Making Everything Easier!™

BMC Special Edition

SecOps For Dummies®

A Wiley Brand

Learn to:

- Align security and IT operations teams for maximum efficiency
- Optimize multi-cloud security and compliance at scale
- Transform vulnerability management capabilities

Brought to you by

bmc

Rick Bosworth
Lawrence C. Miller

About BMC

BMC is a global leader in innovative software solutions that enable businesses to transform into digital enterprises for the ultimate competitive advantage. BMC's Digital Enterprise Management solutions are designed to make digital business fast, seamless, and optimized from mainframe to mobile to cloud and beyond. BMC digital IT transforms 82 percent of the Fortune 500 and serves more than 10,000 customers worldwide.

SecOps For Dummies

A Wiley Brand

BMC Special Edition

by Rick Bosworth and
Lawrence C. Miller

For Dummies
A Wiley Brand

SecOps For Dummies®, BMC Special Edition

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

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-48219-2 (pbk), ISBN 978-1-119-48223-9 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. Some of the people who helped bring this book to market include the following:

Project Editor: Martin V. Minner

Editorial Manager: Rev Mengle

Senior Acquisitions Editor: Amy Fandrei

Business Development Representative: Molly Daugherty

Production Editor: Siddique Shaik

Table of Contents

Introduction

No company is impervious to cyberattacks. It has famously been noted that there are now two kinds of companies: those that have been hacked and those that don't know they've been hacked. Security threats are a more serious and frequent problem than ever. As hackers demonstrate increasing sophistication, enterprises are bracing for the worst. At a recent Black Hat conference, 72 percent of attendees responding to a survey said it was likely that their organizations would suffer a major data breach in the next 12 months, and 15 percent said they had "no doubt" their organization would suffer a major data breach.

This pessimistic view of the threat environment is consistent with the security worries expressed by many other business executives. Case in point: A whopping 97 percent of the executives polled in a recent BMC *Forbes Insights* survey expected a rise in data breach attempts in the next 12 months. Not only are the security challenges facing IT greater than ever, but the price of failure is also climbing. Since 2013, the total cost of a data breach has increased 29 percent to an average of $4 million per incident. The heightened threat landscape means that enterprises must learn to manage what Gartner describes as an "acceptable" level of digital risk.

There are also new potential points of vulnerability. As organizations migrate data to the cloud, expand their deployment of mobile computing, and embrace the Internet of Things (IoT), security and operations professionals confront threat environments with more potential digital touchpoints to control and protect. Within this greatly expanded attack surface, traditional security and operations approaches are no longer sufficient, as the network "perimeter" now extends well beyond the corporate firewall.

Collaborative workflow processes that eliminate friction and misalignments between the security and operations teams sharply lower the risk of data breaches and operational downtime. Now, more than ever, enterprises can advance their overall business agenda by closing the security and operations gap and minimizing communications breakdowns that leave organizations vulnerable to cyberattacks.

In this book, you learn how SecOps can transform your organization's security and operations teams to enable a more effective enterprise security posture.

About This Book

SecOps For Dummies, BMC Special Edition, consists of six chapters that explore

- The business need for SecOps, fundamentals of SecOps, and key SecOps roles (Chapter 1)
- Important SecOps capabilities (Chapter 2)
- How to evaluate SecOps tools (Chapter 3)
- Preparing for SecOps in your organization (Chapter 4)
- How to transform your organization with SecOps (Chapter 5)
- The truth about common SecOps myths (Chapter 6)

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays.

TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these tips. This icon points out useful nuggets of information.

Chapter 1

An Introduction to SecOps

In This Chapter

- Defining SecOps
- Exploring IT operations and security challenges
- Changing the paradigm with SecOps
- Achieving security and compliance with policies and regulations
- Defining key SecOps roles and responsibilities

In this chapter, you learn about everyday challenges in a traditional siloed IT operations and security model, what SecOps is, the benefits and positive outcomes SecOps enables for a better security and compliance posture, and the roles and responsibilities of key people in the SecOps model.

What Is SecOps?

SecOps is a new paradigm for seamless collaboration between IT Security and IT Operations to more effectively mitigate risk, in much the same way that DevOps established a new way of working between application developers and IT Operations. Where traditional approaches to security and compliance have failed, SecOps deploys new work processes and solutions that enable teams to prioritize and remediate critical vulnerabilities. With SecOps, teams can systematically address compliance violations through an integrated and automated approach across all environments, whether on-premises, hosted, private, public, or multi-cloud.

Recognizing the Need for SecOps

Disruptive technologies such as cloud services and the Internet of Things (IoT) are driving fundamental changes to how organizations achieve their objectives. According to a 2017 study by BMC and Forbes, 69 percent of C-level executives cite *digital transformation* as the number one issue affecting their security strategy. Many of the respondents considered current security and compliance practices to be a barrier to growth. So, what are some of these changes that are causing problems for IT security and operations teams?

First, public cloud use is growing explosively, with an estimated $122 billion spent by enterprises in 2017. Next, the widespread adoption of DevOps has accelerated the release of code to production environments, particularly in the cloud, thus rapidly accelerating an already tenuous software development process. Finally, while cloud and DevOps have taken some focus off the data center, on-premises IT workloads are still projected to more than double from 2015 to 2020, requiring organizations to manage security and compliance for both on-premises and cloud environments.

In the face of these challenges, IT Operations and Security teams must work together, but often have different priorities. Operations teams must ensure business-critical IT systems are always available and performing at a high level. Security teams must ensure these same systems are secure and compliant with various regulatory standards and internal policies. Although both teams have the best interest of the organization in mind, balancing security and system performance requirements is challenging because their goals and priorities often conflict.

TIP

According to a 2017 BMC and Forbes study, 65 percent of respondents reported that they believe security would improve if the security staff collaborated more closely with operations teams.

Additionally, the two teams often use different tools, each optimized to its specific needs. For example, although security teams often acquire tools to detect vulnerabilities, they are rarely authorized to make changes directly to server, network, or cloud resources to address the vulnerabilities. These responsibilities rest with the IT operations team, who must manage performance and availability of business-critical systems. Taking down a system to remediate a security vulnerability must be done with proper planning, approval, testing, execution, and tracking to maintain system integrity.

When the security team runs automated scans of the IT environment for compliance issues, the results are frequently shared with the operations team via massive spreadsheets that can contain thousands of lines of data and lack any context. The discovered vulnerabilities often are not ranked in terms of impact or priority and are often just passed to the operations team with an edict to “get it done,” leaving remediation decisions up to the IT operations team.

IT Operations must then manually identify which systems are affected by the vulnerabilities, which remediation actions must be taken, the relative priority of the vulnerabilities, and the urgency with which they must act. When that assessment is completed, the updates are then tested, ticketed, scheduled against maintenance windows, approved by change boards, and finally implemented.

This process is fragmented, manual, and disjointed. In a report by BMC and Forbes, 60 percent of more than 300 C-level executives who responded to the survey said that security and operations did not understand each other’s requirements.

Competing priorities, disparate tools, poor communication, and lack of visibility conspire to increase friction and inefficiencies that can create gaps in the security posture and leave businesses susceptible to increased risk and cyberattacks — commonly known as the *SecOps gap.*

REMEMBER

Cybersecurity breaches can be costly for organizations, averaging close to $4 million per breach, according to the Ponemon Institute. For those organizations doing business in the European Union (EU), violations of the new General Data Protection Regulation (GDPR) mandate will be subject to penalties of up to €20 million or 4 percent of global annual sales, whichever is greater. Businesses must also consider the impact of lost revenue, customers, and future business.

