating threats against host intelligence — either manually or automatically through a SIEM (security information and event management) platform — IT security professionals can dismiss the majority of IDS security alerts and focus on those that really matter.

Ensuring Compliance

The final use case for implementing a continuous network monitoring solution is ensuring compliance with internal policies and/or external industry or government regulations.

A continuous network monitoring system dramatically simplifies the tasks of validating and documenting compliance through interactive dashboards and automated reports, respectively. (More in these in Chapter 3.) Examples of external regulations commonly faced by continuous network monitoring users include:

- ☑ Payment Card Industry Data Security Standard (PCI DSS)
- ☑ Health Insurance Portability and Accountability Act (HIPAA)
- ☑ North American Electric Reliability Corporation (NERC)
- ☑ Federal Information Security management Act (FISMA)

Chapter 4 explores how continuous network monitoring facilitates compliance with these four regulations.

Key Components of a Continuous Network Monitoring Solution

Now that you understand the key buying motivations for continuous network monitoring, let's explore the components of a typical solution. There are four: active vulnerability scanners, passive vulnerability scanners, log correlation engines, and management consoles.

Active vulnerability scanners

An *active vulnerability scanner* (such as Nessus) is a software application designed to identify hosts connected to the network and assess their weaknesses by uncovering operating system and application vulnerabilities and security misconfigurations.

Active vulnerability scanner software is usually installed by IT on their own hardware. Leading vulnerability management providers support Microsoft Windows, Mac OS X, Linux, Free BSD, and Solaris platforms. Some even provide vulnerability scanners packaged as VMware-based virtual appliances.

Passive network sensors

A *passive network sensor* is an essential component of continuous network monitoring solutions. Instead of actively scanning hosts on a periodic basis (often monthly or quarterly), passive network sensors continuously inspect network traffic to identify and classify hosts, detect their vulnerabilities, and monitor for suspicious traffic.

While a passive network sensor is not intended to replace an active scanner, it helps identify systems as they connect to your network and extract basic vulnerability information based on the traffic they generate. A passive network sensor also provides network topology and monitors communications between hosts and to cloud services, identifying trust relationships and looking for unusual connections and configuration changes indicative of malware or compliance violations.

Log correlation engine

A *log correlation engine* is designed to extract log data from key infrastructure components, such as firewalls, intrusion detection and prevention systems (IDS/IPS), DNS servers, DHCP servers, web proxies, and certain application logs. These logs provide powerful context for pinpointing anomalous traffic that may indicate abuse, errors, malicious activities, or unusual insider activity.

The ability to correlate log data with vulnerability intelligence from both the host and network perspective provides actionable context for forensics, and extends vulnerability analysis to systems that can't be easily scanned or aren't permitted to be scanned. Organizations can also leverage log correlation engines (typically built into the management console; see next section) to demonstrate compliance with many industry and government mandates that require system log aggregation.

Management console

The management console is the central nervous system of every continuous network monitoring deployment. Typically installed and configured by IT administrators on company-provided hardware, the management console is responsible for key functions, including:

- ☑ Assigning granular user permissions
- ☑ Creating scanning policies
- ☑ Load balancing active scanning tasks
- ☑ Distributing daily software updates
- ☑ Aggregating results from active scanners and passive network sensors
- ☑ Displaying real-time dashboards
- ☑ Generating alerts and custom reports

Youngstown State University IT security team scores perfect marks

Youngstown State University (YSU) in Ohio is home to more than 15,000 students and 2,000 staff members. It's comprised of seven separate colleges spread over a 145-acre campus. With thousands of records containing confidential students and staff data, along with a plethora of intellectual property, YSU places high importance on protecting its networks.

The university's IT security team faced three distinct challenges: reducing their network's attack surface, detecting threats missed by perimeter defenses, and generating regulatory compliance reports. Those challenges were met head on with SecurityCenter Continuous View from Tenable Network Security (www.tenable.com).

Tenable's Nessus Vulnerability Scanner and Passive Vulnerability Scanner afforded YSU continuous network monitoring of system vulnerabilities and security misconfigurations, helping the organization to prioritize its patching efforts. Tenable's SecurityCenter Continuous View uncovered several botnet-infected hosts by analyzing abnormal bandwidth usage, and it completely streamlined the university's compliance reporting process through PCI and other compliance report templates.

YSU's IT security team estimates they save hundreds of hours annually, enabling them to reinvest that time in other top IT projects.

Chapter 3

Exploring Key Features and Functions

In this chapter

- Review the standard features found in both continuous network monitoring and everyday vulnerability management offerings
- Explore the advanced functionality found only in enterprise-class continuous network monitoring solutions

By now, you may sense that continuous network monitoring is the evolution of vulnerability management (VM) technology. Its ability to identify system vulnerabilities and security misconfigurations is its core foundation. But unlike typical VM products that rely on periodic active monitoring, continuous network monitoring solutions afford IT organizations a plethora of additional capabilities impossible to achieve with traditional VM offerings alone.

This chapter first reviews the features that are common between VM and continuous network monitoring offerings, and then delves into the powerful capabilities that only continuous network monitoring solutions can provide.

Standard Features

The features in this section are commonly found in enterprise-class VM offerings, as opposed to standalone vulnerability assessment scanners. These features establish a foundation for the continuous network monitoring capabilities described later in this chapter.

Management console

As I state at the end of Chapter 2, the management console is the central nervous system of a continuous network monitoring deployment. You can say the same about its role in a VM deployment, too.

VM vendors typically offer management consoles in one of two forms — software to be installed by the customer using company-approved server hardware and a cloud-based offering hosted by the VM vendor. In the latter case, the customer installs software (or appliances) on premises to perform active network scanning, which then relays scan results to the management console in the cloud.

Although I generally favor software-as-a-service (SaaS) offerings, such as Salesforce.com, there are considerable drawbacks to a cloud-based VM management console with regard to privacy and deployment flexibility. (See the "Don't get your head stuck in the cloud" sidebar in Chapter 7.)

Policy templates

Whether you're motivated by regulatory compliance or reducing your network's attack surface, creating active scan policies is at the heart of a good VM solution. Today's VM vendors make it easy by incorporating a library of scan policy templates into their offerings.

Regulatory compliance policy templates

Following is a sampling of common regulatory compliance templates you'll find in virtually any VM solution:

- ☑ Payment Card Industry Data Security Standard (PCI DSS)
- ☑ Health Insurance Portability and Accountability Act (HIPAA)
- ☑ Federal Information Security Management Act (FISMA) with CyberScope application support
- ☑ North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- ☑ Gramm-Leach-Bliley Act (GLBA)

IT security framework policy templates

The following IT security frameworks are used to help reduce your network's attack surface:

- ☑ SANS Critical Security Controls (CSCs)
- ☑ Control Objectives for Information and Related Technology (COBIT)
- ☑ Center for Internet Security (CIS)
- ☑ NIST SP 800-53
- ☑ ISO 27001

Interactive dashboards

Organizations that acquire VM solutions to reduce the likelihood of cyberthreats will find an interactive dashboard critical to this task. Unlike reports (see next section) that are generated periodically, the dashboard provides a real-time view of system vulnerabilities and security misconfigurations across the enterprise.

A good dashboard (see Figure 3-1) should be highly interactive, enabling users to "drill down" into tables, charts, and graphs to uncover underlying data.

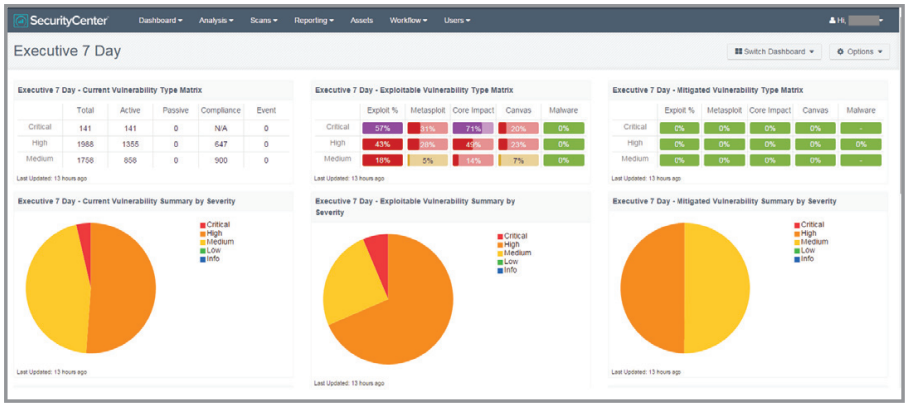

Figure 3-1: Sample executive summary dashboard

Better VM vendors provide customizable dashboard templates, making it easy to monitor areas of concern based on your role in the organization. Common dashboard templates include:

- ☑ Vulnerability metrics
- ☑ Accounts, authentication, and password audits
- ☑ Cyberthreats (APTs, exploits, botnets)
- ☑ Regulatory compliance (PCI, HIPAA, FISMA)
- ☑ Mobile device security

Pre-built and custom reports

Reporting is a critical function of any VM solution, enabling you to provide required information to internal and external regulatory compliance auditors and to satisfy the wide-ranging needs of IT security managers. Better VM management consoles include a report creation wizard that makes it easy to construct meaningful reports.

