Making Everything Easier!™

Tripwire Special Edition

Security Configuration Management

FOR DUMMIES®

Learn to:

- **Reduce your network's attack surface by hardening system security configurations**
- **Achieve and maintain compliance with industry and/or government regulations**
- **Recognize best-of-breed security configuration management solutions**

Compliments of

tripwire®

Steve Piper, CISSP

About Tripwire

Tripwire is a global provider of award-winning IT security solutions, with a long history of innovation and enterprise-class service.

Tripwire products include:

- Tripwire Enterprise, the leading solution for both security configuration management and integrity monitoring
- Tripwire Log Center, a robust, industry-class log and event management solution
- Tripwire VIA Data Mart, which translates "raw security data" into "useful business intelligence" and aligns it with the organization and its missions

Tripwire's *VIA Platform* merges these products into effective IT security solutions, while providing continuous visibility, intelligence, and automation across the largest of global enterprises. Learn more at www.tripwire.com or follow us @TripwireInc on Twitter.

Tripwire has been awarded 9 US Patents for unique innovations in IT security, compliance management, and security automation.

2011 Winner

Best Enterprise
Security Solution

2012 Winner

Best Policy
Management Solution

Security Configuration Management FOR DUMMIES®

TRIPWIRE SPECIAL EDITION

by Steve Piper, CISSP

John Wiley & Sons, Inc.

Security Configuration Management For Dummies®, Tripwire Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN 978-1-118-54516-4 (pbk); ISBN 978-1-118-54553-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Development Editor: Kathy Simpson

Project Editor: Jennifer Bingham

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Sr. Project Coordinator: Kristie Rees

Layout and Graphics: Jennifer Creasey

Proofreader: Susan Moritz

Special Help from Tripwire: Michael Thelander, Eric Stalker, Harold Metzger

Business Development

Lisa Coleman, Director, New Market and Brand Development

Table of Contents

Introduction

Today's enterprises and government agencies face two enormous challenges: minimizing network security risks and maintaining compliance with industry and/or government regulations. Fortunately, an information security solution is available to help IT organizations achieve both objectives at the same time.

Security configuration management (SCM) enables IT security professionals to reduce their networks' attack surfaces by proactively and continuously hardening the security configurations of operating systems, applications, and network devices. At the same time, SCM enables compliance auditors to monitor compliance with mandated policies.

If you're in charge of securing your organization's network, reducing its attack surface, or maintaining and proving compliance with regulations, this book is for you.

How This Book Is Organized

This book is organized so that you don't have to read it cover to cover, front to back. You can skip around and read just the chapters that interest you:

- **Chapter 1, "Understanding Security Configuration Management,"** provides a high-level overview of SCM and its components and describes how a typical SCM solution works. It also defines the role of file integrity monitoring (FIM) in the context of a full-featured SCM solution. The chapter closes by exploring typical components of SCM policies.
- **Chapter 2, "Modern SCM Features,"** explores the basic features of today's SCM product offerings, as well as the advanced features available only in leading SCM solutions. This chapter discusses the importance of remediation guidance and workflows, asset tags, and policy waivers,

and it shows you how SCM can integrate within your existing IT infrastructure.

- In **Chapter 3, "Reducing Your Network's Attack Surface,"** I describe the first of two key use cases for SCM: reducing risk by hardening network assets to minimize the potential for network security breaches. In this chapter, I provide an overview of common IT security frameworks, including SANS 20 Critical Security Controls, NIST SP 800-53, ISO 27001, and COBIT.
- **Chapter 4, "Achieving Regulatory Compliance,"** details the second of two SCM use cases: achieving compliance with industry and/or government regulations. In this chapter, I discuss how SCM is a critical part of maintaining compliance with six common regulations, including the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX).
- In **Chapter 5, "Getting Started,"** I outline the items that you must consider before purchasing an SCM solution. Then I discuss best practices for implementing an SCM system, including deploying agents, scanning network devices, and optimizing dashboards and reports.
- In **Chapter 6, "Ten Buying Criteria for SCM,"** I describe what to look for — and what to avoid — when evaluating SCM solutions.

Icons Used in This Book

This book uses the following icons to indicate special content.

You won't want to forget the information in these paragraphs.

These paragraphs provide practical advice that will help you craft a better strategy, whether you're planning a purchase or setting up your software.

Look out! When you see the Warning icon, it's time to pay attention. You won't want to miss this important cautionary information.

Maybe you're one of those highly detailed people who really need to grasp all the nuts and bolts, even the most techie parts. If so, these tidbits are right up your alley.

Chapter 1

Understanding Security Configuration Management

In This Chapter

- Defining SCM
- Recognizing ideal SCM customers
- Understanding the pivotal role of file integrity monitoring
- Getting grounded in SCM policies

Enterprises and government agencies that must comply with industry and/or government regulations face two enormous challenges: continuous defense against sophisticated cyber-threats and periodic verification of regulatory compliance.

Fortunately, a single solution can help IT departments meet both challenges. I'm speaking, of course, of *security configuration management* — SCM for short.

In this chapter, I discuss how SCM works, identify its ideal buyers and users, and review some of its key components. I also describe why a subset of SCM functionality called file integrity monitoring is a critical component for any successful SCM deployment.

First, though, I define SCM itself.

What Is SCM?

Security configuration management exists at the point where IT security and IT operations meet. It's a software-based solution that combines elements of vulnerability assessment, automated remediation, and configuration assessment. The

goal of SCM is to reduce security risks by ensuring that systems are properly configured — *hardened* — to meet internal and/or regulatory security and compliance standards.

SCM combines network monitoring and endpoint protection methodologies to compare monitored systems against an approved configuration baseline. Deviations from this baseline, known as *test failures,* can often be corrected with little to no human intervention (see Chapter 3).

Security configuration management is sometimes referred to as *secure configuration management.* The terms are equally acceptable, although the former is more commonly used in nongovernment agencies. In this book, the SCM acronym applies to both terms.

How SCM is used

Over the past five years, SCM has evolved from a "nice-to-have" to a "must-have" solution for hardening IT systems and network devices (routers, switches, and other network components) and for demonstrating compliance with regulatory standards. Today, virtually every enterprise and government agency uses SCM as part of a *defense-in-depth* strategy (layers of IT security defenses that mitigate cyberthreats) and as a means of verifying compliance with regulatory standards.

SCM matters greatly to both IT security and IT operations professionals, as you see in the following sections.

SCM in IT security

From an IT security perspective, hardening computer systems is a fundamental step toward securing the network. The 2012 Data Breach Investigations Report published by Verizon (`www.verizonbusiness.com/about/events/2012dbir`) analyzes 855 network breaches worldwide and provides some alarming statistics:

- **Vulnerability:** Most of the victims (79 percent) were targets of opportunity — that is, they had exploitable weaknesses.
- **Ease of attack:** Nearly all the attacks (96 percent) were relatively simple to carry out.
- **Lack of security controls:** Almost all the breaches (97 percent) could have been prevented by simple or intermediate controls (like hardened configurations).

CM to SCM

The concept of configuration management (CM) as a formal management approach dates back to the 1950s, when the U.S. Air Force developed it as a technical discipline for hardware. CM became its own technical discipline in the late 1960s, when the U.S. Department of Defense (DoD) developed a series of CM-based military standards.

In 2010, in the face of increasingly targeted cyberthreats, the National Institute of Standards and Technology (NIST) began circulating new guidance about "the need for configuration management to protect information and information systems." This document, *Special Publication (SP) 800-128,* advocated a new method of security-focused (rather than operationally focused) management for IT configurations.

