WHITE PAPER

Navigating Cybersecurity with an Effective Security Operations Center

Uncover which SOC model is the best fit for your organization's needs.

SOPHOS

Executive summary

The cybersecurity landscape is in a constant state of flux, with threats becoming more sophisticated and pervasive. In this environment, Security Operations Centers (SOCs) are essential for organizations to quickly detect, analyze, and respond to cyber incidents. Organizations need to decide whether an in-house, hybrid, or outsourced SOC model is best for them, and then ensure they use the right metrics to measure its performance for continued security while remaining aligned with business objectives.

63% of businesses

Fall victim to ransomware due to lack of people or skills.[1]

The role of a SOC in today's cybersecurity landscape

The digital age has brought with it an increase in cyber threats, with cybercriminals and state-sponsored actors launching sophisticated attacks. Current trends indicate a worrying reduction in the time from initial breach to ransomware deployment, which now averages just 2 days.[2] The cybersecurity industry also continues to face a significant talent shortage, further complicating the establishment and maintenance of an in-house SOC.

A SOC is an organizational function dedicated to managing processes for identifying, investigating, and remediating security incidents. Specific responsibilities may include asset management, change management, vulnerability management, security event management, incident management, as well as the incorporation of threat intelligence and various DevOps activities such as automation and quality assurance. While SOCs do not control every aspect of an organization's security, they play a crucial role in coordinating their response to security issues. The specific mission and goals of a SOC can vary widely, influenced by factors such as the organization's risk tolerance, industry sector, maturity level, and the tools and processes it employs.

Talent shortage

The cybersecurity industry continues to face a significant talent shortage.

Types of SOC models

Organizations can choose from several SOC models, each with its own set of characteristics and benefits:

In-house SOCs are typically found in well-funded organizations that can support continuous operations with a dedicated team. These SOCs may still outsource certain specialized functions, such as penetration testing, expert threat hunting, or threat intelligence. Large or geographically dispersed organizations may use a tiered model with multiple SOCs operating under a unified command structure.

Hybrid SOCs have become increasingly popular, combining in-house resources with external services to create a tailored security function in a partnership model. The security services provider is commonly responsible for 24/7 monitoring and alert triage, incident investigations, threat hunting, and providing expert support. This enables the internal team to maximize their resources through activities such as security architecture and design, policy and compliance management, risk mitigation, security awareness training and executing response actions when the organization prefers to keep remediation in-house. This is particularly attractive due to the flexibility it offers and the ability to address skill shortages and budgetary constraints.

A fully outsourced SOC is a third-party service that provides comprehensive cybersecurity monitoring and response capabilities. Organizations that need to quickly establish a baseline SOC without the necessary in-house expertise may turn to this model, putting their trust in an established managed detection and response (MDR) provider. The organization can enable the external vendor to integrate with their existing IT and security technologies for broad visibility across the environment, and to coordinate incident response activities.

Did you know?

88% of ransomware attacks are deployed outside of standard business hours.[2]

Which model is right for you?

Determining the right SOC model for your organization depends on multiple factors, including your overall risk profile. You must weigh your organization's acceptable risk level versus the budget willing to put toward cybersecurity. Several key considerations come into play, including:

1. Internal resource constraints (the availability of expertise or people/capacity)
2. The balance between what needs to be owned in-house versus outsourced
3. The current maturity of your security operations
4. The challenge of hiring, training, and retaining key talent with specialist skills
5. The need for continuous engagement with emerging technologies and staying ahead of the ever-evolving threat landscape and active adversary techniques
6. Interdepartmental dependencies on IT, legal, risk, compliance and other business departments

Whichever model you pursue, it's important to develop a business case to justify the model and resources required for long-term sustainability. Regular assessments of your SOC's capabilities are also crucial to ensure it aligns with the intended design and operational goals.

Most organizations are facing a cybersecurity talent shortage, and many budgets simply preclude building and maintaining a fully staffed 24/7 in-house SOC. Experienced CISOs also understand the value of retaining strategic control over their cybersecurity operations, and by extension the long-term sustainability of their organization, by maintaining oversight and control.

Benefits of a hybrid SOC model

- ✓ The hybrid SOC model offers a compelling blend of the benefits of both in-house and outsourced approaches. It allows organizations to leverage the expertise and efficiency of a third-party provider while maintaining a level of customization and control over their security operations.