Most VM vendors give their customers a head start in creating reports by providing a library of pre-built report templates. While vendors may offer more templates, here is a small sampling of ones that are commonly available:

- ☑ Regulatory compliance (PCI, HIPAA, FISMA, SOX)
- ☑ Vulnerability trending (by OS and application)
- ☑ Network service vulnerabilities
- ☑ Virtual computing vulnerabilities
- ☑ Web browser vulnerabilities
- ☑ Platform-specific vulnerabilities (Oracle, EMC, Cisco, Adobe, Microsoft SQL Server, Apache, Apple)
- ☑ Consolidated report for missing patches

Granular access control

In virtually every enterprise IT security organization today, the "principle of least privilege" prevails, meaning that IT users are only granted access to the systems and administrative privileges they need to do their jobs — nothing more.

VM systems support this practice by enabling administrators to granularly control access permissions to perform the following tasks:

- ☑ Administer user permissions
- ☑ Configure scan policies
- ☑ Create and modify dashboards and reports
- ☑ View scan results by network or asset list
- ☑ Modify system settings

IPv6 support

Although only 1 percent of Internet traffic is transmitted using the IPv6 protocol (with the other 99 percent using IPv4), the ability to scan IPv6 hosts is a growing concern. When evaluating VM solutions, be sure to select one that can detect vulnerabilities within IPv6-only hosts and can passively identify these hosts (see the "Vulnerability assessment in an IPv6 world" sidebar). You may not appreciate it today, but you will in the years ahead.

Vulnerability assessment in an IPv6 world

IPv6 is the next-generation Internet protocol address standard intended to supplement, and eventually replace, the IPv4 protocol commonly used today. IPv6, which uses 128-bit addresses, was created in response to the rapid depletion of 32-bit IPv4 addresses. Although IPv4 accommodates 4.3 billion addresses, virtually all of them have already been allocated. IPv6, on the other hand, can accommodate 3.4 x 1038 addresses. Put another way, IPv6 allows every human on Earth to have trillions of IPv6 addresses!

Once IPv6 really takes off and IPv4 becomes a thing of the past (okay, many years from now), actively scanning a 48-bit IPv6 subnet would take about 69,000 years, assuming your scanners can handle a million hosts per second!

By incorporating an IPv6-capable passive vulnerability scanner into your VM solution, you are essentially future-proofing your VM investment, while identifying vulnerable hosts and security misconfigurations in between full active scans. IPv6-only hosts are identified and profiled as they naturally communicate over the network. Active scanners now know exactly which IPv6 hosts to scan when the time comes to do so.

Trouble ticketing

Most VM systems offer a basic trouble-ticketing component to assign remediation requests to IT personnel. Some offer APIs to integrate with existing ticketing systems. In either case, trouble ticketing enables IT managers to view a queue of remediation requests by system, by business unit, and even by user.

Advanced Features

Now that you're grounded in the basics of VM features, let's explore the more advanced features that differentiate leading continuous network monitoring solutions.

Passive network sensor

Passive network sensors deliver continuous network profiling. Rather than actively "probing" network hosts, they "listen" to traffic to uncover security risks. The benefits of deploying passive network sensors are compelling. This technology:

- ☑ Inventories all active assets on the network, including transient devices
- ☑ Alerts you to vulnerabilities and security misconfigurations in between periodic active scans
- ☑ Pinpoints potential insider threats undetected by your perimeter security defenses
- ☑ Provides an alternative to active scanning for mission-critical components, such as medical devices and industrial process controllers in SCADA environments
- ☑ Evaluates security risks of mobile devices
- ☑ Identifies new IPv6-only hosts
- ☑ Supports U.S. federal government continuous monitoring guidelines

If you actively scan your network for vulnerabilities quarterly, you'll have an accurate snapshot four times per year. Passive network sensors keep you abreast of your network's security risks the other 361 days of the year.

Log correlation engine

Log correlation functionality is built right into the management console. It helps you to identify new hosts on network segments not monitored by passive network sensors or hosts that were not connected to the network during the last active network scan. As new hosts are identified, they are grouped in dynamic asset lists (see the "Asset lists" section ahead) and scanned by active scanners to detect system vulnerabilities and security misconfigurations.

Scan agents

An innovative new capability provided by leading continuous network monitoring vendors is the scan agent. Scan agents are ideal for monitoring assets that are frequently unavailable during periodic active scans, such as Windows-based laptops used by remote employees. They're also ideal for monitoring hosts that cannot participate in credentialed scanning or any form of active scanning.

Scan agents are deployed locally on monitored hosts, receive instructions from the management console, and report results back to the console at pre-determined intervals for centralized analysis and reporting.

Mobile device scanning

Today, mobile device management (MDM) vendors provide enterprises with critical capabilities to secure and monitor mobile devices such as smartphones, tablets, and point-of-sale (POS) devices. MDM solutions can provision mobile devices, distribute applications, maintain security configurations, and secure data — but they can't monitor for mobile device vulnerabilities. That's where continuous network monitoring solutions come in, as they can:

- ☑ Enumerate iOS-, Android-, and Windows-based mobile devices that are accessing the network
- ☑ Detect known mobile device vulnerabilities
- ☑ Audit the efficacy of MDM controls
- ☑ Detect jailbroken smartphone devices

Virtualization platform scanning

Today's continuous network monitoring solutions incorporate special APIs enabling active scanners to authenticate privileged credentials when performing credentialed scans of virtualization platforms such as VMware vSphere and vCenter. This helps to identify vulnerabilities and security misconfigurations within virtualization components. Most solutions contain special plugins (checks) specifically designed for this task.

Intelligent load balancing

No single active vulnerability scanner can handle the load of scanning all hosts on all network segments across the enterprise — at least not in a timely fashion. In fact, in larger, geographically dispersed enterprises, it's not uncommon to find dozens — or even hundreds — of vulnerability scanners in use.

Leading continuous network monitoring solutions provide the means to aggregate the collective resources of vulnerability scanners by balancing their respective workloads to optimize efficiency and complete full network scans more quickly. However, some solutions require load balancing to be configured manually, and most vendors use a rudimentary round robin algorithm to distribute scanning assignments equally.

The optimal load-balancing solution requires no human intervention (beyond simply enabling the load-balancing feature) and considers the resource utilization of the scanners to avoid overloads. Intelligent load balancing can shorten a full enterprise network scan from weeks to days.

Asset lists

These days, *asset lists* have become a critical feature of the vulnerability management process. But surprisingly, not all continuous network monitoring solutions incorporate them.

Asset lists enable administrators to categorize hosts (assets) into groups using predefined or user-defined tags (metadata). This allows an administrator to construct policies, monitor dashboards, and create reports just for the hosts assigned to his or her asset list(s). Assigning hosts to asset lists can be performed manually and/or dynamically (automatically).

Common asset list tags include:

- ☑ Business criticality (low, medium, high)
- ☑ Geography (United States, Europe, Asia)
- ☑ Host type (desktop, server, mobile device)
- ☑ Business division (finance, sales, marketing)

Configuration auditing

Mitigating host vulnerabilities is certainly critical to reducing your network's attack surface, but it's only part of what a full-featured continuous network monitoring solution can do. Leading solutions can also evaluate the security configurations of hosts and devices against custom-created configuration assessment policies and predefined policies that align with common IT security frameworks.

With a configuration-auditing feature built into your solution, you can monitor the security configuration settings of a wide range of assets:

- ☑ Operating systems (Windows, Unix, Linux)
- ☑ Databases (Oracle, MySQL, IBM DB2, Informix)
- ☑ Applications (Apache, IIS, Exchange, SharePoint)
- ☑ Web browsers (Internet Explorer, Firefox, Safari)
- ☑ Antivirus software (McAfee, Symantec, Trend Micro)
- ☑ Network infrastructure (firewalls, routers, switches)
- ☑ Virtual infrastructure (VMware, Microsoft Hyper-V)

Patch auditing

Patch auditing is available only in a select few continuous network monitoring solutions. This feature integrates patch scanning with patch management system information to

eliminate time-consuming manual comparisons needed to resolve discrepancies between network security and IT operations teams regarding the patch status of IT assets. This integration compares the results of vulnerability scanning against the status of patch management systems to identify inconsistencies.

Continuous network monitoring solutions that support patch auditing commonly integrate with popular patch (and endpoint) management solutions, including:

- ☑ Microsoft Windows Server Update Services (WSUS)
- ☑ Microsoft System Center Configuration Manager (SCCM)
- ☑ VMware Go (formerly Shavlik)
- ☑ IBM Tivoli Endpoint Manager (TEM)
- ☑ Red Hat Network Satellite

Threat intelligence

Every VM vendor offers ongoing updates of vulnerability *plugins* (or *checks*), which enable the VM system to scan for new OS- and application-level vulnerabilities. Better continuous network monitoring vendors also include additional sources of security intelligence, enabling their customers to uncover indicators of compromise through the following threat intelligence feeds:

- ☑ IP, URL, and domain reputation feeds
- ☑ Botnet feeds
- ☑ Malware feeds

Antivirus and anti-malware security products can't keep up with the deluge of new cyberthreats — with reports of up to 160,000 new malware strains per day! Don't rely on threat intelligence from crowd-sourced vendors as they don't stand a chance of keeping pace with today's rapidly changing threats.

