LEARNING MADE EASY

Securonix Special Edition

Cloud SIEM

for dummies®
A Wiley Brand

Discover cloud SIEM fundamentals

Understand the benefits of the SaaS model

Learn steps for successful deployment

Brought to you by

securonix

Chris Minnick

About Securonix

Securonix is redefining the next generation of cyber threat detection by using the power of machine learning and big data. Its purpose-built security analytics platform delivers real-time threat detection, threat hunting, and incident response capabilities on a single unified platform for end-to-end security operations management.

The Securonix security analytics platform has four key differentiating capabilities:

- Built on an open Hadoop stack, the solution provides unlimited scalability and data retention.
- Machine learning based analytics enables you to detect unknown and advanced cyber threats.
- Integration text-based search and threat hunting capabilities enable rapid investigation.
- Automated incident response and case management enable consistent and rapid response to incidents.

Securonix offers customers a visionary security analytics platform that's built for the next-generation of threat detection and response. The solution is priced by identity to provide consistent low pricing that doesn't increase exponentially with data. Learn more at www.securonix.com.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud SIEM

Securonix Special Edition

by Chris Minnick

for dummies®
A Wiley Brand

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud SIEM For Dummies®, Securonix Special Edition

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

Copyright © 2022 by John Wiley & Sons, Inc.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Securonix and the Securonix logo are registered trademarks of Securonix. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHORS HAVE USED THEIR BEST EFFORTS IN PREPARING THIS WORK, THEY 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 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES REPRESENTATIVES, WRITTEN SALES MATERIALS OR PROMOTIONAL STATEMENTS FOR THIS WORK. THE FACT THAT AN ORGANIZATION, WEBSITE, OR PRODUCT IS REFERRED TO IN THIS WORK AS A CITATION AND/OR POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE PUBLISHER AND AUTHORS ENDORSE THE INFORMATION OR SERVICES THE ORGANIZATION, WEBSITE, OR PRODUCT MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR YOUR SITUATION. YOU SHOULD CONSULT WITH A SPECIALIST WHERE APPROPRIATE. FURTHER, READERS SHOULD BE AWARE THAT WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ. NEITHER THE PUBLISHER NOR AUTHORS SHALL BE LIABLE FOR ANY LOSS OF PROFIT OR ANY OTHER COMMERCIAL DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.

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: 978-1-119-85373-2 (pbk); ISBN: 978-1-119-85378-7 (ebk). Some blank pages in the print version may not be included in the ePDF version.

Publisher’s Acknowledgments

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

Project Manager: Carrie Burchfield-Leighton

Acquisitions Editor: Ashley Coffey

Sr. Managing Editor: Rev Mengle

Business Development Representative: Molly Daugherty

Table of Contents

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Security information and event management (SIEM) technology has been around and widely used for over 25 years. When SIEM technology was new, we lived in a different world. Enterprise computing was centralized, applications and users did their work behind the corporate firewall, and the focus was on guarding the perimeter. And here's the biggest one — almost everyone used to go to the office every day. Imagine that!

In today's enterprise, remote work has become a fact of life, the types and numbers of devices with access to a company's data has multiplied, and data is no longer centralized but is spread out over different data centers, cloud platforms, and cloud-based applications. A modern SIEM must take advantage of advanced analytics techniques, such as machine learning (ML), to help make sense of the flood of data faced by any security operation. However, to be able to detect and respond to threats to your distributed environment, you also need the scalability and resiliency that can only be achieved by leveraging the cloud.

About This Book

This book is written with the expectation that anyone in your company should be able to read it, understand the content, and articulate the value and need for cloud SIEM. Executives and board members are becoming more aware and eager to find better ways to enable security teams to detect something happening to a company. They're also looking for ways to take advantage of cloud technologies to gain greater elasticity and reduced total cost of ownership (TCO).

Often, cybersecurity books go into significant technical depth, which is great for IT and security professionals, but little material is available for everyone else. In *Cloud SIEM For Dummies,* Securonix Special Edition, you discover the basics about how cloud SIEM can help your organization detect and deal with evolving distributed cyberattacks and better protect all its assets.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

As an added bonus, after reading this book (assuming you read the whole thing), you'll join the elite club of people on the teleconference whose eyes don't glass over when someone suggests the solution may be a cloud SIEM operating on a hybrid, multicloud environment.

Icons Used in This Book

You find several icons spread throughout this book. *For Dummies* icons help highlight additional information, particularly important information, and more.

REMEMBER

Similar to trying to act on billions of security logs, you have to identify what's most important. Unless you have a photographic memory or a ML brain, pay attention to these points. These are your key takeaways.

TECHNICAL STUFF

These nuggets are great pieces of technical information that the average reader doesn't need to know but may find interesting.

TIP

For time- or frustration-saving ideas, pay attention to these tips. There are plenty of ways in cybersecurity where you can get tripped up and make something more complicated than it needs to be. These tips help you focus on what matters and be effective in your efforts.

WARNING

Warning icons are for serious situations, where you can cause personal harm or harm to your work in the context of the book's subject matter. These are things that can keep you out of trouble or help you avoid mistakes others have made in the cloud SIEM space.

Beyond the Book

This book gives you an orientation to cloud SIEM and the key things to know to help with the migration of your security analytics to the cloud, but there's only so much that can be covered in a book this size. If you want to learn more about cloud SIEM and security analytics, check out `www.securonix.com`.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Looking at evolving security operations and detection tactics
- Defining security analytics
- Learning how the modern SIEM is different
- Understanding how the cloud fits in

Chapter 1 Introducing Modern SIEM

Information security and cybersecurity have always been about protecting companies, people, information, and assets. However, as technology has changed and the world has become more and more digitally integrated, the cyber risks have become more pervasive. With business applications increasingly becoming cloud-centric, the job of monitoring applications has become more complex, and what's needed is a true cloud-centric approach to security analytics.

Security information and event management (SIEM) has a long and rocky history with many companies. They've realized that integrating logs and data across an organization is complex and challenging, but necessary, to be able to respond to all flagged security events. Companies continue to implement these technologies for many reasons:

- Compliance monitoring
- Threat monitoring
- Log collection and retention
- Detecting hygiene issues
- Incident management

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Regardless of why, detecting security threats and generating actionable alerts are desired as companies seek to reduce their risk profiles.

In this chapter, you explore a bit of the past and present of security operations, and you learn how Software-as-a-Service (SaaS) and the cloud provide profound visibility into all your environments, faster time to value, unlimited scalability, and high availability.

Looking at Security Operations: Past and Present

The IT landscape has evolved. Computing has shifted from highly centralized mainframe environments (large computers that handled all the processing within the server) in the 1970s and 1980s, to client-server applications (where computing power was distributed between the PC and an application server), to the web and cloud-based applications. In the early 2000s, perimeter/data center-based security approaches were the dominant approach. This was often referred to as a *hard candy shell with a soft center.* The focus was only on the perimeter, and security was lax inside. Today, while elements of these historical approaches can still be found within companies, much of computing has shifted to the cloud-based systems and mobile devices such as smartphones and tablets.

Security hasn't kept up

Information security has struggled to lead or even keep pace with some of these shifts. While device, application, and infrastructure log collection and security event detection somewhat worked for mature organizations, security teams struggled with the volume and complexity to get to the right scale. Additionally, it was difficult to keep pace with attackers' new methods of penetrating a company. Legacy SIEMs used rule-based correlation of logs, which is dependent on known historical patterns of "what is bad." As a result, SIEM technology was similar to selecting which flu strains will be added to the annual flu shot using past (known) strains.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Driven by a significant increase in the fragmentation of security solutions (and an increase in use cases), SIEM technology evolved to include data analytics capabilities to aggregate and manage the increasing number and diversity of security data flows.

