Definitive Guide™ to SOAR

How to stop threats faster with security orchestration, automation, and response

Crystal Bedell

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to, and neutralizing damaging cyberthreats. The LogRhythm NextGen SIEM Platform combines user and entity behavior analytics (UEBA); network traffic and behavior analytics (NTBA); and security orchestration, automation, and response (SOAR) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) framework serves as the foundation for the AI-enabled security operations center (SOC), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won many accolades. For more information, visit logrhythm.com.

Definitive Guide™
to
SOAR

Crystal Bedell

CYBEREDGE
PRESS

Definitive Guide™ to SOAR

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

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

ISBN: 978-1-948939-02-7 (paperback)
ISBN: 978-1-948939-03-4 (eBook)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from LogRhythm: Rob McGovern, Manager, Technical Product Management and Seth Goldhammer, Senior Director, Product Marketing

Table of Contents

Introduction

Cybersecurity organizations have their work cut out for them. As the last line of defense in the fight against cyberthreats, they stand between their corporations' valuable IT assets and cyberattackers. But these attackers aren't social outcasts emailing viruses from their parents' basement.

Today's cyberattackers are more formidable and more sophisticated than ever before. Attackers are resourceful and ruthless in their efforts to steal data, commit fraud, abuse resources, and disrupt services. They're also patient and have the power of numbers. Attackers share data and invest in research and development. They are nation-states and organized crime rings with power and motive.

Cybersecurity professionals generally understand that it's impossible to prevent every cyberattack. Implementing a robust defense-in-depth strategy, while still necessary, is not the be-all and end-all of cybersecurity. As a result, organizations are adjusting their focus to include rapid detection and response, and speed is the name of the game. How quickly can the team detect a legitimate threat and shut an attack down? The faster it can detect and respond, the lower the risk of data exfiltration, financial fraud, and service disruption.

Working accurately and quickly when the corporation is at risk and tensions are high is no easy feat, but it can be done, and this book will show you how. If you or your colleagues are tasked with protecting IT assets against cyberthreats, then this book is for you.

Chapters at a Glance

Chapter 1, "Understanding the Security Operations Center," explains the role of a SOC in fighting advanced cyberthreats and the challenges of building one.

Chapter 2, "Introducing Security Orchestration, Automation, and Response," introduces SOAR capabilities and how they work within a SIEM solution.

Chapter 3, "Deconstructing SOAR," outlines the main components of a SOAR solution.

Chapter 4, "Diving into Orchestration," explains the role of orchestration in a SOAR solution and how it is implemented in the form of case management and playbooks.

Chapter 5, "Understanding Automated Response," explores the power of automation in a SOC.

Chapter 6, "Exploring Common SOAR Use Cases," examines how SOCs leverage SOAR capabilities to improve operational efficiencies and reduce cybersecurity risk.

Chapter 7, "Unleashing the Full Power of SOAR," highlights the benefits SOCs can realize when they implement SOAR capabilities.

Chapter 8, "Buying Criteria: What to Look for in a SOAR Solution," reviews must-have features and capabilities to look for when evaluating SOAR solutions for your SOC.

Helpful Icons

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

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

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

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

Chapter 1

Understanding the Security Operations Center

In this chapter

- Examine the role of the security operations center (SOC) in detecting advanced cybersecurity threats
- Understand the challenges of building an effective SOC
- Review the characteristics of a well-run SOC

The cybersecurity landscape is continuously evolving. Every improvement in security results in an improvement in malware to subvert that security. Modern malware bypasses traditional preventative technologies, moves laterally in unexpected ways, sits dormant for long periods, and may take countermeasures against easy or simple detection processes. Modern attackers use a wide range of techniques to exfiltrate data, disrupt services, commit fraud, or simply steal resources. The longer organizations go before detecting malware, the more time attackers have to reach their objectives and exploit systems.

You Need an Effective SOC

In response to modern cybersecurity threats, many companies are creating a *security operations center* (SOC), an organization responsible for managing the security of the company. The SOC is comprised of a team that can be local, distributed, multi-talented, or multi-departmental.

Simply creating a SOC raises cybersecurity to a level that increases visibility and ownership. After all, it's easier to

fund a SOC than it is to support a single analyst trying to do "extra work."

An effective SOC operates around the clock and has analysts who have the tools and processes they need to respond to threats. Continuous monitoring and analysis of network activity help ensure that security incidents are detected and contained in a timely manner, thus reducing the risk of data exfiltration.

Putting the 'O' in SOC

The operational process for addressing threats consists of the following:

1. A *security information and event management* (SIEM) system collects, parses, and enriches forensic log data.
2. The SIEM performs machine analytics to look for potential issues that qualify as a security event.
3. When the SIEM identifies a security event, it raises alarms for human analysis and response.
4. A security analyst triages alarms by adding context, evaluating risk, and determining impact.
5. A security analyst resolves alarms by mitigating the issue.
6. A security analyst reviews and modifies security controls where needed to prevent the same event from reoccurring.

Building an Effective SOC Isn't Easy

Any business can benefit from a well-run SOC, but building a SOC that is both efficient and effective requires a foundation of people, processes, and technology. Putting these three elements in place and getting to a point where the SOC runs like a well-oiled machine takes time, effort, and budget. Of course, there are countless challenges along the way.

Business challenges

It's hard to imagine a business scenario where cost *isn't* an issue. However, security leaders have it tougher than most. Security is often perceived by upper management and executives as a cost center. Resources going into the organization don't increase profits. Unless the business suffers a data

breach or regulatory compliance violation — and has thus seen the repercussions of inadequate security firsthand — then chances are good that security leaders have to fight for every penny.

With a limited budget for hiring personnel, many security leaders simply can't afford to fully staff a SOC, never mind purchase technology solutions that need to be managed by these personnel.

Therein lies another challenge. It's difficult to prove the security organization's value when success means that nothing bad has occurred. But consider: can your company afford a two-year trial, over $100 million in fines, and millions more in legal fees resulting from a typical breach?

Operational challenges

Depending on the number of devices, systems, and applications in an environment, a security team may receive thousands of logs per second, hundreds of events per hour, and dozens of alarms per day. With a giant haystack of data, an analyst needs a tool to help organize the hay and find the interesting needles. The goal of a SIEM solution is to help organizations collect and classify the hay while highlighting possible needles.

SIEMs are intended to serve as an organization's security hub, gathering data from other devices and analyzing it all to identify real threats that require a response. Thus, SIEM solutions are supposed to reduce the overall "noise" and false positives generated by the devices on the network.

Anyone who has experience with a SIEM solution knows that the noise and false positives have increased — not decreased. This increase in noise is a result of IT environments generating more and more data. SIEMs must perform threat detection by connecting multiple, disparate activities. Unfortunately, SIEMs are not always able to differentiate between high- and low-risk threats, and false positives and harmless anomalies. As a result, these solutions often perpetuate the problem they were intended to solve. They fire off a tremendous number of unqualified security alerts, resulting in alarm fatigue.

Staffing challenges

In its annual global survey on the state of IT, the Enterprise Strategy Group asks respondents to identify areas in which they have a "problematic shortage" of skills on an annual basis. Since 2014, respondents have consistently answered that a shortage of cybersecurity skills is their greatest problem.

What's more, every year the percentage of respondents who claim a problematic shortage of cybersecurity skills has increased. In 2018, 51 percent of respondents identified a lack of cybersecurity skills as being problematic — more than double the percentage in 2014. This suggests that the cybersecurity skills shortage is getting worse.

A scarcity of cybersecurity talent bodes poorly for everyone involved. A short-staffed SOC simply can't operate effectively. To begin with, there are too many manual tasks that can pull analysts' focus away from more important work. Instead of threat hunting, or qualifying or investigating threats, seasoned analysts are doing the work of a Tier 1 analyst. If analysts are overwhelmed by the sheer volume of data and alerts, then they can only reactively investigate events. Meanwhile, newer analysts lack the skillset to accurately interpret data. An inexperienced analyst may miss valuable clues, and therefore, come to incorrect conclusions that result in wasted time and effort chasing down the wrong thing.

All of these issues contribute to rapid staff turnover. No one likes to be mired in work they've outgrown or to receive more responsibility than they're ready for. Analysts are likely to burn out from stress and a lack of personal fulfillment, leading them to look for work elsewhere. In addition, the market is so hot that even a half-trained analyst can find another job, often at a higher pay rate! If organizations aren't losing analysts to fatigue, then they're losing them to the broader market.

Rapid employee turnover in the SOC leads to myriad other problems. It's difficult to establish consistent and effective incident response procedures when staffing is constantly in flux. The SOC gets stuck in a vicious cycle of hiring and training. It can't progress past rudimentary processes and reactively investigating threats. Meanwhile, the industry as a whole suffers from a continual churn of seasoned analysts who

are overworked and underutilized, and newbies who lack the experience they need to bring value to their employers.

Organizational challenges

The structure within IT organizations also makes it difficult for SOCs to work efficiently and effectively. The IT organization often consists of disparate teams with distinct responsibilities. The infrastructure, security, development, help desk, and operations teams often work in parallel to one another, with very little coordination or communication.