Policy-based assurance

With today's changing IT landscapes, CISO's are looking for solutions that enable them to align security policies with business goals and gain assurance that the underlying security controls are working properly to prevent security breaches. Advanced continuous network monitoring solutions provide ways to express business objectives in terms of security policies, which get automatically translated to discrete controls. These controls are monitored by sourcing in appropriate data from vulnerability scanners, network sensors, and system logs. Policies are evaluated on a continuous basis to simplify compliance and foster business assurance.

Compliance summary dashboards

To extend the basic dashboard functionality of typical VM offerings, leading continuous network monitoring vendors provide powerful compliance summary dashboards (see Figure 3-2) to provide instant macro- and micro-level insight into the organization's regulatory compliance status.

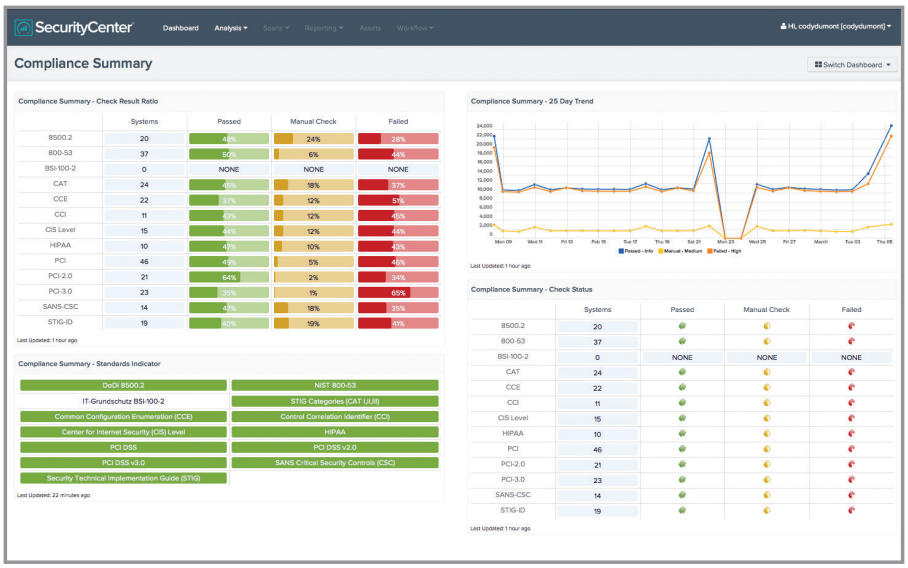

Figure 3-2: Sample compliance summary dashboard.

Remediation scanning

Once a host's vulnerabilities have been patched or its security configuration errors rectified, cautious continuous network monitoring users may wish to re-scan the host to gain an

additional level of assurance that it's no longer vulnerable. This practice, called remediation scanning, can often be triggered by a single mouse click. But some rudimentary solutions require a manually configured scan job to validate host remediation.

Remediation scanning saves valuable time throughout the day when security analysts wish to validate host remediation.

Automated software updates

A sometimes overlooked capability of a continuous network monitoring system is its inherent ability to update its software and its vulnerability plugins (or checks) without human intervention. Take active scanning software, for example. Some VM vendors require their customers to manually deploy such software updates among dozens of scanners spread across the enterprise. However, better continuous network monitoring vendors fully automate this process.

Leading continuous network monitoring vendors give customers the choice of whether to automatically update scanning software, plugin updates, or both. As plugin updates typically occur daily, I would definitely start there.

Management console tiering

Large, geographically dispersed enterprises often implement multiple management consoles to delegate administrative control to local IT security teams. Each IT security team constructs its own scan policies, manages its own users, and monitors the results of active/passive vulnerability scans and configuration audits.

Such organizations typically have a centralized security operations center (SOC) to monitor the security posture of the entire enterprise from one location. Management console tiering enables vulnerability and configuration-auditing data from multiple continuous network monitoring management consoles to be aggregated to a master console at the SOC.

Although it's entirely possible to replicate ALL data from underlying management consoles to the master console, in practice, only data relevant to critical systems is transmitted, preserving bandwidth across regional offices and disk space on the master console.

Chapter 4

Achieving and Sustaining Regulatory Compliance

In this chapter

- Review common government and industry regulatory frameworks required for today's enterprises
- Learn how continuous network monitoring can help enterprises achieve and sustain regulatory compliance

IT organizations spend millions of dollars trying to meet the requirements of, and demonstrate ongoing compliance with, industry and government regulations pertaining to information security. Continuous network monitoring aids these initiatives by proactively identifying issues prior to an audit and demonstrating compliance.

Vendors that separate compliance and vulnerability management capabilities into different modules prolong regulatory compliance processes. These solutions should be highly integrated. A unified continuous network monitoring system, for example, can enable IT users to trace the root cause of a compliance issue to an unpatched system compromised by a botnet. Such automated insight is nearly impossible with separate VM and compliance functions.

In this chapter, I discuss how VM — and to a larger extent, continuous network monitoring — plays an important role in helping IT organizations achieve and sustain compliance with four of the most common regulations facing enterprises today.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS (or just PCI, for short) was established in 2004 by the five founding brands of the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The objective of PCI is to increase controls on payment (debit/credit) card data to reduce organizations' exposure to payment card theft.

PCI DSS v3.0, released in November 2013, is comprised of 12 requirements organized into logically related groups called "control objectives." You can access all PCI documentation at http://www.pcisecuritystandards.org.

The process of validating PCI compliance varies based on an organization's annual payment card transaction volume. Merchants that process more than 6 million Visa and/or MasterCard transactions or more than 2.5 million American Express transactions annually (categorized as level 1 merchants) must hire a PCI Security Standards Council-approved qualified security assessor (QSA) to conduct an annual assessment, which results in a Report On Compliance (ROC). Merchants that process fewer payment card transactions annually (level 2, 3 and 4 merchants) may validate compliance by completing a Self-Assessment Questionnaire (SAQ).

Whether self-assessing or submitting to a QSA-driven assessment, an organization whose payment systems are networked must submit quarterly vulnerability scans of its Internet-facing systems, performed by an Approved Scanning Vendor (ASV). To determine whether a vendor is an ASV, connect to: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php.

Although PCI isn't law, payment card companies enforce compliance by providing more-favorable exchange rates and/or imposing contractual penalties and sanctions, including revocation of a merchant's right to accept their brand of payment cards.

VM plays a significant role in demonstrating PCI compliance. VM solutions are required for internal scanning as well as external scanning (by an ASV). However, continuous network monitoring enables organizations to satisfy many more PCI-related mandates, as depicted in Table 4-1.

Req.	*PCI DSS 3.0 Standard*
1	Use offline firewall audits to meet the six-month firewall review requirement
2	Monitor systems to detect configurations that deviate from standard builds and audit configurations against industry standards
3	Use data discovery to detect violations of encrypted card data storage
4	Continuously monitor network traffic for unencrypted transmissions of payment card data
5	Detect malware in systems, network traffic, or log files on a real-time basis
6	Continuously monitor all systems to ensure critical patch updates are applied
7	Continuously monitor use of access control systems and detect abuses of privileged access
8	Detect user account violations and audit systems for appropriate user account control settings
9	Monitor electronic and physical access systems and logs
10	Continuously monitor and review all access to network resources and payment card data
11	Meet or exceed network vulnerability scanning requirements – both internally and externally
12	Continuously monitor all security and system events as part of an incident response capability

Table 4-1: Sample of satisfied PCI requirements

Crosskey Banking Solutions Adopts Continuous Monitoring to Strengthen Security and Reduce Risk

With banking customers relying on Crosskey to prevent data breaches, protect cardholder data, and ensure the integrity of their operations, the organization sought a way to validate the effectiveness of its security practices. Tenable Network Security (www.tenable.com) helped Crosskey reduce risk and ensure compliance with PCI DSS requirements by implementing SecurityCenter, Nessus, and Nessus Cloud.

To reduce risk and improve its overall security posture, Crosskey decided to transition responsibility for vulnerability scanning from an outsourced managed security service provider (MSSP) to internal resources. This allowed Crosskey to better integrate vulnerability and patch management, shrink the patch window, and eliminate exploitable gaps in coverage. Meanwhile, Crosskey's continued success and growth led to another significant problem with its outsourced scanning services – costs were not scalable.

After evaluating multiple enterprise-class continuous network monitoring platforms, Crosskey selected Tenable SecurityCenter. SecurityCenter offers extensive reporting capabilities as well as the means to address a variety of audit policy needs (including customizable scripting to meet Crosskey's unique requirements), and has enabled Crosskey's successful transition from an MSSP to internal control of vulnerability management processes.

Since implementing SecurityCenter, Nessus, and Nessus Cloud, Crosskey has streamlined and improved the effectiveness of its vulnerability management program. Tenable has enabled Crosskey to identify vulnerabilities and compliance gaps across its externally facing systems, while providing extensive reporting and analytics.

Implementing Tenable products has given Crosskey better control of its environment. Vulnerability management is more collaborative and better integrated with the operations team. This integration has fostered a "DevOps" mindset, as Ops and Security teams work together to secure the Crosskey enterprise.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is maintained by the U.S. Department of Health & Human Services (www.hhs.gov). Designed to protect the confidentiality and integrity of patient health information (PHI), HIPAA had only a muted effect on the security industry until 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) imposed mandatory audits and fines for noncompliance.

Penalties for noncompliance range from $100 to $50,000 per violation (up to $1.5 million in a calendar year), depending on whether the violation relates to willful neglect. Personnel who knowingly disclose PHI face up to 10 years in prison.

