ARCTIC WOLF

FAQ

Security Operations Center

What is a SOC?

A SOC is a combination of cybersecurity personnel, threat detection and incident response processes, as well as supporting security technologies that, in sum, make up an organization’s security operations. As cyberthreats evolve and grow, SOCs are gaining momentum. Increasingly, mid-size enterprises are forgoing decentralized security operations, and enjoying the many benefits a SOC offers.

Why do businesses need a SOC instead of just a SIEM?

Security information and event management (SIEM) is a core technology within a SOC. A SIEM combines log management tools and correlation engine capabilities to provide actionable intelligence from a high volume of diverse log data collected from various endpoints.

But a SIEM without a full-time staff of security experts to manage and monitor it leaves many security gaps within a company’s security posture. Only a SOC, with 24x7 network monitoring, provides a fully comprehensive security solution capable of combating the inevitable cyberattacks of today’s ever-evolving threat landscape.

What security services does a SOC offer?

Among the essential services a SOC provides are continuous threat monitoring, managed detection and response, incident response, machine learning for data analysis, and network configuration and management. To ensure enhanced and optimized security, many of these features require human expertise and rely on experienced security analysts and engineers. Through a combination of machine intelligence and human experts–hybrid AI–a SOC greatly reduces false positives while simultaneously increasing threat intelligence.

What is the difference between a SOC and a NOC?

A SOC and a network operations center (NOC) both identify, investigate, prioritize, escalate and resolve issues. However, while a SOC’s role is focused on protecting the company’s data and digital assets, a NOC responds to incidents and alerts related to performance and availability of networks and systems, so that a company meets service level agreements (SLAs) concerning downtime.

What are the different types of SOCs?

According to Gartner, there are five traditional SOC models: virtual SOC; multifunction SOC/NOC; co-managed SOC; dedicated SOC; and command SOC. Recently, SOC-as-a-service arose to address the needs of mid-size enterprises who require a cloud-based SOC with all the benefits of in-house models, but also one that is affordable and more easily managed.

Where are SOCs typically deployed?

SOCs may be deployed on-premises, in the cloud, or as part of a hybrid cloud model.

What is SOC-as-a-service?

Under the newest SOC model, SOC-as-a-service, businesses pay a subscription fee in exchange for a dedicated, cloud-based SOC.

Arctic Wolf offers a SOC-as-a-service that meets the critical security needs of mid-size enterprises. The AWN CyberSOC™ is affordable, deploys in 60 minutes, and provides continuous monitoring, incident response, managed detection and response services, as well as ongoing consultation to improve a company's overall security posture.

ARCTIC WOLF

Contact us
arcticwolf.com
1.888.272.8429
ask@arcticwolf.com