LogRhythm™

Modernizing Your SOC Strategy

Contents

Introduction

Modernizing your security operation center (SOC) strategy means investing your time, budget, or resources to enhance security maturity, improve resilience against cyberattacks, and reduce risk to the business in the modern-day digital world.

Over the last decade, the cybersecurity industry has evolved immensely. Organizations across the globe face a multitude of new security challenges due to things like digital transformation, mobile devices, disparate and remote workforces, and the convergence of IT and operational technology (OT). To reduce risk to the business, chief information security officers (CISOs) must develop a robust and reliable SOC strategy that is scalable amid a diverse set of security threats.

A modern SOC strategy leads to many business benefits, such as enabling growth while securing proprietary and sensitive data, building customer confidence and brand loyalty, increasing return on investment, preventing operational disruptions, and exceeding compliance requirements.

Drivers for SOC Modernization

Before we dive into tips for *how* to modernize your SOC, let's cover *why* this is so important. Along with overarching benefits to the business, here are several key drivers to modernize your SOC strategy.

Enhance the cybersecurity analyst experience

A fundamental reason for modernizing your security operations is to make the analyst experience as simple and effective as possible. There is a lot riding on the shoulders of security professionals. The workload can be substantial and SOC teams face pressure to properly manage cyber risk. Attrition rates tend to run high in the cybersecurity industry, but there are meaningful steps you can take to streamline operational workflows and improve the day-to-day analyst experience.

To keep pace with the high volume of daily alerts, many CISOs have invested in machine learning (ML) or automation capabilities to streamline operations and help security analysts better manage time-consuming or mundane tasks. Following a systematic approach can decrease false positives and lead to high-fidelity alerts that security analysts can prioritize. Improving the analyst experience will reduce fatigue and allow your team to focus on targeted and strategic tasks that foster a more productive and happier workforce.

Align with shifts in IT infrastructure, applications, and data

Over the last decade, the way organizations manage their infrastructure, applications, and data has evolved—and therefore, so has the attack surface. There are several major contributing factors to this evolution which has changed the way security teams defend their organization.

LogRhythm partnered with Ponemon Institute to conduct a research study with over 1,400 cybersecurity professionals across the globe. Our research found that the top three security challenges organizations face, include:

64%

Securing the remote workforce

61%

Managing third-party risks

59%

Finding and remediating vulnerabilities in software applications

In late 2019, the unforeseen spread of COVID-19 forced businesses across the globe to quickly move from an on-premises operation to a remote-work model. This increased risk to sensitive data because of less secure home networks, security protocols were not followed as closely as when in the office, and employees were more likely to conduct work using personal devices.[1] A spike in cloud and software as a service (SaaS) usage, created new pain points for CISOs trying to manage visibility and protection of a remote workforce. Although many organizations were already shifting away from a perimeter defense strategy, the pandemic accelerated and validated the need to modernize security operations and implement Zero Trust principles.

Cloud adoption is also a major reason for the expanded attack surface. Cloud services are more common today than ever before, because they enhance business processes and competitiveness in the market, enable swift innovation, and reduce IT operational costs. With so many benefits, organizations are shifting from legacy infrastructure and on-premises data centers to hybrid or cloud environments. When migrating digital assets, such as data, workloads, IT resources, and applications, to different types of infrastructure, the environment becomes more challenging to holistically protect due to the variety of security process and controls.

Infrastructure as a service (IaaS), platform as a service (PaaS), and SaaS all create new challenges for security teams dealing with a "shared responsibility model." With data moving dynamically across the organization, cloud, and different SaaS vendors, security professionals need a greater understanding of what data exists in all those environments and who should have access to it.

Shared Responsibility Model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification and policy	●	●	●	●
Client and endpoint protection	●	●	●	◪
Identity and access management	●	●	◪	◪
Application level controls	●	●	◪	■
Network control	●	◪	■	■
Host infrastructure	●	◪	■	■
Physical security	●	■	■	■

Figure 1: The shared responsibility model.