As with PCI, VM and continuous monitoring technologies are essential for HIPAA compliance. Table 4-2 summarizes the high-level sections of HIPAA satisfied, in whole or in part, by VM and continuous monitoring capabilities.

Section	*Topic*
§ 164.308(a)(1)	Security Management Process
§ 164.308(a)(4)	Information Access Management
§ 164.308(a)(5)	Security Awareness and Training
§ 164.308(a)(6)	Security Incident Procedures
§ 164.310(c)	Workstation Security
§ 164.310(d)(2)	Device and Media Controls
§ 164.312(a)(1)	Access Control
§ 164.312(b)	Audit Control
§ 164.312(c)	Integrity
§ 164.312(e)	Transmission Security

Table 4-2: HIPAA requirements addressed by VM.

For more information about HIPAA, connect to: http://www.hhs.gov/ocr/privacy/index.html.

North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC; www.nerc.com) is a not-for-profit organization with a mission to "ensure the reliability of the North American bulk power system." It encompasses the interconnected SCADA power grids of the United States, Canada, and a portion of Baja California, Mexico. (See the "Special considerations for SCADA networks" sidebar for more information on SCADA.)

Following the passage of the Energy Policy Act of 2005, funding for an "Electric Reliability Organization" was approved by the U.S. government (and later Canada) to develop and enforce cybersecurity compliance standards for organizations contributing to the U.S. power grid. In 2006, NERC applied for and was granted this designation. NERC then introduced its Critical Infrastructure Protection (CIP) Reliability Standards, labeled CIP-002 through CIP-009. In 2009, it approved version 2 of these standards and began auditing Registered Entities for compliance.

As of June 30, 2010, all Registered Entities must prove "auditable compliance" with all eight categories of CIP controls on a semi-annual basis. Failure to meet any one standard may result in financial penalties of up to $1 million per day, depending on risk and severity.

Of the eight categories of CIP controls, six have components related to VM and continuous network monitoring:

- ☑ CIP-002: Critical Cyber Asset Identification
- ☑ CIP-003: Security Management Controls
- ☑ CIP-005: Electronic Security Perimeter(s)
- ☑ CIP-007: Systems Security Management
- ☑ CIP-008: Incident Reporting & Response Planning
- ☑ CIP-009: Recovery Plans for Critical Cyber Assets

For more information on NERC standards, connect to: http://www.nerc.com/pa/Stand/Pages/default.aspx.

Special considerations for SCADA networks

SCADA (supervisory control and data acquisition) is a term used for computer-controlled systems that monitor and control industrial processes that exist in the physical world. Examples of SCADA systems include power generation, oil refining, water treatment systems, and manufacturing.

From a technology point of view, SCADA networks (that run over routed protocols like IP) are just like any other network. They have various nodes that communicate over various protocols. They are subject to the same sorts of attacks as traditional computer networks. And SCADA manufacturers make the same programming mistakes (causing exploitable vulnerabilities) that Microsoft, Adobe, and other software vendors make.

But SCADA systems are also unique in that aggressive port scanning by typical vulnerability scanners can negatively affect their performance. Vulnerability scans have been responsible for crashing SCADA devices, disrupting processes, and causing erroneous displays in control centers.

To uncover vulnerabilities on SCADA networks without disrupting performance, special precautions must be taken. First, only use active vulnerability scanners that have SCADA plugins (or checks) specifically designed to identify popular SCADA systems, services, and protocols (such as DNP3, ICCP, and MODBUS) and identify their inherent vulnerabilities — all without adversely affecting performance or availability. Second, leverage passive vulnerability scanners — also equipped with SCADA plugins — to monitor systems in between periodic active scans.

Maintaining the integrity and availability of SCADA systems is serious business. In some environments, it can mean the difference between life and death. If you're responsible for securing a SCADA environment, take the time to sit down with prospective continuous network monitoring vendors to thoroughly understand their SCADA scanning capabilities.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 (FISMA) assigns certain responsibilities to U.S. government agencies to ensure the confidentiality, integrity, and availability of federal government data. The act requires program officials to conduct annual reviews of information security programs. However, as of September 2012, the Office of Management and Budget (OMB) requires monthly data feeds to be sent to its CyberScope application portal (see "CyberScope targets FISMA reporting" sidebar).

Several publications from the National Institute of Standards and Technology (NIST) provide guidance on FISMA compliance, including the use of Security Content Automation Protocol (SCAP)-compliant VM solutions to facilitate FISMA reporting. The following four publications are particularly relevant to VM and continuous network monitoring solutions:

- ☑ **NIST 800-37:** Guide for Applying the Risk Management Framework to Federal Information Systems
- ☑ **NIST 800-53:** Recommended Security Controls for Federal Information Systems and Organizations
- ☑ **NIST 800-128:** Guide for Security-Focused Configuration Management of Information Systems
- ☑ **NIST 800-137:** Information Security Continuous Monitoring for Federal Information Systems

To view the full text of FISMA regulations, connect to: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. To access NIST 800-series Special Publications, connect to: http://csrc.nist.gov/publications/PubsSPs.html.

CyberScope targets FISMA reporting

The U.S. Department of Homeland Security, in conjunction with the U.S. Department of Justice, has developed a web-based application (launched by the OMB) called "CyberScope" to standardize manual and automated data inputs for FISMA compliance reporting. FISMA reporting used to take place annually, but with CyberScope that requirement is now monthly.

NIST has assisted by providing data models within CyberScope that leverage existing SCAP (pronounced "ess-cap") primitives (developed by the National Vulnerability Database, or NVD), including:

- ► Common Vulnerabilities and Exposures (CVE)
- ► Common Vulnerability Scoring System (CVSS)
- ► Common Configuration Enumeration (CCE)
- ► Common Platform Enumeration (CPE)

All U.S. federal agencies subject to FISMA must select VM products capable of processing CyberScope-compliant data feeds. Such products must also be designated by NIST as SCAP validated. For a list of SCAP-validated VM products, connect to: http://nvd.nist.gov/scapproducts.cfm.

Chapter 5

Integrating with Your Existing Infrastructure

In this chapter

- Understand the value of integrating continuous network monitoring into your existing network and security infrastructure
- Learn the fundamentals of integrating continuous network monitoring systems with popular third-party products

In today's complex and ever-changing cyberthreat environment, you need all the help you can get to stay ahead of the bad guys. A well-coordinated defense-in-depth strategy is your best bet to avert successful attacks. But if the pieces of your security defense puzzle don't fit well together, cyberthreats will almost certainly slip through the cracks.

Continuous network monitoring is the cornerstone of an effective cybersecurity program. Since *advanced persistent threats* (*APTs*) and other targeted attacks penetrate your network by exploiting an underlying system vulnerability, mitigating those vulnerabilities in the first place is a huge step in fighting advanced threats.

In this chapter, I identify the most common network and security infrastructure platforms appropriate for continuous network monitoring integration. Along with identifying sample vendors in each product category, I describe common third-party integration techniques and the resulting benefits from multi-product integration.

Cloud Infrastructure

Hosting applications and business services in the cloud enables enterprises and government agencies to reduce costs, scale the business, and even "go green." Of course, doing so doesn't mitigate everyday network security risks, and it certain doesn't grant IT organizations a waiver from demonstrating regulatory compliance.

Leading continuous network monitoring vendors offer purpose-built software specifically designed for scanning cloud-based virtualized infrastructure. Packaged as an Amazon Machine Image (AMI), for instance, the software scans hosts and network infrastructure devices in the cloud and exports scan data to the on-premises management console for centralized analysis and reporting.

Sample vendor: Amazon Web Services (AWS)

Security Information and Event Management (SIEM)

A SIEM (pronounced "sim") is often described as a "single pane of glass" for monitoring security events across the enterprise. Correlated alerts from the continuous network monitoring platform can be automatically forwarded to an existing SIEM for processing, along with rich vulnerability and threat information that provides contextual awareness for validating and prioritizing security alerts.

Continuous network monitoring platforms are also useful for auditing the SIEM platform itself for vulnerabilities and security misconfigurations.

Leading continuous network monitoring vendors offer log aggregation and correlation capabilities tightly coupled with threat intelligence. If you're in the market for both VM and SIEM solutions, evaluate continuous network monitoring platforms first. Your vendor just might just have the combined solution you're looking for.

Sample vendors: HP (ArcSight), IBM (QRadar), LogRhythm, Novell (Sentinel), RSA (enVision), Splunk, and Symantec (SMS)

Perimeter Security Defenses

Continuous network monitoring platforms provide rich intelligence to perimeter security defenses so security analysts can better prioritize security events. Examples of such perimeter security defenses follow.

Intrusion Prevention System (IPS)

An inline IPS (or passive IDS) is a security device that sits right behind the firewall to detect a myriad of cyberthreats.

Sample vendors: Check Point, Cisco (Sourcefire), HP, IBM, Juniper, and McAfee

Next-generation Firewall (NGFW)

An NGFW is a multi-function perimeter security device that incorporates three main security components — firewall, IPS, and application control.

Sample vendors: Check Point, Cisco (Sourcefire), McAfee (Stonesoft), and Palo Alto Networks

Unified Threat Management (UTM)

A UTM is also a multi-function perimeter security device that is primarily used by small to midsize organizations.