SP 800-128 also coined the phrase *security configuration management* and defined this capability as "the management and control of configurations for information systems to enable security and facilitate the management of information security risk." Since then *SP 800-128* has become the definitive guide for managing and mitigating the risks of configuration vulnerabilities in information systems.

Implementing SCM to its fullest potential clearly could have prevented a large portion of these data breaches merely by hardening target systems before the attacks occurred.

SCM in IT operations

From an IT operations perspective, failing to comply with industry and/or government regulations can result not only in security breaches but also in costly fines for noncompliance. SCM gives organizations a clear path to achieving regulatory compliance and makes it easy to demonstrate compliance through a variety of prebuilt reports.

These reports are specifically constructed by the SCM vendor in a way that makes it easy for internal and external auditors to demonstrate compliance with virtually any major industry or government regulation — at least for those aspects that specifically relate to SCM and FIM (see Chapter 4).

The anatomy of SCM

To understand how SCM works, you must first understand its components. This section gives you the background you need.

SCM components

Full-fledged SCM systems have three main components:

- **Console:** The console is the central nervous system and primary interface of any SCM solution. It serves as the primary mechanism for scanning network devices that aren't equipped with SCM agents (discussed later in this section), such as routers and switches. The console also enables users to create custom dashboards and reports.
- **Database:** The database is the central repository for all data aggregated and analyzed by the SCM system. It may or may not be housed on the same physical host as the console.
- **Agents:** Critical to the success of any SCM deployment, SCM agents monitor the configuration state of *nodes* (computer systems or devices). They also monitor the integrity of key files, as I discuss later in this chapter.

Agents typically are present for all critical SCM-monitored nodes, with the exception of network devices or low-risk systems. Be sure to configure your SCM console to do agentless scans of such devices — or they may go unmonitored by your SCM solution.

Some vendors promote fully agentless SCM offerings. Although the concept of SCM without any agents may sound appealing, a system of this type provides far fewer features and benefits than a full SCM solution. (See Chapter 2 for a description of basic and advanced SCM features.)

SCM-monitored nodes

Any good SCM system can monitor five types of nodes:

- **File systems:** These nodes include file servers; desktop and laptop computers; and other computing devices equipped with a Windows, Unix, or Linux operating system (OS).
- **Databases:** These physical servers and *virtual machines* (OS instances running in VMware or another virtual computing platform) are configured to host a database

application in a client/server environment. Examples include DB2, Microsoft SQL Server, Oracle, and Sybase.

- **Directory servers:** These nodes include physical servers and virtual machines that host a directory application, such as Lightweight Directory Access Protocol (LDAP), Active Directory, Sun ONE Directory Server, and Novell eDirectory.
- **Virtual infrastructures:** Nodes of this type include components of a typical virtual environment, such as virtual machines, hypervisors, and virtual switches.
- **Network devices:** These nodes include routers, switches, intrusion prevention systems, and other rack-mountable network devices.

Total SCM environment

Figure 1-1 illustrates a typical SCM environment, in which the SCM analyst uses a web browser to connect to the SCM console, which in turn connects to the SCM database, which stores configuration data aggregated from SCM-monitored devices. The outputs of SCM — including reporting and notification, reconciliation, and remediation — are discussed in detail in Chapter 2.

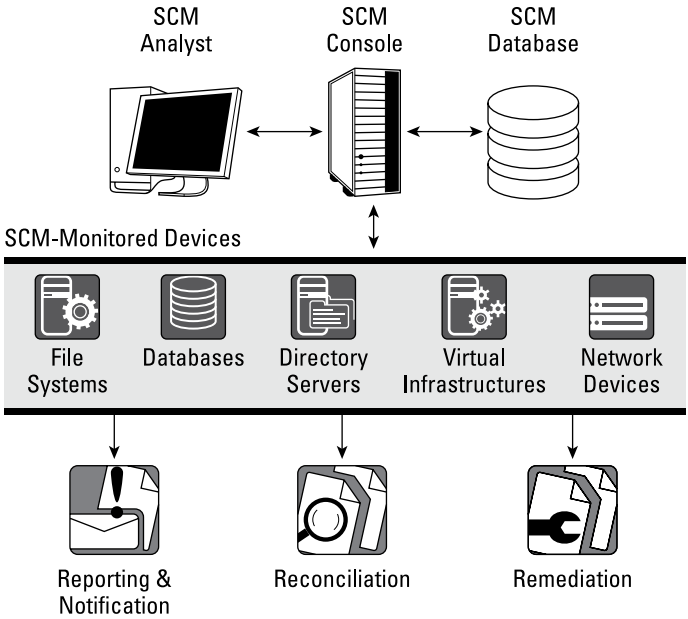

Figure 1-1: SCM conceptual diagram.

Identifying Ideal SCM Buyers

There are essentially two types of ideal SCM buyers (although a single organization may fall into both types), as follows:

- **Organizations with dedicated IT security teams:** SCM is likely to be a good fit for commercial enterprises and government agencies of this type. These organizations understand that every entity is a target for cyberattacks and see SCM as critical to their defense-in-depth strategy against these threats.
- **Organizations that must comply with security mandates:** Various industry and government policies require certain organizations to secure sensitive data. Following are a few examples of these mandates:
  - Payment Card Industry Data Security Standard (PCI DSS) for organizations that hold credit card data
  - Health Insurance Portability and Accountability Act (HIPAA) for organizations that hold or process patient health records
  - Sarbanes-Oxley Act (SOX) for the financial records of publicly held organizations
  - North American Electric Reliability Corporation (NERC) for organizations in power production or transmission
  - Gramm-Leach-Bliley Act (GLBA) for banking and financial organizations
  - Federal Information Security Management Act (FISMA) for government organizations

Organizations that leverage SCM for policy compliance automatically gain the benefit of an increased security posture when the SCM solution is used to its fullest potential.

Seeing Why File Integrity Monitoring Matters

At the beginning of this chapter, I mention a security technology called *file integrity monitoring,* or FIM. Later, in "SCM

components," I allude to the need to monitor the integrity of key files. In this section, I explore FIM in more detail because you can't do SCM right without FIM.

FIM systems are sometimes known as *host intrusion detection systems* (HIDS) or as *change auditing solutions.* Although either name is acceptable, most vendors refer to this technology as FIM, so I use that term in this book.

FIM is the process of validating the integrity of operating-system and application-software files by comparing the current state of files with their known-good baselines. By comparing how files *are* with how they *should be,* FIM helps maintain overall integrity of computer systems and devices.

FIM systems monitor file types such as these:

- OS executable files
- OS and application configuration files
- Registry settings
- Security settings
- File content
- File modification dates and times

Like SCM, FIM is critical to both security and compliance initiatives. In theory, an organization could deploy FIM without SCM but not SCM without FIM (see "Why SCM fails without FIM," later in this chapter).

How FIM works

The components of a FIM solution are quite similar to those of an SCM solution: a console, database, and agents. Instead of monitoring for proper security setting values, however, FIM is monitoring files for deviations from an expected or baseline state.

SCM solutions tell you the range between acceptable or risky configuration settings and where a particular setting lies within this range ("all ports are open" versus "only these two critical ports are open"), whereas FIM tells you that something has changed ("this port was closed yesterday and now it's open").

Why SCM fails without FIM

The purpose of SCM is to assess configuration vulnerabilities within your network infrastructure that hackers could exploit. But what if a system's OS or mission-critical configuration settings have already been weakened, either accidentally or as part of a determined attack? How would you know?