Security vulnerabilities, non-compliance, and out-of-policy conditions lead to potentially catastrophic consequences and must be corrected. Yet the current siloed model can leave organizations exposed to unnecessary risk. On average, it takes 193 days to remediate a vulnerability after it has been identified, according to WhiteHat Security. Delaying remediation actions can open the door to successful exploits. According to a recent Verizon "Data Breach Investigations Report" (DBIR), half of all vulnerability exploitations occur between 10 and 100 days after a vulnerability is known, with the median around 30 days.

Many organizations are now taking a new management approach to bridge the gap between security and IT operations teams, to ensure that systems meet performance and availability needs, and to stay secure and compliant. Much like DevOps, SecOps is an approach that links security and operations teams together with shared accountability, processes, and tools, to ensure a high level of security and compliance while also meeting business requirements for performance, availability, and agility.

Does slow vulnerability patching make you WannaCry?

On March 14, 2017, Microsoft released security bulletin MS-17-010, which included security patches designed to fix a known vulnerability in the Windows Server Message Block (SMB) protocol. Less than 60 days later, on May 12, 2017, the WannaCry attack began, infecting hundreds of thousands of vulnerable Windows computers in more than 150 countries worldwide.

WannaCry encrypted the data on infected computers, rendering the data useless unless a $300 bitcoin ransom was paid within three days (the ransom doubled to $600 if not paid in seven days), although the decryption key often didn't work, even if the ransom was paid.

Despite having almost two months' "advance notice," many organizations were infected by WannaCry because of ineffective patching processes. Notably, up to 70,000 devices were infected at the National Health Service (NHS) hospitals in England and Scotland, and Nissan Motor Manufacturing UK and Renault both temporarily stopped production. Although the WannaCry perpetrator, now widely believed to be North Korea, only collected a little more than $130,000 from 327 ransom payments, the total economic damage to affected organizations worldwide is estimated at hundreds of millions to as much as $4 billion.

According to a survey conducted by Forrester, 69 percent of respondents predict that improving SecOps will result in fewer security breaches. In the same survey, 49 percent of respondents indicated that improved SecOps would reduce the cost of patching, and 47 percent indicated it would lower the cost of compliance.

Understanding SecOps

The SecOps model aims to improve the security posture of the organization by facilitating better collaboration between Security and IT Operations. The goals are to

- Keep the operations and security teams aligned and operating efficiently
- Provide visibility into changes that must be made to shore up security defenses, as well as the impact of those changes on other parts of the business
- Provide a record of the changes that have been made and the exceptions that have been granted

When these teams don’t have an effective way to transfer and consume information, organizations often struggle to achieve a secure and compliant environment in a cost-effective and efficient way.

Effective SecOps transforms disconnected initiatives into a unified, flexible, and closed-loop process that accelerates and scales vulnerability resolution, prioritizes and mitigates risk, and streamlines change tracking and documentation. These capabilities enable operations and security teams to become more agile and move to a proactive security position, quickly addressing vulnerabilities when they are first known, rather than reacting to exploits after they’ve breached systems and hit the news.

To more effectively close the SecOps gap, organizations need to automate manual steps, streamline the detection to remediation process, and remove vulnerabilities faster. To do this, they need better

- **Vulnerability information:** Security-based vulnerability scanners often identify the server name and associated vulnerabilities. However, IT Operations needs to understand whether the scanner covered all servers in the environment, how those servers relate to business applications or services, what remediations are available, and how critical the vulnerabilities are.
- **Planning analytics:** IT Operations needs to plan remediation actions based on the type of remediation (for example, configuration change, patch, script execution, and so on) while also considering the criticality of the system impacted and the agreed-upon maintenance window of each system.
- **Tools integration:** Whether consuming vulnerability scan data, entering change tickets, or executing remediation actions, removing manual steps is necessary to accelerate actions, improve scalability, and reduce errors.
- **Remediation execution:** Once the vulnerability is known and matched against a remediation action that has been tested and approved, it must be effectively executed. This requires visibility into ongoing remediation actions, automatic error handling, verification of successful changes, and automated rollback when changes cause issues.

SecOps is the seamless collaboration between Security and IT Operations to effectively mitigate risk. There are three imperatives for an effective SecOps strategy:

- **Operational intelligence:** Make security visual and actionable with vulnerability information enriched by context and operational data, such as application or business service, to prioritize vulnerability handling based on the potential impact within your operating environment. Specifically:
  - Identify blind spots so all systems are analyzed.
  - Combine security and operations data for more accurate and actionable analysis.
  - Prioritize and fix the most critical flaws first.

- **Multi-tier remediation:** Drive consistency, scalability, and flexibility with automated remediation that considers the application, the process, and the severity of the issue. Specifically:
  - Automate response to violations.
  - Fit the process to the environment.
  - Use a tiered approach to remediation based on severity and application impact.
- **Continuous security monitoring:** Improve multi-cloud security and compliance while simultaneously enhancing innovation for development teams. Specifically:
  - Automate security assessment for any asset, on-premises or in the cloud.
  - Automate cloud service configuration checks and ongoing monitoring.
  - Manage configurations consistently and with an audit trail.
  - Embed security checks into DevOps pipelines to find code security issues before they are released to production, where the risk and cost are greater.

SecOps enables companies to take a comprehensive and proactive approach to security issues by managing known vulnerabilities, rather than simply reacting to the latest attacks. Organizations can manage by policy and automatically address security issues to protect their businesses. Today, network and systems administrators and IT staff are stretched thin and manual tasks consume key cycles and drive up costs. Automation can help them reduce that burden.

Redefining How We Look at Security and Compliance

The myriad security and privacy regulations and standards today require close collaboration between operations and security teams to ensure continuous compliance. New mandates are frequently being passed and existing ones revised.

Several examples of important security and privacy regulations and standards include:

- **U.S. Health Insurance Portability and Accountability Act (HIPAA),** which protects patient data privacy
- **U.S. Sarbanes-Oxley (SOX) Act,** which prevents fraudulent accounting practices and errors in public corporations and mandates data retention requirements
- **U.S. Federal Information Security Management Act (FISMA),** which requires federal agencies to conduct annual information security program reviews
- **Canada Personal Information Protection and Electronic Documents Act (PIPEDA),** which protects the privacy of personal information for Canadian citizens
- **EU General Data Protection Regulation (GDPR),** which strengthens data protection for EU citizens and addresses the export of personal data outside the EU
- **Payment Card Industry (PCI) Data Security Standards (DSS),** which protects personal data related to credit, debit, and cash card transactions

However, barriers to security and compliance arise from applying a traditional operations and security model to new paradigms and environments, such as DevOps and multi-cloud. For example:

- **Legacy tools and processes do not work with DevOps or multi-cloud environments.** Vulnerability scans cannot keep pace with rapidly changing cloud infrastructure and application environments, penetration testing is immediately outdated in rapidly changing DevOps/continuous delivery (CD) environments, and audit and compliance is too slow and too manual to keep up with the myriad scenarios.
- **Multi-cloud security operations are immature, too often driven by manual effort with limited visibility and without controls.** The security of cloud services often depends on how those services are configured, requiring skills, expertise, and diligence to maintain correct settings.
- **Speed, scale, and complexity of dynamic multi-cloud environments is often beyond human scale.** Manual intervention cannot keep pace and is prone to error.

