LogRhythm

How to build a SOC with limited resources

Your guide to detecting and responding to threats fast – Even if you don't have a 24x7 SOC

By: James Carder
LogRhythm CSO and Vice President, LogRhythm Labs

TABLE OF CONTENTS

How to build a SOC with limited resources

Introduction

Some organisations have formal security operations centres (SOCs). Formal 24x7 SOCs are tightly secured areas where teams of dedicated analysts carefully monitor for threats around the clock, every day of the year. Analysts are checking their organisation's enterprise security controls to identify possible signs of intrusion and compromise that may require a response by the organisation's incident responders.

Unfortunately, most organisations cannot afford a 24x7 SOC. The cost of having well-trained analysts onsite at all times outweighs the benefit for almost every organisation. Instead, most organisations either make do with an informal SOC comprised of a small number of analysts who have many other duties to perform or have no SOC at all and rely on borrowing people from other roles when needed. Security events are not consistently monitored around the clock. This leads to major delays in responding to many incidents, while other incidents go completely unnoticed. It's a dangerous situation that results in damaging cyber incidents. It is also highly unlikely that analysts will have any time to be proactive in looking for threats and attacks. And when an event occurs, many organisations can't efficiently and effectively respond because they lack formal incident response processes and capabilities.

For organisations caught between the prohibitive cost of a formal SOC and the wholly inadequate protection from an informal SOC, there is a solution: building a SOC that automates as much of the work as possible. Automation can help a team perform constant security event monitoring and analysis to detect possible intrusions. It can also provide incident response automation and orchestration capabilities to manage and expedite incident handling.

The purpose of this white paper is to show you how you can successfully build a SOC, even with limited resources. The paper explains the basics of SOCs, providing details of what SOCs mean in terms of people, processes, and technology. Finally, you'll learn the methodology of building a SOC with limited resources, focusing on tactics to make your rollout smooth and successful. After reading this paper, your organisation should be ready to start planning its own SOC.

What makes a SOC effective? Fusing people, processes, and technology

To create an effective SOC, you need three components—people, processes, and technology—to build an efficient security operation. This minimises reliance on people and enables decentralisation of the SOC team.

For SOCs, the power of automation cannot be overstated. Consider a type of incident that happens all the time: a phishing attack campaign. A strong security operations platform can automatically take care of nearly every aspect of the detection, response, and recovery processes, including:

- Detecting the campaign and investigating its purpose and scope
- Comparing the observed characteristics to threat intelligence to improve understanding of the threat
- Automating the entire remediation, including blocking the threat from continuing the campaign, deleting all phishing emails from user mailboxes, determining if any phishing emails triggered malicious payloads to be downloaded and installed, quarantining any infected systems, and wiping malicious code from systems
- Generating a report on the incident and providing it to appropriate stakeholders

Similar benefits can be achieved for other types of attacks and threats as well through automation of the SOC. This enables your organisation to have a small number of analysts who focus on the most complex and challenging tasks instead of legions of analysts who spend most of their time performing time-intensive, mundane tasks. Automation also greatly improves the efficiency of SOC operations so that incidents are detected, stopped, and recovered from much more quickly, thus minimising damage and other costs.

The following sections further explain the SOC in terms of people, processes, and technology.

People

No matter how well automated a SOC is, people are an absolute necessity. The two most fundamental roles in a SOC are the security analyst and the incident responder. Security analysts work primarily in the monitoring and detection phases of a SOC. Typical tasks include monitoring alarms from an all-in-one platform and performing triage to determine which alarms require intervention from the incident responders. Incident responder tasks may include:

- Conducting deeper analysis of suspicious security events using:
- Search analytics capabilities
- Threat intelligence sources
- Basic forensics techniques
- Malware analysis tools
- Performing response activities whenever an incident necessitates
- Keeping management apprised of the status of incident response efforts. Other possible SOC roles include forensic analysts and malware reverse engineers.