Sample vendors: Check Point, Dell (SonicWALL), Fortinet, Sophos (Astaro), and WatchGuard

Network Access Control

Network access control (NAC) technology is designed to detect and (optionally) quarantine endpoint devices that fail to comply with the organization's security policies. Such policies may mandate the application of critical system patches, the presence of updated antivirus signatures, and the enablement of a personal firewall.

Many NAC solutions are capable of triggering full active vulnerability scans from third-party continuous network monitoring solutions to help validate compliance with company endpoint security standards.

Sample vendors: Aruba Networks, Cisco, and ForeScout

Mobile Device Management (MDM)

Although the proliferation of smartphones and tablets has dramatically increased employee productivity and responsiveness, inherent vulnerabilities within mobile device operating systems and applications introduce new risks that most organizations are ill-equipped to mitigate.

Thankfully, continuous network monitoring solutions uncover both vulnerabilities and security misconfigurations within mobile devices. Some have also begun to integrate their products with mobile device management (MDM) solutions to monitor these devices even when active and passive vulnerability scanning is not possible. MDM integration yields the following benefits:

- ☑ Enumerate iOS, Android, and Windows mobile devices accessing the corporate network
- ☑ Detect known mobile vulnerabilities, including out-of-date OS versions
- ☑ Provide detailed mobile device information, including serial number, model, version, timestamp of last connection, and user
- ☑ Discover jailbroken iOS devices

Sample vendors: AirWatch, Apple (Profile Manager), Citrix (XenMobile), Fiberlink, Good Technology, Microsoft (ActiveSync), MobileIron, and SAP (Afaria)

Systems Management

Monitoring the health and performance of your continuous network monitoring systems is paramount. The failure of a single active or passive vulnerability scanner, or of the management console, can cause a short-term network visibility gap that, if undetected, could be exploited by cyberattack. Configuring your underlying continuous network monitoring platforms to be monitored by your systems management platform is a wise course of action.

Sample vendors: Dell (KACE), IBM, and Landesk

Incident Management

Although most continuous network monitoring solutions offer a built-in incident management (ticketing) capability, many enterprises prefer to leverage their existing incident management platform for receiving, prioritizing, and assigning critical security events.

Some continuous network monitoring solutions integrate with external incident management applications by way of an API, while others simply generate emails to be received and processed by the incident management system.

Sample vendors: BMC (Remedy), CA, HP, and IBM

Risk Management

Continuous network monitoring platforms integrate key functions complementary to risk management solutions — including asset discovery vulnerability assessment, configuration audit, threat detection, and compliance validation — into one consolidated view. The continuous network monitoring platform can feed policy violations into a larger governance, risk, and compliance (GRC) solution, enhancing the value of the organization's GRC investment.

Sample vendors: Agiliance and RSA (Archer)

Access Management

One of the challenges of *authenticated scans* is safely managing administrative credentials configured within the continuous network monitoring management console. To mitigate this concern, some continuous network monitoring solutions offer agent-based scanners, which eliminate the need for disclosing administrative credentials. If deploying additional agents is not acceptable, then customers can perform credentialed scanning using robust password vault solutions that centrally manage and encrypt administrative passwords. This technology helps mitigate the risk of stolen credentials, which especially concerns customers using rudimentary SaaS-based VM products.

Sample vendors: CyberArk and Thycotic

Patch Management

Better continuous network monitoring systems enable users to audit the efficacy of their patch management solutions. Active vulnerability scanners scour the environment for vulnerabilities and then correlate discovered vulnerabilities with those reportedly patched by the patch management system. This quickly identifies inconsistencies that may result.

Sample vendors: IBM (TEM), Microsoft (WSUS and SCCM), VMware (Go), and Red Hat (Network Satellite)

Penetration Testing

"Pen tests" attempt to compromise systems by simulating the actions of an attacker. Experienced continuous network monitoring users often turn to penetration testing to better understand their organization's risk. Integrating vulnerability scanning results into the pen testing console better equips the pen tester to identify the cost and consequences of exposure.

Leading continuous network monitoring vendors use threat intelligence derived from penetration testing tools by inserting exploit information directly into vulnerability scan results. This approach reduces the burden of pen testing and prioritizes remediation of vulnerabilities.

Sample vendors: Core Security, Immunity, and Metasploit.

Chapter 6

Scaling for Tomorrow's Network

In this chapter

- Ensure your continuous network monitoring investment satisfies your organization's needs today and well into the future
- Review special considerations affecting large, multi-national continuous network monitoring deployments

When evaluating continuous network monitoring platforms, it's important to select a solution that meets not only your needs today, but also your potential future requirements as your organization evolves and expands.

In this chapter, I discuss five important considerations that will help you to ensure your continuous network monitoring investment satisfies your organization's security and compliance needs for years to come.

Supporting Global Enterprise Environments

Mitigating system vulnerabilities, security misconfigurations, and advanced cyberthreats in one geographic location is challenging enough. When you need to defend a global enterprise, that's where the nightmare begins — unless you have the right continuous network monitoring solution.

Achieving enterprise-class scalability

Monitoring a global network with 10,000, 50,000, or even 100,000 nodes (including network infrastructure devices) sounds daunting. And, to be fair, it is. But it's entirely feasible with the right continuous network monitoring platform.

The following are questions to pose to prospective vendors to ensure their solutions can scale to the demands of today's global enterprises:

- ☑ Does your offering include intelligent load balancing to maximize the use of active scanners based on their available resources?
- ☑ Does your offering include the ability to dynamically classify asset groups based on risk-based policies?
- ☑ Does your offering include management console tiering so that organizations can administer their systems locally, but monitor security events centrally?

Another important consideration for large, growing enterprises is active scanning performance. From my experience, the performance of active scanners varies widely from one vendor to another. What might take one vendor's scanner a week to accomplish can be completed by another vendor's scanner in a day.

Securing heterogeneous platforms

It's simple. The larger the organization, the greater the diversity of client, server, and network infrastructure platforms. And the more platforms you have, the greater your exposure to vulnerabilities and security misconfigurations.

When evaluating continuous network monitoring offerings, be sure to ask vendors about their respective libraries of plugins (or checks). Leading vendors offer 60,000 or more plugins to cover virtually every platform imaginable.

Embracing the cloud

I doubt there's an enterprise on the face of the planet that's not leveraging the cloud to deploy at least one application or business service. But, unfortunately, too many organizations are failing to secure their cloud-based assets. As organizations grow, the problem only becomes amplified.

When exploring your continuous network monitoring options, be sure to evaluate how each solution protects cloud-based assets. Questions you may wish to ask vendors include:

- ☑ Can your offering detect usage of SaaS-based applications, such as Dropbox and Facebook?
- ☑ Can your offering scan Amazon Machine Image (AMI) files for vulnerabilities before deploying them in production?
- ☑ Can your scanning software be implemented as a pre-packaged AMI file to accelerate deployment?
- ☑ Can your active scanners running in the cloud export their results to an on-premises management console?

Rightsizing administrative access

The larger the organization, the greater the propensity for specialized IT security roles. Unlike small businesses whose IT professionals wear many hats, enterprises employ highly trained security professionals with specialized skill sets.

Make sure that the continuous network monitoring solution you select enables you to assign access permissions relevant to the roles of your users. For example, a compliance officer who requires the ability to view dashboards and reports should not have the ability to configure scan policies or modify system settings. Avoid solutions that restrict your ability to assign granular access permissions.

Monitoring for change

Sometimes the toughest part of defending an enterprise network is knowing what you're defending in the first place. With mobile devices coming and going, users subscribing to new SaaS-based applications without consent, and network administrators rolling out new virtual machines without following proper change management procedures, it's no wonder why we're constantly reading about major data breaches in the headlines.

Continuous network monitoring extends far beyond legacy vulnerability management capabilities. VM vendors may claim to offer continuous network monitoring simply because their scanners can be configured to repeat scan jobs continuously. Although such repetition increases the frequency of scanning — from, say, once per quarter to once per week — that only provides a fraction of the visibility of a bona fide continuous network monitoring solution.

Be sure to select a solution capable of monitoring network changes in real time, such as:

- ☑ Detection of new hosts on network segments monitored by passive vulnerability scanners
- ☑ Detection of new hosts on (usually remote) network segments not yet monitored by passive vulnerability scanners by triggering active vulnerability scans through dynamic asset lists (see Chapter 3)
- ☑ Detection of new cloud-based hosts through AWS-based scanners
- ☑ Identification of potentially compromised assets by detecting network anomalies and network connections with blacklisted IP addresses and URLs

Chapter 7

Getting Started

In this chapter

- Understand the steps involved in getting your continuous network monitoring system up and running
- Pick up tips and tricks to maximize the security effectiveness of your continuous network monitoring investment

Whether you're replacing your legacy VM system with a modern continuous network monitoring solution, or you're initiating a new program from scratch, this chapter provides 10 actionable steps for getting your continuous network monitoring system up and running. But before diving into these 10 steps, let's first look at the "big picture" of how continuous network monitoring supports the typical IT security operations process in four ways (see Figure 7-1).