Detection is why FIM is so critical, especially in the context of SCM. SCM helps prevent cyberattacks by creating *known and trusted* states for servers and databases; FIM automatically detects when those states have been changed and a threat may be present.

FIM-powered SCM can be thought of as dynamic SCM, able to continually and dynamically assess vulnerabilities as they arise. SCM powered by external scans, on the other hand, is passive SCM and can only tell if a setting was compliant at some point in time. Because of this important difference, many SCM vendors view FIM as the irreplaceable detection engine powering their SCM solution.

If you plan to deploy FIM as a stepping stone to SCM, be sure to select a vendor that has expertise in both FIM and SCM. Migrating from FIM to SCM should be as simple as entering a license key on your FIM management console.

Some vendors promote fully agentless FIM solutions. Although some auditors may view these solutions as being good enough for meeting certain compliance requirements, in practice, fully agentless solutions lack the depth of agent-based solutions or of hybrid solutions that use both methods. Moreover, they don't operate in real time — the data is only as current as the last active scan, which is most often performed in weekly or monthly intervals.

Understanding SCM Policies

I discuss the basic and advanced features of typical SCM offerings in the next chapter. Here, however, I want to level-set you on the concept of SCM policies — partly so that Chapter 2 makes sense to you.

An *SCM policy* is a collection of *standards* (intended device states) to which monitored systems on your organization's network must conform to comply with internal and/or external regulations.

Policy origins

You can create both internal and external SCM policies, as follows:

- **Internal:** You can create an internal SCM policy from scratch, or you can select an existing policy in your SCM solution's policy library and then modify it. Your SCM solution enables you to capture *baselines* (depictions of all current configuration states) of your monitored nodes and then compare those baselines to an SCM policy.
- **External:** To create an externally motivated SCM policy to assess compliance with a regulatory authority (such as PCI DSS), simply start by selecting the corresponding template in your SCM's policy library.

Many users begin with broad, externally oriented policies, like those from the Center for Internet Security (CIS) and then customize them to create specific, internally oriented IT security policies that are unique to their organizations.

Policy components

Whether your SCM policies are sourced internally or externally, their components are the same: tests, scores, weights, and thresholds. In the following sections, I describe these components in detail.

Tests

A policy is made up of individual *tests* that describe the intended state of a specific configuration setting. It might verify, for example, whether the local administrative password on a specific node is a minimum of eight characters long.

You can collect individual tests in test groups for easier administration, as well as bundle multiple child test groups under a single parent test group.

Scores

A policy *score* is a percentage measurement indicating the overall conformance of a system or device with the policy tests contained in an SCM policy. A policy score of 0 percent indicates that the node has no elements that satisfied the pass/fail criteria of a policy's tests, whereas a score of 100 percent indicates that all the node's elements are in compliance.

Weights

In the context of an SCM policy test, a *weight* indicates the relative importance of a test or test group that is assigned to a node or a group of nodes. Weights typically are assigned on a scale of one to ten, with ten being highest. If minimum password length is of utmost importance to your organization, for example, you may want to assign a weight of ten to password-length tests so that any configuration errors of this type are elevated in the SCM test results.

Thresholds

A scoring *threshold* is a property of an SCM policy that sets a color and a score ranging from 0 (lowest) to 100 (highest) in order to separate urgent failures from important failures. By default, most SCM offerings assign a default value of 100 to the Pass threshold and 0 to the Fail threshold, but thresholds can be customized. Table 1-1 provides an example of how your organization might customize scoring thresholds.

Table 1-1 Sample SCM Policy Scoring Thresholds

Threshold Name	*Score*	*Color*
Pass	80–100	Green
Needs Work	40–79	Yellow
Fail	0–39	Red

This chapter covers a lot of ground, but all this information is fundamental to understanding what SCM is and how it works. Now that you have this information, turn to Chapter 2, which reviews the basic and advanced features of modern SCM offerings.

Chapter 2

Modern SCM Features

In This Chapter

- Recognizing the basic features of SCM products
- Appreciating the advanced features of leading SCM offerings

Although the goals of all SCM products are the same — hardening network assets and maintaining regulatory compliance — their capabilities vary greatly. In this chapter, I describe the basic and advanced features of modern SCM systems.

For the purposes of this book, *basic features* are those that appear in virtually all SCM offerings and are expected by all SCM consumers. *Advanced features* are provided only in leading SCM products and are most often sought by large enterprises and government agencies that have sophisticated SCM requirements.

Basic SCM Features

This section reviews the basic features provided by most SCM offerings.

Policy library

A *policy library* is a collection of policy tests that are relevant for IT security (see Chapter 3) and regulatory compliance (see Chapter 4). Each SCM product comes equipped with some sort of interface that allows users to select policies from the policy library and configure them based on the needs of the organization.

System baselining

System baselining is the act of capturing the state of a monitored node. This state, once captured, is known as the node's *current baseline.* If a node already has a baseline, you can update its current baseline at any time by executing another baseline operation. When the node is baselined again, its former baseline is archived as a *historic baseline version.*

Agents

As noted in Chapter 1, SCM agents for Windows, Unix, and Linux systems are important parts of any SCM system. Active agents provide a greater level of detail than passive scanning alone, and they update the SCM console in real time as the configurations of monitored nodes change.

Better SCM offerings allow you to update SCM agents centrally from the SCM console as new agent software becomes available.

Periodic agentless scanning

For nodes that don't support persistent SCM agents — including network devices such as routers, switches, and intrusion prevention system (IPS) appliances — periodic agentless scanning is needed to detect deviations from approved configuration baselines. This process uses technology similar to that in vulnerability assessment scanners (such as Nessus), but is focused on harvesting detailed configuration items, rather than operating system or application patch levels.

Dashboards

Every SCM solution provides a dashboard for viewing SCM data in the aggregate. Users generally can customize the dashboard, based on their roles in the organization (security- or compliance-focused). Better SCM dashboards enable users to drill down into dashboard *widgets* (individual charts and graphs) to see the underlying host configuration data.

Figure 2-1 depicts a typical SCM dashboard with dashboard widgets configured to monitor compliance with PCI DSS (see Chapter 3) and ISO 27001 (see Chapter 4) configuration policies.

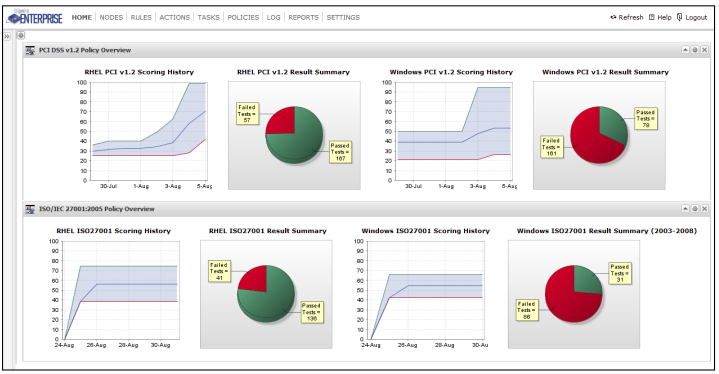

Figure 2-1: SCM dashboard with user-configurable widgets.

Reports

Reports are at the heart of any SCM solution, especially for organizations that must comply with industry or government regulations. Most SCM vendors offer dozens of templates, which make it easy to construct meaningful reports. Popular report templates include the following:

- Overall policy scoring
- Compliance history and trends
- Configuration changes by severity
- Specific failure details

Remediation guidance

When configuration errors are uncovered, they must be *remediated* (fixed). Many SCM offerings provide step-by-step remediation guidance (see Figure 2-2), which means that the user interface provides instructions for resolving the configuration error. (See "Advanced SCM Features" later in this chapter to learn how remediation can be automated.)