Staffing can't keep up

Traditional SIEM are often heavy and inefficient and require full-time staff just to keep them running. Just a few of the tasks involved in running a SIEM include

- Configuring data inputs
- Upgrading servers
- Adding storage capacity
- Monitoring uptime

These tasks must happen before the work involved in sifting through and responding to alerts can even begin.

Additionally, the cybersecurity talent crisis makes it difficult to support and staff large classic SIEM-related operations. The staffing issues keep security programs from progressing and effectively supporting what's created.

Recognizing Evolving Data Analytics Capabilities

With today's threat landscape, your detection tactics must evolve. Today, sensitive data, applications, and critical business processes occur in a distributed landscape. Cloud hosting, SaaS providers, mobile devices, mobile apps, and the Internet of Things (IoT) all collect, process, and store data. So, if it was historically difficult to get to scale and value with a traditional SIEM, with the complexity and volume of today's hybrid datacenters, it seems nearly impossible to be successful in today's environment. Enter security analytics and real-time behavior analytics.

The next generation security technology leverages machine learning (ML) and artificial intelligence (AI) to automate sifting through massive amounts of data and statistical algorithms to find patterns of highly advanced threats.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Centralizing Security Information

The primary utility of legacy SIEM technology was to provide security operations center (SOC) analysts with a centralized point of view for all security information. At first, many SIEMs were deployed as an answer to Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS) requirements. Today, most SIEMs are used for threat detection.

Figure 1-1 shows you a bare-bones concept of a SIEM, whether it's a traditional SIEM or a next-gen SIEM.

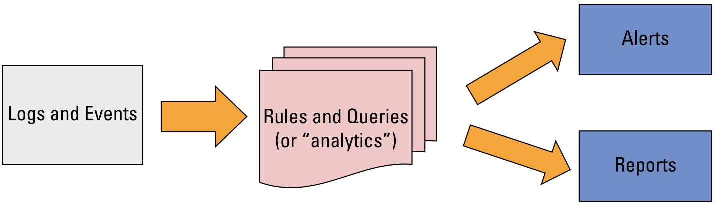


FIGURE 1-1: A bare-bones SIEM.

Threats from every direction

It was easy to detect threats when they were common to find single events that could be easily detected by simple pattern matching rules. But attacks have evolved to a point where multiple events from multiple sources must now be assessed in isolation and together as a pattern to determine the existence of malicious intent.

Providing a centralized view is still valuable, and improved analytics can reduce the number of false positives. However, the sheer volume of data that must be parsed and analyzed from a multiplying number of sources has caused storage and computing power to be a serious limiting factor with traditional SIEM technology.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Managing the Data Flood

With the number of data sources burgeoning, parsing of the different data formats in use, along with normalization to ensure that relevant data with the same context stayed together, became a monumental task. Over time, the data flowing in became a flood, and analysts were unable to resolve events at that pace. As capacity and system performance demands skyrocketed (with terabytes of data that needed to be searched through and analyzed at scale, in near real-time), matching available technology with requirements became a challenge, making it necessary to invest in new technology.

Increasing on-premises resources is always a temporary fix. Throwing more servers and more storage at the problem is one way to deal with the increasing volume and complexity of alerts. However, installing more servers means more resources are needed to support them, and knowing how much additional capacity to add is largely a guessing game. In traditional networks, you always have either too much capacity or too little (but usually too little).

Over time, the limitations of on-premises SIEMs have become clear, and they affect their ability to be effective and stretch the capabilities of the organization to support them. Fortunately, the same technologies that have contributed to much of the overwhelming data flood can remediate it.

TIP

Security analytics platforms aim to provide ready-to-deploy content and analytics to detect threats. Security analytics platforms and SIEMs have multiple hosting and implementation options based on the size and needs of a company. Three common options are

- On-premises
- Cloud (multi-tenant solution hosted and maintained by the vendor)
- Managed security service provider (MSSP) that hosts and operates your capabilities

Figure 1-2 gives you the advantages of the various hosting and support options.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

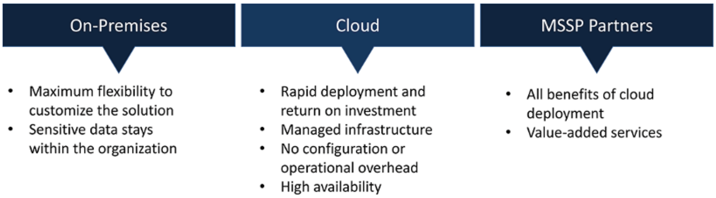

On-Premises
Maximum flexibility to customize the solution
Sensitive data stays within the organization
Cloud
Rapid deployment and return on investment
Managed infrastructure
No configuration or operational overhead
High availability
MSSP Partners
All benefits of cloud deployment
Value-added services

FIGURE 1-2: The advantages of different hosting options.

Understanding How Modern SIEM Is Different

Enter the cloud.

The next generation of security technology leverages the cloud to scale dynamically and ingest the complex data coming from all your company's data, from every source and environment.

Being able to capture this data is one thing, but it's just the beginning. A modern SIEM must also be able to sort through all the data and accurately narrow it down to a manageable level.

Accurately identifying threats with UEBA

User and entity behavior analytics (UEBA) was originally conceived as a data analytics capability. Firms quickly realized that it also served as a ready-made solution to the alert flood problem emerging with SIEM in conjunction with modern data lake technology that utilized big data to handle data scale problems. UEBA capabilities allowed SIEMs to reduce alerts to a manageable level for SOC analysts, allowing them to work more efficiently and focus their attention on alerts that matter.

UEBA uses ML algorithms and other statistical techniques to run advanced analytics on security data, identifying user profiles and correlating alerts from the same entity to define risk scores for each user. This allows UEBA to identify emerging threats that are of real concern and avoid individual events that are simple activity outliers that didn't pose a security risk. By utilizing behavioral analytics, UEBA helps identify actual threats by linking a series of suspicious activities that could, put together, constitute a concern.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

While individual events could also indicate threats (such as a malware alert), UEBA helped identify long-chain threats that were not immediately visible through alerts. Combined with the scalability of the cloud, UEBA has a much larger pool of data from which to create models and the computing power with which to do it.

Storing and using data efficiently

Modern SIEMs needed better performance and scalability than what could be provided by traditional data storage or big data-based data management systems. The modern SIEM must move to cloud-native architectures, providing dynamic, unlimited scalability.

But just as important as the ability to scale up to meet an increasing demand is a concept called *elasticity*. If you think of cloud computing as a rubber band that can be stretched to any length needed to handle increases and bursts of traffic, elasticity is the ability of the rubber band to return to the level (or even smaller, if needed) where it was. This capability simply doesn't exist if scaling up means purchasing more hard drives, more servers, and higher bandwidth rates.

Integrating into a broad landscape

Modern SIEMs need to be able to integrate with and ingest data from a wide variety of data sources, including on-premises and cloud. Therefore, the analytics model needs the ability to map this content as well as a robust set of integrations and parsers to cover the huge landscape of security platforms available today.

Figure 1-3 shows some of the possible sources of event data that must be integrated into a modern SIEM.