A security architect is the final important part-time role for any SOC. The security architect is typically someone within the security organisation with a deep understanding of the organisation's security program and infrastructure. This person should help design the initial SOC solution and oversee its implementation to ensure it is efficient and effective. Over time, the security architect can plan and implement adjustments to the SOC solution, including expansions to meet the additional needs of the organisation. The security architect role is particularly important because the architect's decisions will significantly affect the security program and thus affect the whole organisation.

Organisations have many options when it comes to how to staff a SOC. Following are a few examples of possible SOC staffing models:

Fully outsourced

In this model, all SOC roles are filled by a managed security service provider (MSSP) or other outsourcer. The outsourcer contacts the organisation only when required to participate in incident response efforts or answer a question about the particulars of the organisation's environment.

Hybrid (combination of employees and outsourcing)

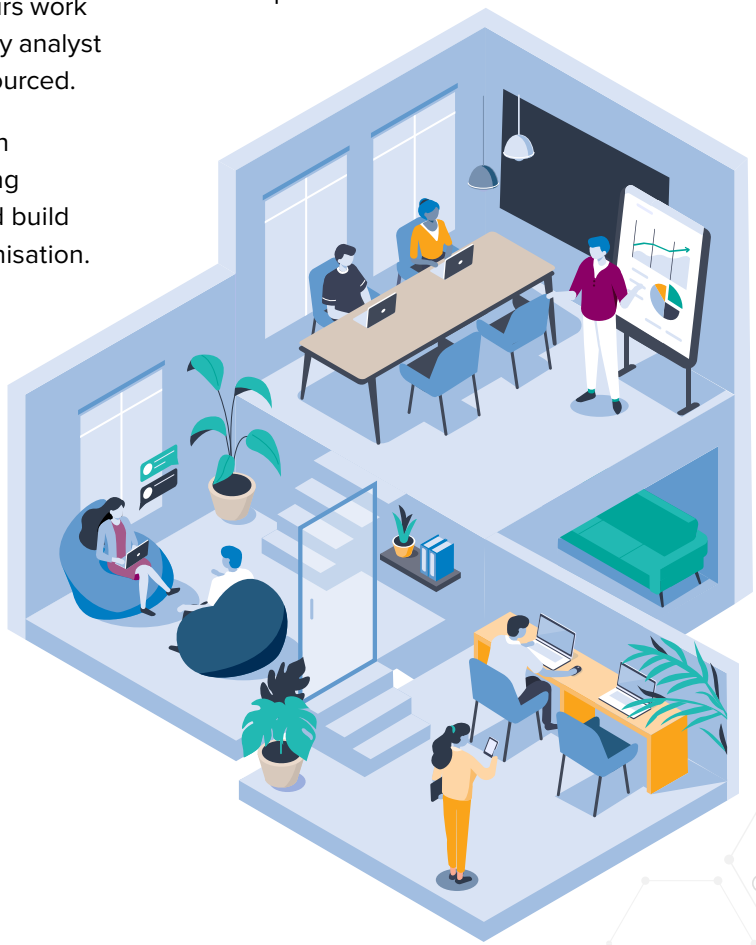
Hybrid models often involve employees covering key business hours and outsourcers handling the rest. For example, in an 8x5 business hour environment, an organisation might need to staff a minimum of two full-time equivalent (FTEs): one security analyst FTE and one incident responder FTE. All off-hours work and all work for roles other than security analyst and incident responder would be outsourced.

Another hybrid model is to augment an in-house SOC with an MSSP performing 24x7 "eyes on glass." The MSSP would build custom use cases tailored to the organisation. The success of such a hybrid model is dependent on providing the MSSP with as much business context as possible so the MSSP can be effective at meeting the organisation's needs and expectations.