Even though each of these groups may function in a silo, the systems and devices they manage do not. Inconsistencies and inefficiencies are issues across the organization because of ownership, control, and access levels. The group that has ownership over a system does not necessarily have the control or access to make changes to the system, or vice versa. For example, if a user account is suspected of being compromised, a security analyst in the SOC can't disable it if IT retains full control over Active Directory. The analyst must go through the proper communication channels (if they have been established) and separate ticketing systems (if they exist) to request disabling the account, and hope that the recipient responds in a timely manner. Meanwhile, the time to resolve the suspected threat grows longer and longer.

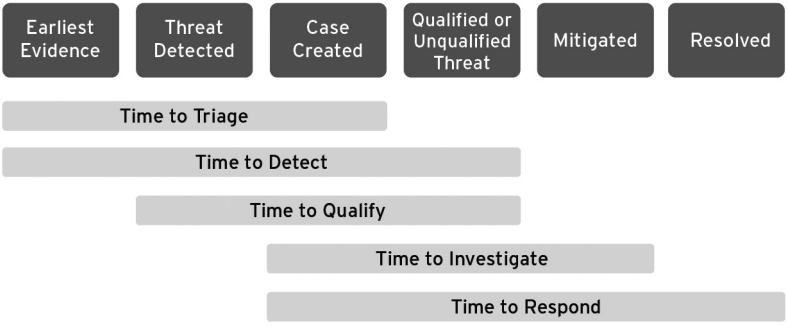

Figure 1-1: The stages of the security operations process are important milestones to measure when determining a SOC's effectiveness.

Characteristics of a Well-run SOC

What does a well-run SOC look like? An efficient and effective SOC measures and reduces the following metrics, as shown in Figure 1-1:

- Mean time to triage (MTTT): The MTTT is the average amount of time it takes to parse security data and generate an alert.
- Mean time to detect (MTTD): The MTTD is the average amount of time it takes for the SOC to discover a potential security incident. The faster the SOC detects an attack, the sooner the SOC can shut it down.
- Mean time to qualify (MTTQ): The MTTQ is the average amount of time it takes for the SOC to determine that a security alert is a true positive (rather than a false positive) and requires mitigation.
- Mean time to investigate (MTTI): The MTTI is the average amount of time it takes for the SOC to study and understand a threat so that it can determine how best to mitigate it.
- Mean time to respond (MTTR): The MTTR is the average amount of time it takes for the SOC to shut down an attack. A SOC's ability to stop an attack in a timely manner helps reduce security risk.

A well-run SOC also demonstrates the following characteristics:

- Efficient incident response workflows. Processes and procedures are outlined in advance of an incident with tasks clearly defined. Team member responsibilities are also defined so tasks can be assigned quickly and accurately.
- Repeatable processes and procedures. Incident response workflows are consistent. Security analysts and incident response teams follow the same steps for similar incidents.
- Optimized automation. As many tedious, manual tasks are automated as possible, thereby freeing analysts to work more efficiently and focus on more-complex tasks.
- Consistent reporting. Reports on the metrics described earlier enable SOC teams and management to monitor SOC efficiencies and measure improvements.

The Missing Pieces

While it would be nice if SOCs didn't have to deal with the challenges previously described, the fact of the matter is that these challenges never completely go away. For one thing, security leaders will always contend with resource constraints. The IT organization is unlikely to undertake an organizational overhaul just to suit the needs of the SOC. That said, it's not impossible to build an effective and efficient SOC. Security leaders just need to think pragmatically about what it takes to create one:

- ☑ *Create defined workflows to train and guide analysts*. Defined workflows guide analysts through a consistent, repeatable process when responding to a cybersecurity threat. This structure ensures that analysts don't miss any steps and helps the SOC scale by enabling new and Tier-1 analysts to carry out the same processes as more-advanced analysts.
- ☑ *Implement automation to reduce the effort required to manually add context, analyze, and respond to threats*. The low-level, manual tasks that pull analysts away from higher-level work need to be automated. Even processes with actions that must be approved before they can be executed should be automated as much as possible. With manual work reduced, analysts can focus on complex incident response that requires skill and creativity.
- ☑ *Leverage case management to keep track of actions, activities, and needs*. Case management enables organizations to greatly improve the maturity and efficiency of their security operations and incident response efforts. The case file serves as a centralized place to collaborate as well as an archive of all the information related to previous investigations. It makes it easy for analysts to create and track remediation and recovery efforts during a threat investigation. Thus, case management assists teams with their regulatory compliance efforts, as compliance mandates are increasingly requiring incident response tracking. Finally, by streamlining investigations, case management helps teams resolve incidents more quickly.

- ☑ *Use ticket management to help expedite threat mitigation and incident response*. Analysts and incident responders can easily submit help desk tickets for IT support tasks that are part of the response workflow.
- ☑ *Monitor metrics to evaluate effectiveness*. Security leaders have likely heard the saying: "If you can't measure it, you can't improve it." A SOC needs metrics and reports on MTTD and MTTR to help teams work more efficiently and reduce the risk posed by security threats already on the network.

This extensive list shouldn't imply that achieving efficiency and effectiveness is wishful thinking. It just means that SOCs need a little bit of help. Fortunately, that help is available in the form of *security orchestration, automation, and response* (SOAR).

Chapter 2

Introducing Security Orchestration, Automation, and Response

In this chapter

- Learn about SOAR and its value to the SOC
- Understand the relationship between SOAR and SIEM solutions
- Review capabilities of a next-generation SIEM solution

SOCs that struggle with resource constraints and longer-than-ideal response times can benefit from security orchestration, automation, and response (SOAR). SOAR technologies collect security data and alerts from myriad sources, identify alerts that require a response, and drive measurable, standardized workflows for executing responses in an efficient manner.

SOAR to the Rescue

SOAR makes the security analyst's job easier and more efficient by automating workflows and accelerating threat qualification, investigation, and response processes. SOAR often integrates with other technologies to provide event context that enables analysts to more rapidly identify the scope and root cause of an incident or breach. Through efficiency and integration, SOAR capabilities facilitate higher-

quality incident response and optimize analysts' workload by reducing manual tasks and increasing consistency of the process. SOAR also provides a framework for metrics to evaluate the SOC and enable continuous training and improvement.

SIEM, meet SOAR

At this point, it's logical to ask: what is the relationship between SOAR and a security information and event management (SIEM) system? SOAR capabilities either sit within or on top of a SIEM (as a standalone component). Next-generation SIEMs, which have evolved from traditional SIEMs, often have SOAR capabilities built in.

As SIEMs became better at recognizing real threats, solution providers saw the opportunity to add purpose-built, coordinated, and automated workflows to their SIEMs. Combining risk-based monitoring and alerts with task automation and orchestration to enact countermeasures helps protect a company from cyberattacks and expands the SIEM mission. If that sounds a bit like SOAR, that's because it is. The result is a next-generation SIEM with integrated SOAR capabilities.

Tomorrow's SIEM, today

But that's not all. It's important to note that SIEM technology is ever evolving. The goal for SIEM providers is to develop a dynamic platform that provides actionable insights based on advanced analytics, data forensics, and incident response capabilities. As shown in Figure 2-1, these capabilities will be made possible through a powerful collection of core competencies:

- ☑ Real-time user and application monitoring
- ☑ Threat intelligence generation and consumption
- ☑ User and entity behavior analytics (for more on UEBA, see sidebar on page 12)
- ☑ Advanced analytics for complex scenarios
- ☑ Log management and reporting
- ☑ Streamlined deployment and effective support

It may be difficult to find a next-gen SIEM that can deliver all of these capabilities today, so organizations should look for a solution provider that has a plan to achieve these capabilities over time.

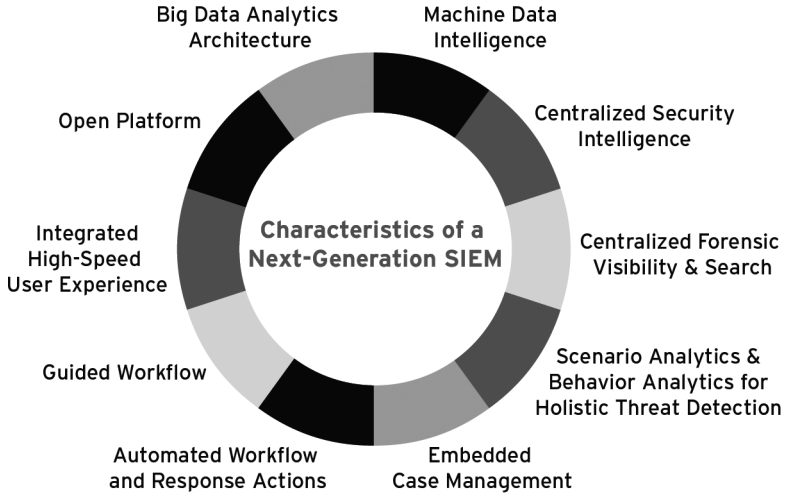

Figure 2-1: A next-generation SIEM provides a number of advanced functions to deliver actionable insights and help SOCs realize a return on investment.

In the meantime, a next-generation SIEM should allow security leaders to accelerate return on investment (ROI). In addition to a low total cost of ownership (TCO) over the life of the SIEM platform, organizations should see greater ROI from their existing technology and staff, thanks to the SIEM's end-to-end threat management capabilities that reduce manual tasks and improve efficiencies. ROI is realized by connecting threat detection, qualification, and mitigation with cohesive workflows and automation.