Bringing integration where data is

With an increasing amount of the enterprise's data and logs being generated and stored in the cloud and by remote workers, it no longer makes sense to attempt to consolidate all this data on a private network. Even the most robust private network isn't going to be able to integrate as efficiently with cloud-based applications and data as another cloud-based application. Gathering, analyzing, storing, and backing up cloud-generated data on a private network can become a bottleneck that can slow down your entire security operation.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

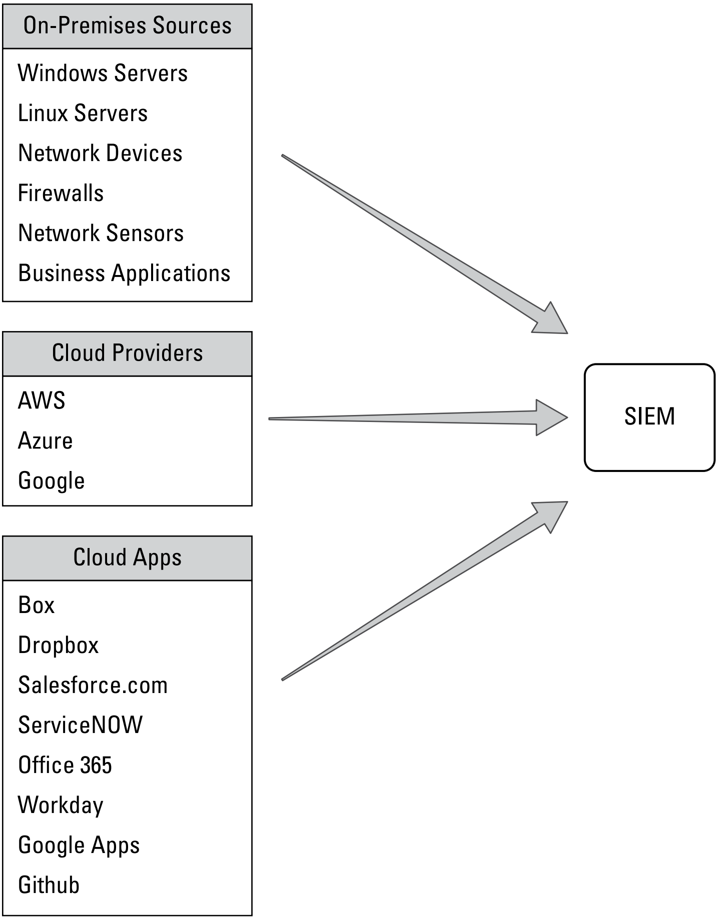


FIGURE 1-3: The sources of event data.

Prioritizing threats

Beyond scalability, elasticity, and resiliency, cloud SIEM also excels at providing useful real-time data. But, if all you needed was real-time data, you could get this from just viewing your various log files as they're generated. Oh, if only it were so simple.

A company may generate gigabytes or terabytes of log files each day. Most of this is perfectly normal and doesn't require any action. A portion of this data may be the result of malicious behavior that can be handled by rules and security policies. This data also doesn't normally need to be sent to SOC analysts because it can be dealt with in an automated way.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Knowing the real threats

Behavior that would've looked suspicious in the past, such as a large number of users logging into the internal network remotely, has become the norm. Most remote logins are perfectly routine. Failed remote logins may warrant additional scrutiny, but if it's just Phil the salesperson who never remembers his password, your security analysts shouldn't have to receive alerts each time he flubs or forgets his password. Combined with additional context, such as that Phil was trying to log in from a strange computer in a strange location, what might in isolation look innocent can be an indicator of a potential threat. If someone managed to log into Phil's account and use it to install malware, this is the kind of event that can't wait.

Real-time prioritization and enhancement

Looking at the bigger picture using ML and accurately prioritizing alerts is computationally expensive, but it's critical that it be done well and quickly. Only a SIEM with the power of the cloud can accomplish all of this.

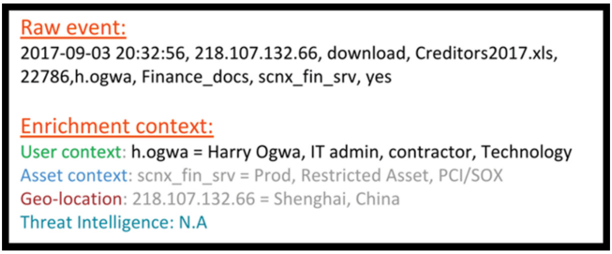
Interactive search capabilities allow threat hunters to make text-based searches on raw and enriched security data and events. You're asking questions to narrow down your search to the most interesting event(s). Searching with enriched data means data that has been cleaned, improved with context information, and organized to make it more usable. Searching allows threat hunters (as well as incident response analysts) to accelerate their investigations into potential incidents.

When you couple interactive text-based searching capabilities with the ability to visualize potential linkages and insights across enriched data, you allow threat hunters to see things they may not see with the raw or even enriched data.

Figure 1-4 shows a Securonix example of what data enrichment can look like as it analyzes the raw event shown at the top.

Within the visualization from a search, the analyst should be able to visually get into more detail of a specific root cause. This helps keep everything organized and bucketed so the hunters don't get confused, waste time, or make incorrect assumptions.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.



Raw event:

```
2017-09-03 20:32:56, 218.107.132.66, download, Creditors2017.xls,
22786,h.ogwa, Finance_docs, scnx_fin_srv, yes
```

Enrichment context:

User context: h.ogwa = Harry Ogwa, IT admin, contractor, Technology
Asset context: scnx_fin_srv = Prod, Restricted Asset, PCI/SOX
Geo-location: 218.107.132.66 = Shenghai, China
Threat Intelligence: N.A

FIGURE 1-4: Real-time data enrichment.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Ensure an IT solution is up and running
- Focusing on SIEM content
- Watching the SIEM for alerts and insights

Chapter 2 The SIEM Operational Model

Whether done by automated processes, dedicated staff, or your Software-as-a-Service (SaaS) vendor, certain activities must be done for a security information and event management (SIEM) system to be successful. These activities can be grouped into three categories:

- **Run:** This includes the activities required to manage servers, install patches, install updates, and so forth.
- **Adapt:** The adapt activities include creating and tuning rules and other content of the SIEM system.
- **Watch:** You don't have much of a monitoring and reporting system if no one looks at the generated alerts or reports. The activities related to consuming the output of the SIEM happen here.

REMEMBER

The ideal end result of a successful SIEM system is that security threats are identified and responded to quickly and accurately. With interconnected services and systems that can exceed billions of transactions every day, however, and with countless attackers looking for vulnerabilities, no number of available security personnel can possibly keep pace.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Companies have invested in plenty of skilled security professionals, and the average enterprise has 25 different security tools. Security spending may take up 11 percent or more of your overall IT budget. The fact is that hiring can't keep pace, and there's never enough room for additional investment. New security approaches must pay for themselves with efficiency.

To understand how cloud SIEM can help, consider each of the activities that must be done for SIEM to be successful. This chapter is built on Figure 2-1, which shows you the relationships between the three categories of SIEM activities.

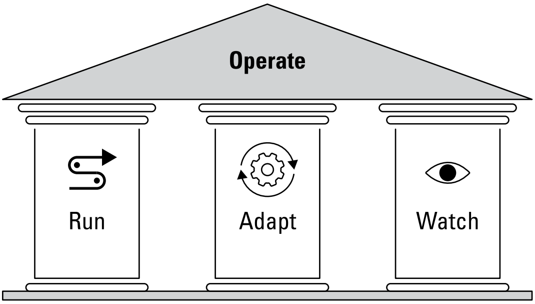


FIGURE 2-1: The SIEM operational model.

In this chapter, you take a look at each of these activities and how they can be aided by cloud technologies.

Run

Run covers the activities required to ensure an IT solution is up and running as expected. In a traditional SIEM running on on-premises servers, these activities can consume a tremendous amount of time, and they often involve dedicated staff who handle these critical, but often tedious, time-sensitive, and time-consuming tasks. Furthermore, the staff that keeps the servers running must be available 24/7.