Fully in-house

Options for bringing a SOC in-house include:

- **24x7 SOC:** Having 24x7 SOC coverage by staff would necessitate having several security analyst FTEs and several incident responder FTEs. In addition, most specialised positions would be handled by staff. Outsourcing would be minimised.
- **8x5 SOC:** Organisations greatly reduce risk by using an all-encompassing security information and event management (SIEM) platform to automate and facilitate its capabilities. With this approach, you can build in automated escalations and notifications to your analyst staff based on criticality and impact of any alert as a compensation for not staffing a full 24x7 operation.



Processes

Every SOC, no matter what staffing model an organisation uses, relies on processes. Technology brings people and processes together—such as an all-in-one SIEM platform that notifies a security analyst of something that needs immediate attention, or an incident responder commanding a SIEM platform to do something on the incident responder's behalf. But processes also help people to work with each other. For example, a security analyst may mark a set of events in the SIEM platform that an incident responder needs to further investigate. The SIEM platform provides workflow capability that transfers responsibility for the work from the security analyst to the incident responder.

All-in-one SIEM platforms can foster much more sophisticated communication, collaboration, workflow, and orchestration capabilities for SOCs. When a major incident occurs, numerous security analysts, incident responders, and forensic specialists may all help to resolve it, and others within the organisation such as system and network administrators may also be involved. By integrating a SIEM platform and a SOC with existing business processes and workflows, an organisation can promote the SOC's adoption and viability while ensuring rapid and effective efforts throughout the organisation to detect and respond to threats. This avoids a mistake many organisations make—forcing all existing business processes to change to accommodate the SOC.

In these cases, having an all-in-one SIEM is essential because it performs security automation and orchestration to ensure that everyone is kept up to date on the status and has access to all necessary information. It can also provide people with the tools they need to work together and to route tasks from one person or team to another. Finally, a full SIEM platform provides the ability to check on workflows to ensure that nothing is overlooked or handled too slowly.

Technology

An all-in-one platform is ideal for building a SOC because it includes and integrates all the needed forms of security automation and incident response orchestration into a single display. Here are some examples of what a SIEM platform can do:

- Centralise all forensic data supporting effective machine analytics and enabling rapid investigations, so it can be monitored at all times and analytics can be utilised to identify events of particular interest, this eliminates the need to have people looking at the raw security event data on monitors 24 hours a day.
- Provide context for security events and incidents by integrating critical threat intelligence sources and vulnerability data, as well as information from integrated systems in human resources, finance, contracting, etc. regarding business systems and assets. This context enables security analysts to better determine what an attacker may be attempting to do and why.
- Prioritise events of interest based on their relative risk to the organisation so that SOC staff can pay attention to the most concerning events first.
- Pull evidence together in one location and safely and securely share it with authorised individuals, such as remote staff and outsourcers involved in an incident response effort.
- Use workflow capabilities to alert each person/role when it is their turn to do something for the SOC, such as reviewing an event it has flagged as high risk.
- Interface with asset management, vulnerability management, trouble ticketing, intrusion prevention, and other existing systems to automatically integrate SOC processes with business processes. This greatly expedites workflow and reduces workload for staff in numerous departments.
- Enable automated responses that are automatically associated with specific alarms. Actions that can be initiated without human interaction, or that require single-click approval, can greatly benefit your team's time to respond to an incident. An all-encompassing SIEM platform should recognise common situations, such as a basic malware compromise, and automatically respond so the team can focus on more complex and impactful events and incidents.

A SIEM platform used in conjunction with a sensible SOC staffing model and robust processes can provide seamless integration, workflow, and communication for all SOC-related tasks, regardless of the use of outsourcing. This combination also enables immediate access to the information, data, events, and investigation records that are needed by authorised in-house and outsourced parties at any time and from any location.

How LogRhythm powers your SOC

LogRhythm brings together historically disparate solutions into one unified platform, which we call the LogRhythm NextGen SIEM Platform. The LogRhythm NextGen SIEM Platform gives your SOC a single pane of glass from which to evaluate alarms, investigate threats, and respond to incidents.