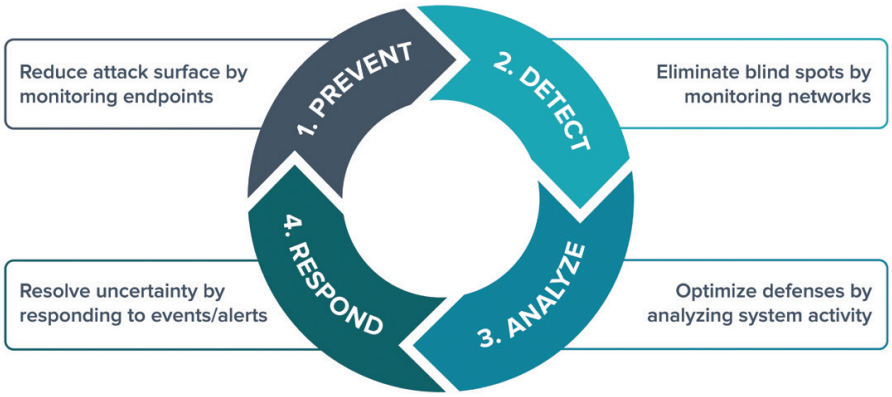

Figure 7-1: Typical IT security operations process.

1. **Prevent:** Identify all vulnerabilities in all known/managed assets in your enterprise. Automatically classify them into asset groups based on OS and applications/services running on them. Perform configuration audits and patch them to prevent bad configurations and known vulnerabilities. This enables you to reduce attack surface and prevent known attacks.
2. **Detect:** Discover unknown/unmanaged assets on your network, including mobile devices, virtual machines and cloud services. Automatically identify OSs and application services that have exploitable vulnerabilities. Detect known threats based on threat intelligence from intrusion detection/prevention devices on your network.
3. **Analyze:** Correlate anomalous activity with real-time threats (events) and monitor for changes to systems/endpoints to see if they match known indicators of compromise. Collect accurate forensic data and present it in a consumable way. Sophisticated analytics are required to tie together the asset and vulnerability data across assessment scans, sniffed networks, and log files, and produce actionable reports.
4. **Respond:** Use forensic data to generate alerts that initiate prioritized manual (workflow-based) actions or automated (API-based) actions to prevent threats from resulting in security breaches.

Continuous network monitoring has evolved from a tactical method for monitoring a network's security state into a strategic, holistic approach for improving cyberthreat defenses, reducing network security risks, and ensuring regulatory compliance.

10 Steps for Getting Started

These 10 steps are listed in a logical, methodical order. However, two pairs of steps are completely interchangeable: Steps 7 and 8 (construct vulnerability scanning and configuration auditing policies) and Steps 9 and 10 (customize dashboards and reports).

Step 1: Determine what to scan

The first step in getting started is to identify the assets that you want to scan, as well as those you want to exclude from scanning. Most organizations start with servers and network devices, as they are mission critical to company operations. Examples of assets typically scanned are:

- ☑ File servers
- ☑ Databases
- ☑ Web servers
- ☑ SMTP/POP servers
- ☑ FTP servers
- ☑ Firewalls
- ☑ Switches
- ☑ Load balancers
- ☑ LDAP servers
- ☑ Wireless access points

When configuring your active scan policies, you'll need to specify ranges of IP addresses or individual IP addresses for hosts that you want to scan. Many continuous network monitoring solutions offer lightweight "discovery scans" to catalog network assets before performing a full-network vulnerability scan. Discovery scans help you to make better-informed decisions regarding which hosts to include and exclude in your scanning policies.

Step 2: Architect your solution

Once you know which hosts you need to scan, you'll need to answer a few more questions to properly design your solution:

- ☑ Where are these hosts located?
- ☑ How frequently will active scans be performed?
- ☑ Does the organization want to detect vulnerabilities (and potential rogue hosts) in between active scans?
- ☑ What third-party systems will your system need to integrate with? (More on that in Chapter 5.)

By answering these key questions, you and your vendor will be in a better position to design your continuous network moni-

toring solution. But, there's another important consideration to ponder. Leading vendors offer three types of solutions: software, hardware (appliances), and software-as-a-service (SaaS).

Most enterprises choose a software-based continuous network monitoring solution for the flexibility it provides. Software can be installed on the organization's platform of choice and can even be deployed within virtual machines. Software-based solutions are ideal for scanning both internal and external hosts. However, some vendors also offer a SaaS-based perimeter scanning service for organizations that want to scan externally facing assets in their DMZ (to demonstrate PCI compliance, for example).

Step 3: Install your management console

Before deploying your active and passive scanners, it's best to install your management console software. That way, when you bring new scanners online, they can instantly connect to your management console to receive security intelligence updates and network scanning instructions.

Management consoles are typically deployed at an organization's headquarters or security operations center (SOC). But remember, better continuous network monitoring providers support distributed management architectures for larger, geographically dispersed organizations. You may want to deploy multiple management consoles — one per geographic location — and implement a master management console at the SOC to aggregate critical security events.

Step 4: Deploy your active scanners and passive sensors

With your management console (or consoles) in place, it's time to deploy your active scanners and passive sensors.

Active vulnerability scanners are essentially nodes on the network that actively probe hosts and network devices (i.e., initiate network connections with them) in search of vulnerabilities and security misconfigurations. For best results, you should deploy at least one active scanner for each LAN, as

scanning hosts on the other end of a WAN can significantly extend the time necessary to complete a full network scan.

Popular active scanners, such as Nessus, require as little as 2GB of available memory to operate, although 4GB of memory is recommended for scanning larger networks. Active scanners usually support a variety of Windows, Unix, and Linux platforms. They can run on your own approved hardware or within virtual machines from VMware or other vendors.

Unlike active scanners, which generate network traffic, passive sensors merely "sniff" (inspect) network traffic. When deploying passive vulnerability scanners, you'll want to connect them to the network in a way that enables them to listen to the largest possible amount of network traffic. To this end, I recommend that you either connect them to the SPAN port of your network switches or interface them with aggregation TAPs or network packet brokers (NPBs) so a single passive sensor can inspect traffic from many network segments simultaneously. Just be sure the network interface card (NIC) is fast enough to keep up with the cumulative speed of your aggregated network segments.

Step 5: Assign user permissions

As I mention in the "Granular access control" section in Chapter 3, most enterprise IT security organizations follow the principle of least privilege, assigning only the access permissions required for IT users to do their jobs.

Invest the time up front to identify the many types of users who will need to interface with your continuous network monitoring solution. Document the access permissions associated with each role so you don't need to reinvent the wheel each time you create a new user account.

Step 6: Categorize your assets

Grouping hosts into asset lists is a relatively new innovation in the industry. Instead of manually tracking (static) IP addresses of grouped hosts, each group is essentially assigned metadata — such as business criticality, geography, host type, and business division — to simplify monitoring of these groups of hosts. This will help later on when creating policies.

Step 7: Construct vulnerability scanning policies

Constructing effective vulnerability scanning policies is critical to the success of any continuous network monitoring deployment. In this step, I discuss the differences between authenticated and unauthenticated scans, considerations for determining active scan frequency, and typical configuration settings associated with your vulnerability scanning policies.

Authenticated versus unauthenticated scans

A vulnerability scanner can only gather a fraction of the details about a system without authenticating to it. A scan without pre-configured administrative credentials is called an *unauthenticated scan*. Such scans can enumerate OSs, network ports open on the system, services listening on ports, and a limited number of vulnerabilities and other security misconfigurations. But the accuracy and thoroughness of this data will be much less than if the scanner had authenticated to the system.

Authenticated scans (or credentialed scans) provide deeper and more-accurate assessment of the target systems. By pre-configuring your active scanners with administrative credentials (preferably dedicated to the scanning process), you'll know exactly which systems are vulnerable and how to remediate them.

Most organizations perform both authenticated and unauthenticated scans. When authenticated scans are not possible, you also have an option of deploying scan agents for deeper scans, without using administrative credentials.

Determining your active scan frequency

Enterprises typically conduct full network scans on a quarterly basis. More security-savvy organizations conduct them monthly, while less-security-conscious organizations conduct them annually. The frequency at which an organization scans may be motivated by industry and/or governmental regulatory compliance standards (see Chapter 4), or simply based on its ability to keep up with processing scan results and patching systems.

Most organizations configure their scanners to operate during off-peak hours, such as evenings, weekends, and holidays. This is because scanners generate traffic that could, in certain circumstances, degrade network performance. And there's always the off chance that a scanner could disrupt an active IT system.

Typical vulnerability scanning policy settings

Today's vulnerability scanners offer dozens of configuration options. Following is a list of the most common ones:

- ☑ Range of target system IP addresses and system ports
- ☑ Administrative credentials for authenticated scans
- ☑ Maximum number of simultaneous target systems that can be scanned by a single scanner
- ☑ Maximum number of simultaneous plugins (or checks) that can be run against a single target host
- ☑ SMTP settings to automatically email scan results to predetermined recipients
- ☑ Automatic plugin update frequency
- ☑ Use of IPv4 and/or IPv6 protocols for scanning

In preparation for your first active scan, I recommend you start small with an initial scanning policy for a few critical systems, and limit the scope of vulnerabilities to those with known exploits granting remote access. That way, you won't be overwhelmed with thousands of identified vulnerabilities in your first scan.

Step 8: Construct configuration auditing policies

Better continuous network monitoring solutions offer the ability to scan hosts and network devices for security misconfigurations that violate internal acceptable use policies (AUPs) and/or external compliance regulations. When configured properly, your system can detect a variety of misconfigurations:

- ☑ Unauthorized applications and protocols
- ☑ Unnecessarily opened ports
- ☑ Violations of minimum password strength
- ☑ Default accounts with default passwords
- ☑ Improper file and directory permissions
- ☑ Misconfigured encryption settings
- ☑ Use of default SSL certificates

Be sure to leverage your management console's library of policy templates for a head start in constructing effective configuration auditing policies.