The run activities include

- Maintaining the servers that run the SIEM and store the data it consumes and generates
- Updating the operating systems on the servers

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Applying patches to the SIEM software
- Adding more storage and computing power as required
- Configuring collectors and log sources
- Monitoring the entire system to ensure that it's up and running and performing well at all times

In a cloud-native environment, the effort required for the run part of the SIEM operation model is greatly reduced. Resources that were previously devoted to making sure servers are running correctly can be reapplied to working on content (the adapt activities) and to investigating and responding to alerts (the watch activities).

TIP

Reducing time spent on run tasks is just the beginning of the benefits of using cloud-based SIEM. The saving and efficiencies gained by reducing time spent on these activities alone can justify the effort involved in migrating to the cloud.

Adapt

Adapt includes the activities focused on the SIEM content. Content is the set of rules, machine learning (ML) models, data parsers, reporting definitions, and everything else that can be customized on a SIEM solution according to the user needs.

In both traditional, as well as modern SIEM, the SIEM vendor provides content out of the box, but the user still needs to select the content to be deployed and enabled, tune content such as rules and log parsers, and develop custom content according to the specific needs of the organization.

Just as cloud technologies have reduced the time spent on run activities, supervised ML tools have increased the effectiveness and reduced the effort involved in creating and tuning content.

Through the combination of ML and the cloud, modern SIEM technology can reduce the effort spent on defining and tuning rules. For example, ML running in a traditional SIEM environment only has access to a single organization's experience, but cloud SIEM benefits from the wisdom of the crowd. The data generated by every customer on a cloud-native SIEM platform can be used to tune the ML system and improve detection for all of a SIEM's customer.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Watch

Watch activities, such as alerts and reports, are those that consume the output of the SIEM. These can be seen as the real user activities of the solution. A SIEM provides no value if the output isn't being consumed by anyone. Alerts need to be investigated and response actions need to be taken. This activity is often human-resources intensive because organizations usually need to have it running in a continuous, 24/7 manner.

Modern SIEM capabilities can augment and inform your security professionals — weeding out, and even handling, low-priority alerts. A SIEM platform with SOAR (security orchestration, automation, and response) capabilities can automate threat validation and respond to threats in an automated way. This frees up your staff to focus on responding to high-priority alerts and on further tuning the SIEM.

TECHNICAL STUFF

SOAR and related technologies can be used to enrich SIEM alerts by providing more context and even automatically closing some categories of alerts. The focus of SOAR, however, is on making the security analyst more effective, rather than on replacing humans.

WARNING

Regardless of what you hear, no holistic tool or capability exists that's so fully automated that it doesn't require human decisions and actions from security and IT teams. The key to maximizing the autonomy and automation that's available today is understanding what's possible and where to use it and rely on it.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- » Explaining the modern cloud SIEM
- » Understanding the benefits of cloud SIEM
- » Learning about the three cloud SIEM models
- » Understanding the pros and cons of managed security services

Chapter 3
Getting to Know the Modern Cloud SIEM

The term *cloud* grew in popularity almost ten years ago, and just several years ago predictions that 50 percent of infrastructure would be in the cloud were impressive, and perhaps not entirely believable.

The COVID-19 pandemic changed everything, however, and dramatically increased the urgency and the pace of cloud adoption. According to the 2020 IDG Cloud Computing Survey, 59 percent of businesses plan to migrate "most" or "all" of their infrastructure to the cloud in the next 18 months.

In this chapter, you find out the benefits of cloud security information and event management (SIEM) and about the three models of cloud computing.

Defining the Modern Cloud SIEM

The migration of computing power and storage matters for information security professionals. Historically, you could theoretically monitor everything in your network because it was in your network. Legacy cybersecurity strategies were based on protecting

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

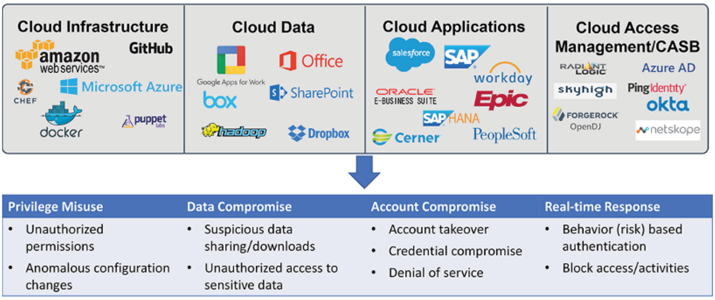
a closed system from attack by defending the perimeter. Over the last 25 years, closed corporate networks have been replaced by open systems. These days, corporations employ dynamic workforces using multiple devices to access data stored in hybrid datacenters and cloud applications around the world. Traditional perimeter security techniques to detect and respond to threats aren't effective in addressing modern challenges.

As infrastructure, application, and data are moving to cloud, security teams are faced with a huge challenge to secure this environment. This expands the attention from monitoring corporate networks to monitoring cloud resources (or leveraging third-party monitoring). Any security solution you choose, including security analytics, needs to be cloud ready.

REMEMBER

A modern cloud SIEM is one that's not just cloud-ready; it's cloud native. Cloud native means that it was developed for and runs in the cloud and takes full advantage of cloud computing. The questions to ask your vendors include "Do you offer a Software-as-a-Service (SaaS) solution in cloud?" and "Do you have the connectors to integrate with my cloud infrastructure to collect and analyze data?"

To give a better idea of how your IT infrastructure and cloud presence can affect the things you need to be able to monitor, Figure 3-1 shows a sample of cloud providers by service type and the types of use cases that rely on data coming from them.



Privilege Misuse	Data Compromise	Account Compromise	Real-time Response
• Unauthorized permissions • Anomalous configuration changes	• Suspicious data sharing/downloads • Unauthorized access to sensitive data	• Account takeover • Credential compromise • Denial of service	• Behavior (risk) based authentication • Block access/activities

FIGURE 3-1: Cloud security analytics.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Understanding Why You Need the Cloud

When you think about the qualities that are desirable in an enterprise security software system, some of the things that may come to mind include scalability, elasticity, resiliency, and lower total cost of ownership (TCO). In every case, when compared with a traditional application running on traditional infrastructure (such as a SQL database running on hardware you own), cloud computing wins.

Figure 3-2 shows A SIEM implementation with a native cloud architecture.

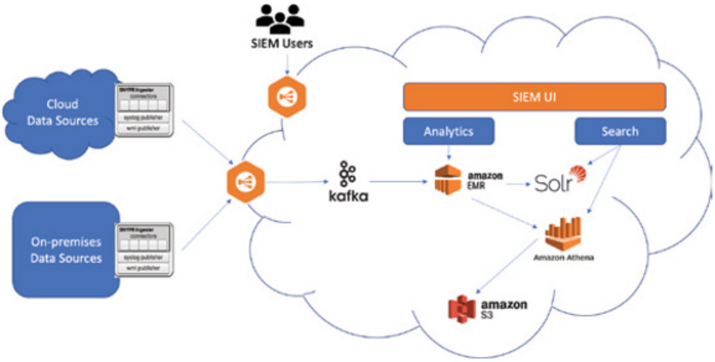


FIGURE 3-2: A cloud-based SIEM architecture.

In this section, you discover how every aspect of the modern SIEM is best delivered by one computing model — the cloud.

Scalability

With terabytes of data that must be searched through and analyzed in near real time, traditional data storage and big data-based management systems can't keep up. The modern cloud-native SIEM solutions provide dynamic and unlimited scalability.