To nimbly address these compliance barriers while scaling to handle the volume and rate of change in these dynamic environments, SecOps teams need to automate the process for detecting, analyzing, and remediating non-compliance. By combining a policy-based approach, one that consistently applies recommended practices in securely configuring cloud services and resources, with automated remediation, security and compliance across the entire multi-cloud environment are increased and SecOps productivity is raised.

How does SecOps work with DevOps?

The level of competition driven by digital disruption is intense. Coping with the demand for application delivery life cycles measured in seconds — with shrinking resources and increased complexity — requires a new approach. To compete today, leaders are automating application delivery to operationalize their competitive advantage.

Using a DevOps approach, companies can deliver applications faster, at a higher level of quality, and at a lower cost. In fact, a study by McKinsey found that companies that embrace an agile DevOps approach to development, testing, and operations see an 83 percent improvement in time to market, 90 percent faster updates to servers, and a near 50 percent reduction in handoffs per process.

As organizations "shift left" (test early and often in the software development life cycle process) to improve agility, this naturally creates new challenges and exposes different bottlenecks in their DevOps processes. For example, compliance and security remains a manual, ad-hoc activity at the end of a release, which forces tough decisions about risk acceptance versus costly late code fixes. Furthermore, cloud adoption and containerization introduce mode-two (new and innovative) resources into these processes that create real security and compliance gaps that most organizations haven't considered. Without a comprehensive compliance strategy that addresses these issues, organizations will eventually fall behind competitors and increase their risk of data breaches and ransomware.

SecOps helps organizations gain a competitive advantage by increasing agility, while closing security and compliance gaps associated with the latest cloud and container technologies. A comprehensive SecOps program provides a unified view of compliance data collected across data center, cloud, and container resources that is analyzed against flexible predefined policies. Compliance checks can also be embedded directly in DevOps pipelines for instant feedback regarding go and no-go decisions in the process.

Understanding SecOps Roles and Responsibilities

Within a SecOps organization, key traditional roles still exist, but work more collaboratively to achieve the business and security goals of the organization. These roles include:

- **Security:** In a SecOps model, much like in a traditional model, the security team identifies and prioritizes vulnerabilities that must be remediated. However, unlike a traditional model, in which Security hands off these tasks to IT Operations, Security is fully involved during implementation, and is accountable for helping the operations team to understand the risk of the vulnerabilities at the time of discovery as well as if new information, such as an exploit in the wild, requires reprioritization or a change in tactics.
- **Operations:** IT Operations works closely with Security to remediate vulnerabilities in a timely manner, regardless of whether it is a server, application, network, or cloud service vulnerability. They also communicate business requirements for uptime and availability, the change process, and maintenance windows, so that expectations are aligned.
- **Development:** App developers partner with the SecOps team to understand and address security requirements early in the software development life cycle (SDLC). Within a secure DevOps process, developers address security and compliance requirements in the continuous integration (CI) and continuous delivery (CD) DevOps models. Whereas DevOps deploys "infrastructure as code," SecOps requires "secure infrastructure as code." In a secure SDLC, developers know how to write secure code and deploy it securely.
- **Compliance and legal:** These organizations work closely with SecOps teams to ensure automated policies and auditing tools satisfy changing legal and regulatory requirements.
- **Business stakeholders:** Line of business managers and corporate executives increasingly understand the critical nature of security and compliance, and the need to promote "top-down" support for proactive SecOps.

Chapter 2

Exploring SecOps Capabilities

In This Chapter

- Improving vulnerability management in your organization
- Using shared visibility and analytics to align security to business needs
- Managing compliance across all multi-cloud environments
- Embedding security in software development

This chapter explores SecOps capabilities, including vulnerability and patch management, alignment of security activities to the needs of the business stakeholders, multi-cloud security and compliance, and improving the security of new applications.

Optimizing Vulnerability Management

A steady increase in the number of vulnerabilities each year has put a fresh focus on the importance of vulnerability management. Although the 2016 Verizon "Data Breach Investigations Report" (DBIR) found that the top ten vulnerabilities made up 85 percent of successful exploits, the remaining 15 percent were attributed to more than 900 common vulnerabilities and exposures (CVEs). Although this might seem to support focusing on the highest priority vulnerabilities — assuming you know what those are — such a strategy leaves organizations at risk, and often in a reactive, "fire-drill" mode, responding to any of the other 900 vulnerabilities in an ad-hoc, point-shoot-aim manner. Moreover, more than 80 percent of attacks focus on already known vulnerabilities, whose average age is well over a year.

Despite all the talk about zero-day attacks, this type of undisclosed vulnerability and subsequent exploits make up a small percentage of the vulnerabilities being exploited today. This realization is becoming evident in enterprise security spending. In the recent Forbes Insights security survey, 60 percent of the 300 C-level respondents said that "expanded vulnerability discovery and remediation" was a primary initiative. In contrast, only 30 percent of the respondents made putting more resources into defending against zero-day exploits a primary initiative — a logical response given that most exploits are still targeting known vulnerabilities.

Thousands of CVEs continue to be discovered each year. With each vulnerability taking 193 days on average to remediate, security and operations teams need a better way of working — not more bodies to throw at the problem. They need new capabilities that help them

- **Understand the severity of the vulnerabilities,** which can be represented by the Center for Internet Security (CIS) severity score, vendor-based scoring systems, or even internal assessments
- **Know whether the vulnerability has previously been exploited or not,** because previous exploits are much more likely to be exploited again
- **Gain visibility into where the organization is exposed —** that is, how many vulnerable systems there are in the environment
- **Visualize how critical business systems are affected by the vulnerabilities,** to help set timing or the order of remediation activities
- **Automate remediation through patching or configuration change,** including ticketing, approval, scheduling, and validation

Armed with this understanding and capability, the SecOps team can shrink the time to remediate, and more closely align IT security to the needs of the business.

Aligning to the Needs of the Business

Integrated SecOps solutions that leverage automation and deep analytics quickly identify, prioritize, and remediate security exposures. Software as a Service (SaaS)-based and on-premises products are available that detect, analyze, and prioritize the remediation of vulnerabilities. These solutions use data from vulnerability scanners, map IT assets to the weaknesses found, develop action plans for their remediation, and track resolution status and burn-down rates. Provisioning and patching offerings integrate with these solutions to deliver a policy-based approach for managing servers using advanced analytics and automation to provide rapid, high-quality, and consistent deployments of security patches, along with new features and applications. They often include out-of-the-box content that supports the automation of compliance checks and remediation to ensure adherence with regulatory requirements and internal policies.

As described in Chapter 1, the old paradigm, in which IT Operations and Security work in silos, is disjointed and wrought with inefficiency. By comparison, in a mature SecOps organizational model, the security and operations teams are jointly accountable to the business stakeholders for assuring security and compliance. Security identifies vulnerabilities and partners with the operations team to ensure the vulnerabilities are resolved. Operations then creates remediation packages and schedules deployment. The mature SecOps team operates under service-level agreements (SLAs) for each of these stages — identification/prioritization, remediation package creation, and deployment/execution. Working together, these teams prioritize vulnerabilities, create remediation plans, and ultimately implement them. Ideally, highly specialized tools, such as vulnerability scanners and asset discovery, integrate within a common SecOps platform to holistically visualize the security and compliance posture, apply context specific to the organization's unique IT environment, and facilitate risk assessment, planning, and remediation. In so doing, the SecOps teams work from a common understanding of risks and priorities, and more efficiently use available resources.

TIP

Use of SecOps tooling which readily integrates with existing IT tools increases the team's efficiency, delivering maximum value back to the business stakeholders.