LogRhythm's patented security analytics capabilities automate the detection and prioritisation of real threats. In addition, the platform provides mechanisms to orchestrate and automate the incident response workflow. The delivery of all SIEM capabilities, combined with strong automation, ensures that your SOC can work more efficiently and effectively to realise faster mean time to detect and respond.

The LogRhythm NextGen SIEM Platform enables organisations to build cost-effective SOCs that reduce risk and prevent major data breaches and other compromises. This also frees organisations to get much better value from their staff, utilising them more for strategic projects with long-term benefits rather than manual daily operations. For more information on the LogRhythm NextGen SIEM Platform, visit **logrhythm.com/demo**

Estimating SOC costs and savings

How much a SOC will cost an organisation is dependent on many factors, as is how much a SOC may save an organisation. Let's start by looking at estimated annual labour and services costs for common SOC staffing models for small, medium, and large SOCs. (See cost comparisons of various SOC staffing models on page 12.) These estimates show that for all sizes of SOCs, labour and service costs are highest for SOCs not based on an all-in-one security information and event management (SIEM) platform. This is because there is far more monitoring, analysis, investigation, prioritisation, forensic data collection, incident response, management, and reporting work to be done by humans instead of the SIEM platform.

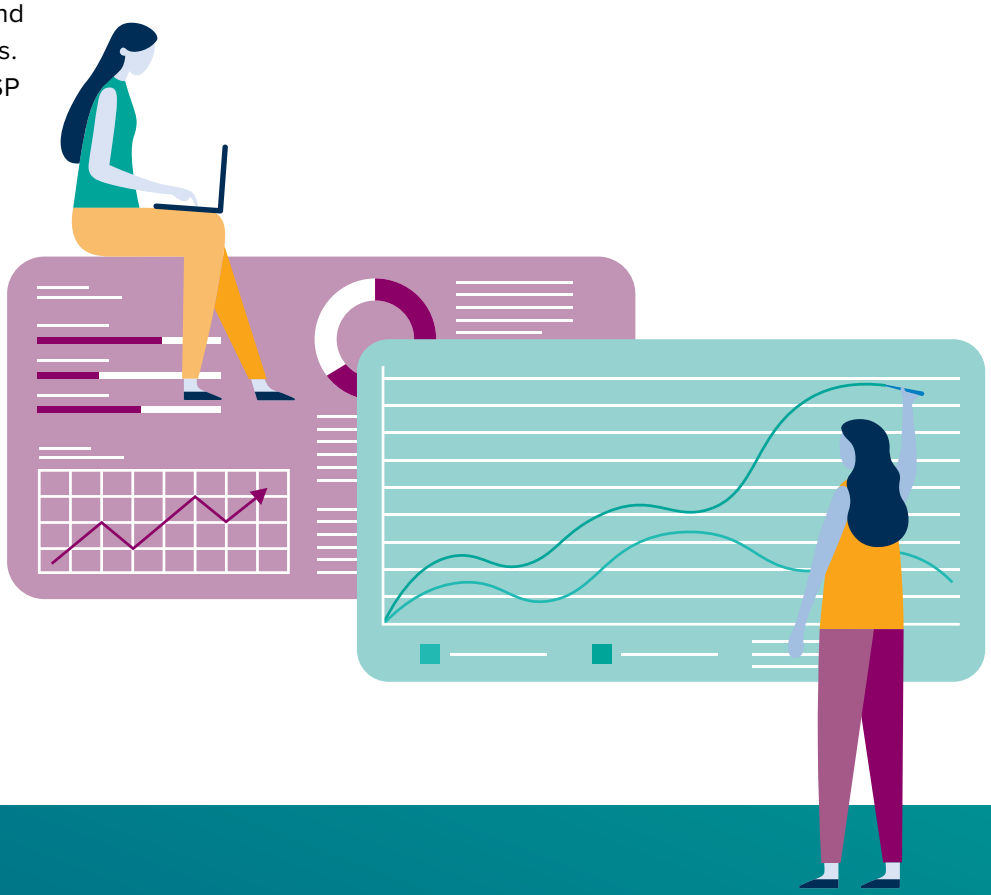
The second major type of cost for SOCs is the infrastructure, including facilities, equipment, networks, systems, software, and subscription fees (e.g. threat intelligence feeds). These costs are hard to generalise. For example, one organisation might have unused facility space available for immediate SOC use, while another organisation may need to acquire and prepare new space. One organisation might have networks and systems readily available for the SOC, while another may need to design, procure, and implement them. However, in general, the infrastructure costs are fairly consistent across models for a particular size SOC because most of the same infrastructure needs to be in place whether you have 8x5 or 24x7 onsite staffing. The only exception is the fully outsourced SOC model, because it doesn't require facilities, equipment, or systems for SOC staff.