● Cloud customer ■ Cloud provider

[1] https://gallery.logrhythm.com/analyst-reviews-and-reports/na-report-ponemon-security-and-csuite.pdf

Manage the lifecycle of cyberthreats and streamline incident response

Modernizing your security operations is essential for an effective end-to-end threat management process. SOC analysts need a unified approach to manage threats and effectively respond to an incident before exploitation or exfiltration occurs. To meet the demand of today's modern threat landscape, you must implement solutions or processes that will help to:

- Prioritize indicators of compromise (IOCs) and threat actors
- Leverage context with security alerts and tell an accurate story with the data
- Improve KPIs such as mean time to detect (MTTD) and mean time to respond (MTTR)
- Retain visibility and enhance threat detection and response across a diverse environment

Reduce siloes and security gaps

Siloed teams, workflows, and technologies are a constant and growing headache for many professionals. Security tools can enhance maturity and ensure compliance, but only with proper resources, management, and continuous validation. SOC analysts need a unified approach to navigate multiple tools and effectively correlate data from different security controls.

Cross-functional collaboration is also critical to align data security teams, IT staff, and SOC professionals with common goals and objectives. Departments should work together to identify valuable data that must be protected and improve fragmented policies, workflows, and visibility. Modernizing your SOC can help reduce siloes and security gaps across the organization, thus streamlining your people, processes, and technology.

Measure and report on the overall security posture

Cybersecurity should be treated as a critical business component because a mature program will extend efficiency and innovation across key areas of the organization and increase return on investment (ROI). Aligning security outcomes with business objectives provides visibility into how risk posture impacts the organization, its operational priorities, annual trends, future outcomes, and more.

Many security professionals have trouble quantifying or telling a story about how their security or compliance operations enable the business and saves money in the long run. SOC modernization can help streamline methods for reporting KPIs that tie to business objectives to gain board-level support and justify future funding.

How to Modernize Your SOC

Faced with a shortage of SecOps talent, a distributed or remote workforce, and a plethora of cyberthreats, you need to create a SOC strategy that streamlines your people, processes, and technology.

Everyone's path to achieving a modern SOC looks different. How you move forward is largely dependent on your business objectives, the requirements of your security team, what resources and skill sets you have available, and the infrastructure you have in place. Here are actionable steps to consider when modernizing your SOC strategy.

1 Align your security strategy with business objectives

It's an ongoing issue that cybersecurity is too focused on technology at the expense of business value. The lack of a cohesive top-down strategy and continuous communication across the organization leads to siloed teams with different goals or competing priorities. Today's modern CISO requires a level of business acumen to build relationships with stakeholders and communicate in terms of risk to corporate boards. If you want to develop a solid program that is supported and funded, you must work with key stakeholders to determine how security aligns with business objectives.

Get started by conducting interviews with business and risk management teams and IT leaders to understand the top priorities and threats that pose the most risk to the organization. Consider these topics to address with stakeholders:

- Understand the business objectives and how stakeholders plan to scale and grow in the future.
- Determine which compliance or industry standards are mandated, and which requirements stakeholders may want to exceed for business reasons.
- Discuss risk management and understand the highest risks (e.g., reputational damage, financial disruption, and loss of life).
- Cover key security metrics relevant to company initiatives and goals.
- Review budget or funding limitations for security to support business efforts and discuss whether top initiatives are obtainable with an insource, outsource, or hybrid SOC model.

As you develop your plan and define your strategy, determine operational-driven metrics that prove how security drives better business outcomes. This will help you set expectations and communicate impactful results to the board. By building strong, long-term relationships with various stakeholders, security executives have a much greater chance of creating meaningful change and making security a company-wide priority.

2 Assess security maturity

Another key step to modernizing your security operations is to evaluate the maturity of your security posture and identify any security gaps. To guide you through this process, LogRhythm developed the Security Operations Maturity Model, which is a vendor-agnostic tool to help you assess and improve the maturity of your security operations.

Whether you are a security team of two, or have the resources to run a 24/7 SOC, you can use this free resource as a starting point to measure the capabilities of your security program. The SOMM tool is a great way to benchmark your current maturity and develop a roadmap to improve your posture based on available resources, budget, and risk tolerance. With this insight, you can present concrete evidence that you're improving the organization's security stance over time and tie reports to better business outcomes that will garner additional support from the board.