Understanding UEBA

Next-gen SIEMs that profile user and system behavior can help teams detect threats that are otherwise difficult to identify. User and entity behavior analytics (UEBA) technology uses analytics to establish a baseline of behavior. The technology then monitors user activity data captured in logs, audit trails, and sensors for behavioral changes that might indicate a threat.

UEBA can, for example, help identify malicious insider activity. It's notoriously difficult to detect insider threats due to the fact that they originate from trusted users. However, deviations from baseline behavior as seen in activity data and contextual information can help identify anomalous activity that could pose a threat. Potential indicators include new or unusual system access, unusual login times, and excessive authentication failures.

Next-gen SIEM: (Almost) a Silver Bullet

It's unlikely that there will ever be a single silver bullet for solving all security use cases with ease. However, a next-generation SIEM gets security teams pretty close. Here are some of the capabilities currently delivered by a next-gen SIEM:

Next-gen SIEM Capabilities	Qualifications	Why is this Important?
Data Processing & Normalization	• Flexible data acquisition • Capture forensic data in its native unstructured form • Unstructured data processing • Consistent and normalized view of data	More accurate threat detection of security events and search to visualize disparate data sets
Big Data Architecture	• High-scale indexing • Months- to years-long storage of forensic data	Greater flexibility for scaled growth to support high data velocity, variety, and volume for structured and unstructured search
Scenario & Behavioral Analytics	• Security analytics • Modern machine analytics approaches for scenario and behavior analytics • Accurate visibility into user and network-borne threats	Faster threat detection across the broad spectrum of attacks requiring minimal tuning

Security Orchestration, Automation, and Response	• Integrated case management and task automation functions • Ability to align tasks to observed activities (automated or semi-automated) • Capability to standard SOC workflows with editable playbooks • Enable metrics to be generated to help increase security maturity	Increases efficiency and enables higher quality incident response
Forensic Analysis	• Centralized search • Precise access to forensic data without knowing the underlying data structure • Access to contextual forensic details, including telemetry generated from endpoint and network sensors • Leverage alarms organized by risk levels with guided workflows	Increases efficiency and effectiveness of security teams and enables a low mean time to respond
Open Platform	• Integration with threat intelligence services • Supports IOC threat detection and analyst workflow • APIs allow custom integrations with both administrative and incident response workflows • Data lake capabilities for business applications beyond security	Increases effectiveness and value of next-gen SIEM

Chapter 3

Deconstructing SOAR

In this chapter

- Learn about the different components that comprise SOAR
- Understand the capabilities enabled by case and ticket management
- Analyze the dangers of deploying a standalone SOAR solution vs. a SIEM with integrated SOAR capabilities

SOAR delivers two primary capabilities: incident response workflow management and security operations process automation. Different technologies come together to enable these capabilities and, of course, those technologies vary from vendor to vendor. However, the following components form the core of a SOAR solution.

Workflow and Collaboration Engine

Naturally, a solution designed to support operations must have a workflow and collaboration engine. Well-defined processes and procedures are hallmarks of a mature SOC. A workflow and collaboration engine defines operational procedures and ensures consistent execution of procedures at scale.

Formalized processes in the **workflow and collaboration engine** can have both manual and automated steps. Where tasks aren't automated, the tool should guide analysts to perform the right tasks in the right order to ensure consistency. Where tasks are automated, the engine should ensure successful execution, proper approval and oversight, and formal collection of the results of the automated task.

Security Case Management

When investigating a possible attack, analysts review a variety of information to help understand the nature, intent, and scope of the anomalous behavior. If these efforts — and the data — aren't well managed, they can lead to incorrect conclusions or result in an incident slipping through the cracks. Case and ticket management helps SOCs manage and track the multi-step incident response and investigation processes, as well as the output they generate.

By nature, security teams are involved in topics sensitive to their organization because of their investigation into potential compromises or breaches. As a result, security teams recognize a need to control information and communications regarding evidence collection. Sometimes, the evidence collection and response even need to be hidden from the IT organization, especially when an administrative user is suspected of wrongdoing. Security teams find value in a technology separated from IT ticket management systems that allows for team coordination, evidence collection, and communication about security case progress or findings.

Integrated case and ticket management enables organizations to protocolize incident response workflows and provides consistent investigative tools throughout the incident response process. Thus, case and ticket management helps SOCs increase efficiencies throughout remediation and recovery, thereby minimizing their MTTD and MTTR.

Collection of forensic evidence and annotations also helps expedite threat detection and response. Forensic evidence may include firewall logs, memory dumps, infected files, suspicious emails, or exact copies of a complete drive. Storing all this data and the conversations around the data together makes it easier for an analyst to keep track of an investigation, identify a root cause, and gauge the scope and severity of an attack.

Users can easily store investigative artifacts in a secure, central evidence repository. This simplifies the identification and collection of evidence, and enables users to more quickly qualify a threat and understand its root cause and scope. Artifacts can include internal information from a dashboard, alarm, or search result, or external evidence like a screen capture. When

a case opens in the SOAR, an artifact can be added to the repository in one click. Analysts can restrict access to ensure confidentiality. And they can track all case activity to provide a tamper-proof audit trail.

Case and ticket management often supports:

- ☑ Case playbooks for incident management
- ☑ Case tasks with automated due dates
- ☑ Tagging and workflow customization
- ☑ Group collaboration supporting tiered operations
- ☑ Threat intelligence and contextual lookups
- ☑ Real-time feed of investigation and response activities
- ☑ Customizable dashboards, including multi-case task views
- ☑ REST API for third-party integrations
- ☑ Metrics and reports on MTTD, MTTR, time to qualify (TTQ), and time to investigate (TTI)
- ☑ Automated and approval-based execution options for task automation, including support for multi-party approval chains

Orchestration and Automation

Orchestration and automation are two separate capabilities that work together. Orchestration focuses on determining the steps necessary to achieve an operational goal, including chaining together the results of each step and providing for alternative paths and feedback-driven approaches. Automation focuses on providing context, executing remediation, or removing repeatable manual efforts that impede effective orchestration.

During incident investigation and response, SOCs use and refer to multiple tools. These can be external, online services like a service portal or sandbox, as well as tools deployed internally like SIEM and endpoint detection and response

(EDR) systems. As analysts work between these tools, they often have to copy and paste data from one user interface to another. This manual work is both inefficient and risky — analysts, especially when under pressure to respond to an incident, can easily make a mistake or forget to include critical data in a case log.

An orchestration engine serves as a centralized hub that connects the various tools through their inputs, outputs, and APIs. This integration facilitates automation. The orchestration engine moves data from one tool to another, as defined by a process, automating as many actions as possible and prompting analysts to perform actions that are not automated.

There's more to say about orchestration and automation, so we'll cover these in greater depth in Chapters 4 and 5, respectively.

Threat Intelligence Management

Threat intelligence plays an important role in incident investigation and response. Threats are dynamic and attack vectors change constantly. Analysts can respond more quickly and minimize damage in their environment if they understand how threats are behaving. For example, they can immediately learn about dangerous IP addresses, files, processes, and other risks in their environment based on what's happening on the Internet at large.

Don't SOAR Alone

As we mentioned in Chapter 2, there are various ways to deploy SOAR capabilities. SOCs can deploy a dedicated SOAR solution or implement a SIEM solution that has fully built-in and integrated SOAR capabilities. While it might be tempting to deploy a dedicated solution (especially if the organization already has a SIEM), an integrated solution is almost always the better choice.

One of the primary benefits of SOAR is integration of disparate technologies that exist both inside and outside the organization. This capability helps teams respond to threats faster because all the information they need is in one place. It also reduces the risk of human error and the time analysts spend moving between tools because they can do all their work through one unified interface.

Unfortunately, when teams choose a standalone SOAR solution, they miss out on some of these benefits. They also incur additional costs:

- Integration and maintenance: More time and effort are required to simply keep the data flowing from the SIEM to the SOAR system.
- Training: Analysts must learn two completely different tools and user experiences. Training must be continuously renewed as staff changes occur.
- Administrative/support: Organizations must support two systems instead of one, often with different purchasing, maintenance, and upgrade schedules!

Bottom line: By optimizing the SOC's efficiency and effectiveness with a SIEM that features integrated SOAR capabilities, organizations can increase their ROI and reduce their TCO.

SOAR empowers analysts with a variety of threat intelligence data, as shown in Figure 3-1. Threat intelligence management incorporates threat intelligence feeds from open source providers, as well as the various commercial providers within the SOAR vendor's partner ecosystem. By integrating this data with the machine data collected throughout the organization, SOAR can generate highly contextualized security intelligence. This threat context can accelerate detection of and response to:

- ☑ Dangerous IPs accessing internal infrastructure
- ☑ Users visiting risky URLs

- ☑ Phishing attempts
- ☑ Malware propagation

Known Attacks	Botnets	Associated with Fraud	Associated with Malware	Used for Phishing	Suspicious
• IP Addresses • URLs • User Agents	• IP Addresses • URLs	• IP Addresses • URLs	• IP Addresses • URLs • User Agents • Processes • File Paths • File Names	• IP Addresses • URLs • Email Addresses • Email Subjects	• IP Addresses • URLs

Figure 3-1: Threat intelligence providers in the SOAR vendor's partner ecosystem can deliver different types of threat data.

Playbooks

Following a *playbook* (sometimes referred to as a runbook) helps ensure that the SOC responds to specific threats the same way every time. A playbook is a standard, documented process that details repeatable steps for responding to specific types of incidents. A playbook can be thought of as a checklist. And who doesn't benefit from a checklist — especially when tension is high, as it often is during a security investigation?