Remediation
To remediate failure of this policy test, disable the apache2 service.

Disabling the apache2 service:

1. Become superuser or assume an equivalent role.
2. Stop the **apache2** service using the **/etc/init.d/apache2 stop** command.
3. Prevent the apache2 service from starting at boot time using the **chkconfig –level 0123456 apache2 off** command.

Figure 2-2: Sample remediation guidance for disabling the Apache web service.

Granular administrative access control

A best practice for configuring access to any IT system is to assign only those administrative rights that a user needs to do his or her job — nothing more. This practice is commonly known as the *principle of least privilege.* Most SCM systems make it easy to assign administrative access permissions to users granularly, based on users' roles in the organization.

Advanced SCM Features

The advanced features in this section are included in sophisticated SCM products from leading SCM vendors.

FIM-powered assessment

Although file integrity monitoring (FIM) would be a desirable standard feature in SCM offerings (for reasons that I discuss in Chapter 1), it isn't always included. When you evaluate SCM alternatives, select a vendor that leverages a FIM-powered assessment engine. Such engines are far more efficient than passive scanning systems because they don't need to assess every configuration item with every scan. Instead, they retain a baseline of all configuration states and only report on configuration items that have deviated from their previously

captured known-and-trusted states. Your organization can also reap the benefits of both solutions: one for security assessment and one for anomaly detection.

Asset tags

Better SCM offerings enable users to assign attributes to hosts called *asset tags* (like metadata) to classify assets with business-relevant attributes, such as risk, priority, geographic location, and which regulatory policies govern which assets. Some SCM products even allow you to import asset tags directly from existing IT systems, saving valuable time and effort.

Policy waivers

A *policy waiver* (sometimes called a *policy exception*) is a unique property of an SCM solution that overrides failed policy-test results when the SCM console calculates a score for the policy. This is helpful for systems physically incapable of meeting a configuration requirement, for instance, when legacy systems that only support four-character passwords are tested against policies prescribing passwords of eight or more characters.

Multipolicy capabilities

Most enterprises and government agencies must comply with multiple regulations, and a single host or network device in such an organization may have to comply with multiple regulations concurrently. A single network router at a hospital, for example, may route patient records from the emergency room (related to HIPAA) and credit card information from the cafeteria (related to PCI DSS).

Automated remediation workflows

Remediation guidance is a basic feature of most SCM solutions that provides step-by-step instructions on mitigating configuration violations. Some SCM products take this feature a step further by providing an automated workflow that enables users to approve, deny, defer, and even execute

remediation of failed configurations. This feature can save organizations considerable time and effort, especially when dozens or even hundreds of configuration errors must be mitigated daily.

Support for distributed environments

Some large, geographically dispersed organizations deploy multiple SCM systems to monitor configuration compliance across the entire organization. Administration of each SCM system is delegated to local personnel, but personnel at the organization's security operations center (SOC) may need to monitor configuration compliance centrally. To satisfy this need, certain leading SCM solutions can aggregate SCM data from disparate systems to a centrally located database. Then IT security and compliance personnel can slice and dice the data however they see fit, using their existing reporting tools.

Integration with third-party products

No IT security product should operate in isolation, and SCM is no exception. Following are examples of third-party solutions that should support SCM integration through application programming interfaces (APIs) or other means:

- **Security information and event management (SIEM):** These solutions can use configuration test scores to triage events and see whether systems under attack are truly vulnerable.
- **IT governance, risk management, and compliance (IT GRC):** These systems can consume SCM data to show an objective, data-derived measure of overall security posture, as well as progress toward security goals.
- **Configuration management database (CMDB):** Increasingly, SCM solutions are tracking business-relevant information about the systems they're monitoring (see this chapter's section on "Asset tags") and then updating stale CMDB systems with this same asset information.

Chapter 3

Reducing Your Network's Attack Surface

In This Chapter

- Contrasting IT security frameworks and regulations
- Exploring common frameworks that can harden your network

In this chapter, I delve into IT security frameworks, specifically discussing how SCM and file integrity monitoring (FIM) help an organization comply with these frameworks to reduce its network's attack surface (and also achieve regulatory compliance, as I discuss in Chapter 4).

First, however, I explain the differences between IT security frameworks and IT security regulations.

Differentiating Frameworks from Regulations

When you're dealing with IT security controls, it's important to understand how frameworks and regulations differ:

- **Framework:** An IT security *framework* is a set of voluntary controls that security-conscious IT organizations choose to adopt to help improve security.
- **Regulation:** An IT security *regulation* is a set of rules that IT organizations must follow to achieve or maintain compliance with a government- or industry-mandated regulation (see Chapter 4).

Sometimes, however, the line begins to blur because some IT security regulations leverage IT security frameworks — a topic that I cover in Chapter 4.

Complying with IT Security Frameworks

There are dozens of IT security frameworks available to security practitioners. The frameworks in this section depict those most commonly used in large enterprises and government agencies today.

SANS 20 Critical Security Controls

The SANS Institute (`www.sans.org`) is a cooperative research and education organization, as well as one of the largest and most-trusted sources of information about security training and certification. It develops and maintains a large collection of research documents on various topics related to information security, including the SANS 20 Critical Security Controls, or *20 CSC,* a risk-prioritized list of IT security controls.

The 20 CSC is so highly regarded that enterprises and government agencies alike are beginning to follow these best practices to harden their networks and reduce the likelihood of successful cyberattacks.

Without an SCM solution built on a FIM engine, it's impossible to achieve alignment with the 20 CSC — which, as you discover in Chapter 4, is tied to multiple regulatory-compliance frameworks. Although SCM doesn't apply to every critical control, it addresses two of them in full, which I discuss in the following sections.

For more information on SANS's 20 CSC, connect to `www.sans.org/critical-security-controls`.

Critical control #3: Secure configurations for hardware and software

The intent of this control is to apply secure configuration standards for hardware and software on laptops, workstations, and servers. To achieve this objective, SANS offers 12 guidelines for implementation, automation, and measurement. SCM applies to the eight guidelines listed in Table 3-1.

Table 3-1 SCM-Pertinent Guidelines in SANS Critical Control #3

Guideline	*Description*
3-1	Strict configuration management should be followed. Build a secure image that is used to build all new systems.
3-2	System images must have documented security settings (such as within an SCM policy) that are tested before deployment. These images should be validated on a regular basis.
3-4	Any deviations from the standard build should be documented.
3-7	Run the last version of software and make sure it is fully patched.
3-9	At least once a month, run assessment programs on a varying sample of systems to determine which ones are configured according to the secure configuration guidelines.
3-10	Utilize file integrity checking tools on at least a weekly basis to ensure that critical system files have not been altered.
3-11	Implement an automated configuration monitoring system to analyze hardware and software changes, network configuration changes, and other modifications affecting the security of the system.
3-12	Provide senior executives with charts showing the number of systems that match configuration guidelines versus those that don't.

Critical control #10: Secure configurations for network devices

The second SANS critical control to which SCM and FIM apply is #10, which relates to secure configurations for network devices, such as firewalls, routers, and switches. SCM and FIM support the three guidelines listed in Table 3-2.