The final major considerations for SOC costs involve how effective the SOC will be at preventing incidents, detecting and stopping incidents quickly, and restoring normal operations. Converting an informal SOC into a well-structured SOC utilising a SIEM platform could reduce costs by millions of pounds a year for incident handling, loss of user productivity, and loss of business from incidents that prevent the organisation from conducting its normal operations.

Consider a simple malware incident at a 5,000-user organisation. The organisation's informal SOC isn't staffed around the clock, so the malware incident isn't detected until approximately 100 systems have been affected. Each of these systems needs to be rebuilt, with each rebuild, restore, and redeployment taking on average four hours of system administrator time. The users of these 100 systems can't do most of their work

during this time. If you assume a total loss of productivity of 500 hours, plus 400 hours of system administrator time, this malware incident costs 900 hours of labour. At roughly $100 an hour, that's nearly $100,000 lost in a single day. Around-the-clock monitoring from a SIEM platform and an MSSP would have detected and stopped the malware incident very early, preventing almost all of those systems from being affected and saving nearly $100,000 in costs. That's more than what the MSSP services would cost for three months.

Transitioning a SOC to a model with an all-encompassing SIEM platform can provide large ongoing cost savings for your organisation.



Expert note

Around-the-clock monitoring from a SIEM platform and an MSSP would have detected and stopped the malware incident very early, preventing almost all of those systems from being affected and saving nearly $100,000 in costs. That's more than what the MSSP services would cost for three months.

Cost comparisons of various SOC staffing models

	Small SOC < 10,000 users	Medium SOC 10,000-50,000 users	Large SOC > 50,000 users
SOC without a SIEM platform	**8x5 onsite**	**16x5 onsite**	**24x7 onsite**
Security analysts	2 FTEs @ $120K each	8 FTEs @ $120K each	20 FTEs @ $120K each
Incident responders	1 FTE @ $145K each	4 FTEs @ $145K each	8 FTEs @ $145K each
Specialists (malware reverse engineers, forensic analysts, etc.)	0 FTEs; outsource and pay when needed (est. $50K/year)	2 FTEs @ $150K each	5 FTEs @ $150K each
Management	1 FTE @ $150K	2 FTEs @ $150K	3 FTEs @ $150K each
Total	$585K	$2,140K	$4,760K
Fully in-house SIEM-powered SOC	**8x5 onsite**	**16x5 onsite**	**24x7 onsite**
Security analysts	1 FTE @ $120K each	4 FTEs @ $120K each	8 FTEs @ $120K each
Incident responders	1 FTE @ $145K each	2 FTEs @ $145K each	4 FTEs @ $145K each
Specialists (malware reverse engineers, forensic analysts, etc.)	0 FTEs; outsource and pay when needed (est. $25K/year)	1 FTE @ $150K each	2 FTEs @ $150K each
Management	0.25 FTE @ $150K	0.5 FTE @ $150K	1 FTE @ $150K
Total	$328K	$995K	$1,990K

	Small SOC < 10,000 users	Medium SOC 10,000-50,000 users	Large SOC > 50,000 users
Hybrid SIEM-powered SOC	8x5 onsite, offsite MSSP all other times	IR onsite 16x5, all others offsite MSSP 24x7	24x7 onsite
Security analysts	0.5 FTE @ $120K each	0	0
Incident responders	0.5 FTE @ $145K each	2 FTEs @ $145K each	4 FTEs @ $145K each
Specialists (malware reverse engineers, forensic analysts, etc.)	0 FTEs; outsource and pay when needed (est. $25K/year)	0 FTEs; outsource and pay when needed (est. $50K/year)	0 FTEs; outsource and pay when needed (est. $100K/year)
Management	0.25 FTE @ $150K	0.25 FTE @ $150K	0.5 FTE @ $150K
MSSP service	$250K	$400K	$750K
Total	$445K	$778K	$1,505K
Fully outsourced SIEM-powered SOC	Offsite MSSP 24x7	Offsite MSSP 24x7	Offsite MSSP 24x7
Security analysts	0	0	0
Incident responders	0.5 FTE @ $145K each	1 FTE @ $145K each	4 FTEs @ $145K each
Specialists (malware reverse engineers, forensic analysts, etc.)	0	0	0
Management	0.25 FTE @ $150K	0.5 FTE @ $150K	$900K
MSSP service	$350K	$600K	3 FTEs @ $150K each
Total	$460K	$820K	$1,268K

Steps for building a SOC with limited resources

Based on experiences helping a wide variety of organisations, LogRhythm experts developed a methodology for building a SOC that uses a full SIEM platform. The following seven items describe each step of the methodology.

Step 1: Develop a strategy

Two particularly important parts of developing a strategy for the SOC are as follows:

A. Assess the organisation's existing SOC capabilities in terms of people, processes, and technology. Note that when building a SOC, the SOC's initial scope should be limited to core functions: monitoring, detection, response, and recovery. Some SOCs support additional functions, such as vulnerability management, but such non-core functions should be delayed until the core functions are sufficiently mature.

B. Identify the business objectives for the SOC. To be effective, the SOC should focus on helping the organisation meet its business objectives. Creating a SOC for the sake of security without factoring in the business, such as which systems and data are most critical to sustaining operations, will inevitably cause problems showing value to the business, and could result in the SOC missing a key threat that results in a damaging cyber incident.

Step 2: Design the solution

Echoing the advice under Step 1 about limiting the initial scope of the SOC, it may be best to pursue a few quick wins instead of creating a full-scale, broad-function SOC solution. Choose a few business-critical use cases and define the initial solution based on those use cases, keeping in mind that the solution must scale in the future to meet additional needs. Having a more narrowly scoped initial solution also helps to reduce the amount of time needed to implement it and achieve initial results more quickly. When designing the SOC solution, important actions include the following:

A. Define the functional requirements. These requirements should be tied to business objectives whenever applicable.
Functional requirement areas include:
   i. identifying the sources of log and event data to be monitored
   ii. identifying the sources of threat intelligence to be utilised
   iii. determining performance requirements, such as response times

B. Choose a SOC model. This should be based on the functional requirements just defined, as well as the strategy defined in the first step. Decisions to make include which hours and days to staff versus outsource, which responsibilities to staff versus outsource, which roles the SOC will have, and how many FTEs will be needed per role.

C. Design the technical architecture. This includes:

   i. Planning the composition and configuration of the components of the solution, most notably the SIEM platform

   ii. Identifying the business systems and information systems that should be integrated with the SIEM platform to provide business context for security events and incidents

   iii. Defining the workflows for events and incidents to align with the organisation's existing processes

   iv. Planning to automate the solution as much as possible, including the necessary technologies to have complete visibility of the threat landscape for the systems and data in the initial SOC scope and to thwart attacks as early in the attack lifecycle as possible

   v. Determining if the technical architecture is sound, such as performing tabletop exercises for all use cases to identify potential issues

Step 3: Create processes, procedures, and training

If the SOC staffing will be partially outsourced, it is important to work with the outsourcer to ensure that processes, procedures, and training on both sides take that into account.