Elasticity

Elasticity is the ability of a system to match resources allocated with the actual number of resources needed. Traditional computing systems require a company to attempt to anticipate future workloads and purchase enough computing power to meet those

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

unknown needs. Increased efficiency or reduced workloads meant that resources were going unused.

In a cloud environment, resources can be dynamically added or removed as needed to meet application demands.

Resiliency

Resiliency refers to the ability to adapt to changing conditions and to recover from disruptions. A traditional SIEM solution running in your datacenter is vulnerable to local hardware failures, power and network outages, and the same types of attacks it's meant to help prevent, but cloud-based applications run in highly redundant and secure environments spread over multiple locations with built-in backup and disaster recovery.

Reduced TCO and maintenance complexity

Cloud computing spreads the cost of servers, maintenance, upgrades, and innovation over many clients. As a result, enterprise class service is made available to each client at a lower cost. Combined with the ability to scale dynamically and the reduced need for onsite personnel to maintain physical and software infrastructure, SaaS can offer a significantly lower TCO and reduce maintenance complexity.

Being closer to your data sources

Today, much of the data consumed by enterprises has migrated or is in the process of migrating to the cloud. Rather than consuming log files generated behind the firewall, modern SIEM systems consume data securely over the internet from a variety of application programming interfaces (APIs).

A cloud SIEM system can access APIs from other cloud-native applications directly, without depending on the available bandwidth at a central corporate datacenter.

The wisdom of the crowds

Cloud-based SaaS environments can leverage insights from the other organizations running in the same SaaS environment in real time. The resulting increase in the size of the dataset available to machine learning (ML) and human analysts greatly increases the speed and accuracy of detection of threats and responses.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Moving away from "run"

With resource management handed off to the vendor, cloud SIEMs remove one significant responsibility area from the enterprise, while not affecting their ability to track threats. Less time spent on run activities can free up resources to focus on the adapt and watch activities. Flip back to Chapter 2 for more info on run, adapt, and watch.

Introducing the Three Cloud SIEM Models

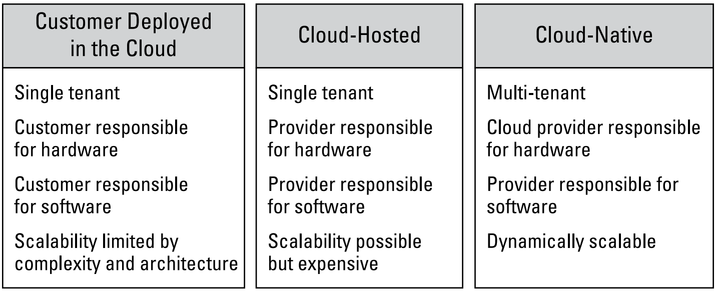
When selecting a cloud SIEM solution, you can choose from three types of clouds:

- Customer-deployed in the cloud
- Cloud-hosted
- Cloud-native

The differences between these three models come down to

- What parts of the stack you're responsible for
- What parts the cloud provider is responsible for
- Single tenant versus multi-tenant
- Scalability

These differences are shown in Figure 3-3.



Customer Deployed in the Cloud	Cloud-Hosted	Cloud-Native
Single tenant	Single tenant	Multi-tenant
Customer responsible for hardware	Provider responsible for hardware	Cloud provider responsible for hardware
Customer responsible for software	Provider responsible for software	Provider responsible for software
Scalability limited by complexity and architecture	Scalability possible but expensive	Dynamically scalable

FIGURE 3-3: The three cloud SIEM models.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Customer-deployed in the cloud

The first model is the Infrastructure-as-a-Service (IaaS) model. It makes use of cloud computing platforms to virtualize servers that were previously hosted onsite. IaaS is a common first step into cloud computing for many organizations, and it provides the highest level of control over your data but at the highest ongoing maintenance costs. In IaaS, hardware is virtualized, but everything running on top of the virtualization layer is your responsibility.

Cloud-hosted SIEM

In cloud-hosted SIEM, a system originally designed for on-premises environments is deployed to the cloud by a service provider. The goal of cloud-hosted SIEM is to move from a Capex (capital expenditure) to a Opex (operating expense) model. It is easier to scale, as well, because resources can be provisioned faster in the cloud. However, cloud-hosted SIEM doesn't provide many of the other benefits of migrating to the cloud.

Like customer-deployed SIEM, cloud-hosted SIEM can't reach the scale and reduced cost of cloud-native.

Cloud-native SIEM

The third model is SaaS. In this model, responsibility for the underlying platform, as well as the applications and the data falls on the provider. SaaS removes the responsibility of deploying and maintaining the application from the customer. Only SaaS, also known as cloud-native applications, can deliver the full value of cloud SIEM.

Cloud-native applications leverage multi-tenant architecture and deployment. A multi-tenant architecture is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a *tenant.* In a multi-tenant deployment, each tenant receives a user interface (UI) specifically designed for them, and the backend components are shared across the entire customer base. This significantly reduces the cost per tenant, resulting in a quicker time to value for each tenant.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

Although a single application serves multiple customers in a multi-tenant architecture, each customer's data is isolated and invisible to other tenants. Eliminating the need to maintain bulky databases on-premises allows you move away from large upfront capital expenditures in favor of flexible operational expenditures.

WARNING

Putting your data in the hands of the vendor may not be desirable or even allowed by certain regulatory requirements. To address this concern, cloud SIEM can take advantage of a hybrid cloud, as I discuss in Chapter 4.

Using Managed Security Services

While all three cloud SIEM models can reduce the infrastructure and resources needed to properly operate a SIEM, responsibility for administering the SIEM still belongs to you. Managed security services (MSS) and managed detection and response (MDR) are additional options for organizations that want to offload more of their cybersecurity responsibilities. With MSS, a trusted partner handles part or all of a company's security processes. MSS can be done either in-house or remotely. The company gains the expertise and skill of the MSS partner's researchers and engineers, who may provide services ranging from installation to threat detection and response.

TECHNICAL STUFF

MDR is a subset of MSS. MSS is like a catch-all term that encompasses MDR. When I refer to MSS, I'm talking about any managed security services, which may include MDR.

By using MSS, you can eliminate the need for an onsite security operations center (SOC), but it adds dependencies and relinquishes control over your data.

WARNING

Working with an MSS provider creates a significant dependency for your organization, and the relationship will require trust and safeguards. Check out Chapter 5 to discover what questions to ask and the importance of regular audits.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding how much control you need
- Analyzing regulatory constraints
- Looking at cloud compatibility
- Taking a look at integrations support
- Evaluating scalability of cloud solutions

Chapter 4 Considerations When Choosing a Cloud SIEM

While cloud Security Information and Event Management (SIEM) provides important benefits to the modern company over traditional SIEM, there are considerations to keep in mind while you're determining whether and when to migrate.

In this chapter, you look at some of the potential issues and considerations associated with migration of your security analytics to the cloud.

Giving Up (Some) Control

With the vendor ensuring that the required resources are highly available, this adds a layer of robustness to the security infrastructure — but also takes away a little control. On the cloud, resources are naturally backed up, are always available, and increasingly, allow a degree of control on data both at rest and in motion.

In some instances, however, an organization may need to maintain control of all its data. The solution is a "bring your own

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

cloud" strategy, in which the organization can keep their data in their own cloud storage and maintain total control and access to their data.

Understanding Constraints

Organizations planning a migration to cloud-native SIEM should consider the possible constraints of Software as a Service (SaaS) in general.