Improve Visibility

- Identify and eliminate blind spots
- See events across different systems/domains
- Accelerate threat investigation and incident response

Quickly Identify Threats

- Detect threats earlier in the attack lifecycle
- Surface difficult-to-detect threats
- Reduce business impact

Decrease Response Time

- Gain insight to make better decisions
- Be organizationally efficient
- Respond more quickly to threats

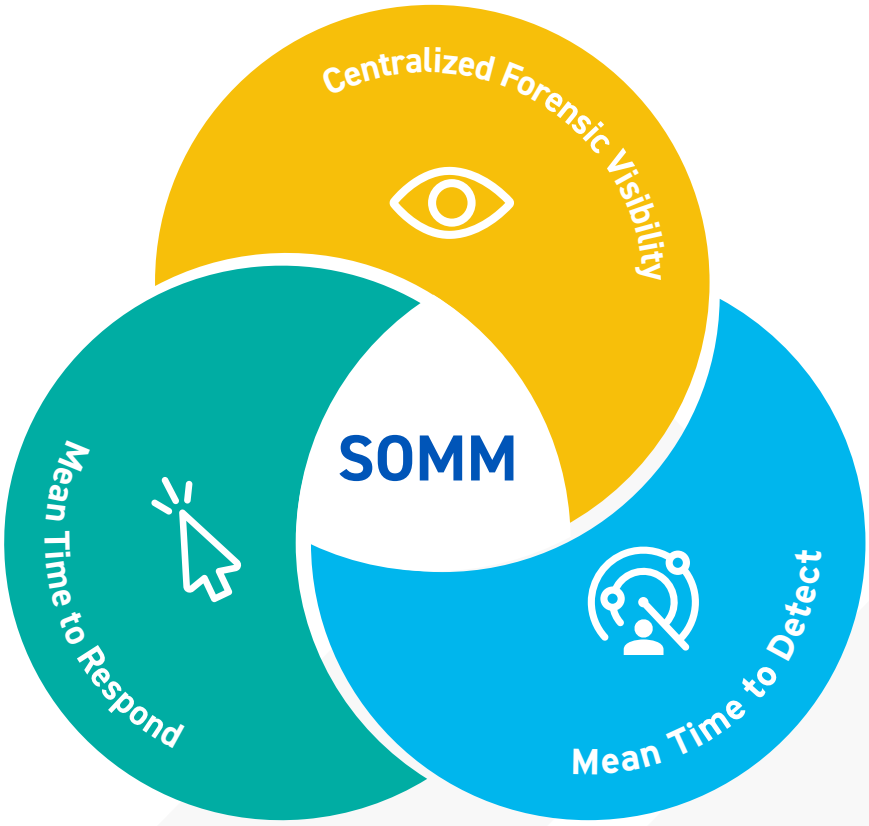

Figure 2: LogRhythm Security Operations Maturity Model.

3 Prioritize threat use cases

Once you understand the risk to the business and gaps in your security posture, you should devise a concrete plan to develop threat use cases. Determine the most important problems or gaps to address first based on the activities happening within your environment and the goals defined from step one and two. This will provide a top-down approach to prioritize use cases and report progress back to the board.

External threats like ransomware and phishing run rampant across all industries. Security vendors may provide out-of-the-box use cases to quickly reduce risk to common threats, but even with thousands of use cases at your disposal, you must focus on the top ones that apply to your environment. It's critical to develop a plan for the lifecycle management of use cases as well.

For SOCs building a workflow using a security information and event management (SIEM), LogRhythm Analytic Co-Pilots recommend applying the six-step methodology shown in Figure 3. To maximize return on investment, revisit use cases every three months and create a continuous process to test and tune rules.

If your security team is strapped with little resources, there are threat intel networks that you can join at little cost to stay up to date on trending threats tailored to your industry. Information sharing and analysis center (ISAC) groups are great sources to gain insight from other cybersecurity professionals regarding trending tactics and techniques, indicators of compromise, and ways to lower false positives.

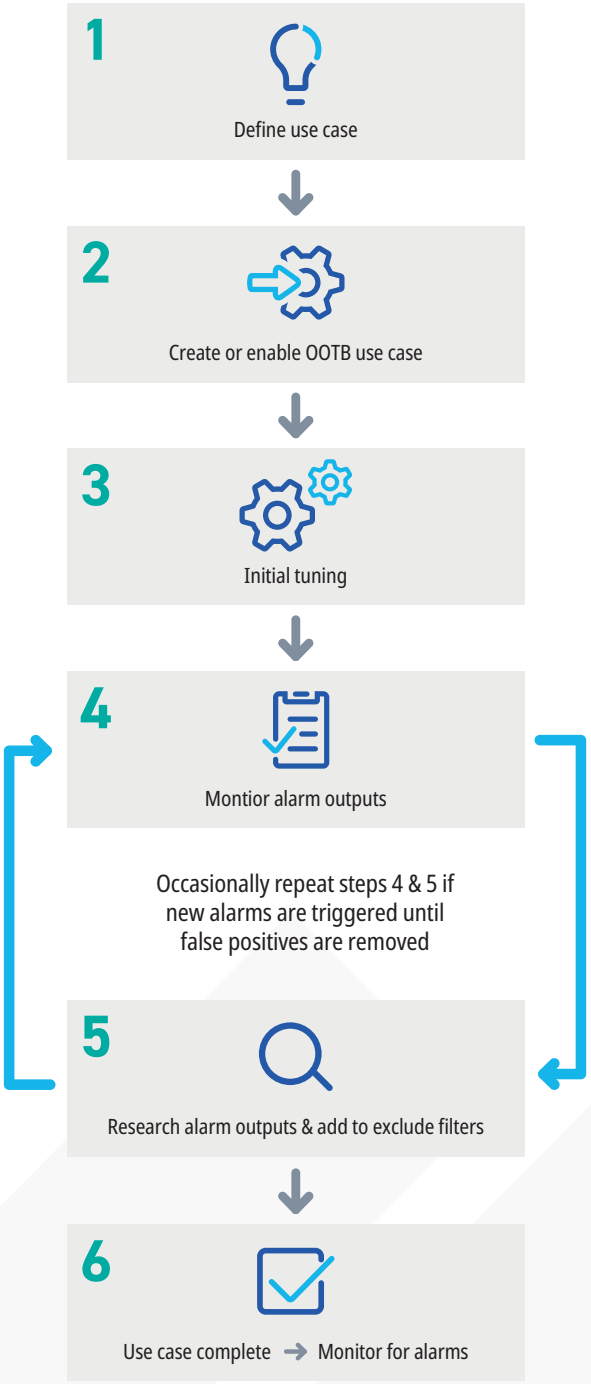

Figure 3: Lifecycle management of use cases.

4 Work towards a Zero Trust architecture

Over the past couple of years, severe cyberattacks have compromised national intelligence and disrupted critical infrastructure; instances ranging from the SolarWinds breach and Colonial Pipeline ransomware attack to the widespread Log4j vulnerability exemplify the need to make security a top priority. Over the past decade, it's become clear that a perimeter-based defense strategy is not sufficient to holistically secure systems and data, but that an assume-breach approach is required. To address these challenges, Zero Trust is a leading security model of choice, with the foundation of "never trust, always verify" as a core principle. Rather than focusing on the corporate perimeter, this strategy is an identity-centric model that focuses on securing resources (e.g., data, identities, and services), regardless of their location. A Zero Trust strategy presumes all networks are untrusted, applies least privilege access, and assumes breach, therefore requiring the inspection and monitoring of everything.

In 2021, the White House announced significant investments to modernize federal government cybersecurity with the mission to transition to a new defensible architecture; President Biden's Executive Order on Improving the Nation's Cybersecurity detailed Zero Trust at the forefront of their strategy and stated how the "Federal Government must lead by example" to make the prevention, detection, and remediation of cyber incidents a top priority.[2]

Sec. 3. Modernizing Federal Government Cybersecurity

(a) To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including by increasing the Federal Government's visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including SaaS, IaaS, and PaaS; centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals.

Read the Executive Order

[2] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Although only federal agencies are expected to meet Zero Trust security goals by the end of the Fiscal Year (FY) 2024,[3] organizations in both the public and private sector looking to transform their architecture can leverage the government's process as a guide to implementing Zero Trust. That said, everyone's path to Zero Trust looks different, and there are many roadmaps from other companies that you can reference. To help you implement the strategies, tactics, and solutions required for a robust Zero Trust architecture, here are some useful resources:

- CISA Zero Trust Maturity Model: The Cybersecurity & Infrastructure Security Agency developed a maturity model to help agencies comply with Biden's executive order. This will help you assess your security posture regarding their five pillars of Zero Trust (e.g., Identify, Device, Network, Application Workload, and Data), as well as their three capabilities for Visibility and Analytics, Automation and Orchestration, and Governance.
- NIST Special Publication 800-207: The National Institute of Standards and Technology offers a formalized approach to implementing Zero Trust without vendor lock-in.
- Forrester Zero Trust eXtended Ecosystem: Forrester's ZTX model will help you clearly define what you need to achieve Zero Trust from a technical and operational standpoint. It also lists notable vendors that enable Zero Trust capabilities.
- The Identity Defined Security Alliance (IDSA) Framework: IDSA has an identity-defined Zero Trust approach that practitioners can use as a blueprint to achieve better security outcomes.
- How to Build a Zero Trust Ecosystem: Gain practical tips for charting a strategy from our real-world example. In this white paper, you'll learn about LogRhythm's road to Zero Trust, including our process, technology roadmap, and timeline deliverables.
- Free Zero Trust resources: LogRhythm developed a collection of templates to help you organize and manage your Zero Trust initiatives (e.g., business case, project charter, budget, project plan, status report, and technology architecture).

