# Understanding the Security Operations Center

CHAPTER FOUR

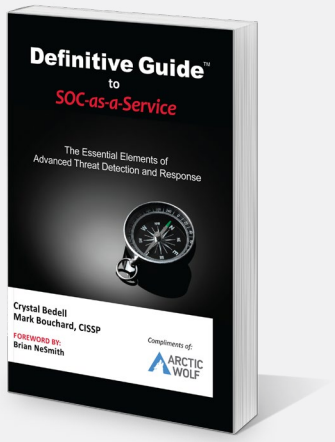
## Definitive Guide to SOC-as-a-Service

As mentioned in the previous chapter, a SIEM is a powerful tool. However, it needs to be managed effectively. A security operations center (SOC) includes security experts to effectively manage the SIEM, as well as built-in processes for incident response to help reduce your business risks.

### End-to-End Security Capabilities

A SOC defends network data and assets via prevention, detection, investigation, and response to potential threats and incidents. It provides full visibility into the activity within an environment, such as devices connected to the network, who's logging into what system, status of security devices, and the threats that are present. It brings together the people, processes, and technology needed for complete cybersecurity protection:

- **SIEM technology and more:** While a SIEM is its essential technology, a SOC includes a number of other valuable software tools. In sum, a SOC is comprised of intrusion detection, workflow, and reporting tools, plus threat intelligence feeds that provide real-time information and application programming interfaces (APIs) used to connect cloud-based resources to the SIEM
- **Staffed by security experts:** Technology alone can only do so much. It needs to be configured and continuously monitored by people with the right cybersecurity skills to ensure the SOC runs smoothly, eliminate false alarms, and identify and mitigate threats that pose maximum business risk. A security team within a SOC may include security operators, security analysts, security researchers, security managers, an incident response team, a forensics teams, and a compliance audit team
- **Operational processes:** For ensuring the SOC runs efficiently and effectively, strategic processes must be implemented. These include best practices for threat hunting, incident response, trouble ticketing, and the right threat intelligence sources to accurately identify the latest threats




Read about this and more by downloading the eBook, the Definitive Guide to SOC-as-a-Service.

Download Guide



arcticwolf.com
1.888.272.8429
info@arcticwolf.com