Secureworks®

WHITE PAPER

Navigating Cybersecurity with an Effective Security Operations Center

The cybersecurity landscape is in a constant state of flux, with threats becoming more sophisticated and pervasive. In this environment, Security Operations Centers (SOC) are essential for organizations to quickly detect, analyze, and respond to cyber incidents. Organizations need to decide whether an internal, 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.

The Role of a SOC in Today's Cybersecurity Landscape

The digital age has brought with it an increase in cyber threats, with both cybercriminals and state-sponsored actors launching sophisticated attacks. Recent trends indicate a worrying decrease in the time from initial breach to ransomware deployment, now as low as 24 hours.

Gartner's research suggests that by 2025, a third of organizations will struggle to establish an effective internal SOC due to limitations in budget, expertise, and staffing. Additionally, the cybersecurity industry faces a significant talent shortage, further complicating the establishment and maintenance of an in-house SOC.

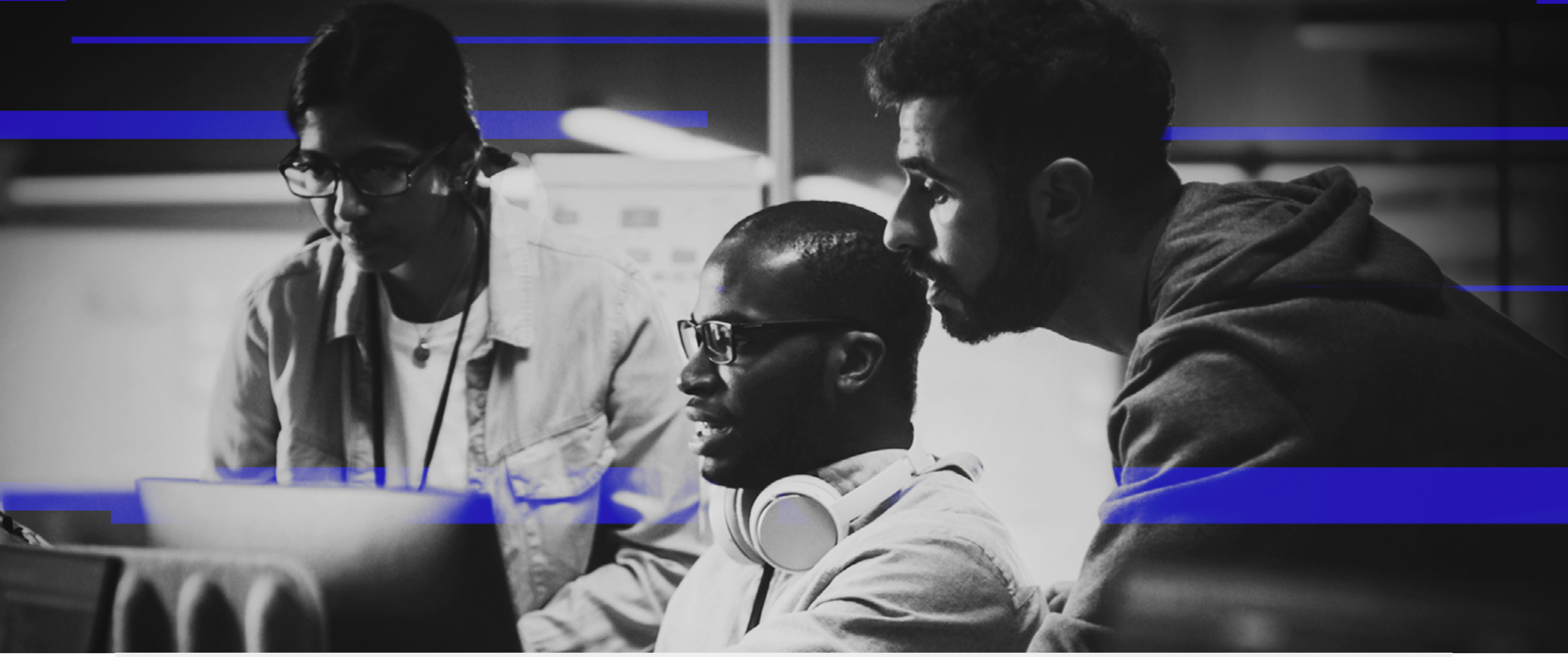
A SOC is an organizational function dedicated to managing processes for identifying, investigating, and remediating security incidents. Specific responsibilities may include asset management, change management, vulnerability management, security event management, incident management, as well as the incorporation of threat intelligence and various DevOps activities such as automations and quality assurance. While SOCs do not control every aspect of an organization's security, they play a crucial role in coordinating the 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.

by 2025

a third of organizations will struggle to establish an effective internal SOC

the cybersecurity industry faces a significant

talent shortage



TYPES OF SOC MODELS

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

Internal 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 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 internal resources with external services to create a tailored security function in a partnership model. The security vendor 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 taking response actions when preferred to keep 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 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, but they must have complete trust in an external vendor and an ability to govern the outsourcer aligned with their risk-informed business case. The organization must allow the vendor to integrate with their IT operations to coordinate prevention, remediation, and infrastructure changes.

What 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 amount of spend you're willing to put towards cybersecurity. Several key considerations come into play, including:

1. internal resource constraints
2. the balance between what needs to be owned versus outsourced
3. the current maturity of your security operations
4. it's also important to consider the challenge of hiring, training, and retaining key talent
5. necessity for continuous engagement with emerging technologies and threats
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.

It's no secret that most organizations are facing a scarcity of cybersecurity talent, and many budgets simply preclude building and maintaining a fully staffed 24/7 internal 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 even with a limited team. It's no wonder that Gartner has found that by 2025, 90% of SOCs in the Global 2,000 will use a hybrid model and outsource at least 50% of their operational workloads.

BENEFITS OF A HYBRID SOC MODEL

- ✓ The hybrid SOC model offers a compelling blend of the benefits of both insourced 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 a wide range of threats, enabling them to stay abreast of the latest developments in the cybersecurity field. This exposure is something that a stand-alone organization may struggle to match, given the rapid evolution of the threat landscape.

- ✓ Moreover, 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 third-party partners will conduct this on their behalf, integrating 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.

- ✓ Furthermore, cybersecurity training, which can be costly and time-consuming, is streamlined in a hybrid model. The third-party provider ensures that their staff is 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 the business.

- ✓ The hybrid SOC model also offers the 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 selectively.

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 both 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 volume 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.

Find an Advanced SOC Solution

Every organization is different, with varying levels of security maturity. With an ever-evolving threat landscape, access to a competent SOC is a must for any organization serious about their cybersecurity. Unless organizations have substantial resources for an internal model, or are comfortable outsourcing this critical function to a third party, hybrid SOCs have become a go-to option for many.

Hybrid SOCs offer a range of benefits that can help organizations navigate the complexities of cybersecurity while optimizing their resources and capabilities. Secureworks® Taegis™ stands as a testament to the potential of advanced SOC solutions to bolster an organization's defense against the ever-evolving landscape of cyber threats.

Learn more about the Secureworks SOC at **secureworks.com/soc**.

Secureworks®

Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that secures human progress with Secureworks® Taegis™, a SaaS-based, open XDR platform built on 20+ years of real-world detection data, security operations expertise, and threat intelligence and research. Taegis is embedded in the security operations of over 4,000 organizations around the world who use its advanced, AI-driven capabilities to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

CORPORATE HEADQUARTERS

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

EUROPE & MIDDLE EAST

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111 00971
4 420 7000

ASIA PACIFIC

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp