LogRhythm®

The Security Intelligence Company

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 CISO and Vice President, LogRhythm Labs

Table of contents

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. The 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 does occur, many organisations are not able to efficiently and effectively respond, because they do not have formal incident response processes and capabilities in place.

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 SOC work as possible. Automation can help a team perform constant security event monitoring and analysis in order to detect possible intrusions. It can also provide incident response automation and orchestration capabilities to manage and expedite incident handling. A threat lifecycle management platform is the ideal foundation for building a SOC because it provides all of these automated capabilities in a single, fully integrated system.

The purpose of this white paper is to show you how you can successfully build a SOC, even with limited resources. The paper first explains the basics of the Cyber Attack Lifecycle and the need to address it through the Threat Lifecycle Management framework. Next, the paper explains the basics of SOCs, providing details of what SOCs mean in terms of people, processes, and technology. Finally, the paper walks you through a methodology for building a SOC with limited resources, focusing on tactics to make your rollout smooth and successful. After reading this paper, you should be ready to start planning your own SOC.

The Cyber Attack Lifecycle

Understanding the Cyber Attack Lifecycle is a prerequisite to understanding the Threat Lifecycle Management (TLM) framework—the foundation of SOC operations. The Cyber Attack Lifecycle consists of six phases:

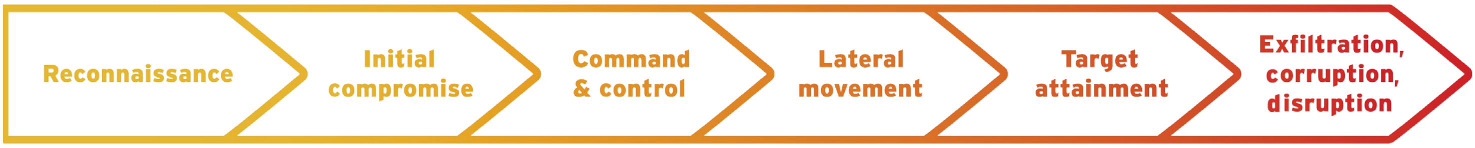


Figure 1: The Cyber Attack Lifecycle

Phase 1: Reconnaissance

This phase can involve a wide range of activities, but at its core, the attacker identifies a target and determines how to start the attack against that target.

Phase 2: Initial compromise

In the next phase, the attacker attacks a system on the internal network and gains access to it. This system is usually not the ultimate target.

Phase 3: Command and control

The attacker installs tools on the compromised system in order to maintain access to it.

Phase 4: Lateral movement

Next, the attacker uses the compromised system and its user accounts to identify additional systems to access and compromise. This may be repeated several times so that the attacker can move throughout the enterprise.

Phase 5: Target attainment

In the final system compromise, the attacker gains access to the target system.

Phase 6: Exfiltration, corruption, and disruption

Finally, the attacker accomplishes the attack's objective, such as exfiltrating the system's sensitive data to an external location, or disrupting the organisation's operations by corrupting the target system's files or databases.

The Cyber Attack Lifecycle indicates that organisations often have numerous opportunities to detect and respond to an attack in progress because a single attack involves many steps. The earlier in the lifecycle an organisation detects an attack, the more likely it is that the organisation can respond in time to prevent a serious data breach or other major compromise from occurring.

The Cyber Attack Lifecycle indicates that organisations often have numerous opportunities to detect and respond to an attack in progress because a single attack involves many steps.

Threat Lifecycle Management basics

Threat Lifecycle Management is the key to detecting and stopping attacks as early as possible in the Cyber Attack Lifecycle. TLM is a unified capability for detecting new threats and attacks against the organisation's systems, determining the level of risk the threats and attacks pose, mitigating those risks, and performing any necessary recovery actions to restore normal operations. The goal of TLM is to completely mitigate and avoid damaging cyber incidents that could be caused by successful attacks against systems, networks, and data.

For your SOC to be successful in achieving cost-efficient reductions in mean time to detect (MTTD) and mean time to respond (MTTR), there are six phases in the TLM framework that you must implement for end-to-end detection and response. Here we'll delve into the TLM framework—the foundation of a efficient and functional SOC—before moving deeper into how to effectively build a SOC from the ground up.

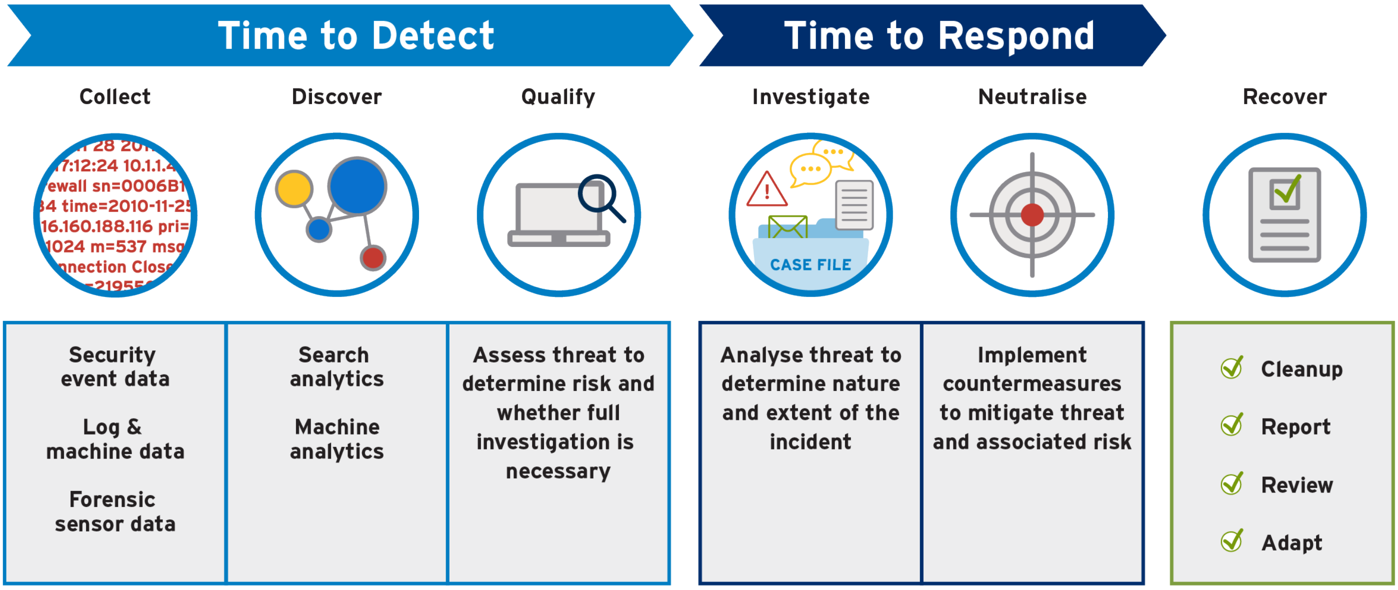


Figure 2: The Phases of the Threat Lifecycle Management Framework

Forensic data collection

This phase involves continually collecting data from sources that might be recording evidence of attacks. Three of the most important types of sources to utilise are:

Security event data

Most organisations have an array of security products to prevent a wide range of attacks from being successful. However, in some cases, these technologies can only warn that an attack may be in progress, resulting in alarms being generated. But the challenge is then rapidly identifying which alarms or events to focus on—as tens of thousands might be generated on a daily basis.

Log and machine data

Log data can provide deeper visibility into your IT environment—recording on a per user, per system, per application basis—to illustrate who did what, when, and where. This rich set of data can support more effective and rapid investigations of suspicious attacks. The ability to comprehend what is normal within the IT environment is also within this dataset—enabling machine analytics to detect behavioural anomalies that might indicate a more advanced attack is in progress.

Forensic sensor data

Once your organisation is effectively collecting security and log data, forensic sensors can provide even deeper and broader visibility. This data can fill gaps when logs aren't available or when the level of forensic detail is insufficient. There are two primary types of forensic sensors:

- Network forensic sensors that capture packets and flows
- Endpoint forensic sensors (e.g., EDR agents) that can record all activity occurring on the monitored system with high fidelity

Forensic sensors data can also provide additional gains in investigative and incident response efficiencies. This data enables more powerful and capable machine-driven approaches for detecting the most sophisticated attacks.

Discover

In the Discover phase, the collected data is analysed to identify potential threats. The two types of analytics are search analytics and machine analytics. Search analytics are performed by people with assistance from technology that provides different ways for people to perform searches and view the data. Machine analytics are performed automatically by software using combinations of advanced techniques, such as machine learning, in order to find potential threats within enormous volumes of data.

Qualify

Each potential threat must be qualified, which means that it is assessed to determine if it is a legitimate concern, its level of risk, and whether the risk merits further investigation or mitigation. During this phase, alarms are generated from machine analytics and then reviewed, qualified, and prioritised.

Investigate

Once a threat has been qualified, it needs to be fully investigated to undeniably determine whether a security incident has occurred or is in progress. Rapid access to forensic data and intelligence is paramount. Automation of routine investigatory tasks and tools that facilitate cross-organisational corroboration is ideal for optimally reducing mean time to respond. (See Figure 3.) Ideally, your team would have a facility in which to keep track of all active and past investigations so that this information is well organised and available for future investigations.

Neutralise

The ultimate objective of the Neutralise phase is to mitigate the risk presented by the threat. The actions to be performed depend on the threat's progress, but common examples include isolating compromised systems and deactivating user accounts with stolen credentials.

Recover

The last phase, Recover, focuses on recovering normal operations and making sure that the threat cannot successfully perform a similar attack in the future. This phase is when exploited vulnerabilities are identified and addressed so that they are not exploited again, as well as where systems are rebuilt, user credentials are reset, and altered data is restored from backups so that operations can resume. Many other tasks also occur within this phase, including reporting on the root cause of incidents, reviewing how efficiently and effectively incidents were handled, and adapting the organisation's practices to take lessons learned into account.

The ribbons at the top of Figure 2 indicate that the first three TLM phases involve detection and the next two phases involve response. In order to identify threats as early in the Cyber Attack Lifecycle as possible, TLM's detection phases must be performed at all times. Similarly, TLM's response phases must be performed rapidly whenever needed. The combination of near-immediate detection and rapid response promotes finding and stopping attacks long before they are able to reach their ultimate targets and accomplish the attackers' objectives.

As if the need for around-the-clock monitoring, detection, and response was not daunting enough, consider the sheer volume of data. People simply cannot study all this data in a timely fashion, nor can they readily correlate pieces of data from different times to piece together a serious attack– especially when there is not a large staff to do so. The only practical solution to TLM is to rely heavily on automation techniques that do as much of the work as possible and involve people only when needed.

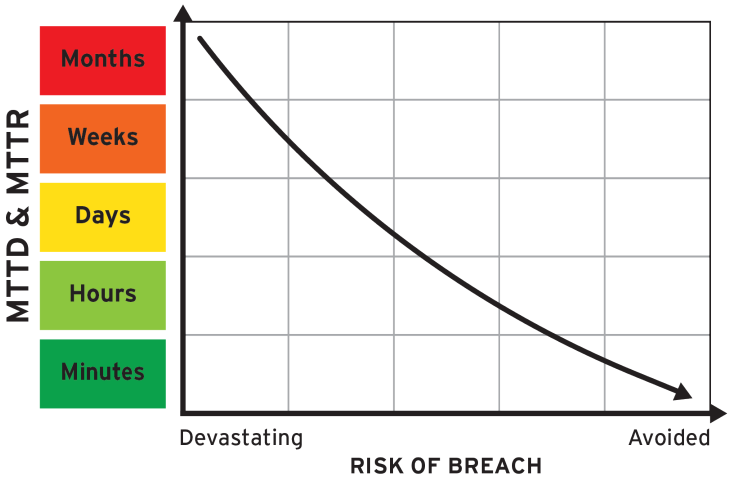


Figure 3: The impact of a breach is directly related to mean time to detect (MTTD) and mean time to respond (MTTR).

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

A SOC leveraging an effective TLM platform provides highly sophisticated and fully integrated automation techniques for all six phases of the TLM. The TLM platform fuses people, processes, and technology into an efficient security operation. This minimizes reliance on people and enables decentralisation of the SOC team by fostering collaboration through the TLM platform.

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 TLM 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 TLM platform-provided automation for the SOC. This enables an 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 minimizing damage and other costs.

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

People

No matter how well automated a SOC is, people are still absolutely necessary. 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 TLM. Typical tasks include monitoring alarms from the TLM 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. Here 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 equivalents (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 minimized.
- 8x5 SOC: Organisations greatly reduce risk just by performing effective Threat Lifecycle Management during business hours (or even partial business hours). But this option is most successful if the 8x5 SOC is relying on a TLM 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 is used, relies on processes. Technology brings people and processes together—such as a TLM platform notifying a security analyst of something that needs immediate attention, or an incident responder commanding a TLM 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 TLM platform as needing further investigation by an incident responder. The TLM platform is providing workflow capability that transfers responsibility for the work from the security analyst to the incident responder.

TLM platforms are capable of fostering 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 TLM 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 a TLM platform is essential, because it performs security automation and orchestration to ensure that everyone is kept up to date on the current 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, TLM platforms provide the ability to check on workflows to ensure that nothing is overlooked or handled too slowly.

Technology

A TLM 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 TLM 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 the TLM and 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. The TLM 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 TLM 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 delivers end-to-end Threat Lifecycle Management by bringing together historically disparate solutions into one unified platform. The LogRhythm 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 TLM 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 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 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 labor and services costs for common SOC staffing models for small, medium, and large SOCs. (See Cost Comparisons of Various SOC Staffing Models on page 11.) These estimates show that for all sizes of SOCs, labor and service costs are highest for SOCs not based on a TLM platform. This is because there is far more monitoring, analysis, investigation, prioritisation, forensic data collection, and incident response, management, and reporting work to be done by humans instead of the TLM 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 TLM-enabled 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 TLM platform could reduce costs by millions of dollars 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 are unable to 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 labor. At roughly $100 an hour, that's nearly $100,000 lost in a single day. Around-the-clock monitoring from a TLM 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 a TLM platform can provide large ongoing cost savings for organisations.

Around-the-clock monitoring from a TLM 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 TLM 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 FTEs @ $150K	2 FTE @ $150K	3 FTEs @ $150K each
Total	**$585K**	**$2,140K**	**$4,760K**
Fully in-house TLM-enabled 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 FTEs @ $150K each	2 FTEs @ $150K each
Management	0.25 FTEs @ $150K	0.5 FTE @ $150K	1 FTE @ $150K
Total	**$328K**	**$995K**	**$1,990K**
Hybrid TLM-enabled SOC	**8x5 onsite, offsite MSSP all other times**	**IR onsite 16x5, all others offsite MSSP 24x7**	**Offsite MSSP 24x7**
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 FTEs @ $150K	0.25 FTE @ $150K	0.5 FTE @ $150K
MSSP service	$250K	$400K	$750K
Total	**$445K**	**$778K**	**$1,505K**
Fully outsourced TLM-enabled 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	1.5 FTEs @ $145K each
Specialists (malware reverse engineers, forensic analysts, etc.)	0	0	0
Management	0.25 FTEs @ $150K	0.5 FTE @ $150K	1 FTE @ $150K
MSSP service	$350K	$600K	$900K
Total	**$460K**	**$820K**	**$1,268K**

Steps for building a SOC with limited resources

Based on experiences helping a wide variety of organisations, LogRhythm experts have developed a methodology for building a SOC that leverages a TLM platform. The seven items below 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 be able to 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 TLM platform

ii. identifying the business systems, information systems, and so forth that should be integrated with the TLM platform in order 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 Cyber 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

These must cover all six phases of TLM. 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 minimize 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 important 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. Testing should be performed 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. Other maintenance will be needed periodically, including reviewing the SOC model, SOC roles, FTE counts and so forth, so that adjustments can be made.

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

Conclusion

Having a security operations centre has become an absolute necessity for implementing Threat Lifecycle Management to minimize damage caused by successful attacks. A resource-efficient 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 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 minimizes 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-TLM-emea/

LogRhythm®

About LogRhythm

LogRhythm, a leader in Threat Lifecycle Management, empowers organisations around the globe to rapidly detect, respond to and neutralise damaging cyberthreats. The company's patented award-winning platform unifies next-generation SIEM, log management, network and endpoint monitoring, user entity and behaviour analytics (UEBA), security automation and orchestration (SAO) and advanced security analytics. In addition to protecting customers from the risks associated with cyberthreats, LogRhythm provides compliance automation and assurance, and enhanced IT intelligence.

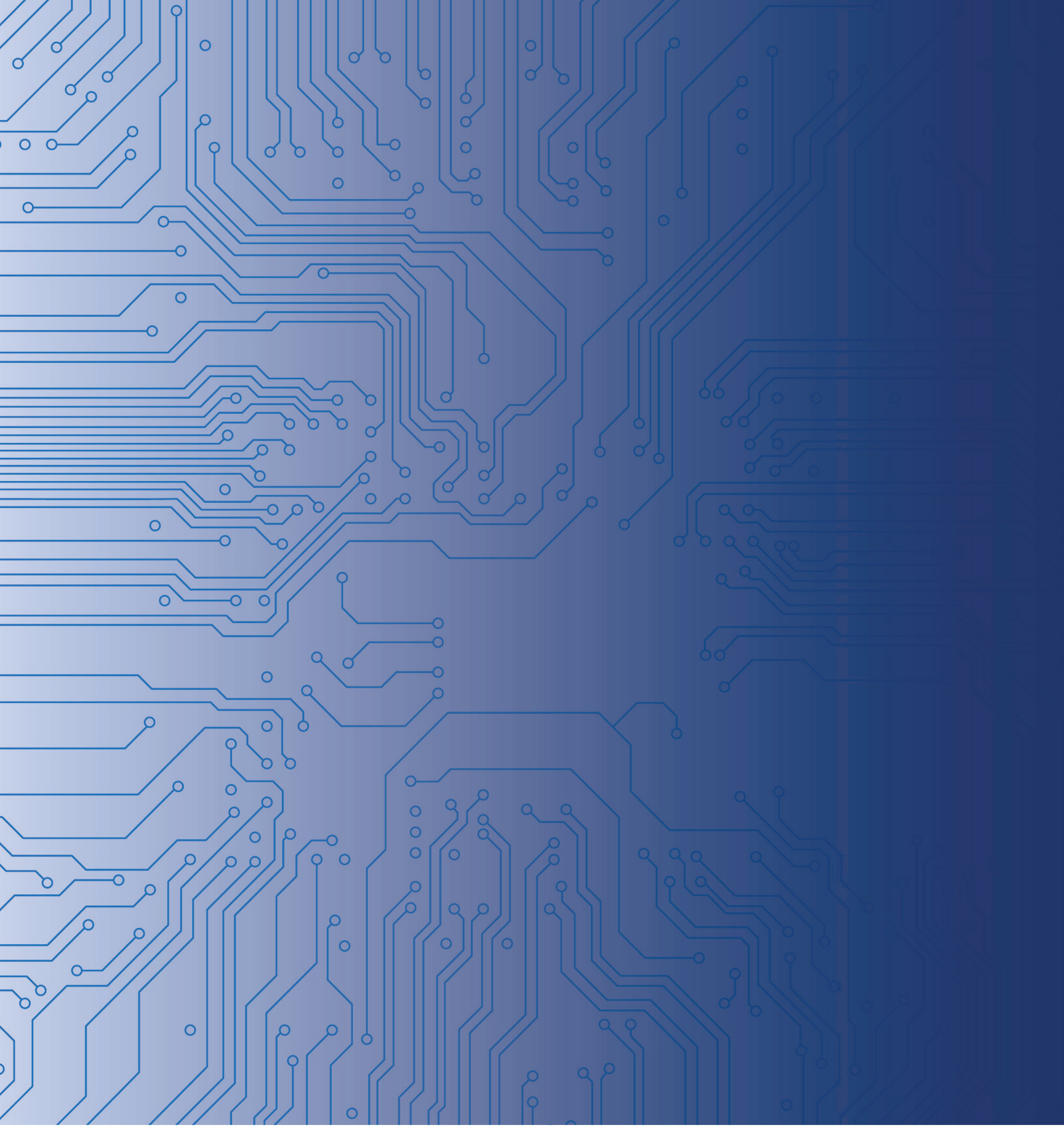
Among its many industry accolades, LogRhythm has been positioned as a Leader in Gartner's SIEM Magic Quadrant, received SC Labs' "Recommended" rating for SIEM and UTM for 2017 and won "Best SIEM" in SANS Institute's "Best of 2016 Awards."

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.)



Contact us:

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

europe@logrhythm.com
www.logrhythm.com
+44 (0)1628 918 300

LogRhythm®
The Security Intelligence Company