Playbooks enable consistent, predefined responses to threats by providing a guided workflow and executable best practices to lessen analyst workload and improve SOC efficiency and efficacy.

SOAR solutions come with prebuilt playbooks for common threats. However, these out-of-the-box playbooks often require customization by analysts to align with their organization's internal operations processes. Analysts can also create their own playbooks from scratch, or adopt playbooks developed and shared by other organizations.

We'll talk about playbooks further in Chapter 4, "Diving into Orchestration."

Unified Dashboards

The inner workings of a SOAR solution are complex. There's a lot going on under the hood. It's therefore critical that analysts are able to interact with the SOAR solution and perform tasks through a user-friendly, customizable dashboard.

SOCs should have the flexibility to either view data, tasks, metrics, and workflows in a single, unified dashboard or to create multiple dashboards for specific use cases. For example, the team might have one dashboard for "work in progress," one for "high-risk monitoring," and another for "HIPAA compliance." Either way, the dashboard should allow users to access all applicable data, and that data should be displayed in a task-oriented fashion.

Through a dashboard, analysts and incident responders can:

- ☑ Filter and sort cases based on specific incidents, status, case owner, and age
- ☑ Easily add playbooks, escalate a case, set a priority, and assign an investigator
- ☑ Search or filter by case tags and view a timestamped news feed of all completed actions

A dashboard also provides much-needed visibility into the environment and SOC operations. Security organizations traditionally lack centralized visibility into the enterprise IT and OT environments, which makes it difficult to corroborate data to identify threats and secure the whole environment.

A single interface that contains all critical security detection and response functionality provides a holistic approach for effectively reducing risk, creating cohesive workflows, improving SOC efficiency, and increasing ROI.

Running Lean – and Mean – with a Next-gen SIEM

Running a lean IT department is one thing. Empowering that IT team to work efficiently and effectively is quite another. An IT asset recovery solution provider found that a next-gen SIEM was just the tool it needed.

The solution provider's IT team oversees IT operations for nine dedicated production facilities, corporate offices, more than 40 field workers, and numerous international partners. Prior to correlating system activities related to operations, the team used about 10 different tools for reading logs.

"Plain and simple, we needed a better way to troubleshoot IT issues," says the IT manager. "It was painful to sit through all the logs to get an understanding of what was going on with our systems."

The company had previously deployed LogRhythm to meet security and compliance needs. But after seeing the LogRhythm NextGen SIEM Platform in action, the IT manager decided to use the platform to improve operational processes, as well. Now, every source of activity logs is fed into the SIEM, giving the team all the data it needs in one location to troubleshoot operational issues. The team has also set up alerts that indicate an emerging situation before it turns into a real issue.

The most critical example of an early warning alert comes from the server room and some troublesome A/C units. The Syslog output from the system that monitors the temperature in the data center feeds into LogRhythm. If the room temperature starts to increase, an alert goes off, triggering an email to the on-call team. Someone can quickly respond to the situation before the rising temperature can cause an outage.

The insights from LogRhythm also enable the team to address other operational challenges, such as server failures. The terminal servers used by remote users would frequently fail, grinding work to a halt. LogRhythm provided the visibility the IT team needed to discover that the externally facing terminal servers had been experiencing numerous and frequent cyberattacks for years.

LogRhythm now alerts on any unusual or suspicious activity on these servers so that attacks can be rebuffed and outages prevented. "We have actually decreased downtime because we now have alerts and good, insightful data," says the IT manager. "We've stopped attacks on our terminal servers because of alerts generated from LogRhythm as precursors to bad stuff happening."

Chapter 4

Diving into Orchestration

In this chapter

- Understand the role of orchestration in a SOAR solution
- Learn why case management is a key component of orchestration
- Explore the benefits of playbooks

Just as a coach orchestrates the play of a soccer team, a SOAR solution guides the myriad tasks involved in security processes so that all members of a SOC function as a unit working toward the same end.

What Is Orchestration?

Orchestration is about bringing together pieces that are related to each other and aligning them for maximum efficiency and mission success. Whether in cybersecurity or on a soccer field, orchestration creates something that is greater than the sum of its parts.

In the context of information security, orchestration coordinates the various tasks involved in threat analysis and response:

- ☑ Collecting data
- ☑ Analyzing data
- ☑ Acting on the analysis
- ☑ Logging the results

Orchestration employs a set of integrated features that includes case management, playbooks, and contextualization and enrichment.

Case management

In the context of SOAR, *case management* is a means of keeping track of the various moving parts related to the investigation of a specific security event or incident (i.e., a case). As shown in Figure 4-1, case management encompasses the entire threat lifecycle.

Case management can do wonders for a SOC. By optimizing workflows and providing consistent investigative tools, case management helps SOCs more effectively and efficiently complete critical tasks while ensuring that nothing falls through the cracks. Case management helps streamline investigations and expedite incident resolution. As a result, organizations improve the maturity and efficiency of their security operations and incident response efforts.

Threat Detection	Case Creation	Investigation	Collaboration	Mitigation & Response
Case Management can be started from any concerning activity or high-impact event.	A Case can be created with one click, streamlining threat qualification within the incident response process.	Following an assigned playbook, a Case can be updated throughout the UI to include relevant alarm details, log data, and notes.	Case tasks enable multiple level security operations teams to divide responsibilities to best leverage differing skill sets and expedite incident response.	Automate countermeasures that mitigate risks presented by the threat and review incident details to eliminate future exposure.

Figure 4-1: A case management workflow extends through the entire threat lifecycle.

Playbooks

Whether the organization considers them playbooks, checklists, or runbooks, their function is the same: to provide a defined set of actions for incident management. A *playbook* is

a standard, documented process that details repeatable steps for responding to specific types of incidents. A playbook provides guidance in times of crisis and consistency in operation. In essence, a playbook is built-in documentation describing how to execute case management for a particular type of incident. The playbook itself is version controlled while the work items within the playbook are traceable on a per incident basis.

Most SOCs have some playbooks in place. The most common playbooks address:

- ☑ Phishing attacks
- ☑ Employee termination
- ☑ Suspicious host investigations
- ☑ Unauthorized access investigations
- ☑ Data loss investigations
- ☑ Malware outbreaks
- ☑ Regulatory breaches
- ☑ Critical system failures
- ☑ Disaster recovery
- ☑ Phone trees
- ☑ Emergency management

A physical playbook is a static document disconnected from the data that kicked it off, whereas a playbook in a SOAR solution is dynamic because it's integrated with rich tools, dashboards, data, and automation. Think of it as the difference between a paper checklist and a fully integrated software workflow. A playbook allows organizations to:

- ☑ Add due dates, assignees, and notifications to tasks
- ☑ Add automation, branching logic, or attachments
- ☑ Version the playbook

- ☑ Investigate which version was used to respond to a specific incident in the past
- ☑ Integrate the playbook in tools
- ☑ Generate and report on statistics
- ☑ Meet mandatory compliance requirements

Playbook automation

A playbook, as shown in Figure 4-2, helps ensure a consistent, productive, and accurate investigation by spelling out, step-by-step, how analysts should respond to specific threats. That's not all. SOAR takes the concept of a playbook a step further by adding automation.

A playbook accelerates investigations by automating context enrichment and approval countermeasures. Analysts can enable actions to be executed automatically, without user intervention, or they can configure tasks to follow appropriate approval channels. Contextual automation also allows personnel to analyze data presented within SIEM dashboards and investigations.

Automation removes remedial and/or mundane tasks, freeing analysts to focus on more complex aspects of the investigation. The playbook provides prescriptive guidance, so analysts always know what to do next, making it easier to collaborate on and prioritize multiple cases.

Benefits of a playbook

Playbooks are a powerful component of SOAR. They enable greater efficiency and consistency in incident response processes, and provide a number of benefits to a SOC.

Playbooks improve SOC efficiency

Playbooks allow SOCs to scale and accelerate their security investigations and incident response. Analysts and incident responders can focus on the task before them with confidence that they are doing the right thing. They can also delegate tasks to the appropriate staff members.

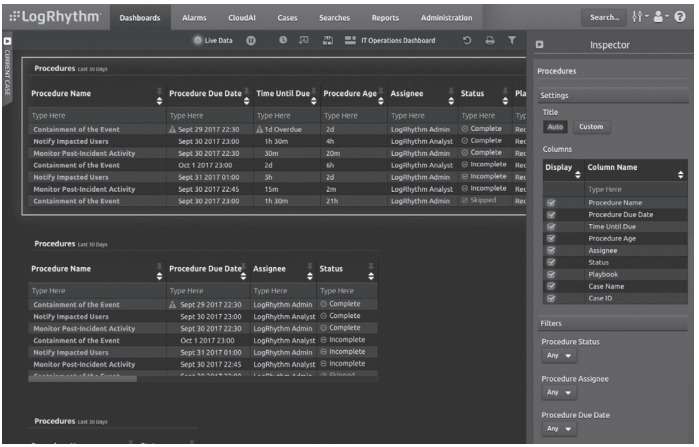

Figure 4-2: Playbooks provide defined steps to follow when resolving a case.

Similarly, less experienced staff can pitch in because processes are detailed step by step. This frees up time for security analysts to perform more advanced and complex investigations and proactive exercises (e.g., threat hunting).