To get started with Zero Trust, you need a strong business plan that details new investments and estimates ROI for security and operational efficiency gains. For example, eliminating legacy technology such as VPN software or corporate perimeter firewalls can reduce maintenance costs that you can redirect to technology that enables your Zero Trust goals. Security and IT leaders should work together to implement Zero Trust and determine solutions for the highest value data assets first. When transforming your security architecture, you'll likely operate in a hybrid Zero Trust and legacy mode as you make incremental changes to incorporate new processes or shift technology infrastructure.

[3] https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

5 Map to industry standards and detection frameworks

With Zero Trust principles in mind, always assume there is a breach, and proactively hunt for threats. To strengthen the detection approach, you can leverage the MITRE ATT&CK™ framework alongside standards like NIST, further closing any gaps in your security ecosystem.

ATT&CK delivers actionable intelligence based on known adversary behaviors modeled from specific threat observations. When implemented optimally, it helps defenders understand how techniques and tactics map to adversary behavior in their specific environment and ensure that no incident goes unnoticed. To improve accuracy and scale threat detection, you can use a SIEM solution for high-fidelity visibility into ATT&CK tactics, techniques, and procedures (TTPs).

For example, organizations leverage MITRE ATT&CK's framework with LogRhythm's SIEM platform using network, endpoint, and user-based analytics, as well as threat intelligence to generate higher-value alarms. The LogRhythm MITRE ATT&CK Module provides prebuilt content mapped to ATT&CK which enables security teams to gain better visibility of adversary behaviors and improve security operations.

LogRhythm Labs

LogRhythm Labs is a dedicated team that delivers security research, analytics, and threat intelligence services to mature SOC capabilities and better protect organizations from cyberthreats.

To learn more about MITRE ATT&CK and how to apply common techniques to your defense, read this comprehensive break down from our threat research team.

Learn More

How LogRhythm Can Help with SOC Modernization

Your organization and security goals are unique. We're here to listen and provide guidance for the best possible solution based on your needs. To modernize your SOC strategy, here's how LogRhythm can help streamline your people, process, and technology.

Security maturity assessment

With two decades of experience in cybersecurity, LogRhythm provides a consultative approach to gauge your current security posture and then we work together to create a roadmap for increased maturity to help you achieve your goals.

LogRhythm Labs threat research

Our LogRhythm Labs team is our mission control center, proactively analyzing emerging threats and building new rules, dashboards, and modules to help you defend against them. We give you the upper hand by providing continuous intelligence, tools, and out-of-the-box solutions based on threats and compliance requirements your organization faces.

Cutting-edge security technology

The LogRhythm SIEM Platform is built to provide unmatched visibility, protection, and threat detection across the environment using the latest security functionality and security analytics. With LogRhythm SIEM, your team has embedded modules, dashboards, and rules that help you quickly and effectively deliver threat monitoring, threat hunting, threat investigation, and incident response.

Services to support your team

When you work with LogRhythm, you have a team of experts available to help you with your security goals. We offer targeted services to maximize your return on investment and improve your organization's security maturity.

Schedule time with one of our security experts to discuss your use cases and learn how LogRhythm can help modernize your SOC strategy.

Contact Us

About LogRhythm

LogRhythm helps busy and lean security operations teams save the day—day after day. There's a lot riding on the shoulders of security professionals—the reputation and success of their company, the safety of citizens and organizations across the globe, the security of critical resources—the weight of protecting the world.

LogRhythm helps lighten this load. The company is on the frontlines defending against many of the world's most significant cyberattacks and empowers security teams to navigate an ever-changing threat landscape with confidence. As allies in the fight, LogRhythm combines a comprehensive and flexible security operations platform, technology partnerships, and advisory services to help SOC teams close the gaps.

Together, we are ready to defend.
Learn more at logrhythm.com.

www.logrhythm.com // info@logrhythm.com

United States: 1.866.384.0713 // United Kingdom: +44 (0)1628 918 330
Singapore: +65 6222 8110 // Australia: +61 2 8019 7185