Step 9: Customize your dashboards

In organizations that conduct frequent active scans and/or have implemented a real-time continuous monitoring solution, a customizable dashboard is the primary interface for security analysts to monitor security posture. A good dashboard should adapt to the needs of the user, rather than forcing the user to adapt to an inflexible dashboard. A good dashboard should also enable users to "drill down" into data displayed in intuitive charts, graphs, and tables, making it easy to find the details they're looking for.

Better continuous network monitoring providers offer a selection of dashboard templates to accommodate any role within the organization.

Step 10: Customize your reports

While security analysts primarily interface with dashboards, IT security managers and compliance auditors generally access the information they need through reports.

A good continuous network monitoring management console will offer a variety of pre-built reports. The reporting engine must enable users to customize reports to meet their specific needs.

Chapter 8

Selecting the Right Solution

In this chapter

- Recognize telltale signs of inferior continuous network monitoring offerings
- Know what to look for when evaluating enterprise-class continuous network monitoring solutions

As is the case with most information security products, no two continuous network monitoring solutions are alike. Some focus purely on vulnerability assessment, while others offer a broad portfolio of advanced features like the ones depicted in the latter half of Chapter 3.

Selecting the right solution is a critical decision for any enterprise — especially given the volume and sophistication of today's cyberthreats. In this chapter, I provide 10 criteria to consider when evaluating continuous network monitoring solutions — some related to the product and others to the provider. But before I describe what you should look for, I'd like to take a few moments to educate you about what to avoid:

- ☑ Avoid solutions that don't offer passive network sensors or a log manager for continuous monitoring.
- ☑ Stay away from solutions that only issue security intelligence updates (with new plugins) weekly rather than daily.
- ☑ Ignore solutions that require a degree in rocket science to use.

- ☑ Steer clear of solutions that offer little to no integration with your existing security infrastructure.
- ☑ Rule out solutions that take several days (or possibly weeks) to complete one full network scan.
- ☑ Be wary of so-called SaaS-only solutions that require you to lease the vendor's scanner hardware appliances, inhibiting your ability to deploy new scanners at will.

Vulnerability assessment is a key component of every continuous network monitoring solution. IT research firm Gartner publishes an annual report called "MarketScope for Vulnerability Assessment." In it, Gartner rates more than 10 leading vendors on a five-point scale (from worst to best): Strong Negative, Caution, Promising, Positive, and Strong Positive. When creating a shortlist of vendors to consider, start with those designated by Gartner as "Strong Positive." You'll be glad you did.

Let's now review the 10 most important criteria to consider when shopping for an enterprise-class continuous network monitoring solution.

Passive Network Sensors

If I had to pick one attribute of an enterprise-class continuous network monitoring solution that, frankly, is a "showstopper" if missing, it would be passive network sensors. Without them, continuous visibility into vulnerabilities and security misconfigurations of your mission-critical systems will only be accurate once every month, quarter, or year, depending on your active scanning frequency. You might be satisfying the "meets minimum" requirement of PCI, HIPAA, or another industry regulation, but you certainly won't be improving your network's security posture.

Beware of so-called continuous network monitoring offerings that lack a passive network sensor capability. These vendors may offer a feature that automatically triggers the next active scan immediately following completion of the last active scan. Although increasing the frequency of active scanning is good, it pales in comparison to what organizations can uncover with

real-time passive vulnerability scanning — especially since active scans usually take place at night when laptops and other mobile devices aren't connected to the network.

Flexible Deployment Options

Enterprises like choices. Some prefer to deploy vulnerability scanner software on vendor-provided hardware appliances. Others (most, actually) prefer to distribute scanner software on their own company-approved hardware platforms and operating systems, or as pre-packaged VMware virtual appliances. Still others prefer to leverage cloud-based solutions for scanning perimeter assets.

Regardless of your preferred scanner platform — vendor-provided or homegrown — it's best to select a vendor that supports all of the aforementioned scanner delivery options. You may prefer one scanner delivery model at headquarters and another for smaller branch offices. Or you simply might change your mind down the road.

One advantage of software-only scanners is that the vendor usually licenses its software based on monitored IP addresses, thus providing scanner software at no charge. The benefit here is that you can deploy five scanners or 500 scanners without paying an additional penny. This affords you the freedom to design a solution that is right for your environment without having to worry about how many scanner software licenses you need to purchase.

One more thing: beware of SaaS-based vendors that tout their 100 percent cloud-based deployment model. This is a fallacy. To scan internal hosts, they typically lease you hardware appliances or virtual appliances — charging you for each one. This limits your flexibility when you decide at a moment's notice that you need another scanner, as you must go through the purchasing process to procure an additional physical or virtual appliance from your provider.

Enterprise-class Scalability and Performance

The performance and scalability of continuous network monitoring solutions vary dramatically from one provider to the next. There are two considerations here: the performance of an individual scanner and the scalability of a cluster of scanners.

The ratio of monitored IPs to active scanner varies by organization and, frankly, has a lot to do with the organization's targeted active scan frequency. The faster a scanner completes its assigned scan jobs, the better it is for the organization. Some scanners can scan a 1,000-node Microsoft Windows network segment in a single day, while others take a week or longer. The only way to determine this for yourself is to put competing scanners to the test during an evaluation phase.

Although scanner performance is important, so is the scalability of the continuous network monitoring solution. Most vendors offer a basic, round robin load-balancing capability, where assigned hosts are equally distributed among active scanners. This strategy has been replaced by intelligent load balancing capabilities that distribute scan load based on available scanning resources. This dramatically reduces the time needed to conduct full-network active scans.

Recently, scanning agents have been introduced by leading continuous network monitoring vendors. By installing a lightweight agent on Windows-based laptops, for example, IT organizations can monitor risks on these devices even when they're not connected to the corporate network. When evaluating continuous network monitoring solutions, look for vendors that offer this capability.

Comprehensive Policy Coverage

A good continuous network monitoring vendor makes it easy for organizations to track mandated compliance with industry and government regulations and voluntary compliance with IT security frameworks — although many of these frameworks are referenced by regulations.

At a minimum, a robust continuous network monitoring platform should provide customizable dashboards and reports that support the following:

- ☑ Regulations: PCI, HIPAA, FISMA (with CyberScope support), NERC, GLBA (Gramm-Leach-Bliley Act)
- ☑ IT security frameworks: SANS 20 Critical Security Controls, Center for Internet Security (CIS) Configuration Benchmarks, NIST 800-53

Daily Security Intelligence Updates

As I mention in Chapter 3, software vendors disclose more than two dozen new operating system and application vulnerabilities every day. And new malware is created virtually every minute of the day.

If your continuous network monitoring vendor publishes security intelligence updates on a weekly — rather than a daily — basis, there's a good chance your scanners lack the ability to detect the latest vulnerabilities when conducting a full network scan. And with so many APTs exploiting recently disclosed vulnerabilities, this is a chance you simply can't afford to take.

Best-of-Breed Feature Set

To maximize your organization's ability to mitigate cyberthreats and maintain regulatory compliance, be sure to select a continuous network monitoring solution that incorporates a broad feature set, including:

- ☑ Customizable, interactive (not static) dashboards
- ☑ Pre-built and custom reports
- ☑ Granular access control
- ☑ Trouble ticketing
- ☑ Passive network sensors
- ☑ Log correlation engine
- ☑ Scanning of mobile devices (smartphones and tablets)

- ☑ Automated, intelligent load balancing
- ☑ Customizable asset lists
- ☑ Patch auditing
- ☑ Threat intelligence
- ☑ Remediation scanning
- ☑ Automated software updates
- ☑ Management console tiering
- ☑ Scan agents
- ☑ Policy-based assurance

For a quick refresher on any of the aforementioned features, flip back to Chapter 3.

Accuracy of Authenticated Scans

Two attributes determine the accuracy of authenticated scans — the quantity and quality of plugins (checks). Some scanners offer only 10,000 to 20,000 plugins, while others come equipped with 50,000 or more.

But offering the most plugins doesn't guarantee vulnerability-detection accuracy. Vendors must thoroughly test their plugins before they are published to minimize the potential of false positives (reported vulnerabilities that do not exist) and false negatives (missed vulnerabilities).

Broad Integration Support

Another important concept to which I dedicate an entire chapter (see Chapter 5) is integration support. The best security solutions share intelligence with other security solutions. Look for continuous network monitoring products that integrate with:

- ☑ Cloud infrastructure
- ☑ Security information and event management (SIEM)
- ☑ Intrusion prevention systems (IPS)

- ☑ Next-generation firewalls (NGFW)
- ☑ Unified threat management (UTM)
- ☑ Network access control (NAC)
- ☑ Mobile device management (MDM)
- ☑ Systems management
- ☑ Incident management
- ☑ Risk management
- ☑ Access management
- ☑ Patch management
- ☑ Penetration testing

If you're considering a continuous network monitoring vendor that offers few ways to integrate with your existing IT infrastructure, it's a telltale sign of a rudimentary product. It's definitely time to move on.