Step 4: Prepare the environment

Before deploying the SOC solution, it is critically important to ensure that all the elements are in place to provide a secure environment for the solution. Notable elements include tightly securing SOC staff desktops, laptops, and mobile devices; having secure remote access mechanisms in place for staff (and outsourcers if applicable) to interact with the SOC solution; and requiring strong authentication for remote access to the SOC solution at a minimum (and preferably for local access as well).

Step 5: Implement the solution

The key to implementing the solution itself is to focus on taking full advantage of the technology to minimise the workload on people. This solution is a ground-up process that begins by:

A. bringing up the log management infrastructure

B. onboarding the minimum collection of critical data sources

C. bringing up the security analytics capabilities

D. onboarding the security automation and orchestration capabilities

E. begin deploying use cases that focus on end-to-end threat detection and response realisation

Another essential element is achieving seamless interoperability with other systems, both to collect data from sources and to issue actions and commands to help apply context, contain, and remediate in alignment with workflows. The latter is particularly helpful for reducing the mean time to detect and to respond to incidents. The solution should also incorporate threat intelligence feeds and other intelligence sources as automated inputs to improve detection accuracy.

Step 6: Deploy end-to-end use cases

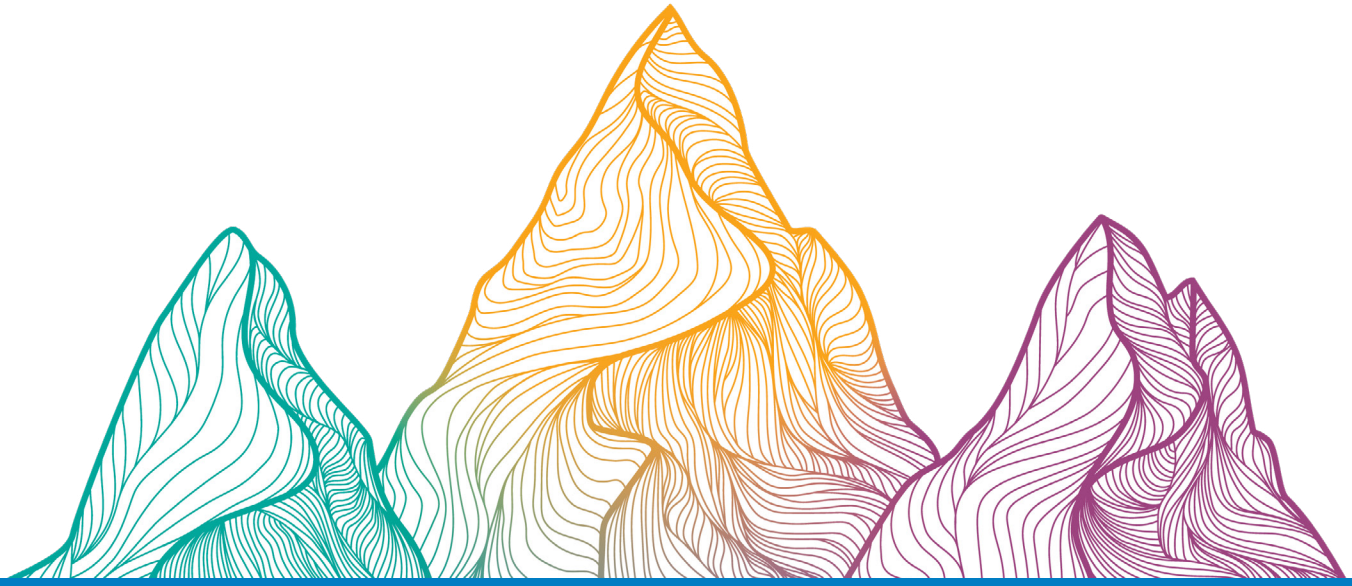
Once solution capabilities are deployed, you can implement use cases across the analytics tier and security automation and orchestration tier, such as detecting compromised credentials and successful spear phishing campaigns. You should test during a variety of shifts and during shift changeovers. All the forms of solution automation mentioned earlier are particularly important to test rigorously. The reliability and security of remotely accessing the solution should also be verified to the extent feasible.