Regulatory constraints

While one of the common use cases of SIEM is to fulfill regulatory requirements, there may also be regulatory and legal constraints to consider while choosing a cloud SIEM solution. These constraints may include data sovereignty laws, data privacy laws, and more.

Bandwidth

Cloud-native SIEM requires bandwidth for ingesting on-premises data as well as for accessing the SIEM user interface. If you don't have enough bandwidth on-premises to supply a cloud-based SIEM with the log files it requires and access the SIEM user interface, you'll lose most of the benefit of migrating your SIEM to the cloud. With remote workers and cloud-based applications becoming common, if you don't have sufficient bandwidth to interact with cloud-based resources, you may already be experiencing this issue.

TECHNICAL STUFF

To estimate the amount of bandwidth required, you can multiple the number of events per second by the average event size. For example, if the average event size is 1 kilobyte (8 kilobits), the bandwidth required to transfer 1,000 events per second is 8,000 Kbps, or 8 Mbps.

Network reliability

While applications and data stored in the cloud are highly redundant and available, the connection between your on-premises data and the cloud, or between the cloud-based SIEM and other cloud-based data sources, must also be reliable.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

REMEMBER

As with bandwidth, network reliability is one of those problems that not only affects your ability to use a cloud SIEM but also increasingly affects your organization's ability to do much of anything.

Looking at Compatibility with Your Cloud

Different public clouds have different capabilities and pricing models. Depending on an organization's requirements, it may be most beneficial to use a single cloud provider or to use a hybrid or multi-cloud strategy.

Hybrid cloud

A hybrid cloud connects on-premises computing, storage, and services with those in the public cloud. Hybrid clouds allow organizations to retain control over on-premises data while taking advantage of the benefits of SaaS. This simple design, shown in Figure 4-1, can address many regulatory concerns and make SaaS SIEM viable to organizations that couldn't even consider it as an option before.

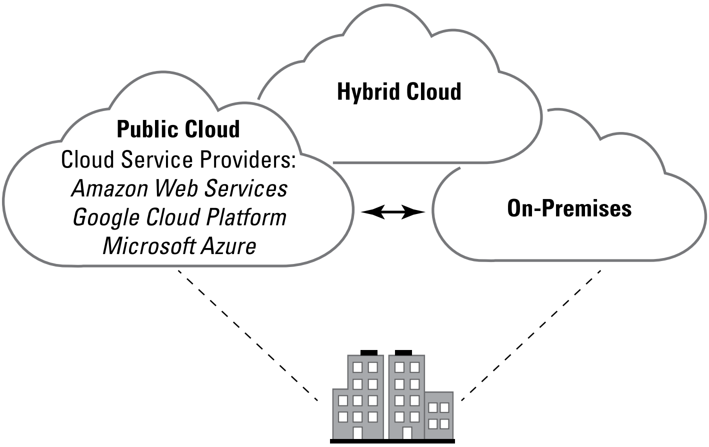


FIGURE 4-1: The hybrid cloud design.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Multicloud

A multicloud strategy, shown in Figure 4-2, uses multiple public cloud providers. With multicloud, an organization can gain increased reliability and the lower latency that can result from choosing a local cloud based on each facility location. Using multiple public cloud providers may also enable certain organizations to comply with governmental regulations and data sovereignty laws that require data to reside in a specific geographic location.

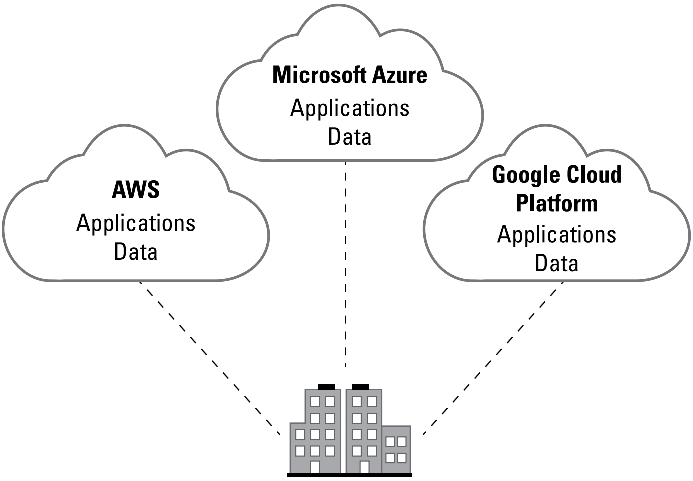


FIGURE 4-2: The multicloud strategy.

Federated SIEM deployment

Most organizations moving their on-premises systems to the cloud go through a long migration process, during which considerable pieces of their infrastructure reside on each side. Many migrations, in fact, are never complete, leaving a residual presence in the organization's datacenters. To make matters even more complex, the multicloud scenario is also frequently part of the process: Many will adopt services from more than one provider, such as Amazon AWS and Microsoft Azure. In fact, even those strongly pushing to standardize on AWS are often using Microsoft services such as Office 365 and Azure Active Directory.

In a federated SIEM model, multiple SIEM instances can be deployed on multiple clouds and locations, but another SIEM layer is added that consolidates events and searches from the multiple SIEM instances. Figure 4-3 shows you this model.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

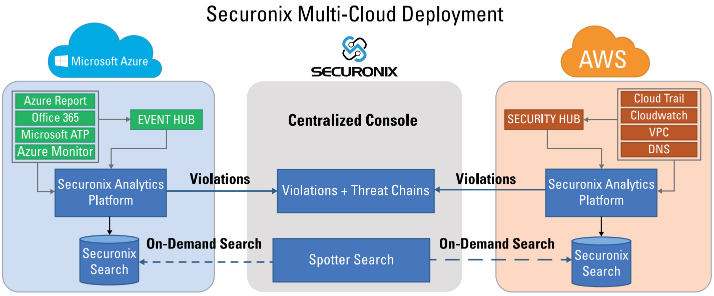


FIGURE 4-3: The federated cloud SIEM model.

This additional layer presents a centralized management console, allowing local teams to work on their own policies and threat chains, for example, while still allowing a global team to retain visibility across the multiple teams and locations.

For many organizations, a federated SIEM deployment model presents the best of both worlds approach when considering a fully centralized model or a fully distributed model.

Evaluating Integrations Support

Security analytics is all about data. To be of use, a SIEM must integrate with all of an organization's existing data sources and devices and be able to parse all its log data. The more high-quality data you have the better the results. You need to plan your data requirements carefully.

It comes down to knowing the three Vs: volume, velocity, and variety. Knowing the volume and velocity helps you plan for cloud storage costs and bandwidth. Variety helps you evaluate the vendor to see if it supports the data types you have.

TIP

Securonix provides a unified platform base that enables unlimited scalability and data retention. Its connector library provides you out-of-the-box (OOTB) integration with a variety of data sources and applications. The built-in regular expression (REGEX) feature enables you to parse any custom data feed through simple configuration steps from the user interface. For more information, visit `www.securonix.com/products/security-data-lake`.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Knowing if It Scales

If there's one thing that's certain about the future of cybersecurity, it's that its attacks will continue to become more sophisticated. It also seems highly likely that organizations will continue to become more distributed. With both of these factors, the amount of log data to be analyzed and the complexity of that analysis will continue to grow. One key factor for being able to handle an increasing and unpredictable number of threats is rapid and massive scalability.