Maintaining Multi-Cloud Visibility and Consistency

Public cloud adoption and usage provide well-known benefits, such as flexibility and cost savings, and have become key components of digital transformation. For many companies, multi-cloud environments, those that consist of multiple cloud service providers (CSPs), can yield additional service offerings, optimized cloud cost/performance options, and greater flexibility. Similarly, containerization (for example, Docker and the Open Container Initiative) is helping businesses compete by driving digital services with simpler and faster configurations and more rapid deployments. Although these cloud and container technologies provide for digital disruption, the increased speed and business agility they provide heighten the need for consistent, secure provisioning and configuration.

CSPs often introduce new services, resources, and objects that could create security and compliance issues if improperly managed. For example, Amazon Web Services (AWS) accounts contain valuable services that must be configured consistently and securely to conform to industry, regulatory, and organizational standards. These include

- ElasticSearch
- Identity and Access Management (IAM) credentials
- Password policy
- Relational Database Service (RDS)
- Simple Storage Service (S3) buckets
- Security groups
- Key Management Services (KMS)
- CloudTrail

Containers and container hosts also pose security risks if improperly configured. If misconfigured, seemingly secure containers can have openings for unintended access. To properly ensure security and compliance, container environments should be checked at three levels:

- Host configuration
- Daemon configuration
- Images

As organizations begin leveraging multi-cloud services and new container technologies, new attack surfaces are introduced that are outside the view of typical server and network compliance tools. These new attack surfaces are making news as more data breaches exploit them. Some of the cloud and container vendors offer security solutions that work only with their service, creating islands of visibility that lack a holistic view to help manage the broad risks to organizations. Security teams need vendor-agnostic solutions that work seamlessly across on-premises and multi-cloud environments, regardless of the location or provider.

REMEMBER

Cloud services and containers are dynamic and often short-lived, breaking the traditional compliance model. Organizations need a comprehensive compliance coverage strategy that encompasses on-premises and multi-cloud or container resources to fully manage their security risk.

Developing Secure Applications

The level of competition driven by digital disruption is intense. Coping with the demand for application delivery life cycles measured in seconds — with shrinking resources and increased complexity — requires a new approach. To compete today, IT leaders are automating application delivery to operationalize their competitive advantage. For example, by using a DevOps approach, companies can deliver applications faster, at a higher level of quality, and at a lower cost. In fact, a study by McKinsey found that companies that embrace an agile DevOps approach to development, testing, and operations see an 83 percent improvement in time to market, 90 percent faster updates to servers, and a near 50 percent reduction in handoffs per process.

Surveys show that agile DevOps methods are increasingly the answer for organizations to quickly deliver products and services to meet customer demands while outpacing the competition. The problem resulting from this adoption is that as most of the software development life cycle (SDLC) process becomes more efficient, other processes are exposed as bottlenecks. This is especially true for compliance and security because they often remain manual, ad-hoc activities at the end of a release. According to Gartner, by 2020, 60 percent of digital businesses will suffer major service failures because of the inability of the IT security team to manage risk in new technology and use cases.

One major issue is that security scans that are run late in the SDLC — usually right before production code release — routinely find unexpected problems, resulting in costly rework and delays. Vulnerabilities can be introduced into software by code changes or by using third-party libraries. Even libraries that were previously deemed to be "clean" can still have new risks identified after release to production; such was the case with XStream library, which led to the Apache Struts vulnerability at Equifax in 2017. Finding a means of testing code security earlier in the development process not only reduces the cost of rework, but also the number of security issues released to production. This should be done in a way that minimizes the impact on developers, allowing them to utilize their DevOps tools and processes to automatically trigger security checks at critical gateways. With quick feedback, developers can find and fix vulnerabilities before they become entangled in the software and require more extensive rework.

REMEMBER

To implement *secure* continuous innovation and delivery in application development, organizations must have a vigilant security scanning capability embedded within their DevOps process. Testing earlier reduces cost and minimizes delays.

Accelerating migration to the cloud with SecOps

As IT leaders strive to meet the demands of the business, they are facing several new realities. They are prioritizing their cloud adoption strategies, with IDC estimating $122 billion spent on public cloud in 2017. IT leaders are also embracing new trends like DevOps, with 84 percent of enterprises adopting DevOps in 2017. Traditional data centers continue to be the workhorse, with workloads expected to grow 2.6x from 2015 to 2020, per Cisco's Global Cloud Index. Organizations need to balance supporting growth in the traditional data center while accelerating their adoption of public cloud infrastructure and DevOps processes.

Many organizations are turning to the cloud but quickly find that traditional approaches and tools fail with DevOps and multi-cloud environments. Cloud security operations tools are immature and heavily dependent on manual steps. Using one set of approaches and tools for cloud and one for traditional data centers leaves organizations in a position where they have a proliferation of security tools, which is costly. They also lack visibility and cannot consistently enforce and ensure security and compliance. Furthermore, the speed, scale, and complexity have gone far beyond human scale.

Organizations can accelerate their cloud migration strategy with a robust SecOps solution that can deliver the following capabilities and benefits:

- **Continuous security monitoring:** Ensure cloud security and compliance keeps pace with the growth of cloud services usage through regularly scheduled policy-based scans of cloud configurations, as well as automated remediation to restore compliance.
- **Cloud and on-premises data connectors:** Simplify connections to the clouds and technologies in your environments with prebuilt connectors or templates.
- **Flexible policies:** Extensive out of the box (OOTB) policies speed your time-to-value and should be easily customizable to suit security and compliance requirements specific to your organization.
- **Embed security and compliance in DevOps:** Policy-based testing for application component vulnerabilities should be run early and often during software development to find issues sooner, reduce rework costs, and improve software security before it is released to production.

Chapter 3

Evaluating SecOps Tools

In This Chapter

- Recognizing the importance of seamless integration
- Addressing the need to prioritize security vulnerabilities
- Accelerating remediation with automation
- Ensuring scalability and flexibility
- Maintaining a secure and compliant enterprise environment

When evaluating tools for your SecOps journey, you naturally think of common use cases such as vulnerability management and configuration management. Equally important considerations, however, include how readily SecOps tools connect to your existing tools, increase efficiency, provide scale, and manage security and compliance both on-premises and in the cloud. These critical capabilities are the focus of this chapter.

Integrations across the Tool Chain

The first evaluation criterion of a SecOps tool should be how it fits into your organization's overall security and compliance strategy and processes. The security and operations teams often use different tools for different environments — on-premises and multi-cloud — and different purposes, such as performance monitoring, vulnerability scanning, server automation, ticketing, and troubleshooting. To be effective, a SecOps tool should take input from a variety of sources, synthesize results, and present visualizations that can be readily tuned to meet the needs of both Security and IT Operations.

Ask if the SecOps tool you are considering uses open standards-based application programming interfaces (APIs) to integrate with a wide range of IT tools.

Many enterprises have already purchased or deployed a scanning tool (such as those available from Qualys, Tenable, or Rapid7) to help them understand the vulnerabilities that exist across their environment. However, these tools often generate huge lists of raw vulnerabilities that must be sorted, parsed, and analyzed to determine priorities, ownership, and/or the proper remediation. This can become a colossal manual task that causes enterprises to struggle to keep pace with the volume and velocity of new vulnerabilities.

However, organizations can accelerate this task with tools that take raw vulnerability scanner inputs and enrich them with data from other sources to provide better context for decision-making or identifying additional risks. For example, this data can be enriched with the output from application dependency discovery tools to help provide operational context, such as which applications or business services run on which servers and network devices, or to identify blind spots — servers and network devices that are not visible to the vulnerability scanner and are therefore not scanned. This data can also be enriched to provide security context, such as which vulnerabilities are more severe or have been previously exploited. This operational intelligence makes security analysis faster, more accurate, actionable, and proactive to help organizations better manage and mitigate risk.

Prioritizing Remediation

Because of the sheer volume of vulnerabilities, the need to keep business services up and running, and the labor cost of remediation activities, eradicating all vulnerabilities is often an impractical goal. Organizations need to appropriately and efficiently prioritize vulnerabilities to isolate those that have the greatest impact and deploy resources in the most effective manner possible.

Vulnerability knowledge bases and scanning tools enable you to sort security issues by severity, but richer operational and security context is needed to prioritize action. Asset discovery and dependency mapping both augment the vulnerability management process by providing

- **Insight into how applications are deployed and protected:** For example, it might not matter as much that a web server is vulnerable to certain attacks if it is sufficiently protected by a web application firewall.
- **Business context to infrastructure components:** For example, adjust the priorities based on the business impact that would result from loss of data or disruption of services.
- **Vulnerability information:** For example, identify which vulnerabilities have been previously exploited in the wild and therefore are more likely to be exploited again.

Automating Remediation

IT operations staff typically live in a dual state — a proactive state of maintaining system availability or making configuration changes to support business initiatives and a reactive state of fixing performance issues or patching when a security vulnerability is identified. To be proactive in both states, the resolution of security vulnerabilities must be accelerated, so that both patching and configuration changes can be completed during planned maintenance windows.

To accelerate the patching and configuration remediation process, organizations need tools that help them match the proper remediation task with the vulnerability on the specific version of the operating system affected. As an example, when the WannaCry ransomware worm was released, the fix had 38 potential patches, depending on which operating system (OS) configuration was running. Matching the correct patch or remediation action to the specific OS variant can significantly accelerate patching.

Documenting changes — including creating change requests, submitting change tickets, obtaining approval, and then closing tickets after verification of a successful change — can take, on average, more than 40 minutes per change. Multiplying this documentation effort by hundreds of patching jobs reveals a huge opportunity for saving time and resources through automation. Look for tools that automate this process by integrating with change management tracking tools that help streamline the change process.

REMEMBER

Cybersecurity talent is scarce and, according to the U.S. Bureau of Labor Statistics (BLS), is projected to remain so for years to come. The thousands of new vulnerabilities identified each year underscore what you probably already know: You cannot solve IT security and compliance issues by throwing more bodies at it. The environment is changing too quickly, and the old way of working is too inefficient. These challenges are further exacerbated in the cloud, where resources are even more quickly provisioned and deployed. Automation reduces the dependency on scarce and expensive talent, freeing your existing staff to take on higher-value tasks.

Effective SecOps tools automate remediation, either through configuration or patching, to shorten the vulnerability time window, reduce the number of errors from manual intervention, document changes, and increase IT productivity.

Scalability and Flexibility

SecOps tools must be able to massively scale to support both enterprise on-premises and multi-cloud environments. Even for small organizations, cloud resources can quickly grow to number in the thousands. For enterprise environments, the need for scalability and flexibility is even greater. To manage tens of thousands of on-premises and cloud resources across multiple geographic locations — potentially around the world — these organizations need tools that not only scale, but also enable flexible and granular role-based management capabilities.

Scale and flexibility necessarily imply that SecOps tools should also be able to connect to a multitude of data feeds, spanning on-premises and multi-cloud environments.

Security and Compliance

Digital initiatives are forcing enterprises to conduct business in new ways, leveraging new technologies and services that have the potential to expose new and unique security and compliance challenges. Failure to understand cloud security can result in improperly applied configurations that expose critical data and applications. Failure to adequately enforce and comply with these complex regulatory standards can result in hefty fines, negative publicity, and worse.

According to Cisco's 2017 *Annual Cybersecurity Report,* 33 percent of breached organizations reported lost revenue and opportunities of more than 20 percent, and 40 percent of breached companies lost more than 20 percent of their customers, setting the stage for future revenue volatility. How readily could your company handle a loss of 20 percent of your customers and revenue? How long, and at what cost, would it take to plug that top-line hole and repair the damage to trust, brand reputation, and — for public entities — stock price?

When evaluating SecOps tools, it's important to determine whether they will help you comply, across all your environments, with relevant internal and regulatory compliance mandates, such as

- Payment Card Industry Data Security Standard (PCI DSS)
- U.S. Health Insurance Portability and Accountability Act (HIPAA)
- U.S. Sarbanes-Oxley Act (SOX)
- Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU General Data Protection Regulation (GDPR)

TIP

For those organizations doing business in the European Union (EU), violations of the new General Data Protection Regulation (GDPR) mandate will be subject to penalties of up to €20 million or 4 percent of global annual sales, whichever is greater. Even if your organization doesn't currently do business in the EU, GDPR compliance is still worth paying attention to because it reinforces good business practices for data protection and privacy — and you'll be ready when your business announces it's expanding operations to Europe!

New ways of working driven by digital transformation also pressure security and compliance efforts. As organizations embrace DevOps to more nimbly respond to increasingly competitive markets, it is important to select SecOps tools that do not create bottlenecks in the DevOps processes. SecOps tools should readily integrate with continuous integration (CI) tools (like Jenkins, TeamCity, Bamboo, and Codeship) to provide seamless security gates at multiple phases of the software build and test process, to release code with fewer vulnerabilities and without delay.

Cloud and containerization adoption also introduces "mode-two" (new and innovative) resources into these processes, creating new security and compliance gaps that many organizations have not considered. In smaller environments, these gaps can often be addressed by a few subject matter experts. However, as cloud and container usage quickly grows in an organization, this approach becomes unsustainable. SecOps tools must therefore supplement the organization's skills, allowing subject matter experts to focus on policies that can be applied programmatically and frequently to better manage the associated risk in these technologies.

The pace of change required by digital transformation also makes asset inventory data challenging to accurately collect and maintain. Enterprises are increasingly adopting a multi-cloud strategy to use services optimally suited to a specific business need. There are many benefits to establishing good discovery practices, including identifying integrations with virtualization or cloud APIs, as well as identifying previously unknown use application and server usage, commonly referred to as "shadow IT."

Finally, as if regulatory compliance mandates weren't enough, companies also have their own internal policies and governance requirements. Security and compliance tooling should allow organizations to customize and extend out-of-the-box policies to suit requirements unique to their business.

REMEMBER

Balancing IT performance and availability with security and compliance mandates can be a Herculean challenge. The combination of public and private clouds, multiple cloud service providers and accounts, new technologies, and new ways of working brought on by digital transformation exacerbate complexity. SecOps tools can enable organizations to thrive despite these challenges and not only enhance productivity, agility, and security, but also create a sustainable competitive advantage.

Chapter 4

Ready, Set, Go: Getting Started with SecOps

In This Chapter

- Creating a SecOps vision
- Determining your organization's capability maturity level
- Planning to succeed
- Defining success
- Evolving SecOps toward a competitive advantage

In this chapter, you take the first steps toward implementing SecOps, including creating your vision, assessing your organization's current capability level in key areas, building an execution plan, and defining success criteria.

Building Your Vision

First, you need a clear vision of where you want to go. Acknowledge the current pains in the traditional security and operations silos. Work toward building a "win-win" SecOps culture in which security, operations, and development work together as a unified team to achieve the same objectives. Foster a culture in which security is a part of the everyday work of development, transforming the software development life cycle (SDLC) into a secure SDLC. The entire IT organization will change from being reactive to proactive by applying operational intelligence and analytics to vulnerability management, continuously monitoring security and compliance, and seamlessly aligning to the needs of the business.

Assessing SecOps Maturity in Key Capabilities

Increasing SecOps maturity can help enterprises address rising security challenges in their multi-cloud and on-premises environments. However, SecOps maturity is not just about identifying and patching vulnerabilities. It also includes:

- Policies and procedures
- Regulatory compliance
- Maintaining a secure operating environment
- Writing secure code
- Effective incident response
- Blind spot detection
- Change management

Assessing your organization's maturity in these key capabilities will help you identify gaps between your security, operations, and development teams. One way to begin this capability assessment is by bringing the relevant stakeholders together to discuss challenges from each of their perspectives. Cross-organizational value stream mapping is useful in uncovering opportunities for process improvement. When each of the teams understands what the others are doing and why, and how the pieces fit together, they can often find creative solutions that streamline the entire SecOps system instead of focusing on siloed optimizations.

A recent Forrester Research study found that enterprises have varying SecOps maturity:

- Four percent of enterprises have no distinct security operations programs.
- Eighteen percent of enterprises have ad hoc security processes, primarily reacting to industry news about emerging threats as they arise.
- Twenty-two percent of enterprises have security operations capabilities and common practices that are employed on occasion.
- Only 5 percent of enterprises have an optimized SecOps approach.

Cross-organizational value stream mapping

Value stream mapping is a method to help organizations visualize and improve key processes, among other things.

There are many approaches to value stream mapping, but at a basic level, organizations can begin by mapping their core processes for core business functions. This process map should be "horizontal," depicting the entire process (for example, to deliver a product or service to the customer from start to finish) regardless of which departments perform any given steps. The map should not be "vertical," depicting siloed operations within individual departments. This technique provides you with an "as is" current-state view of your value stream.

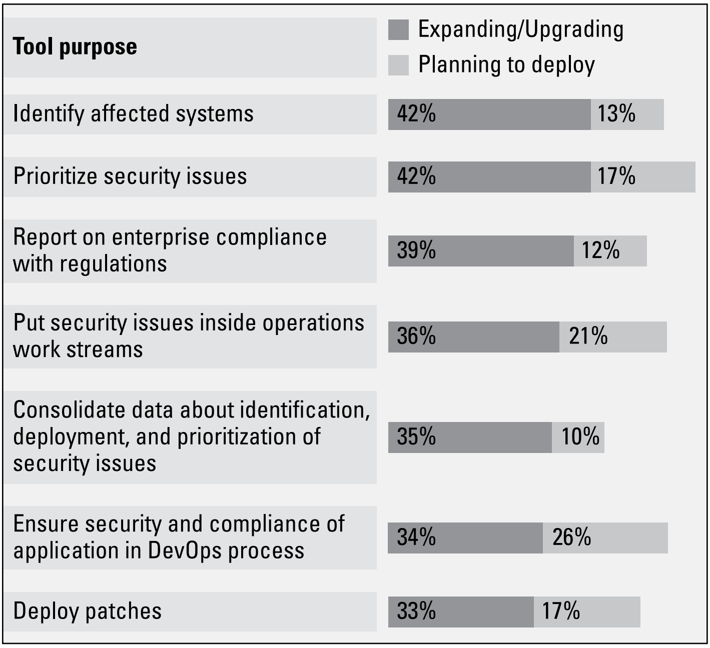
Next, you can analyze your current state for inefficiencies and identify opportunities for improvement. For example, there may be identical steps in the value stream that are performed unnecessarily by several departments, or it might make sense for a given step to occur earlier or later in the process, or to be eliminated altogether. This analysis becomes the "to be" future-state vision for your value stream.

Finally, develop and implement a plan to get you from where you are today (your "as is" current state) to where you want to be (your "to be" future state).

As a result, enterprises struggle to keep up with evolving security operations and compliance requirements. According to Forrester Research:

- Sixty percent of enterprises lack proper staffing.
- Fifty-five percent of enterprises can't keep up with regulations.
- Fifty-four percent of enterprises report day-to-day activities take up too much time.
- Forty-nine percent of enterprises experience challenges preventing an effective security posture.

Further complicating security operations, enterprises deploy multiple tools to identify and prioritize vulnerabilities and manage compliance, which increases procurement, training, maintenance costs, and complexity (see Figure 4-1).



Source: Forrester Research

Figure 4-1: Enterprises deploy multiple tools to identify and prioritize vulnerabilities and manage compliance.

Creating a Plan of Action

Now that you know where you're going as an organization (you have built your vision) and where you are (assessing your current maturity), you can develop a plan of action — your road map — to help you get from where you are today to where you're going.

Your action plan must be ambitious, but also realistic. Transformation doesn't happen overnight. Ensure you have executive support that is reinforced at all levels of the organization, which is imperative to driving a lasting organizational SecOps transformation. Executive sponsorship must begin where Security and Operations meet — for example, the chief information officer (CIO) or chief executive officer (CEO) — and flow across the organization from there. After all, if a major breach happens, it'll be that executive's neck on the line. Address any skills gaps with training or new team members, as appropriate. Include any new tools, training, head count, and other needs in your budget. Communicate your plan to the entire team and confirm that everyone understands their responsibilities. Finally, expect challenges at different phases throughout the implementation and be flexible.

Defining Success

How do you know when you've reached your goal? You have to define success metrics, of course!

Defining metrics will help you benchmark your progress toward your vision. Key performance indicators (KPIs) might include

- Number of vulnerabilities patched
- Number of critical vulnerabilities patched
- Remediation service-level agreements (SLAs)
- Percent of assets scanned and addressed
- Vulnerability aging
- Business-critical system evaluations

You should also define KPIs for individual team members, such as achieving relevant certifications, proficiency with SecOps tools and processes, teamwork, efficiency, and so on.

Iteratively Evolve

Just as the Agile framework transformed software development and set the stage for DevOps, so too can Agile principles be applied to develop your SecOps capabilities. At their core, Agile practices are iterative — based upon a design, build, test, measure, and learn methodology. As Agile teams form, they hone their skills and apply learnings to continuously improve. This can also be true of your SecOps organization.

This book emphasizes the need to prioritize security activity that minimizes risk and maximizes value to the business. Security and IT Operations need to take a structured approach to planning patches over the next two-week sprint. They can use SecOps tools' dashboards to visually communicate the security and compliance posture, monitor KPIs, and inform future activity. The team can conduct periodic reviews to identify learnings and apply them to the next iteration to support continuous improvement. Such an iterative approach fosters teamwork, shared learnings, and SecOps agility. When properly implemented, SecOps can be a competitive advantage.

Avoiding common pitfalls

Here are a few common pitfalls to avoid as you build your SecOps team:

- **Insufficient training:** SecOps isn't just about combining two teams and expecting a different result. Team members must be cross-trained and measured to ensure mutual understanding of their viewpoints and bring about a cultural change.
- **Patching without testing:** Software patches aren't always stable and can conflict with deployed hardware or software. Ensure patches are properly tested in development and QA, then promoted to staging and production environments.
- **Skipping change management:** Change request tickets must be created for patches just like any other change in the environment to ensure proper planning, testing, internal and customer communications, scheduling, and contingency or back-out plans. Once a change is successfully implemented, it should be documented in your configuration management database (CMDB).
- **Human-based checks:** People get reassigned, get distracted by other tasks, or simply can't scale to meet security needs in growing environments. Implement security policy templates that can be applied against rapidly changing services and resources to test for non-compliance in the environment.

Chapter 5

Making the SecOps Transformation

In This Chapter

- Assembling the SecOps team
- Setting automation criteria and priorities
- Determining which processes to automate
- Demonstrating a return on investment (ROI)

This chapter explores SecOps team considerations, including determining how to prioritize your team efforts, set goals, decide what to automate, and calculate the SecOps return on investment (ROI).

Putting Together the Team

To create a high performing SecOps team, you need to answer several questions:

- **Who should be on the team?** You should assemble a small team of five to nine people spanning both IT Security and IT Operations. Teams that grow too large are inefficient. If the team is charged with securing a hybrid cloud environment, ensure that both Security and Operations have representatives with expertise in cloud and on-premises environments. Consider bringing in an application development manager as the SecOps team gains momentum.

- **How should the team work together?** The team should conduct brief, daily stand-up meetings of no more than 15 minutes in length, ideally at the same time and in the same location each day. All team members should briefly summarize what they accomplished the previous day to help achieve the team's short-term objectives, what they will accomplish today, and what assistance they may need from other team members. A moderator who is experienced in Agile methodologies can help facilitate this process.
- **What should the team report, and to whom?** Select an executive sponsor to whom the team reports results and who can clear obstacles as needed. The sponsor should not attend daily stand-up meetings or otherwise influence the team's day-to-day activities. The most effective teams are self-organizing and accountable for delivering results.

Choosing Your Targets (Wisely)

The old, siloed approach to vulnerability management is inefficient and breeds dysfunction instead of teamwork. Throwing scan reports over the wall to IT Operations does not make the organization more secure. True, effective change requires more than simply bringing security and operations together. To be effective, SecOps teams must work together with shared tooling that enriches raw vulnerability scan data with operational context (for example, which applications and business services are dependent on which IT assets, which applications are mission-critical, and so on). This technique makes security analysis accurate, actionable, and tuned to your specific IT environments.

Using a risk-based approach to vulnerability assessment, SecOps teams can focus their efforts on the vulnerabilities that are not only the most likely to be exploited in their environment, but also represent the greatest risk to the business. By analyzing the vulnerability backlog, mapping each to known remediations, and cross-referencing against IT asset discovery scans, the team can break an overwhelming challenge into more manageable tasks that systematically address the highest outstanding risks to the business. The team can apply a similar approach for planning security and compliance across multi-cloud environments.

In planning and prioritizing vulnerability and compliance management activities, the SecOps team should

- Assess the current, overall, multi-cloud security and compliance posture.
- Identify which applications and services are most critical to line-of-business owners, and why.
- Cross-reference asset discovery scans, vulnerability scans, and application topology maps to reveal risks and IT assets that touch multiple key applications and business services.
- Filter and/or sort vulnerabilities by severity, age, asset domain, and/or cloud service provider.
- Compare vulnerability scan logs and asset discovery maps to reveal blind spots.
- Regularly check for new zero-days alerts, or new exploits of existing vulnerabilities.
- Determine whether existing policies conform to the regulatory context of your business/industry.
- Develop custom policies suited for the specific needs of your organization.
- Identify any new cloud security risks (such as those resulting from resource configuration or code vulnerabilities) released to production.
- Measure software development teams' relative performance (for example, the number of security risks and non-compliance problems) and identify opportunities for shared learning.

With these considerations, the SecOps team will go a long way toward reducing the security backlog. As time goes by, the team may decide to customize the criteria, iteratively updating them to suit the organization's context.

Deciding What to Automate

Numerous factors combine to complicate multi-cloud security and compliance management. This complexity, combined with the speed and scale of cloud service deployments, outstrips the human ability to keep pace. Automation serves as a countermeasure to such challenges. For automation to create the most value, the team should first focus on process capability assessment and improvement (discussed in Chapter 4). By developing a common, cross-functional understanding of the entire process, bottlenecks can be identified and opportunities for improvement revealed. Once the SecOps process is fully understood and optimized, the team can leverage automation to improve the security and compliance of on-premises and multi-cloud environments.

Even so, some enterprises may choose guided security and compliance remediation as a first step on their journey to embracing automation. Guided remediation is a sequence of remediation instructions to be followed manually. Although still manual (and therefore, not scalable), guided remediation can raise organizational comfort with the remediation process itself. Another example where organizations may be reluctant to automate is an unstable system with applications running on outdated hardware.

REMEMBER

The SecOps team is accountable for the security posture of the enterprise and should make decisions about how it achieves that objective, iteratively improving along the way. Understand, optimize, and automate the process. Your choice of SecOps tools should support this methodology.

Agency reduces the attack surface with BMC SecOps

A U.S. state government agency is well along in its digital transformation, particularly in the area of citizen services. The state delivers centralized IT services to 18 internal agencies and supports 300 online services for its 10 million citizens. The agency needed a next-generation infrastructure to enable faster response to service requests, enhanced operational and regulatory compliance, strengthened security, and streamlined audits across its diverse IT infrastructure.

As a central component of its digital transformation strategy, the agency implemented BMC's BladeLogic Server Automation to automate the management, control, and enforcement of server configuration changes in the data center. With BladeLogic, the agency is accelerating server provisioning to speed fulfillment and ensuring operational consistency to create a more stable and secure environment. Detailed reporting identifies servers that need security patches, enabling more robust security and continuous compliance with regulatory and industry requirements. Capabilities and benefits of the solution include:

- **Patching:** Supports and follows maintenance window guidelines to ensure timely delivery of patches.
- **Remediation:** Links vulnerabilities to identified patches and creates a remediation plan through BMC SecOps Response Service.
- **Compliance:** Integrates role-based access control, pre-configured policies for Center of Internet Security (CIS), Defense Information System Agency (DISA), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Sarbanes-Oxley (SOX), National Institute of Standards and Technology (NIST), and Security Content Automation Protocol (SCAP), documentation, and remediation.
- **Blind spot awareness:** Identifies the areas of the infrastructure that are not being scanned for vulnerabilities, so that they can be scanned or managed.
- **Powerful dashboards:** BMC SecOps Response Service provides security and operations teams unprecedented visibility into their environments' threat stature for efficient remediation of risks. Visualize planned operations actions, predictive service-level agreements (SLAs), and burndowns. Focus actions on the highest priority items and highlight areas of concern for the business stakeholders.

Delivering ROI

For enterprises that have implemented a mature SecOps program in their organizations, SecOps has direct benefits. The top benefits, according to Forrester Research, are

- Fewer security breaches
- Fewer security distractions
- Decreased cost of patching and compliance
- Improved efficiency between operations and development teams

A mature SecOps organization that embeds security and compliance into DevOps release pipelines releases higher quality code, which introduces fewer vulnerabilities into production. This results in fewer production security "fire drills" to drag developers into emergency remediation. Such distractions come at the expense of product innovation. Therefore, fewer interruptions translates into better DevOps efficiency, greater velocity, faster time-to-market, and potentially more innovation.

Improved SecOps maturity also drives clear business benefits, including

- Fewer security vulnerabilities
- Better collaboration between IT security and operations
- Greater ability to mitigate risk
- Faster remediation

Security process optimization and automation sets the stage for faster remediation and greater agility. A well-oiled SecOps team applies operational intelligence to find and fix the most critical risks first. A multi-tier remediation approach, one that factors severity and impact to applications, addresses maximum risk for the given level of effort.

The resulting productivity enhancements from optimization and automation can help to offset the cybersecurity talent shortage. According to the U.S. Bureau of Labor Statistics (BLS), this talent gap is expected to persist through 2021. Such productivity gains are a definitive component of the ROI equation.

SecOps improves productivity, risk management, and DevOps agility. Shorter vulnerability windows and diminished attack surfaces improve the overall security and compliance posture for on-premises and multi-cloud environments alike. Implemented well, SecOps can translate into a sustainable competitive advantage.

Chapter 6

Ten SecOps Alternative Facts — Debunked

In This Chapter

- Getting buy-in from team members
- Supporting mixed environments at scale
- Developing your staff with cross training and mentoring
- Delivering maximum return-on-investment

This chapter gives you information to overcome objections or misperceptions about SecOps in your organization.

It Won't Work at My Company

There's no magic in SecOps. To work effectively, it requires a culture based on

- Communication
- Shared goals
- Collaboration

Most organizations would agree that these are key components of their success in virtually every endeavor. Once you build the right culture, defining, integrating, and automating your processes with the right technology is the easy part.

It Isn't a Silver Bullet

True, but there are no silver bullets. Building a SecOps culture requires buy-in from the top down to promote a collaborative team that has traditionally functioned in isolated silos. Too often, IT Operations and Security are isolated from one another, and do not have clear lines of communication, with insight into the results and value delivered by the other team. Because of this isolated approach to overall security, attackers can take the path of least resistance and exploit vulnerabilities that have existed for months or years.

Gaps that exist between the operations and security teams include

- Lack of process integration
- Lack of automation to quickly implement recommended patches
- Lack of common measurements that both teams are responsible for delivering
- Lack of common priorities shared by both teams (for example, governance versus stability and uptime)
- Lack of visibility by IT Operations to the pipeline of planned patches
- Lack of visibility by Security to actions that will make systems and applications more reliable
- Poor handoffs between Security and IT Operations on context and vulnerability information
- Lack of understanding between Security and IT Operations on initiatives and the requirements of each team
- Lack of coordinated efforts to create a path to operationalize security

While both Security and IT Operations perform discrete functions as they relate to systems and software, by working together to achieve an effective and sustainable SecOps process, they can address some of these gaps, and improve the security posture of the organization to protect sensitive data and assets. Each team must retain independence but work toward operationalizing security for the business. The call for both teams to work together and eliminate the persistent gap is not an option. It is a necessity.

It Isn't My Responsibility

Not long ago, cybersecurity was the exclusive purview of the IT department. That's no longer true. The mainstreaming of cybercrime tools and techniques puts new responsibilities on the entire enterprise to implement best practices.

It's now up to CIOs and CISOs to manage the security of their data and digital assets with strategies that meet the enterprise's overall business objectives while also promoting security as a shared corporate responsibility. Data security and privacy protection now rank as core business concerns and go to the heart of what it means to be a trusted brand, rather than simply an organization that meets basic compliance obligations.

TIP

When discussing strategic objectives, organizations need to include security and customer data protection as chief priorities. Data breaches and regulatory audits following a compromise can affect a company's reputation as well as its competitive ranking when customers, uneasy about a company's ability to protect personal data, vote with their wallets.

SecOps Is Handled by My Public Cloud Vendor

Businesses that are new to public cloud deployments are often confused about their SecOps responsibilities. These security and compliance responsibilities vary based upon the cloud services used. As a guideline, for any part of a service that you can configure, you are accountable for security and compliance.

Although public clouds are not inherently insecure, just as with on-premises resources, effort must be made to manage their compliance and security. Gartner predicts that through 2020, 95 percent of all cloud breaches will be attributable to the customer. This prediction still seems to ring true, as 2017 witnessed many high-profile public cloud breaches caused by organizational failures to secure their cloud deployments. It is vital that organizations understand the shared responsibility model with their cloud service providers (CSPs) and implement processes and controls for managing the risks they can influence.

On-Premises and Cloud Don't Mix

The reality today is that most organizations must not only support a hybrid cloud environment consisting of public and private clouds, but also support a multi-cloud model consisting of multiple public and private clouds, potentially spanning many CSPs, on-premises data centers, and remote locations.

To support such a complex environment efficiently, IT Operations and Security must be able to use the same tools effectively across all the environments that they support and secure.

You Can't Do SecOps without DevOps

For organizations that have already implemented DevOps in their software development practices, integrating SecOps can be a relatively easy and logical progression. However, SecOps can be implemented completely independently of DevOps.

The key to a successful SecOps implementation is to build a collaborative culture between IT Operations and Security, and to ensure they have the right people, processes, and technology.

We're Too Complicated to Use Automation

Complexity exists in every company and will only worsen unless the organization proactively works to address it. Complexity can often lead to bottlenecks, inefficiencies, and, worse yet, security vulnerabilities and downtime.

As systems and applications, as well as their operating environments, become ever more complicated, automation is the only way for operations and security teams to keep pace.

It Doesn't Scale

Ironically, as enterprise environments grow ever larger and more complex, SecOps is the *only* approach to operations and security that enables the organization to scale effectively.

We Need a Whole New Team

When done correctly, SecOps is a force multiplier for operations and security teams. Both teams become more proficient with the tools and processes they use to perform their job functions, and team members can cross-train and mentor one another.

It'll Never Pay Off

Corporate executives and board members increasingly view security and compliance as potential competitive advantages rather than costly burdens that only slow the business down. Calculating a return on investment (ROI) for security expenditures has traditionally focused on worst-case scenarios that compare the direct and indirect costs of a data breach to the proposed investment. However, the security and privacy of their personal data and business transactions is now a key part of the purchasing decision for increasingly tech-savvy customers who actively seek out companies with strong reputations for security, privacy, and compliance, and avoid those that have either suffered a data breach or are perceived as lax in their security initiatives. Underscoring the issue of trust, 42 percent of companies surveyed in Cisco's 2017 "Annual Cyber Security Report" who suffered a data breach lost more than 20 percent of their business opportunities, and 40 percent lost over 20 percent of their existing customers. More than 50 percent of these companies faced increased public scrutiny after the breach.

Bring security and operations together to protect your organization

Collaborative workflow processes that eliminate friction between the security and operations teams sharply lower the risk of data breaches and operational downtime. Enterprises can advance their business agenda by minimizing communications breakdowns that leave the organization vulnerable to cyberattacks. This book shows you how!

- ***Explore SecOps capabilities* — improve vulnerability management, apply shared visibility, and manage compliance across multi-cloud environments**
- ***Evaluate tools* — prioritize security vulnerabilities, automate remediation, and achieve scalability**
- ***Get started* — create your organization's SecOps vision, assess capabilities, and develop an action plan**
- ***Make the transformation* — assemble a team, automate processes, and calculate the return on your SecOps investment**

Rick Bosworth is Director, Solutions Marketing at BMC, specializing in cloud security and compliance. **Lawrence C. Miller** has written more than 60 *For Dummies* books.

Open the book and find:

- **Define SecOps roles and responsibilities**
- **Maintain multi-cloud visibility**
- **Embed security in software development**
- **Accelerate cloud migration**
- **Evolve toward a competitive advantage**
- **Improve processes with value stream mapping**

Go to Dummies.com® for more!

FOR DUMMIES®
A Wiley Brand

Also available as an e-book

ISBN: 978-1-119-48219-2
Not for resale