- ✓ One of the primary benefits of a hybrid SOC is the access and scale it provides to seasoned security experts and validated threat intelligence. These professionals are part of a larger pool of talent that is continuously exposed to an extensive range of threats, enabling them to stay abreast of the latest developments in the cybersecurity field. This exposure is something that a standalone in-house team would usually struggle to match, given the rapid evolution of the threat landscape.

- ✓ In addition, partnering with a third-party provider ensures continuous coverage—24/7, 365 days a year—including nights, weekends, and holidays when internal teams may be offline.

- ✓ A hybrid SOC can significantly reduce alert fatigue by helping organizations fine-tune their detection systems, thereby lowering mean time to respond (MTTR) to incidents. Organizations can also avoid the substantial costs associated with dedicated threat research, as their external partners will conduct this on their behalf, continuously adding new detection capabilities as they are developed.

- ✓ Another advantage is the ability to focus internal resources on core IT, technology, and compliance issues, while the SOC partner concentrates on security incidents. This division of labor allows for a more efficient allocation of resources and expertise. It can also allow other departments to focus on their additional security-related responsibilities.

- ✓ Cybersecurity training, which can be costly and time-consuming, is streamlined in a hybrid model. The external provider ensures that their staff are up to date on all aspects of cybersecurity, from forensics and malware analysis to incident response and cloud security. This relieves the internal team of the burden of maintaining expertise in every facet of cybersecurity, allowing them to focus on areas that are most relevant to their business.

- ✓ The hybrid SOC model also offers flexibility to tier operations based on the organization's risk appetite and to adjust response methodologies accordingly. This can lead to more effective and targeted security measures. Additionally, the cost savings associated with a hybrid SOC make it an attractive option not only for small to midsize enterprises but also for larger organizations looking to outsource certain security functions.

Measuring SOC effectiveness

Whichever model is right for you, to gauge the effectiveness of a SOC, it is essential to employ a set of metrics that reflect the security landscape and the efficacy of the SOC's resources. The suggested metrics below, plus others, can be summed up in a dashboard to show real-time counts, plus weekly, monthly, and quarterly stats to track trends over time, with a focus on SOC responsiveness and investigation quality.

For the security landscape, metrics should provide insight into the scope and volume of potential threats, the organization's vulnerability points, and the overall risk exposure. Examples include the volume of suspicious or malicious emails received, the number of scanning and exploit attempts against external systems, and the number of security incidents by origin.

When looking at SOC efficacy, metrics should track performance against stated policy and posture goals, which are tied to business outcomes such as reduced risk and regulatory compliance. This includes responsiveness and investigation quality, the breakdown of time spent by security staff on various activities, the number of incidents by compliance category, and the amount of engineering work tied to reducing the attack surface. Key metrics also include investigation triage time, the number of investigations with corrective actions taken, the number of corrective actions based on proactive threat hunts, and the number of patched vulnerabilities sorted by severity.

By regularly monitoring these metrics, organizations can ensure that their SOC is not only operating efficiently but also contributing to the overall security posture and business objectives.

Metrics should:

- Provide insight into the scope and volume of potential threats
- Find an organization's vulnerability points
- Show overall risk exposure
- Track performance against stated policy and posture goals

Key metrics:

- Investigation triage time
- Number of investigations with corrective actions taken
- Number of corrective actions based on proactive threat hunts
- Number of patched vulnerabilities sorted by severity

Find an advanced SOC solution

Every business is different, with varying levels of security maturity. With an ever-evolving threat landscape, access to a competent SOC is necessary for any organization serious about their cybersecurity. Whether organizations choose to build in-house capabilities, work with an external provider, or adopt a hybrid approach, the right partnership can ensure both effective defense and alignment with business goals.

Many businesses are turning to hybrid or fully managed SOC models to address talent shortages, budget constraints, and the growing complexity of cyber threats. These models offer flexibility, expert insight, and 24/7 coverage—empowering internal teams to focus on strategic initiatives while trusted partners deliver scalable security operations.

Sophos MDR exemplifies the power of this approach. With tiered offerings designed to meet organizations where they are on their cybersecurity journey, Sophos delivers advanced detection, investigation, and response capabilities tailored to the business's needs. Whether supporting an internal SOC team or operating as a fully outsourced partner, Sophos MDR enhances threat visibility and response, helping organizations strengthen their defenses and protect what matters most.

[1] Sophos, State of Ransomware Report 2025
[2] Sophos, 2025 Active Adversary Report

SOPHOS

Learn more about our managed detection and response services at sophos.com/mdr.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com