# 5 core principles of a SOC framework

**5 core principles of a SOC framework**

Highly effective SOC frameworks have several operational capabilities that include the following:

- **Monitoring.** The most fundamental function a viable security operations centre framework can provide is to monitor activity. The goal of such monitoring, of course, is to determine whether a breach has occurred or is underway. But, before cybersecurity professionals can make that determination, they need to be aware of what's going on. Automated tools and technologies can help with monitoring, including SIEM tools, behavioural threat analytics and cloud access security brokers. These tools may, but not necessarily, use technologies such as AI and machine learning. Cybersecurity analysts typically provide the top layer of such monitoring, reviewing the status of the alarms and alerts.
- **Analysis.** The next function a SOC should provide is analysis. The goal of the analysis is to determine, based on enterprise activity, whether a breach has occurred or a vulnerability is present. As part of the examination function, SOC analysts review alarms and alerts generated by the monitoring system to see if they correlate with known patterns of attack or vulnerability exploits. Once again, AI and machine learning come into play, along with human intelligence. The aforementioned tools may also provide some degree of analysis.
- **Incident response and containment.** If the SOC is internal or if the enterprise's agreement with an outsourced SOC provider calls for assistance beyond alert notification, the next function the security operations centre framework delivers is an incident response -- precisely how to handle the incident depends on the incident's type, scope and severity. A companywide ransomware attack obviously requires a different response than the compromise of a single server. This is where security orchestration, automation and response(SOAR) tools can help.

Incident response and containment include not only the immediate fire drill responses -- isolating affected systems and applications and notifying relevant stakeholders -- but, ultimately, the longer process of remediation. Effective remediation goes beyond fixing the immediate problem; it also addresses the policies, processes and technical issues that fueled the problem in the first place. Although the SOC doesn't always have a direct role to play in remediation, it's a useful source of detailed information that can be reviewed to determine the root causes of the security incident. And, of course, any policy, process or technology change may affect SOC operations.

- **Auditing and logging.** As noted, the SOC has an important, though often overlooked, role to play in logging and auditing: to verify compliance and to document the response to security incidents that may be used as part of a post-mortem assessment. Many SOAR tools contain an impressive array of timestamped documentation, which can be of value both to cybersecurity analysts and compliance professionals.
- **Threat hunting.** Even when systems are operating normally -- that is, no significant incidents are detected in the environment -- SOC analysts have other responsibilities. They monitor and assess threats in the outside environment by reviewing threat intelligence services and, if they are third parties with multiple customers, scan and analyze cross-customer data to determine patterns of attack and vulnerability. By proactively hunting for threats, SOC providers -- whether internal or external -- can stay a step ahead of the attackers and take protective steps in the event an attack occurs.