Step 7: Maintain and evolve

Once the solution is fully in production, it will need ongoing maintenance, such as updating configuration settings and tuning over time to improve detection accuracy, and adding other systems as inputs or outputs to the solution. You will need to include other maintenance periodically, including reviewing the SOC model, SOC roles, FTE counts and so forth, to make adjustments.

Expert note

The key to implementing the solution itself is to focus on taking full advantage of the technology to minimise the workload on people.



CONCLUSION

Having an all-in-one SIEM platform has become an absolute necessity for implementing a SOC to achieve greater efficiency. A hybrid SOC is the just-right solution for organisations that cannot justify the overwhelming expenses of a formal SOC and cannot tolerate the inadequate protection provided by an informal SOC.

The LogRhythm NextGen SIEM Platform is the ideal technology for building a SOC. Organisations that adopt this strategy can achieve immediate and ongoing cost savings as compared to adopting any other SOC model. This strategy also leads to a material reduction in risk for the organisation. Specific ways in which the LogRhythm platform benefits organisations include the following:

- Uses advanced capabilities for threat detection and analysis, such as user and entity behaviour analytics, that can find and understand the significance of many types of threats that cannot easily be detected by other means. This is particularly helpful for identifying insider threats attempting to access and steal sensitive data.
- Provides highly sophisticated workflow capabilities that transfer responsibility for specific tasks from person to person or role whenever needed. This keeps things moving and minimises miscommunications that could inadvertently delay action or cause duplicated efforts.
- Automates incident response orchestration so that all people involved in incident response have immediate access to necessary information

LogRhythm's security automation and orchestration capabilities significantly improve the efficiency and effectiveness of incident response.

To see how you can build your own SOC with LogRhythm, schedule a customised demo today: logrhythm.com/schedule-online-demo

About LogRhythm

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behaviour analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralisation of threats.

Built by security professionals for security professionals, LogRhythm enables security professionals at leading organisations like Cargill, NASA, and XcelEnergy to promote visibility for their cybersecurity program and reduce risk to their organisation each and every day. LogRhythm is the only provider to earn the Gartner Peer Insights' Customer Choice for SIEM designation three years in a row. To learn more, please visit logrhythm.com.

About James Carder

James Carder brings more than 20 years of experience working in corporate IT security and consulting for the Fortune 500 and U.S. government. As CISO and Vice President of LogRhythm Labs, he develops and maintains the company's security governance model and risk strategies, protects the confidentiality, integrity, and availability of information assets, oversees both threat and vulnerability management, as well as the Security Operations Centre (SOC). He also directs the mission and strategic vision for the LogRhythm Labs machine data intelligence, strategic integrations, threat, and compliance research teams.

Prior to joining LogRhythm, James Carder was the Director of Security Informatics at Mayo Clinic, where he had oversight of Threat Intelligence, Incident Response, Security Operations, and the Offensive Security groups. Prior to Mayo, Mr. Carder served as a Senior Manager at Mandiant, where he led professional services and incident response engagements. He led criminal and national security-related investigations at the city, state and federal levels, including those involving advanced persistent threats (APT) and the theft of credit card information.

James is a speaker at cybersecurity events and is a noted author of several cybersecurity publications. He holds a Bachelor of Science degree in Computer Information Systems from Walden University, an MBA from the University of Minnesota's Carlson School of Management, and is a Certified Information Systems Security Professional (CISSP.)

LogRhythm®

Regional HQ, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom