BRIEF

The Five Types of Security Operations Center Models

To continuously monitor and respond to threats, organizations often turn to a security operations center (SOC), which provides centralized and consolidated cybersecurity incident prevention, detection, and response capabilities.

According to Gartner, there are five different models for building and maintaining a SOC. Some of these models only apply to very large enterprises, while other models work for businesses of all sizes.

Here we explain the difference between these models. We weigh the models in terms of cost, their benefits and downsides, provide guidelines that will help you make the best choice, and suggest alternatives for organizations that are in need of more affordable options.

✓ Virtual SOC

What: A virtual SOC (VSOC) does not reside in a dedicated facility, nor does it have dedicated infrastructure. It's a web-based portal built on decentralized security technologies, which allows off-site teams to monitor events and respond to threats.

Benefits: It saves you the significant costs of on-premises hardware and other infrastructure, and you can rely on virtual teams to become active when there's an incident.

Downsides: A VSOC is mostly a reactive approach. Decentralized technologies and processes are much more likely to leave security gaps, which makes threat detection and response less efficient. And because the VSOC typically operates with part-time, geographically distributed personnel, you won't be able to count on having a 24x7 team dedicated to security.

Alternative approaches: The VSOC can be improved through automation, SIEM technology, and analytics.

Some organizations also choose to outsource their VSOC. While this increases security capabilities and access to expert resources, it also decreases internal visibility across the environment and may lead to longer response times when an event escalates.

✓ Multifunction SOC/NOC

What: A combination of a SOC with a network operations center (NOC), this model has a dedicated team, facility, and infrastructure. A multifunction SOC/NOC goes beyond security functions to include IT operations, compliance, and risk management.

Benefits: The main advantage of this model is reduced cost, because it consolidates personnel and minimizes capital outlay. It is best suited for smaller organizations with low-risk exposures and those that already have overlapping security responsibilities across different teams.

Downsides: The multifunction SOC/NOC includes less emphasis on security. While the multifunctional team performs core security tasks, dividing attention over different IT, network, and security needs inevitably results in weaker security defenses.

Additionally, a multifunctional team needs to have broader skill sets to address a wide variety of issues. This means they're not likely to have deep security expertise. That's a big downside, because defending against today's sophisticated and evolving threats requires advanced, up-to-date knowledge of security best practices.

✓ Co-Managed SOC

What: In a co-managed SOC, on-site monitoring solutions increase while some responsibilities may be offloaded to external staff.

Key reasons to choose this model are resource constraints and budget limits. The trade-offs are loss of control and lack of customization of services and responsibilities. You need to find the right balance between the control you keep in-house versus what you outsource to the provider, as the effectiveness of this model depends on those two choices.

Benefits: A co-managed SOC offers more flexibility because you can deploy some technology, like security information and event management (SIEM) tools on-premises or in the cloud. You can also decide what size of an in-house team suits your needs best. When managed well, this model offers great benefits and can deliver good results.

Downsides: A typical co-managed SOC is delivered by managed security service providers (MSSPs) whose core expertise is not IT or security operations. This model is often more expensive because you may have to invest in additional hardware, and you also have increased overhead.

✓ Dedicated SOC

What: A dedicated SOC is a centralized SOC with a dedicated infrastructure, team, and processes focused completely on security. The size of a dedicated SOC varies based on the organization's size, risks, and security needs.

Typically, a dedicated SOC has at least five to eight in-house security experts at various levels for 24x7 monitoring and operations. A dedicated SOC is essential for global companies that have private data in various locations and must comply with regulations and security policies.

Benefits: A dedicated SOC provides complete ownership over technology and processes. The internal team also has the best capability to monitor your environment and will have the best visibility for a complete picture of your threat landscape and security.

Downsides: This model requires a huge upfront investment, which means it doesn't fit the budget of many organizations. It's best suited for large enterprises and government agencies with extensive IT infrastructure that are constantly under attack, as these organizations typically have the resources to build and maintain it.

✓ Command SOC

What: A command SOC has multiple SOCs distributed across multiple locations, often globally. Organizations that use this model include Global 2000 companies, large telecom providers, and defense agencies. The command SOC typically controls other SOCs and also performs forensics and other recovery processes.

Benefits: The command SOC is managed by a large team of security experts and a security research team with threat hunting capabilities.

Downsides: This model is more focused on managing threat intelligence and situational awareness than on day-to-day security operations.

✓ What's the Best SOC for Your Organization?

A SOC can be deployed as part of a comprehensive strategy to protect organizations large and small against advanced threats. But there's no one-size-fits-all solution that provides the perfect balance between cost and effectiveness.

For some businesses, limited security budgets and lack of internal expertise create barriers to implementing a program that is effective and provides sufficient protection. To solve this problem, organizations should consider selecting a managed security operations provider's SOC.

Managed security is an outsourced model that extends the capabilities of your in-house IT or security team. It includes a managed detection and response (MDR) solution, which removes the burden of determining the best methodology or technology for threat detection and response.

A managed security operations model augments current network security tools with continuous threat monitoring, detection, and response. It also can include other security operations solutions that help assess and eliminate vulnerabilities and reduce cyber risk.

How Arctic Wolf Can Help

The market leader in security operations, Arctic Wolf® offers an outsourced, fully managed, security operations solution that helps organizations of every size scale their defenses and mitigate organizational risks. Some of the companies using Arctic Wolf have seen a 411 percent return on investment over three years and have been able to reduce internal efforts to monitor risk and vulnerabilities by 75 percent, according to an analysis by Forrester.

Arctic Wolf is anchored by a Concierge Security® Team, which uses the Arctic Wolf® Platform to provide tactical and strategic insights to improve your security posture and compliance capabilities.

ARCTIC
WOLF

Contact Name
Email Address
Phone
Web Addresss