TIP

Look for a solution that's built by using open technologies such as Kafka, Spark, and Solr. This is important because your data won't be locked in a proprietary black box. You can scale the SIEM solution to meet your needs, and you can build your own analytics by using Spark or even access the data in the cloud SIEM directly.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- » Knowing your roles and responsibilities
- » Understanding the roles and responsibilities of a SaaS vendor
- » Evaluating managed security services
- » Keeping an eye on your MSS provider

Chapter 5 Understanding Roles and Responsibilities in the Cloud

In this chapter, I show you a sample responsible, accountable, consulted, informed (RACI) matrix for cloud security information and event management (SIEM) and then talk about the special case of managed security services (MSS), in which most of the responsibilities are shifted to a trusted third party.

RACI/Roles and Responsibilities Chart

Successful implementation and operation of a cloud SIEM requires not only a list of activities to be completed but also that all stakeholders understand their roles in those activities and processes. One tool for organizing and visualizing the roles and responsibilities of your team and of your cloud SIEM provider is a RACI matrix. Table 5-1 gives you a sample RACI matrix for implementing and managing a cloud SIEM. A blank entry means that party isn’t involved in that activity or has no role in it.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TABLE 5-1 A RACI Matrix for Cloud SIEM

Activities	Cloud SIEM Provider	Customer
Architectural design	RAC	I
Deployment	RAC	I
Log collection setup	CI	RA
Storage maintenance	RA	CI
Datacenter facilities	RAC	I
Provide new content	R	RACI
Adapt/tune content	R	RACI
Software updates and maintenance	RAC	I
Alert monitoring		RACI
Incident response		RACI

REMEMBER

RACI stands for responsible, accountable, consulted, informed.

Outsourcing Roles and Responsibilities with MSS and MDR

MSS and managed detection and response (MDR) can be great options for organizations that don't want to invest resources in a full-time security operations center (SOC). However, it must be done carefully, with a clear understanding of roles and responsibilities, and with thorough processes in place to keep checks on the MSS provider (MSSP).

Table 5-2 shows a sample RACI matrix for managed security services. A blank entry means that party isn't involved in that activity or has no role in it.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TABLE 5-2 A RACI Matrix for Managed Cloud SIEM

Activities	Cloud SIEM Provider	MSSP	Customer
Architectural design	RAC		I
Deployment	RAC		I
Log collection setup	C	RI	RA
Storage maintenance	RAC		I
Datacenter facilities	RAC		I
Provide new content	R	RA	CI
Adapt/tune content	R	RA	CI
Software updates and maintenance	RA	I	CI
Alert monitoring		RA	CI
Incident response		CI	RA

Selecting an MSSP

Selecting a service provider is a complex undertaking that requires assessing multiple factors, including price. The recommended steps to properly assess a candidate include the following:

1. **Review the provider's service level agreement (SLA).**

   Your MSS vendor should work with you to develop an incident response plan that aligns with your goals, priorities, and resources.

2. **Evaluate the provider's transparency and communication.**

   Do they keep an audit trail or record of activities? How often does the provider meet with your internal team? How available is your MSS provider?

3. **Check the certifications.**

   Your provider will help with your compliance reporting, but has your MSS provider earned their certifications?

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

4. **Check the references.**

   A good MSS/MDR partner will be proud to share customer references.

5. **Watch out for lock-in.**

   If, after some time of working with an MSS/MDR partner, you decide to bring your security analytics in-house, will you be starting from scratch or can you transition the existing managed security stack in-house?

Keeping tabs on managed services with audits

If you're using managed services, your organization will necessarily have a strong dependency on your service provider. As a result, frequent audits are recommended to ensure security protocols are followed.

Aspects of your MSSP that you want to audit include

- SOC operations and procedures
- Security clearance credentials of SOC staff who have access to your data
- Data access controls
- Physical access controls and procedures
- Redundancy and business continuity plans

Furthermore, if you have skilled penetration testers on staff, you can test the provider's responsiveness by staging an incident and seeing how they respond.

REMEMBER

A relationship with a MSSP is all about trust, but building trust takes time and verification. Any relationship that's so vital to your operation as that between your organization and your MSSP is worth going slow and easing into, rather than taking the plunge all at once.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Understanding how to rank SIEM capabilities
- Assigning weights to different categories of SIEM features

Chapter 6
Selecting the Right Cloud SIEM

Selecting a cloud Security Information and Event Management (SIEM) can be a daunting task. Factors to consider include your use cases, the capabilities of the SIEM, support for your applications and clouds, and, of course, cost. In this chapter, I present a framework you can use to rank solutions according to these factors and more.

Ranking Cloud SIEM Features and Capabilities

At the end of the day, your main goal with any SIEM is to detect security incidents. Other goals may be to meet compliance regulations, reduce the strain on your already stretched security operations center (SOC) resources, and reduce costs.

Along the way to achieving these goals, other important factors that contribute to the success of your endeavor include the following:

- An easy-to-use user interface (UI)

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Easy integration with your applications and network hardware
- Scalability
- Speed
- Strong analytics
- Support for multiple clouds

Evaluating Cloud SIEMs

Although it can be difficult to decide which components of a SIEM are the most important, it seems logical to start with the factors that will, over time, produce greater and greater returns.

WARNING

One-size-fits-all solutions don’t exist when it comes to an enterprise SIEM. Likewise, you shouldn’t look for a new SIEM that can exactly replicate an existing system. You can expect to do some amount of customization of any solution you choose, and the process of making a change from an on-premises SIEM to a cloud SIEM is a great opportunity to think in terms of what capabilities you’d ideally like to have, rather than what you currently have.

Table 6-1 assigns a weight to several categories, along with criteria for evaluating a SIEM according to each of the categories. The categories break down as follows:

- **Base SIEM capabilities:** These are the basic things you should expect from any SIEM, including a functional user interface, search capabilities, the ability to define policies, and threat identification.
- **Integrations:** Will the SIEM play nice with your existing hardware and software?
- **Analytics and user and entity behavior analytics (UEBA):** This is the most heavily weighted category for a good reason. Without mature support for UEBA and content customized to your industry, you could be spending much more time and effort chasing after false positives and missing the big picture.
- **Features:** Does the SIEM support the other features you need, such as content and search features and support for governance and regulatory frameworks?

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- **Data architecture:** Does it scale? What sort of high availability and disaster recovery is supported?
- **Multicloud support:** With multicloud support, you can gain additional flexibility, performance, and potential cost savings.
- **Analyst reports and industry opinion:** What are others saying about it?
- **Cost and expertise availability:** Cost is important, but just as important is the ability to find people who can operate it. A platform built on open standards is more likely to have a larger pool of analysts with the expertise to work with it, for example.

TABLE 6-1 Framework for Selection of Cloud SIEM

Category	Weight	Criteria
Base SIEM capabilities	15%	Functional UI Policy definition Regex/normal search Threat event identification Deployment options (on-premises/cloud)
Integrations	10%	Integration categories covered: Endpoint detection and response (EDR) Network detection and response (NDR) Other SIEMs Firewalls Load balancers Cloud providers SaaS applications Industry applications, such as the Electronic Privacy Information Center (EPIC) for healthcare providers Integration level (number of data categories covered) Integration difficulty (all graphical user interface [GUI]/part GUI and part command line interface [CLI]/all CLI)

(continued)

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TABLE 6-1 ***(continued)***

Category	Weight	Criteria
Analytics and UEBA	20%	UEBA engine maturity Availability of content for threat use cases Ability to apply analytics to custom use cases Content by industry
Features (search, content, governance and regulatory framework support, standards compatibility)	15%	Search, content, governance and regulatory framework support, standards compatibility (MITRE, NIST, and so on), use cases covered through pre-configured content
Data architecture	10%	Scalability, dependence on infrastructure, speed of operations, reliability, high availability and disaster recovery (HA/DR) capabilities
Multicloud support	10%	Support for multiple public clouds and private cloud architectures
Analyst reports/ industry opinion	10%	Gartner, Forrester, GigaOm, others
Cost and expertise availability	10%	Pricing compared to industry leader baseline, certification, and training

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Knowing your environment and your assets
- Comparing and contrasting SIEMs
- Identifying and prioritizing use cases
- Defining deliverables and operational processes
- Training your users
- Establishing benchmarks

Chapter 7 Ten Considerations for Migrating to a Cloud SIEM

Moving away from tradition is never easy. Sticking with legacy systems can be even more difficult. Legacy cybersecurity that depends on simple rule-based detection and that has limited data scaling limitations is a severe weakness and leaves you exposed to many modern threats.