Table 3-2 SCM- and FIM-Pertinent Guidelines in SANS Critical Control #10

Guideline	*Description*
10-1	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of device.
10-4	All new configuration rules beyond a baseline-hardened configuration should be documented in a configuration management system.
10-7	The latest stable version of a network device's operating system or firmware must be installed within 30 days of release.

NIST SP 800-53

The National Institute of Standards and Technology (NIST), a nonregulatory agency of the U.S. Department of Commerce, provides special publications (SPs) to help federal agencies comply with the Federal Information Security Management Act (FISMA). NIST SP 800-53 in particular provides guidelines on security controls required for federal information systems.

SCM and FIM deliver continuous, automated monitoring of NIST SP 800-53 security controls to help government agencies identify and prioritize assets, identify risk threshold, determine monitoring frequency, and report to authorizing officials. Specifically, SCM and FIM help by

- Implementing security controls and assessing security configurations.
- Providing automated remediation or remediation guidance on misconfigurations across heterogeneous IT infrastructure.

- Continuously monitoring IT configurations and providing real-time alerts when high-risk changes are detected.
- Demonstrating compliance through real-time dashboards and automated reports.
- Extracting actionable information from servers, networks, and systems to provide forensic analysis.

You can find more information about NIST SP 800-53 and other 800-series special publications by connecting to `http://csrc.nist.gov/publications/PubsSPs.html`.

ISO 27001

The International Organization for Standardization (`www.iso.org`) offers a growing family of standards, including ISO 27001, published in October 2005. This standard formally specifies a management system that brings information security under explicit management control. Organizations that claim to have adopted ISO 27001 can be formally audited and certified as being compliant with the standard.

SCM and FIM play pivotal roles in ISO 27001 compliance. Table 3-3 summarizes the guidelines that specifically pertain to SCM and FIM.

Table 3-3 Sample SCM- and FIM-Pertinent Guidelines in ISO 27001

Guideline	*Topic*
10.1.2	Change management
10.2.3	Managing changes to third-party services
10.4.1	Controls against malicious code
10.6.2	Security of network services
10.7.1	Management of removable media
10.8.1	Information exchange policies and procedures
10.10.3	Protection of log information
11.2.2	Privilege management

(continued)

Table 3-3 ***(continued)***

Guideline	*Topic*
11.3.1	Password use
11.3.2	Unattended user equipment
11.3.3	Clear-desk and clear-screen policy
11.4.1	Policy on use of network services
11.4.2	User authentication for external connections
11.4.4	Remote diagnostic and configuration port protection
11.4.6	Network connection control
11.4.7	Network routing control
11.5.1	Secure logon procedures
11.5.3	Password management system
11.5.5	Session time-out
11.5.6	Limitation of connection time
11.6.1	Information access restrictions
12.5.1	Change control procedures
12.5.3	Restrictions on changes to software packages
15.2.2	Technical compliance checking
15.3.1	Information systems audit controls
15.3.2	Protection of information systems audit tools

You can find more information about ISO 27001 and other ISO standards at `www.iso.org/iso/home/standards.htm`.

COBIT

Control Objectives for Information and Related Technologies (COBIT) is a framework created by the Information Systems Audit and Control Association (ISACA; `www.isaca.org`) to help IT security managers bridge the gaps among control requirements, technical issues, and business risks.

The current version, COBIT 5, defines four IT security process domains:

- Plan and Organize
- Acquire and Implement

- Deliver and Support
- Monitor and Evaluate

SCM and FIM support many elements of two process domains: Acquire and Implement, and Deliver and Support. Table 3-4 summarizes the COBIT controls that SCM and FIM specifically address.

Table 3-4 SCM- and FIM-Pertinent COBIT Controls

Control	*Topic*
A13.2	Infrastructure resource protection and availability
A13.3	Infrastructure maintenance
A16.2	Impact assessment, prioritization, and authorization
A16.3	Emergency changes
A16.4	Change status tracking and reporting
A17.6	Testing of changes
A17.9	Post-implementation review
DS4.5	Testing of the IT continuity plan
DS4.8	IT services recovery and resumption
DS5.3	Identity management
DS5.4	User account management
DS5.5	Security testing, surveillance, and monitoring
DS5.7	Protection of security technology
DS5.9	Malicious-software prevention, detection, and correlation
DS5.10	Network security
DS5.11	Exchange of sensitive data
DS9.1	Configuration repository and baseline
DS9.2	Identification and maintenance of configuration items
DS9.3	Configuration integrity review
DS11.6	Security requirements for data management
DS13.3	IT infrastructure monitoring
DS13.4	Sensitive documents and output devices
DS13.5	Preventive maintenance for hardware

You can find more information about COBIT at www.isaca.org/cobit.

SCM schools an education-software provider on COBIT compliance

One education-software company recently discovered the downside of online instruction and campus commerce when it deployed its software through a cloud-based Software-as-a-Service (SaaS) model. That deployment made the company an inviting target for cyberattacks.

To mitigate that risk, the company implemented the COBIT IT security framework to reduce the network's surface area of attack. But to achieve COBIT compliance, it needed to implement an SCM solution — fast.

The company evaluated both agent-based and agentless SCM offerings and quickly realized the benefits of a real-time, agent-based system. Thus, it selected a solution from Tripwire (www.tripwire.com). Initially, the company deployed Tripwire Enterprise on 60 servers and network devices and also integrated it with the company's Track-It change management tool. For approximately two weeks, the team let the Tripwire software monitor its systems to learn the company's environment and alert the team to all the required changes within it. After two weeks, Tripwire was fully configured, alerting IT personnel to all deviations from configuration baselines.

The company found Tripwire's customizable dashboard to be intuitive and easy to use. When configuration COBIT-related test failures occur, the software offers onscreen remediation guidance and, in many instances, automated remediation workflows to resolve the configuration error with little-to-no human intervention.

Although there's no guarantee the company's SaaS infrastructure will never be compromised by cyberattacks, the company has found peace of mind that it has done everything possible to mitigate such risks.

Chapter 4

Achieving Regulatory Compliance

In This Chapter

- Identifying common regulatory compliance frameworks
- Understanding how SCM helps organizations maintain compliance

SCM vendors often tout their products' capability to help your organization achieve regulatory compliance — but rarely describe exactly how. This chapter helps remedy that disconnect by outlining the regulatory guidelines that are applicable to SCM and file integrity monitoring (FIM) and showing how SCM can help.

Dozens of government and industry regulations affect commercial enterprises and government agencies, and SCM and FIM can help organizations comply with many of them. Unfortunately, I don't have enough space to cover them all, but I do want to discuss the top six.

When it comes to SCM, government and industry regulations share a relatively small set of unique policy tests. Vendors that provide policy mappings make it easy to create holistic views of how tests are reused across multiple compliance policies.

A word of caution before you proceed: In Chapter 3, I talk about the importance of asking prospective SCM vendors to describe how their products' features map to your organization's IT security frameworks. This information is doubly important where regulatory compliance is concerned because failure to comply can be costly.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS, or PCI for short) was established in 2004 by the five founding brands of the PCI Security Standards Council (later established in 2006): American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. This standard was an effort to increase controls on cardholder data to reduce organizations' exposure to credit card fraud. Today, PCI is by far the most common regulation that IT organizations must contend with because it affects every enterprise that stores, processes, or transmits credit card transactions.

PCI is a set of 12 high-level requirements and 221 subrequirements covering every major information security domain, including data encryption, system hardening, and auditing. The standard is maintained and enforced by the PCI Security Standards Council.