Playbooks reduce cognitive load in a crisis

During high-stress scenarios it's not unusual for humans to forget the simplest of procedures or make mistakes. They can waste valuable time and energy trying to determine what must be done and second-guessing what *has* been done. Playbooks provide structure and assurance that analysts are following the right steps in the right order. Everyone follows a process that was carefully thought through when all was calm.

Playbooks make it easier to train newbies

Analysts can customize prebuilt playbooks to fit within the organization's workflows, while aligning with industry-standard best practices. Adhering to best practices makes it easier to train new team members and get everyone working at the same level. The workflows should seem familiar to team members, as they're essentially the same workflows taught during security certification training.

By providing a repeatable workflow, playbooks enable organizations to accelerate their investigations and responses, no matter the level of security expertise each team member possesses.

Playbooks improve the maturity of a SOC

Consistent and repeatable processes are hallmarks of a mature SOC. Playbooks provide consistent and repeatable methodologies, as well as a framework for measuring success. Because a playbook defines a set of actions, organizations can measure the time it takes to execute the actions. If a behavior can be measured, then it can be improved! Organizations can also easily document their average response time to phishing (for example), using this metric as justification for more funding or resources.

Playbooks ensure that nothing falls through the cracks

Everyone benefits from a checklist. Playbooks provide a checklist of necessary items to complete before a case can be closed, ensuring that nothing important is overlooked or skipped.

Contextualization and enrichment

Sometimes orchestration requires searching for supplemental information to execute the next step. Pulling in relevant contextual information from both internal and external data sources helps create a more comprehensive picture of what's happening or has happened in the environment. With this improved understanding, analysts make better-informed decisions and thereby resolve incidents faster. The ability to access this information from within the SOAR solution helps streamline tasks such as qualifying threats, determining root cause, and understanding the scope of the threat.

Some of the types of information analysts can gather include:

- ☑ The who, when, and where surrounding an incident. For example, integration with Active Directory can enable automatic retrieval of user data that's presented in the SOAR user interface.
- ☑ Host data from internal inventory systems

- ☑ Threat intelligence data from third-party sources such as IP reputation, URL analysis, and known file hash databases
- ☑ Responses to whois, PING, and traceroute queries
- ☑ Vulnerability status of a host with the ability to trigger immediate scans
- ☑ Reputation results from third-party vendors or public reputation sites like VirusTotal

All of this additional context helps accelerate threat qualification and identify the nature of the threat.

Chapter 5

Understanding Automated Response

In this chapter

- Learn how automation improves SOC efficiency
- Examine different types of execution options
- Review common automation use cases

The No. 1 way to improve a SOC's efficiency is to automate the manual processes and mundane tasks that eat up the staff's valuable time. But automation isn't necessarily about doing *more* things — it's about doing the *right* things to reduce cybersecurity risk.

The Power of Automation

When the SOC detects a compromise, rapid incident response can be the difference between the threat's containment and a damaging data breach. Manual processes increase response times, giving cybercriminals more time to wreak havoc. Automating common investigation and response actions minimizes response times and reduces the organization's exposure, as outlined in Figure 5-1.

Furthermore, teams don't have to spend countless hours automating these tasks. SOAR enables organizations to easily automate common investigation and response actions in minutes — not hours.

	MANUAL RESPONSE VERSUS AUTOMATED RESPONSE	
	MANUAL	AUTOMATED
1	Analyst receives alarm of a possible phishing attack	Analyst receives alarm of possible phishing attack
2	Analyst must evaluate the source domain of the email by opening up a new window and querying an external reputation tool	A case is automatically created with the alarm attached
3	Analyst must open firewall configuration to create new sinkhole rule	The alarm contains reputation data because of an automated task
4	Analyst must open Active Directory tools to disable the affected user	The alarm contains all affected users because of an automated task
5	Analyst must run queries to find any other user who received the email, repeating step 3 for each user	The analyst executes remote automation to change firewall rule and sinkhole the affected domain
6	Analyst must manually create case, copying in all details from all the external tools	The analyst executes approval based automation to block all affected users
7	Manager must manually review case and calculate time to qualify and time to respond	Manager sees progress dynamically and can evaluate time to qualify and respond via a simple dashboard

Figure 5-1: Automating response processes reduces risk exposure.

Flexible execution options

In the context of SOAR, automation means giving software and systems the ability to execute a predefined action. There are times, however, when an organization doesn't necessarily want to trigger an action without an approval. That doesn't mean the action shouldn't be automated — nor should analysts be prevented from approving an automated process. A SOAR solution gives SOCs flexible execution options, like those shown in Figure 5-2, so that they can optimize automation without sacrificing due diligence.

Flexible execution options include:

- ☑ *Automatic execution* means the system is configured to act in a fully automated manner. When a specific activity or behavior occurs, the system reacts and takes action — no questions asked. This capability speeds containment of high-risk threats. Automatic execution is also ideal for reoccurring actions and automated context enrichment actions.
- ☑ *Approval-based execution* means that the system acts after one or more people approve the action. Approval-based execution can be configured for a single approver or a hierarchical chain of approvers before the action triggers. Approval-based executions are ideal for more permanent or drastic actions such as blocking a known internal user or kicking a critical machine off the network.
- ☑ *Analyst-triggered execution* is just that: an action manually initiated by an analyst. A single click within the user interface kicks off instantaneous execution. Analyst-triggered executions are ideal for context enrichment or quick reactions during an investigation.
- ☑ *Remote execution* enables analysts to centrally manage the execution of actions across remote sites. Analysts can invoke actions that trigger locally, but execute globally for incident response. Remote execution actions are ideal for integrating with endpoint detection and response systems on a remote machine, or for managing customer environments in a multi-tenant hosted SIEM.

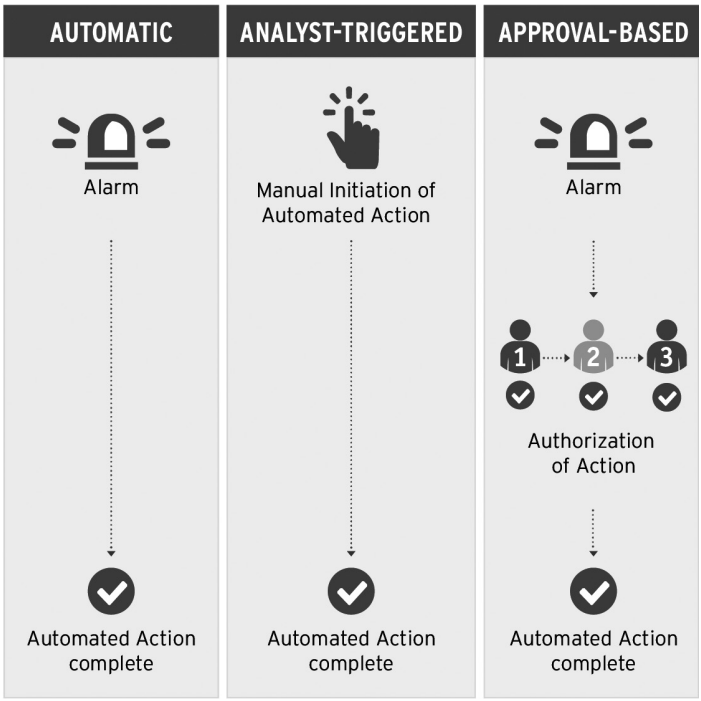

Figure 5-2: Automated responses to suspicious activity can be automatic, approval based, or analyst triggered.

Automation use cases

Pre-packaged, customizable automation makes it easy for analysts to reduce incident response times from days to minutes. Automation use cases, listed in Figure 5-3, are based on playbooks or predefined workflows.

Automation often brings to mind aggressive countermeasures, which some organizations are hesitant to implement. However, automation can also be designed to provide context. This more passive use of automation is ideal for organizations as they become comfortable with automatic task execution. Examples include administrative tasks (automatically opening a case or assigning a playbook) and contextual lookups (checking the reputation of a URL against a threat feed).

Contextualization	Countermeasures & Mitigation
• Upload and scan a file to Cisco ThreatGrid or VirusTotal to see if it contains malware • Query a threat intelligence provider for detailed information on external entities • Perform a lookup to a CSV file • Look up an email address on HavelBeenPwned to see if associated credentials have been compromised	• Block an IP address, port, or URL at the network perimeter • Initiate a forensic dump on a compromised endpoint • End a host process or service • Take a host offline by disabling its NIC • Log off a user • Re-set a user's AD password • Manage users or groups in AD

Figure 5-3: Companies can leverage automated response capabilities to obtain contextualization or execute a countermeasure or mitigation.

More active actions like countermeasures and mitigations imply a maturation as teams become more familiar with the use of automation for specific use cases. Common examples of automation include:

- ☑ *Endpoint quarantine* disables a suspicious device or the port where a suspicious device is located.
- ☑ *User account suspension* disables a user's account access, regardless of what device they use. This action is critical for preventing additional damage caused by a compromised account.
- ☑ *Machine data collection* can be automated so that data, such as process information, additional logs, and/or a forensic image of the drive and/or memory is collected from an endpoint suspected of a malware infection.
- ☑ *Network access suspension* can be invoked in cases of suspected data exfiltration or malware command and control. The automation updates the network infrastructure's access control list to close a network connection and prevent more data from being stolen.
- ☑ *Process termination* can be invoked to kill unknown or blacklisted processes on a device.