Ease of Use

The best continuous network monitoring products are feature rich but also easy to use. The product should be easy to learn and offer comprehensive, well-written documentation to walk you through more-difficult concepts.

A security product could have every feature you could ever wish for. But if it's too difficult to use, your team is unlikely to embrace it.

Superior Customer Service

Selecting a vendor for continuous network monitoring is just as important as selecting a solution, if not more so. When evaluating competing offerings, be sure to consider the customer support provided by each vendor.

Even if you don't come across any difficulties during your product evaluations, make up a few reasons to call and email each vendor's customer support department. Gauge how quickly they respond to your inquiries and how thoroughly they answer your questions.

Healthcare services company cures vulnerability management woes with continuous network monitoring

Recently, an enterprise security architect at a U.S.-based, publicly held healthcare services company performed an assessment of its long-standing VM platform. Upon learning the benefits of modern continuous network monitoring, and wondering if his company is doing enough to mitigate advanced threats, he compared the attributes of his current VM platform to those from the SecurityCenter Continuous View (CV) platform from Tenable (www.tenable.com). He quickly uncovered numerous shortcomings in the company's existing VM platform, including:

- Inability to inspect laptops and tablets in between weekly active scans
- Inability to facilitate shared monitoring with its IT services outsourcer
- Inability to satisfy internal and external compliance reporting needs
- Inability to import scan results from Microsoft Azure and Amazon Web Services infrastructures into its existing on-premises management console

The company registered for a 30-day evaluation of Tenable's SecurityCenter CV platform. After just one week, the company was sold: Tenable's continuous network monitoring platform could solve all its challenges while decreasing its annual software investment by over 50 percent.

Tenable's Passive Vulnerability Scanner (PVS) technology provides the company with unprecedented network visibility. The company configured its PVS sensor to scan egress traffic emitted from its datacenter, totaling 85 to 100 Mbps. This enables Tenable to identify critical vulnerabilities on laptops and mobile devices not present during weekly active scans.

SecurityCenter CV's customizable dashboards enable both internal and external (outsourced) security analysts to monitor the company's networks for security risks, while its powerful reporting engine makes compliance reporting a snap. And since all active and passive scan data is fed into one SecurityCenter console, monitoring cloud-based assets is just as easy as monitoring on-premises assets.

Tenable's scanning performance is second to none. Its high-performance Nessus active vulnerability scanners, coupled with intelligent load balancing, enable the company to complete scans in a fraction of the time required by its former VM platform.

As an added bonus, SecurityCenter CV's Log Correlation Engine satisfied the company's log management needs. The company is now able to correlate third-party security alerts with Tenable vulnerability intelligence to help validate and prioritize security alerts.

https://www.linkedin.com/company/threathunting
https://www.twitter.com/threathunting_

Glossary

active vulnerability scanner: A software application, such as Nessus, designed to assess computers and network infrastructure devices for vulnerabilities and security misconfigurations by actively probing them.

advanced persistent threat (APT): A sophisticated cyberattack that exploits vulnerabilities to gain network access and remain undetected for extended periods of time.

asset list: A grouping of network hosts that share a common attribute, such as business criticality, geography, or host type. Assets lists are used to configure scanning policies, monitor dashboards, and generate reports.

attack surface: The sum of all exploitable system vulnerabilities and security misconfigurations that exist within hosts and devices on a given network.

authenticated scan: A network scan from an active vulnerability scanner configured with administrative credentials, making it possible to uncover all potential vulnerabilities and security misconfigurations. Also known as a *credentialed scan*.

BYOD (bring your own device): A security trend related to organizations' allowing employees to use personally owned devices to access company applications and data.

continuous network monitoring: The practice of continuously monitoring computer network assets for vulnerabilities, security misconfigurations, and cyberthreats through a combination of active and passive scanning techniques.

CVE (common vulnerabilities and exposures): Unique identifiers assigned and maintained by MITRE Corporation for publicly known information security vulnerabilities.

CVSS (common vulnerability scoring system): Open industry standard under the custodianship of the Forum of Incident Response and Security Teams (FIRST) for assessing the severity of vulnerabilities. CVSS scores are incorporated into CVE descriptions. (See *CVE*.)

data silo: A repository of fixed data that is not part of an organization's enterprise-wide data administration.

defense-in-depth strategy: Leveraging multiple layers of security defenses so that a threat missed by one layer of security may be caught by another.

drive-by download: Malware, virus, spyware, or other threat automatically downloaded without a person's knowledge as a result of simply visiting an infected website.

exploit: A piece of software (malware), a chunk of data, or a sequence of commands that takes advantage (or exploits) a security vulnerability to compromise a host. (See *local exploit*, *remote exploit*.)

false negative: In the context of continuous network monitoring, failure to report a vulnerability, security misconfiguration, or threat that is present.

false positive: In the context of continuous network monitoring, falsely reporting the presence of a vulnerability, security misconfiguration, or threat.

infrastructure-as-a-service (IaaS): A form of cloud computing that provides virtualized computer resources to users via the Internet. The IaaS consumer takes responsibility for configuration and operation of operating systems, databases, and applications, while the IaaS provider hosts and maintains the virtualized infrastructure.

local exploit: An exploit that needs prior access to the vulnerable system to increase account privileges. (See *exploit*.)

log correlation engine: The continuous network monitoring management console component responsible for aggregating and correlating log data from network infrastructure devices to help identify network security risks. It is also useful for identifying new hosts on network segments not monitored by passive network sensors.

malware: Malicious software created to infiltrate or disrupt computer networks to gain access to confidential data or adversely affect availability of IT services. (See *worm, virus, Trojan*.)

passive network sensor: A software application designed to discover all assets on the network, continuously monitor network traffic, and inspect this traffic to identify risks associated with applications, hosts, and network devices.

patch: A vendor-supplied software update to correct vulnerabilities in operating systems and applications. (See *patch management*.)

patch management: The cyclical process of acquiring, testing, and installing patches to administered computer systems in a coordinated effort to mitigate vulnerabilities. (See *patch*.)

Patch Tuesday: The second Tuesday of each month, when Microsoft releases security patches to correct vulnerabilities within its operating system and application products.

plugins: Audit instructions used by active and passive vulnerability scanners to check for system vulnerabilities and security misconfigurations. Also known as *checks*.

remote exploit: An exploit that does not need prior access to the vulnerable system to increase account privileges. (See *exploit*.)

search engine poisoning: Creating seemingly innocuous yet malicious websites optimized with key words to appear high up in search engine results in an effort to infect connecting computers with malware.

shadow IT: A term used to describe IT systems and/or applications used inside organizations without explicit consent from the IT department.

software-as-a-service (SaaS): A form of cloud computing where application software is hosted by a vendor or service provider and made available to customers via the Internet.

spear phishing: A phishing attempt directed toward individuals within a targeted organization, often to initiate an APT against that organization. (See *phishing, APT*.)

SQL injection attack: A cyberattack against a database-driven web application during which the attacker executes unauthorized SQL commands to exploit insecure code.

unauthenticated scan: A network scan from an active vulnerability scanner not configured with administrative credentials, thus limiting its ability to detect vulnerabilities and security misconfigurations that can be uncovered by an authenticated scan. (See *authenticated scan*.)

vulnerability: A weakness (i.e., bug) in a host's operating system or application that can be exploited by an attacker in an effort to compromise a computer network. (See *vulnerability management*.)

vulnerability management (VM): The cyclical practice of identifying, classifying, remediating, and mitigating software vulnerabilities and security misconfigurations. (See *vulnerability*.)

watering hole attack: Using malware to compromise a website likely to be visited by a particular target group, rather than attacking the target group directly.

whaling: A spear phishing attack directed at senior executives and other high-profile employees of a targeted organization. (See *spear phishing*.)

window of vulnerability: The time span from discovery through mitigation of a software vulnerability. During this period, unpatched hosts are particularly vulnerable to attack.

zero-day attack: A cyberattack that exploits an unknown (or unreported) OS or application vulnerability before the availability of a corresponding patch.

Learn how innovations in continuous network monitoring can eliminate blind spots, reduce your attack surface, improve your security posture, and simplify compliance.

Today's networks are constantly evolving. Mobile computing is skyrocketing. The cloud is now mainstream. File sharing apps have run rampant. Legacy vulnerability management products simply can't keep up. Fortunately, continuous network monitoring innovations are providing a leg up on mitigating security risks while dramatically simplifying compliance. If you're tasked with securing your network or supporting compliance audits, this book is for you.

- Understanding continuous monitoring — review four common motivations for acquiring a continuous network monitoring platform
- Exploring key features and functions — review the basic and advanced capabilities of leading continuous network monitoring solutions
- Sustaining regulatory compliance — work smarter to achieve and sustain compliance with government and/or industry regulations
- Integrating with your infrastructure — understand why and how to integrate continuous network monitoring with your existing infrastructure
- Getting started — learn how to get your continuous network monitoring system up and running
- Selecting the right solution — know exactly what to look for, and what to avoid, when evaluating continuous network monitoring solutions

About the Author

Steve Piper is an award-winning author, consultant, analyst, and speaker with more than 20 years of IT experience. He has authored over a dozen books on information security, networking, and Big Data. Steve holds a CISSP security certification from ISC^2 and BS and MBA degrees from George Mason University. Follow Steve on Twitter at @StevePiper or learn more at www.stevepiper.com.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9888233-8-9