Enterprises and government agencies spend hundreds of millions (if not billions) of dollars every year on products and services that help them achieve and maintain PCI DSS compliance. Many information security vendors report that more compliance-driven sales pertain to PCI DSS than all other compliance regulations combined! You can download documentation on PCI at `www.pcisecuritystandards.org`.

Most small organizations can demonstrate PCI compliance with their payment brand (such as Visa, MasterCard, or American Express) by completing the PCI DSS Self-Assessment Questionnaire. Merchants that PCI identifies as Level 1, however — those that process more than 6 million Visa or MasterCard transactions per year or more than 2.5 million American Express card transactions per year — must hire a PCI-approved qualified security assessor (QSA) to demonstrate compliance.

Counting the cost of PCI compliance failure

Although PCI isn't a law, credit card companies can enforce it by imposing contractual penalties or sanctions, including

revocation of a merchant's right to accept or process credit card transactions. For large merchants in particular, these penalties can run into millions of dollars.

Under the Visa PCI program, for example, member merchants or service providers can be fined up to $500,000 per incident if they're compromised and found to be noncompliant with the PCI standard. Members that fail to notify Visa immediately of suspected or known theft of transaction information may be fined $100,000 per incident.

In 2007, more than 45 million credit card numbers were stolen from The TJX Companies' credit card processor, Fifth Third Bank — the worst data breach on record at that time. Visa fined Fifth Third $880,000 for that breach. In 2008, however, Heartland Payment Systems topped the record, when more than 130 million credit card numbers were stolen. Heartland eventually agreed to pay a $60 million settlement to Visa, including millions in PCI-related fines.

Using SCM to achieve PCI compliance

SCM can help your organization achieve PCI compliance by providing the following services:

- Addressing 11 of the 12 PCI compliance requirements (all except requirement #9 regarding physical access)
- Identifying non-PCI-compliant settings across your entire IT infrastructure
- Instantly alerting you to all changes or suspicious events that could take you out of compliance
- Versioning configuration states over time to provide continuous compliance information for use in an audit
- Automatically repairing system configurations that have fallen out of compliance

Table 4-1 lists the PCI requirements (paraphrased to accommodate available space) addressed or enabled by SCM and FIM solutions.

Table 4-1 Sample PCI Requirements Addressed by SCM and FIM Solutions

Req.	*PCI Standard*
1.1	Establish firewall and router configuration standards that are critical to business, testing, and review processes.
1.2	Build a firewall configuration that restricts connections between untrusted networks.
1.3	Prohibit direct public access between the Internet and any cardholder data system.
1.4	Install personal firewall software on computers that have direct connectivity to the Internet.
2.1	Change vendor-supplied defaults before installing a system on the network.
2.2	Develop configuration standards for all system components.
2.3	Encrypt all nonconsole administrative access, using a technology such as SSH, VPN, or SSL/TLS.
5.1	Deploy antivirus software on all systems that are commonly affected by malicious software.
5.2	Ensure that all antivirus mechanisms are current, actively running, and generating logs.
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed.
6.2	Establish a process to identify newly discovered security vulnerabilities.
6.4	Follow change-control procedures for all changes in system components.
8.5	Ensure proper user authentication and password management on all system components.
10.5	Use FIM on logs to ensure that log data can't be changed without generating alerts.
11.2	Run internal and external network vulnerability scans at least quarterly and after significant network changes.
11.5	Deploy FIM software to detect unauthorized modification of critical system files.
12.1	Establish, publish, maintain, and disseminate a security policy that addresses the PCI specification.

Restaurant chain satisfies appetite for PCI compliance

One Italian restaurant chain of 93 restaurants, located from New England to Virginia, is a PCI Level 2 merchant, processing more than 3.7 million credit card transactions annually. Because the chain is headquartered in Massachusetts, it also must comply with MA 201 CMR 17, a state regulation that mandates strong controls to protect personally identifiable information and provide breach notifications to residents of Massachusetts. Ensuring automated compliance, security, and operational efficiency across all networks required a best-in-class SCM system with a full-fledged FIM capability.

The company's senior director of IT evaluated several potential SCM providers but selected Tripwire (`www.tripwire.com`). The reason: The Tripwire solution monitors both physical and virtual infrastructure and has built-in capability to remediate noncompliant systems.

Demonstrating compliance with PCI and MA 201 CMR 17 is now significantly easier on the IT staff. They know in real time when any part of the infrastructure has an insecure configuration and can demonstrate regulatory compliance at any time — not just when the auditor stops by for his favorite lasagna.

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`). The regulation was implemented to protect the confidentiality and integrity of electronic protected health information. Compliance means that system configurations — from networks and servers to virtual machines and security devices — are maintained and assessed against HIPAA policies and can be proved in the event of an audit.

HIPAA had only a muted effect on information security until 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) imposed mandatory audits and increased fines for noncompliance. Penalties for noncompliance

range from $100 to $50,000 per violation, depending on whether the violation is due to willful neglect. And personnel who knowingly disclose individually identifiable health information face a prison sentence of up to ten years.

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

SCM helps organizations that process electronic health information by providing the following services:

- Addressing the Technical Safeguard requirements associated with Part 164, Subpart C, Section 164.312 of Title II of HIPAA
- Ensuring that change is measured and controlled and that HIPAA compliance status is always known
- Automatically repairing configurations that fall out of HIPAA compliance
- Generating compliance reports to support HIPAA audits

North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC; www.nerc.com) is an Atlanta-based not-for-profit organization. Its mission is to "ensure the reliability of the North American bulk power system" — the interconnected power systems of the United States, Canada, and a portion of Baja California in Mexico.

Upon the passage of the Energy Policy Act of 2005, an Electric Reliability Organization was created by the U.S. government to develop and enforce compliance with mandatory reliability standards in the United States. In 2006, NERC applied for and was granted this designation in the United States (and soon after in Canada). Today, NERC's Critical Infrastructure Protection (CIP) standards are mandatory and enforceable throughout the United States, in several provinces of Canada, and in Baja California, Mexico, which is interconnected to the United States's western power grid. Entities that are found to be in violation of a NERC standard are subject to fines of up to $1 million per violation per day.

Nine CIP cybersecurity standards are related to NERC compliance. Each standard establishes the responsible party, compliance requirements, and the definition of compliance. SCM and FIM contribute to multiple requirements in the following CIP standards:

- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-005: Cyber Security and Electronic Security Perimeter
- CIP-007: Cyber Security and Systems Security Management

In addition, a new version of the CIPs, CIP Version 5, is under review that includes a new tenth section (CIP-010) that consolidates all configuration change management and vulnerability assessment requirements into one group as CIP-010. This is an indication of how vulnerabilities of all kinds — configuration vulnerabilities, patch vulnerabilities, and eventually, application vulnerabilities — are beginning to be managed by a new breed of vulnerability platforms.

You can learn more about NERC's CIP standards by connecting to `www.nerc.com`.

SCM powers NERC compliance at East Coast energy company

A regional wholesale power generation company, with power plants located in the mid-Atlantic up through the eastern seaboard, faced a challenging dilemma. It needed to secure its mission-critical systems from cyberattacks while demonstrating compliance to NERC CIP standards. To achieve these objectives, the company sought a best-of-breed SCM solution. And the company's CIO insisted it had to be implemented in just five months!

After evaluating three major SCM providers, the company selected Tripwire Enterprise (`www.tripwire.com`) because it offers comprehensive out-of-the-box NERC compliance configuration policies along with an easy-to-use interface.

In addition to meeting SCM-relevant NERC regulations, Tripwire Enterprise has reenergized the company's network security posture by mitigating device configuration errors that could potentially be exploited by savvy hackers. Daily change reports now alert the IT team to potential noncompliant configuration changes.

U.S. federal civilian agency governs FISMA compliance with SCM

A U.S. federal nonpartisan agency recently faced a serious dilemma. Its IT security team was under fire because the agency still hadn't achieved full FISMA (and NIST) compliance. Its 250 file servers, 50 databases, 75 network devices, and 15 directory servers were clearly out of compliance. The agency's internal auditors deduced that a key ingredient was missing: SCM.

The agency's IT security personnel performed onsite evaluations with multiple SCM offerings from leading providers. The team felt that only one SCM solution could meet all of its needs: Tripwire Enterprise (`www.tripwire.com`).

The agency selected Tripwire partly because of its file integrity monitoring capability but also because of its extensive FISMA and NIST policy coverage, its automated remediation workflow capability, its flexible asset tag functionality, and its intuitive user interface.

Now that its Tripwire SCM system is in place, the agency estimates that it will save approximately $2 million annually in outsourced consulting fees and is finally on a path to achieving FISMA compliance.

Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act of 2002 (SOX) is a federal law that applies to all publicly held U.S. companies, requiring the top managers of those companies to personally certify the accuracy of financial information. SOX also increases the independence of outside auditors who review corporate financial statements and expands the oversight role of boards of directors.

Section 404 of SOX requires officers of a public company to establish, monitor, and report on the effectiveness of controls that ensure the integrity and accuracy of financial data. To IT departments, this requirement means implementing information security best practices to ensure continuous monitoring and management of the security and configuration integrity of systems across distributed networks.

To achieve the IT security best practices required for SOX compliance, most publicly held companies turn to Control Objectives for Information and Related Technologies (COBIT).

By demonstrating compliance with COBIT, IT departments effectively fulfill their obligation for SOX compliance. Rather than rehash how SCM and FIM help organizations achieve compliance with the COBIT security framework, I invite you to read the section on COBIT in Chapter 3.

SOX carries no corporate penalties for noncompliance, but it imposes severe individual penalties. A corporate officer who fails to comply with his or her SOX responsibilities, or who submits inaccurate SOX certification, can face $1 million in fines and ten years in prison, even if the noncompliance was the result of an error. If an officer deliberately submits false certification, he or she could pay $5 million in fines and spend 20 years in prison.

To view the full text of the Sarbanes-Oxley Act of 2002, connect to `http://uscode.house.gov/download/pls/15C98.txt`.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 (FISMA) assigns certain responsibilities to government agencies to ensure the security of data throughout the federal government. The act requires program officials and the head of each agency to conduct annual reviews of information security programs, with the goal of keeping risks at or below specified acceptable levels.

Several special publications from the National Institute of Standards and Technology (NIST) provide guidance on FISMA compliance and are available by connecting to `http://csrc.nist.gov/publications/PubsSPs.html`. Four publications in particular are relevant to SCM and FIM:

- **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

SCAP in FISMA compliance

The Security Content Automation Protocol (SCAP), pronounced "S-Cap," is a method of using specific standards to automate vulnerability management (VM) and SCM processes. Any U.S. agency that is subject to FISMA requirements must select SCAP-validated products, as approved by the National Institute of Standards and Technology.

For a list of SCAP-validated VM and SCM products, connect to `http://nvd.nist.gov/scap products.cfm`.

To view the full text of FISMA, connect to `http://csrc.nist.gov/drivers/documents/FISMA-final.pdf`.

Defense Information Systems Agency (DISA)

The Defense Information Systems Agency (DISA) is a U.S. Department of Defense agency that communicates best practices for securing federal IT systems. DISA has created a library of Security Technical Implementation Guides (STIGs). STIGs contain technical guidance for locking down IT systems that may be vulnerable to cyberattack.

SCM helps federal organizations achieve compliance with relevant DISA STIGs by providing the following services:

- Detecting potential unauthorized system configuration changes through FIM
- Providing real-time dashboards and automated reports that detail current compliance scores and trends
- Onscreen remediation guidance and automated remediation workflows for mitigating violations

To download the entire STIGs library, connect to `http://iase.disa.mil/stigs`.

Chapter 5

Getting Started

In This Chapter

- Selecting the right hardware
- Getting your SCM system up and running
- Integrating with your existing infrastructure

In this chapter, I discuss how to deploy your SCM solution.

Give serious thought to leveraging the talents of your vendor's professional services consultants to get your SCM solution off the ground. These consultants can leverage best practices that they've picked up by working with hundreds of organizations like yours and can help shorten time-to-value.

Researching Before Purchasing

There are many factors to consider when deploying an SCM solution. But some of them occur before you even sign on the dotted line. This section provides some pointers.

Scope your environment

First, scope your network environment to ensure that you're acquiring all the right pieces. Organizations must consider the following quantities and types:

- Servers (file servers, database servers, directory servers)
- Virtual infrastructure (hosts, hypervisors, vSwitches)
- Network and security devices

Also, you need to identify the people who will administer and ultimately use the system, including the following:

- Privileged users
- Analysts and auditors
- Consumers

Consumers are the people who will review the SCM reports: executives, IT management, and internal and external auditors. You need to find an SCM solution with a built-in reporting engine that satisfies the needs of these stakeholders.

Choose the hardware

Choosing appropriate hardware to support your SCM console software is critical. If your hardware falls short, it may not have the necessary horsepower to support all your monitored devices and/or administrators and analysts.

Most SCM vendors publish guidance about selecting hardware for small, intermediate, and large (enterprise) deployments. This guidance includes recommendations on CPUs, memory, and storage. Be sure to consult each prospective vendor to ensure that no extraordinary hardware requirements exist that could push the total cost of their solution outside your budget.

Some administrators may prefer to install their SCM console on Windows servers; others may prefer Unix or Linux machines. You may want to consider an SCM solution that supports all three platforms.

Consider support for distributed environments

Large, geographically dispersed enterprises and government agencies may require multiple SCM consoles for local administration. IT security personnel and auditors based at headquarters, however, need to have a global, or *federated,* view of the organization's security posture and its ability to comply with regulations.

To support this need, better SCM solutions allow local security managers to replicate data to a central database. When that

data is in the repository, security managers and auditors at headquarters can use their own reporting tools or dashboards to view SCM data from across the organization.

Deploying Your SCM Solution

After you've acquired your SCM solution, it's time to deploy it. After your SCM console software has been installed, it's time to deploy your agents.

Deploy agents

Most organizations use industry-standard tools to install software on Windows, Unix, and Linux machines. SCM vendors encourage their customers to use those tools to deploy SCM agents as well. Thereafter, the vendor's SCM console should take responsibility for updating agent software as new releases (including improved features and bug fixes) become available.

Be sure to ask your SCM vendor about agent deployment options. More mature SCM solutions include extensive setup wizards that automate certain deployment options, such as agent groupings, policy scoping, and configuring the frequency with which checks are run or the times when reports are created and distributed.

Configure network-device scanning

As I mention in Chapter 1, not all monitored nodes support agents. The exceptions include network devices such as routers, switches, and intrusion-prevention systems. Be sure to configure your SCM console to scan these devices at your desired frequency: daily, weekly, or monthly.

Your highest-risk systems should always have agents installed on them, but many solutions let you treat lower-risk systems like network devices. Schedule these systems for agentless scans of critical configuration items.

Also make sure that your SCM console has sufficient administrative credentials to ensure that you obtain the status of the security configuration settings for all your network devices.

Optimize dashboards and reports

With most IT security solutions, there's no such thing as one size fits all. Better SCM solutions allow you to configure dashboard templates for users who play common roles. You may want to configure dashboard templates for executives, management, analysts, and auditors, for example. Some SCM solutions even allow users to customize their own dashboard settings to align with their own preferences and needs.

As for reports, you can save considerable time by customizing templates from your SCM vendor's report-templates library rather than creating each new report from scratch. This library gives you a considerable head start on creating the reports that your organization requires.

Enable third-party product integration

No IT security solution should operate in isolation. The best solutions integrate with your security infrastructure (through application programming interfaces or other means) to share intelligence and automate certain business functions.

In the case of SCM, you may want to integrate with the following:

- Security information and event management (SIEM)
- IT governance, risk management, and compliance (IT GRC)
- Configuration management database (CMDB)

Train users

Training is often an afterthought in deploying an SCM solution. To ensure the success of your investment, however, you should take advantage of the training options made available by your SCM vendor. Better SCM vendors offer instructor-led training, self-paced training, and even onsite training at your location. They may also provide customized training based on the needs of your administrators and users.

Chapter 6

Ten Buying Criteria for SCM

In This Chapter

- Knowing what to look for in an SCM
- Ensuring that your SCM solution meets your needs

SCM can help reduce your network's attack surface and help your organization efficiently and repeatedly demonstrate regulatory compliance. This chapter explores what you should look for when you evaluate SCM solutions.

Expansive Policy Template Library

At the heart of every SCM solution is its policy library. You don't necessarily need to select the SCM product that has the most policy templates, but you do need to select one with policies that are important for your organization — both for IT security and regulatory compliance.

A great way to ensure that an SCM provider can satisfy your organization's needs is to review its list of sample customers, broken down by industry and by policy adherence. If you don't see any of your industry peers on the list, that fact should raise a red flag. Be sure to ask your vendor to provide at least one reference in your industry — or at least to refer you to a customer that cares about the same IT security frameworks and policies that you do.

Heterogeneous Platform Support

An SCM solution that supports Windows, Linux, and Unix platforms (like Oracle Solaris or IBM AIX) provides the ultimate deployment flexibility.

Also, when you compare SCM vendors, consider the variety of platforms that they support through both agent software and agentless methods. Agents provide the real-time assessments necessary to mitigate risks and to maintain accuracy of compliance reports, while agentless scanning eliminates gaps in security coverage.

FIM-Powered SCM

In Chapter 1, I discuss why file integrity monitoring (FIM) is critical to any SCM solution. Without it, every configuration item must be assessed every time, and you may never know whether an operating system or server-based application is actively experiencing a cyberattack. Some SCM vendors downplay the role of FIM, however, either because they lack FIM offerings or offer only rudimentary FIM solutions.

When you shop for an SCM solution, think in terms of *dynamic SCM* rather than *passive SCM*. Be sure to short-list solutions that offer full-featured FIM capabilities because these are the features that make dynamic SCM possible.

Waiver and Exception Management

When a monitored node can't meet an SCM policy requirement or contains elements that are out of scope with a specific compliance policy, it's best to grant that node a temporary or permanent policy waiver so that analysts can exclude it when they calculate and report on policy compliance. (I discuss policy waivers in detail in Chapter 2.)

Not all SCM vendors offer a policy waiver capability. If this feature is important to you, or will be in the future, be sure to consider SCM solutions that allow you to annotate the rationale for policy waivers to minimize confusion among internal and external auditors.

Support for Distributed Environments

Environmental activists like to repeat the adage "Think globally, act locally." In many ways, that adage applies to IT, including the SCM function. Large, geographically dispersed organizations may allow IT security personnel in each major facility to administer their own SCM consoles, but these organizations typically don't want to lose visibility at headquarters. They want top-down risk and security solutions.

To solve this dilemma, better SCM vendors support distributed environments by enabling each SCM console to replicate its data to a central data repository — typically, at headquarters. Then auditors and IT security management can query SCM data via their existing dashboard and reporting utilities to gain a global perspective on policy compliance.

Comprehensive Third-Party Integration Support

No IT security solution should operate in a vacuum. By sharing data across multiple security platforms, IT can reduce network security risks while reducing costs.

A good SCM solution should provide APIs or other means of integrating with various third-party products, such as SIEMs, IT GRC platforms, and CMDBs (see Chapter 2).

If a prospective vendor offers no means for integrating with these or other platforms, it's definitely time to move on.

Multipolicy Capabilities

Most organizations today must comply with multiple regulatory compliance standards concurrently. If your organization falls into this category, be sure to select an SCM solution that supports a multiple-level view of test results. This view enables an analyst or auditor to view how a single host or network device complies with each relevant compliance policy one at a time.

Remediation Guidance and Workflows

Some basic SCM offerings (especially those built into vulnerability assessment solutions) can identify certain configuration test failures but don't provide any guidance on how to remediate them. Even if you happen to know how to address the problem, you still have to resolve it manually.

Better SCM offerings provide step-by-step onscreen guidance on solving security configuration problems. Some products even provide powerful, multiuser workflows that remediate out-of-compliance nodes with little required human intervention, which takes the guesswork out of mitigating configuration errors while saving valuable time (and money).

Ease of Use

No matter how powerful and feature-rich an SCM solution may be, if it's too hard to use, reaping the full benefits of your SCM investment may be nearly impossible. It's important to test-drive SCM software before you buy it. Put it through its paces by exploring all the interfaces you need to install, configure, and use the software.

Responsive Customer Support

Selecting an SCM vendor is just as important as selecting an SCM product — if not more important. Be sure to select an SCM vendor that provides responsive customer support. Find an excuse to call the company's technical-support number during the evaluation process. Determine how long it takes to get a human tech-support representative on the line; then gauge how long it takes that representative to solve your problem.

Reach out to the vendor's tech-support team by both phone and e-mail. An acceptable level of service by phone doesn't necessarily mean that you'll have a good experience with e-mail support, and vice versa.

Harden your network's security configurations, reduce risk, and maintain regulatory compliance

Today's IT organizations face two key challenges: minimizing security risks and maintaining compliance with industry and/or government regulations. Fortunately, security configuration management (SCM) helps with both. If you're tasked with securing your network or demonstrating regulatory compliance, this book is for you!

- ***Understanding SCM* — *gain a high-level overview of SCM and its components***
- ***Exploring SCM features* — *review basic and advanced capabilities of modern SCM solutions***
- ***Reducing your attack surface* — *harden your network by aligning system configurations with common IT security frameworks from SANS, NIST, ISO, COBIT, and more***
- ***Complying with regulations* — *maintain regulatory compliance with PCI DSS, HIPAA, NERC, SOX, FISMA, and more***
- ***Getting started* — *obtain best practices for rapidly deploying your SCM solution***
- ***Selecting an SCM solution* — *know what to look for — and what to avoid — when evaluating SCM solutions***

Open the book and find:

- **Depictions of key SCM components**
- **Descriptions of modern SCM features**
- **Lists of regulatory controls satisfied by SCM**
- **Criteria for evaluating SCM products**
- **Real-world examples and tips for deploying SCM**

www.tripwire.com/scm

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Steve Piper is a high-tech marketing and product management veteran with over 20 years of experience. A freelance writer and consultant, Steve is the author of *Network Packet Brokers For Dummies* and *Big Data Security For Dummies*. Steve has achieved a CISSP security certification from ISC^2 and BS and MBA degrees from George Mason University. Learn more at www.stevepiper.com.

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-54516-4
Not for resale