☑ *Sinkhole domain* can be configured to block all further access to a suspicious external domain. This type of automation is often used for phishing attacks to mitigate the damage from clicking on a malicious link.

An Additional Advantage of Automation

Integration with third-party systems is key to enabling the wider benefits of automation. Any organization that's attempted to integrate systems knows the headache associated with relying on homegrown integrations or costly consulting services — and then the ongoing issue of supporting that integration.

An additional advantage of automation, when provided by the SOAR vendor, is assurance of integration with third-party systems. The benefit is that an organization can rely on scripted, tested actions. Most SOAR vendors, or SIEM vendors whose products include SOAR, provide a library of available responses and a community for sharing additional responses.

Chapter 6

Exploring Common SOAR Use Cases

In this chapter

- Learn the top use cases for SOAR
- Explore how SOAR supports regulatory compliance efforts
- Understand how SOAR can help triage malware alerts

At first, SOAR can seem overwhelming. If an organization doesn't have time to execute against its current workload, how will it find time to implement automation and additional processes? The answer is one use case at a time! In this chapter, we look at the most common SOAR use cases and how SOCs can grow their SOAR capabilities incrementally.

Handling Suspicious Emails and Phishing Attempts

Handling suspicious emails and phishing attempts is quite possibly the No. 1 use case for SOAR. This is due in part to the fact that phishing is such a high-risk and high-volume threat today. It's also because most organizations have a process in place for responding to phishing attempts. However, that process typically involves a lot of repetitive and meticulous manual steps. Automating the process with SOAR is an easy win.

This use case involves automating or semi-automating the process of reporting suspicious or phishing emails to the security team. If the SIEM collects enough information to definitively conclude that the email is dangerous, then SOAR

capabilities can automatically delete the email from any user's inbox to understand the full impact and whether it was a targeted effort. However, in most cases, a security analyst reviews the email before deleting it.

In addition to phishing emails, SOAR can alert the security team to emails potentially containing malware, strange attachments, or suspicious links. Finally, the SOAR workflow can automate remediation tasks such as blocking the sender's IP or domain, scrubbing the email from other mailboxes, and/or automatically generating reports for threat feeds.

Demonstrating Regulatory Compliance

Many regulations require companies to implement a standardized response for analyzing and reporting compliance violations, including documenting how and when a company investigates and mitigates potential violations. The playbooks and case metrics in a SOAR solution provide clear evidence for an auditor who has questions, and a clear trail of accountability in case of an actual compliance violation.

A SOAR solution also makes it easy to enable auditing and accountability. SOAR tracks and logs all steps companies take to contain and mitigate potential compromises, eliminating the burden of manually capturing incident response activity. Captured audit trails and reportable case metrics enable SOCs to refine their incident response processes, communicate with management, and address compliance requirements. Sometimes simply having a process helps a company respond to a compliance auditor. The first request is almost always, "Show me your process," and the second is, "Show me you've executed this process."

Monitoring Offboarded Employees

Properly offboarding employees when they leave the company is vital. Leaving the accounts of ex-employees active increases the organization's risk. The former worker can continue to access corporate resources — perhaps with malicious intent — or an attacker can use the employee's credentials. Either way,

security controls are unlikely to detect this activity because access was granted via legitimate user credentials.

Despite these risks, employees are not always properly offboarded. It can be difficult in multi-tiered organizations to ensure that all of the access rights and accounts for a given user are deactivated. Often, certain accounts (like email) remain open for some time after an employee leaves in order to monitor or transition business-critical activity. In addition, the SOC is sometimes "the last to know" that an employee has left or been terminated.

SOAR can be used to monitor the accounts of offboarded employees to ensure that they are terminated and/or that there isn't any suspicious activity around them.

Triaging Malware Alerts

Malware alerts can be triggered through many different means by numerous different security products. The malware incident use case enables a SOC to have a standard procedure for verifying the incident, acquiring forensic samples, determining threat vectors for the malware, stopping the spread of the malware, and remediating the system that was infected.

If a threat fails to meet certain predefined conditions providing assurance that an alert is a false positive, then SOAR can close the associated alert, so it doesn't become an incident.

Collaborating with HR on Misuse of Company Resources

When the SOC detects an employee misusing company resources, the proper response often involves collaboration with non-SOC staff such as Human Resources, Legal and/or various levels of management. A next-gen SIEM with SOAR capabilities can enable this collaboration, providing the right access to critical data and facilitating the process without further compromising company security.

Enriching Alarms with Reputation Data

When the SOC receives indications that a user visited a suspicious website, the proper response involves evaluating the website before taking action. After all, just because someone visited a strange site doesn't make the site a security risk. A SIEM with SOAR capabilities enables use cases around enrichment by automating or supporting workflow such as running a URL through a security scan or site reputation service. The results determine the next step, whether it is closing the alarm as benign or blocking the URL by changing a firewall policy.

SIEM Success: Regulatory Compliance is Just the Start

Meeting compliance requirements for the highly regulated insurance industry is no easy feat. But for a mutual life and health insurance provider that implemented a SIEM with SOAR capabilities, meeting its regulatory compliance requirements was just the beginning of realizing the platform's value.

As an insurance provider, this Lincoln, Nebraska-based company is subject to stringent government oversight, from regulating licensing models to standardizing policies and product offerings. Because it follows a brokerage model, providing services to independent brokers nationwide, the insurance company is also tasked with adhering to the state insurance laws where its brokers operate.

The team sought a SIEM that would help keep the company's robust IT environment secure and ensure compliance while eliminating mundane tasks and empowering the team to do more with few resources. LogRhythm's NextGen SIEM Platform with native SOAR did the trick — so well, in fact, that the team worked to adopt an additional use case.

The insurance company wanted to prevent unauthorized domain accounts from functioning. Leveraging LogRhythm's AI Engine and task automation from SmartResponse™, the insurance company is able to recognize and automatically mitigate unauthorized account usage:

- AI Engine detects when users are added to the domain admin group or if an account in the domain admin group is enabled.

- AI Engine automatically cross checks these accounts against a whitelist of approved accounts.
- In either case, automated actions from SmartResponse disable the illegitimate account.

The use case was validated when the insurance provider underwent a penetration test. After numerous failed attempts to compromise the company's system, the pen tester used a known vulnerability to successfully create a new domain account. When the AI Engine detected the unauthorized account, SmartResponse fired and automatically enacted countermeasures to quickly disable the illegitimate account.

Pleased with the domain administration use case, the insurance company continues to improve incident response with additional orchestration and automation. With LogRhythm, the company can demonstrate its adherence to compliance controls in a heavily regulated industry while improving its security posture and reducing their mean time to detect and respond to threats.

Chapter 7

Unleashing the Full Power of SOAR

In this chapter

- Explore how SOAR reduces cybersecurity risk
- Find out how to make the SOC more effective
- Discover tools and tactics for communicating security's value to management

The ultimate goal of a SOC is to manage the organization's cybersecurity risk. As explained in previous chapters, SOAR can greatly enhance risk management on a use case-by-use case basis.

Reduce Cybersecurity Risk

To effectively manage the organization's cybersecurity risk, the SOC must be able to minimize the time it takes to detect and respond to threats. However, SOC teams are often at a disadvantage due to numerous challenges we outlined in Chapter 1. SOAR helps the SOC overcome many of these challenges by making the SOC analysts more effective and more efficient, while providing the right metrics to support SOC management.

As demonstrated with the use cases in Chapter 6, SOAR provides immediate and long-term value for evaluating and responding to critical use cases. These use cases, among others unique to the business, define the types of risks the organization faces. The response plans, and their effectiveness determine how much risk the organization accepts for each use case.

Automation counters threats faster

We can't overstate the value of automation for facilitating more-expeditious threat detection, investigation, and response by SOCs.

Automated countermeasures stop threats around the clock

Automated countermeasures quickly contain and remove threats — even when a security analyst isn't at the helm. Automation reduces the risk of damage from specific threats, while freeing analysts to perform higher-level tasks such as malware analysis and threat hunting, which can further reduce risk.

Analysts are empowered to make informed decisions

Automated context enrichment lets analysts spend less time trying to collect the background information needed to understand a threat, and more time making thoughtful decisions about remediating the threat. The information analysts normally gather manually is automatically pulled into the case by the SOAR feature set, along with external threat intelligence, details about past cases with similarities, and possible responses based on past examples. Instead of spending valuable time and effort assembling the various data sources they need to evaluate the threat situation, analysts can jump right in, knowing they have immediate access to relevant information to make better-informed decisions.

Analysts are more effective

Without automation, an analyst must be fully educated on every possible security system. The analyst must have instructions and training on how to log in, execute an action, interpret the results, and extract the results from the system. With automation via a SIEM platform, the analyst simply has to know how to approve or execute an action. All of the details are handled behind the scenes, reducing the education and access control burden.

Risks related to manual analysis are reduced

Manual analysis introduces additional risk at a precarious time. Analysts could accidentally expose information about the company to the attacker or make a mistake that leads to incorrect conclusions about the threat. Automating analysis minimizes these risks while lessening the analyst's workload.

Increase SOC Effectiveness

SOAR brings order to chaos, enabling teams to work more effectively and get the job done correctly.

Improved collaboration

A SOC cannot operate effectively in a silo. SOAR helps break down barriers to make collaboration and coordination between functions easier. SOAR also ensures that analysts complement each other in their work, rather than duplicating efforts.