A carefully planned and executed migration to cloud security information and event management (SIEM) isn't trivial, but with the right planning and execution, it can be executed without hiccups.

A typical migration to cloud SIEM may take between 8 and 26 weeks and depends on the determination of your organization's leadership as well as the experience and expertise of your SIEM vendor.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Know Your Environment

Knowing your technology environment and getting the right coverage within your company are critical. Some organizations don't have a full knowledge or inventory of their digital assets, which makes it nearly impossible for many security efforts to have the right level of assurance and coverage. Make sure that you understand what parts of your environment the security analytics solutions you're evaluating touch.

You should also have a clear understanding of the human resources available. What skills and expertise do you have, can you hire, and can you buy externally? All those factors come into play when selecting a security analytics provider. Almost every information security team in this industry complains about not having enough talent or the right types of talent. It may be important for you to select a platform that has low operational overhead and enables rapid out-of-the-box (OOTB) connectors, features, and use cases. If you're adopting a cloud strategy, consider platforms available such as Software-as-a-Service (SaaS) or a managed security service provider (MSSP).

TIP

Securonix provides flexible deployment options such as on-premises, Cloud (SaaS), and MSSP-partner operated. Securonix also provides comprehensive OOTB content delivered via its threat library to enable rapid deployment and quick time to value.

Consider All Your Cloud Assets and Applications

We live in a perimeter-less IT world; firewalls and network security controls are no longer sufficiently protecting your data. You need controls where the data sits — in your application and your cloud assets. Your company's collection of cloud assets is critical to your selection of a security analytics platform. Obviously if your company is 60 percent cloud hosted, it would be incredibly shortsighted to pick a solution that can only integrate with servers hosted within your company walls.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TIP

Securonix provides customers an option of fully managed SaaS deployment with robust integration with numerous cloud infrastructure, data, application, and access providers. The direct application programming interface (API) integration ensures you get visibility to all your cloud data, assets, and users. Don't let lack of cloud integration be a reason to fly blind in security.

Compare and Contrast Your SIEMs

Apply the same care to the selection of a new cloud SIEM that you would apply to choosing a house or a car. Know what features and capabilities are most important to your organization, rank them in order of importance, and evaluate each choice based on these criteria. If you need help with this process, check out the sample framework in Chapter 6.

Identify and Prioritize Your Use Cases

Your legacy SIEM has deployed use cases that will be required after the migration to the cloud. Likewise, your new cloud SIEM will have capabilities that will be essential after the move too. Identify what these are early in the migration process. Just as moving from one house to another is a great time to get rid of the old air hockey table and the treadmill no one uses, migrating to a cloud SIEM shouldn't be simply a matter of trying to replicate exactly the capabilities of your current SIEM.

Triangulate business risks and credible threats into a use case prioritization engine for a more comprehensive look into your environment from a business risk and threat standpoint. Knowing these two things in addition to your available use case potentials is key to making security analytics active.

TIP

Securonix provides packaged applications with built-in use cases for advanced cyber threat, insider threat, cloud security, and fraud. The packaged content enables you to deploy use cases with minimal overhead and get quick value for investment. To explore Securonix application options, visit `www.securonix.com/products/security-apps`.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Stagger Your Migration

Migration of your SIEM may take between 8 and 26 weeks and will go through several phases, including planning, design, implementation, deployment, and operationalizing (which includes training, go-live, and hand-over).

Even after the new cloud SIEM is operational, it's common for an organization migrating to cloud SIEM to have a lengthy period of overlap where both the legacy on-premises SIEM and the cloud SIEM are running simultaneously. In some instances, this may even be an optimal solution, because of regulatory or other constraints, and the two SIEMs can be managed and searched using a unified interface through the use of a federated SIEM model (see Chapter 4).

TIP

Securonix migration teams have specific migration guidelines and technical procedures in place for requirements such as migrating settings, policies, and other critical assets from other SIEM solutions. To learn more about Securonix's migration process, download the SIEM Migration Planning white paper at `https://www.securonix.com/resources/siem-migration-planning`.

Define Your Deliverables for Each Stage

Because your migration to a cloud SIEM is likely going to happen in stages, make sure to define deliverables and success criteria for each stage. These deliverables serve as both progress indicators as well as the required inputs for the next stage. For example, the result of the planning stage should (obviously) be a plan of action. This plan of action then shapes the design of the new SIEM, implementation, and so on.

Define Operational Processes

Know what activities will be required both for migration to the cloud SIEM as well as for day-to-day operation, and create a responsible, accountable, consulted, informed (RACI) matrix to ensure that what needs to get done gets done and the proper people are consulted and informed. See Chapter 5 for a sample cloud SIEM RACI matrix.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Train Your Users

Even the best systems can't be fully successful without the right training for those who will use it. Everyone learns differently so provide a variety of ways for your users and administrators to engage. Examples include

- A hands-on class or lab
- Reading (providing a manual)
- Videos
- On-the-job training or having a peer assistant

Formulating a mix of these options and having ongoing training and continuing education are key to the growth and progressive maturity of your staff and overall capability.

TIP

Securonix, through its global education program, provides classroom and online training courses to customers and partners. You can check out Securonix's training options at www.securonix.com/services/training.

Establish Benchmarks

The performance and effectiveness of any kind of data-intensive operation, such as SIEM, can be measured and judged based on standard benchmarks. Examples of benchmarks you can apply to SIEM are Mean Time to Remediate (MTTR), accuracy rates (or number of false positives), and events per second.

Plan the Next Step

Ready to get started with planning your migration to cloud SIEM? Securonix can help. You can also download the SIEM Migration white paper for more information. Visit https://www.securonix.com/resources/siem-migration-planning.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

securonix

Security Analytics at Cloud Scale

Securonix breaks the rules of traditional SIEMs with analytics-based threat detection, cloud-native architecture for effective, scalable cloud monitoring, and simplified management with an as-a-service model.

For more information: **www.securonix.com**

Follow us @securonix

©2021 Securonix. All rights reserved.

These materials are © 2022 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Respond to threats with cloud-scale analytics

Today, data is exploding. Enterprises generate terabytes of data across a multitude of sources. Collecting and analyzing this data to identify actionable threats is like finding a needle in a haystack. Traditional SIEM solutions fail, but cloud-based security analytics leverages the power of machine learning and the scalability of the cloud to analyze data at scale and detect "real" threats. This book helps you understand the tenets of cloud SIEM and strategies to evaluate and adopt it in your environment.

Inside…

- Challenges with traditional SIEM
- The evolution of security analytics
- Leveraging cloud capabilities to scale SIEM
- Strategy to adopt a cloud SIEM

securonix

Chris Minnick has been a software developer, author, trainer, and consultant for 20+ years and trains software developers and network administrators in the world's largest companies. He's written or co-authored over a dozen books, including *JavaScript For Dummies* and *HTML5 and CSS3 For Dummies.*

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

ISBN: 978-1-119-85373-2
Not For Resale

9 781119 853732

for dummies®
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.