Accountability

Playbooks enable the SOC manager to assign individual tasks to the right owner, making it clear who is responsible for what. They also provide visibility into each analyst's workload, encouraging greater accountability and ensuring that no single analyst has too many assigned tasks.

Centralized evidence repository

Nearly every step of an investigation generates new information that adds valuable context or insights to guide an effective remediation. Storing evidence and artifacts in a centralized repository ensures that all of this information is taken into account and available for anyone who needs it.

Improve SOC Efficiencies

SOAR streamlines investigations and enhances efficiency across the entire SOC workflow. As a result, SOAR improves the team's ability to quickly and successfully detect and respond to threats.

Standardized and automated processes

Standardized and automated incident response processes contribute to higher operational efficiency. Automating tasks and implementing playbooks decrease the amount of time spent on detection and response. In addition, the procedural tasks embedded in playbooks remove inconsistencies in the workflow, ensuring that analysts follow appropriate steps when remediating each threat. Finally, having defined processes helps the SOC onboard and train new staff in an effective manner.

Elimination of context switching and broken workflows

By bringing together the processes required for detection, investigation, and response, SOAR native to a next-gen SIEM eliminates "swivel-chair analysis." That is, analysts no longer have to move between disparate tools and systems. All the information they need to develop a comprehensive understanding of potential threats and accurately assess risk is available via one unified dashboard. Analysts don't waste time logging in and out of multiple tools.

Navigating among different tools also creates fragmented workflows that make it difficult — if not impossible — for analysts to piece data together to create a comprehensive picture of the threat. Analysts must perform mental gymnastics as they rely on their own memories to tie seemingly disparate events together. They also spend time inefficiently and insecurely sharing evidence with one another over email, instant messages, and collaboration platforms.

These fragmented workflows hinder security teams in detecting, responding to, and mitigating threats before they impact the organization. SOAR helps ease workflows not only by serving as a unified workplace, but also by providing a central repository for evidence.

Repeatable processes

Repeatable processes are a key characteristic of a mature SOC — and for good reason. First, they improve the integrity

of investigations. It's much easier to defend decisions made and actions taken in the heat of the moment when guided by repeatable processes.

Similarly, following repeatable processes ensures that threats are analyzed in a consistent manner.

Repeatable processes have a beginning and an end, and SOAR tracks them every step of the way. This structure and discipline help ensure that each threat analysis is brought to completion and no step is overlooked or left undone.

Reduced staff turnover and training efficiencies

Staff turnover creates numerous inefficiencies. Hiring and training new staff consumes time and effort by SOC leaders and can distract them from core responsibilities. Meanwhile, existing staff must absorb the work performed by former colleagues.

SOAR reduces the inefficiencies associated with staff turnover. Because SOAR automates tedious tasks, security analysts are free to apply their expertise to more challenging problems. Additionally, SOAR helps analysts be more successful at investigating and responding to threats. As a result, they're happier and more satisfied with their work.

SOAR tools also make it easier to train new staff members. Playbooks help new team members understand internal procedures and requirements. They also reduce the learning curve when procedures are aligned with industry best practices that new hires may already be familiar with.

Communicate Security's Value

By reducing cybersecurity risk, SOAR helps the SOC transform from a resource consumer to a contributor of organizational growth and success. Security leaders will want to share the SOC's maturity and successes with upper management. Fortunately, SOAR provides the tools needed to communicate security's value.

Traceable workflows

SOAR's repeatable, consistent workflows are also traceable. Leaders can look at investigations and see what happened when, and who did what. This is important for establishing an audit trail for regulatory compliance, but it also gives everyone confidence in the SOC's efforts.

Case management metrics

Metrics, as shown in Figure 7-1, provide quantifiable data to describe the SOC's work to business leaders. Metrics serve as a common language that everyone understands. Instead of talking about risk levels or how many alerts were closed (the implications of which are unclear to even the folks doing the work), security leaders can communicate information that is of value to everyone: how quickly threats are detected and remediated.

SOAR technology can provide the following metrics, which we introduced in Chapter 1:

- ☑ Mean time to triage (MTTT)
- ☑ Mean time to qualify (MTTQ)
- ☑ Mean time to detect (MTTD)
- ☑ Mean time to investigation (MTTI)
- ☑ Mean time to respond (MTTR)

Teams can report on these KPIs and track improvements over time. Tracking and reporting helps strengthen the SOC's value to the business and gives security leaders a tool for communicating that value to senior management.

Consistent reporting

Consistent reporting, like consistent processes, indicates a high level of maturity. It also provides valuable insights into SOC operations, enabling teams to identify areas that can benefit from improvement and supplying a means for measuring that improvement over time. Some of the data teams can report on includes:

- ☑ Overall trends, which indicate how effective the SOC is and what types of incidents are most common
- ☑ Drill-downs by priority or tag, which indicate how effectively the team responds to different types of threats
- ☑ Breakdowns by analyst, which indicate how effectively workloads are managed and provide information needed to support requests for additional staff
- ☑ Breakdowns by time, which highlight areas where SOC staff may need additional tools or training, or different playbooks to respond effectively

Figure 7-1: SOAR provides granular insights across SOC performance.

Big Bank Realizes Big Savings with SIEM

Large financial institutions today are challenged with providing "big bank" customer and technological benefits without sacrificing the personal touch of community banking. As cybercriminals find new and more sophisticated ways to breach financial institutions, it's critical to meet these risks head-on to ensure they can meet their customer relationship goals.

An Abilene, Texas-based financial institution knew that it needed to transform its fragmented and manual threat detection. Siloed systems provided a limited and fragmented view into the threat environment. The security team knew it didn't have the visibility it needed to understand what security incidents were occurring, what to prioritize, or how to respond appropriately. The CISO knew that the lack of visibility was dangerous and could potentially lead to a breach, jeopardizing the customer relationships the financial institution had worked so hard to build over the previous 126 years.

Taking a step back, the security team evaluated its current security suite and eliminated tools that didn't provide value. During the process, the team also tried to optimize its current SIEM vendor, Splunk. It soon became clear that while Splunk contained valuable threat intelligence, uncovering that intelligence was difficult at best.

The financial institution turned to LogRhythm for single-pane-of-glass visibility. In addition to the much-needed visibility, LogRhythm provides investigative capabilities and empowers the team to organize and process information faster and more effectively than ever before. "I can just glance at the LogRhythm console, see what's going on, and dive deeper if necessary. It frees up a lot of my time," says a security analyst.

LogRhythm's ease of use benefits the team from both an operational and a security perspective. Prebuilt and customizable features, including AI Engine, rules, alarms, and dashboards, help the financial institution's security analysts organize and funnel the relevant data to the appropriate teams. "With LogRhythm, people are only seeing what they need to see to complete their job," the analyst says. "They're not inundated with a slew of information irrelevant to them."

The result: streamlined workflows and faster response times. But that's not all. "Switching from Splunk to LogRhythm saved us $50,000 in costs per year — and that number is coming directly from our CFO," says the financial institution's CISO.

Chapter 8

Buying Criteria: What to Look for in a SOAR Solution

In this chapter

- Review must-have SOAR features and functionality to increase the return on investment
- Learn how a central evidence repository saves analysts time and effort
- Understand the importance of integrations
- Find out why it's important for SOAR capabilities to be natively built into a next-gen SIEM solution

Organizations have a variety of options when it comes to leveraging SOAR capabilities. Choosing the right solution for a SOC can make the difference between establishing a mature, well-run organization that makes measurable improvements in detection and response times and settling for modest improvements that are inconsistent or wasteful. In this section, we look at the critical buying criteria for a SOAR solution.

A Sophisticated Dashboard

Incident responders and security analysts interact with SOAR via its dashboard. An example dashboard is shown in Figure 8-1. This dashboard should be sophisticated, yet easy to use. Intuitive workflows should guide analysts without requiring

them to understand the underlying data architecture. SOC staff should be able to operate naturally, assigning and working through tasks without giving a thought to the tool itself. Powerful search capabilities and single-click functionality should be available to aid incident investigation. A focused task view can help ensure that users don't miss a step and always know what to prioritize, leading to lower MTTR.

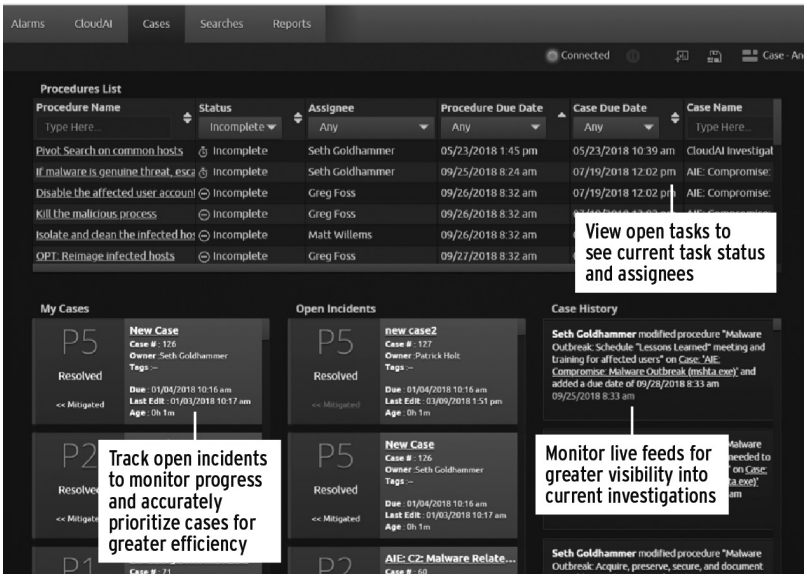

Figure 8-1: Analysts can leverage automated response capabilities to obtain contextualization or execute a countermeasure or mitigation.

Central Evidence Repository

A central evidence repository makes it easy for analysts to share evidence with each other while preventing information from being accidentally exposed to attackers.

Without a central evidence repository, analysts spend valuable time and risk compromise sharing evidence over insecure channels such as email, instant messages, and collaboration platforms like Slack. When analysts need to refer to a specific piece of evidence, they must search for it on multiple channels, with the risk that they might miss something entirely.

A central repository is also critical for supporting any compliance process. If the organization can't prove the process it performed six months ago, was it really done? Most breach settlements take years, and evidence of what was done can make the difference between a finding of "willful negligence" and "accidental exposure."

To be effective, a SOAR solution must accept evidence from a variety of sources that can be searched. If an analyst has to switch to different systems to retrieve a log, an infected file, and a reputation report, the time spent context switching directly increases the time to detect and respond. The SOAR solution should also ensure consistency of visualizations of different data regardless of the source. A next-gen SIEM solution with native SOAR capabilities provides greater effectiveness in analyst investigation and reduced cost of ownership because analysts have all the data within one user interface.

Customizable Workflows

While security best practices should be used to shape and standardize workflows, these workflows also have to accommodate unique environments. A SOAR solution should integrate with existing infrastructure components, enabling teams to develop custom workflows that capture the idiosyncrasies hidden within the organization.

Integrating SOAR with enterprise business and operational systems optimizes sharing of important business context and access to data for other use cases, as well. Think asset inventory systems, external threat intelligence, Development Operations (DevOps), operations, or business analytics, for example. By doing so, SOAR ensures adherence to cohesive workflows, regardless of the size of the SOC.

In addition, the workflows must fully focus on and support security operations. A SOAR solution shouldn't expose a critical incident involving an IT administrator simply because the SOAR platform shares case management inside the IT system operated by that administrator! SOAR workflows must support user isolation and proper security measures.

Playbooks and Their Guidance

The guided workflows — playbooks — within a SOAR solution enable rapid, accurate, and predictable incident response, regardless of an analyst's skill level. Playbooks spell out exactly what to do in a given threat scenario, and when to do it. By guiding analysts through a defined set of steps, playbooks increase their efficiency, raise the quality of their incident response, and optimize their workloads.

Based on security experts' knowledge, playbooks capture institutional knowledge that otherwise may disappear when a senior analyst leaves the organization. They give time back to senior analysts for more-complex investigations, threat hunting, etc., by enabling junior analysts to take on more incident response activities.

Furthermore, a SOAR solution with playbooks enables analysts to respond to and remediate threats from within a single platform for optimal efficiency and efficacy when every second counts.

Data Enrichment

The more high-quality data analysts have, the better informed they will be, and the greater the likelihood they will make accurate decisions. A SOAR solution should, therefore, have extensive capabilities for incorporating context-enriching data into an investigation to facilitate decision making. For example, alert data should be passed from network devices to SOAR. In the case of a potential malware infection, the SOAR solution should collect forensic data from the suspicious endpoint. As much as possible, data collection should be automated.

Library of Automated Responses

An extensive library of out-of-the-box automated responses to threats provides continuity across threat detection and response workflow without the need for APIs or custom integration work. These bulk administrative workflows and workflow templates reduce the TCO for a SOAR solution,

especially in large environments. In addition to eliminating mundane and tedious tasks, automated countermeasures act to contain threats or curb threat progression.

APIs and a Variety of Integrations

As the central hub for a SOC, a SIEM with SOAR capabilities must be able to integrate with both current and future technologies inside and outside the IT environment. Thus, a SOAR solution should provide APIs and a wide range of integrations across multiple vendors and technologies. The solution should have exposed APIs to administrative workflows, incident response tools, and the central evidence repository.

Organizations should be able to easily integrate the evidence repository with other enterprise applications, such as ticketing systems, without major configuration across multiple systems. This integration helps expedite threat mitigation and incident response.

The SOAR vendor should also provide a REST API for third-party integrations. In addition to supporting ticketing system integration, the API can be used for playbook management, programmatic creation of cases, and automatic assignment of tasks to an analyst.

Ease of Use and Supportability

The efficiencies obtained with SOAR should extend to the use and support of the tool itself. The solution should be easy to operate and manage, with one-click functionality for common tasks like case creation and threat intelligence lookups.

Embedded SOAR Capabilities

We wrote in Chapter 3 about the importance of choosing a SIEM solution with integrated SOAR capabilities versus a standalone SOAR solution. A SIEM with integrated SOAR will enable a SOC to optimize the efficiency gains it realizes from SOAR. However, it's important that SOAR capabilities be natively integrated into the SIEM system — not bolted on — for exactly the same reason.

While some vendors offer both SIEM and SOAR capabilities, these may still operate as independent solutions with only light integrations. The resulting solutions are not fundamentally architected to work cohesively. User experience and workflows are typically fractured and less efficient.

Look for a SIEM solution with enterprise-grade SOAR capabilities directly embedded into the platform feature set with end-to-end threat management workflows and a detection and response framework for SOCs.

SOAR Evaluation Checklist

A next-gen SIEM with the following SOAR features and capabilities will deliver the best return on investment.

Case Management

- ☐ Capability to standardize SOC workflowwith editable playbooks
- ☐ Rapid access to contextualized data such as hash integrity and Windows Event detail
- ☐ Ability to create a case from alarm dashboard
- ☐ Playbooks feature that is sharable, editable, searchable, and features version control with backwards fidelity
- ☐ Enables better visibility with operational APIs

Automation

- ☐ Ability to align automation tasks to observed activity as automated or semi-automated actions
- ☐ Utilize vendor's library of prebuilt automated responses for faster ROI
- ☐ Ability to create new automated responses
- ☐ Simple architecture that allows analysts to write their own automated responses

Analyst Experience

- ☐ Risk-based prioritized alarms dashboards that streamline analyst workflow
- ☐ Search across data through the enterprise including endpoint and network sensors
- ☐ Intuitive analyst investigation workflow without understanding the underlying data architecture
- ☐ Support breadth and depth of visualizations in graph and table formats from performance metric dashboards to investigation drill downs
- ☐ Ability to search within the SOAR interface for any related log data by classification or tagged metadata
- ☐ Access within the same interface to all activities from related hosts or users of the incident
- ☐ Ability to review incident response tasks or steps within the same interface as the incident investigation

SOC Metrics

- ☐ Generate metrics off analyst workflows to understand and track mean time to detect (MTTD) and mean time to respond (MTTR)
- ☐ Track time to qualify (TTQ) and time to investigate (TTI) across different types of threats for process improvement
- ☐ Enable organizational security baselines to measure security maturity and identify workflow bottlenecks

Glossary

case management: a means of keeping track of the various moving parts related to the investigation of a specific security event or incident.

mean time to detect (MTTD): the average amount of time it takes for a SOC to discover a potential security incident.

mean time to investigate (MTTI): the average amount of time it takes the SOC to study and understand a threat so that it can determine how best to mitigate it.

mean time to qualify (MTTQ): the average amount of time it takes a SOC to determine that a security alert is a true positive (rather than a false positive) and requires mitigation.

mean time to respond (MTTR): the average amount of time it takes a SOC to shut down an attack.

mean time to triage (MTTT): the average amount of time it takes to parse security data and generate an alert.

orchestration: the coordination and automation of various tasks involved in threat analysis and response.

playbook: a standard, documented process that details repeatable steps for responding to specific types of incidents.

security information and event management (SIEM): a security tool that collects, analyzes, and reports on log and event data.

security operations center (SOC): an organization responsible for managing a company's security. A SOC team can be local, distributed, multi-talented, or multi-departmental.

security orchestration, automation, and response (SOAR): a technology solution that collects security data and alerts from myriad sources, identifies alerts that require a response, and drives measurable, standardized workflows for executing that response in an efficient manner.

workflow and collaboration engine: a technological component of SOAR that defines operational procedures and ensures consistent execution of procedures at scale.

Learn how SOAR can transform your security organization into a high-functioning security operations center that stops advanced threats before they become a high risk.

A well-run security operations center (SOC) is a must-have in today's digitalized world. Unfortunately, transforming security from largely reactive, manual operations to proactive, automated, and consistent processes can feel impossible. But it is achievable, with the right capabilities. This goal can empower your SOC to detect and respond to advanced threats efficiently and effectively. This guide will help you:

- Understand the security operations center — find out the criteria that make up a high-functioning SOC
- Introduce you to SOAR — learn how SOAR capabilities address the challenges of building a SOC
- Deconstruct SOAR — review the various technologies that comprise SOAR
- Dive into orchestration — find out how SOCs can benefit from orchestration with playbooks
- Understand automated response — explore how flexible automation empowers SOCs to improve efficiencies
- Learn the buying criteria — learn exactly what to look for when evaluating SOAR providers

About the Author

A former editor of SearchSecurity.com, Crystal Bedell is a senior marketing consultant specializing in cybersecurity. She's been helping technology providers create engaging content since 2000.

CYBEREDGE PRESS

Not for resale

ISBN 978-1-948939-02-7