blackpoint

GUIDE

How to Evaluate a SOC Prior to Investment

What is a Security Operations Center?

When investigating a new security solution, it's important to cut through the industry buzz and figure out what is legitimate and worth investing in. If you're asking, "What does a standard SOC look like?" or "What is it meant to do?", read on to understand what you should be looking for.

A Security Operations Center (SOC) is a centralized hub that combines dedicated security analysts, processes, and technology to continuously monitor an organization's security posture. SOCs are focused on using telemetry measured from across an organization's IT infrastructure and assets to prevent, detect, assess, and respond to cybersecurity incidents.

Key Functions to Look For

All SOCs are built differently, and many providers allow organizations to select the specific services that best serve their line of business. These are some of the common key functions that a majority of SOCs will offer:

- [ ] **24/7/365 Proactive Monitoring:** SOCs should be scanning your networks on a 24/7/365 basis through proactive behavior monitoring and immediate analysis, regardless of the day or time.
- [ ] **Threat Response:** The SOC is your first responder. They close the gap between the first alert and the time it takes to respond and remediate, which is crucial to protecting you and your clients' data.
- [ ] **Fully Managed SOC:** Well-implemented SOCs provide valuable security insight that may be outside of your staff's capabilities. A fully managed team allows on-demand expertise and saves your company time, while remaining within your salary budget.

- [ ] **Incident Recovery:** In the event of a security event, SOCs work with you during the incident response process by providing expertise and guidance.
- [ ] **Alert Severity Triage:** A significant challenge faced by in-house security teams is dealing with alert fatigue. Experienced SOC analysts can offload this task, sifting through incoming alerts and efficiently assessing whether immediate action is needed.
- [ ] **Post-Incident Investigation:** Post-incident work is just as important as catching and eliminating the threat. A SOC performs a root cause analysis, investigates how and why the event occurred, and reports back with clear action items.
- [ ] **Asset Discovery & Management:** SOCs manage two main categories of assets:
  - the devices, processes, and applications of the organization they are defending, and
  - the specific tools and software in place to protect the former.

In SOC operations, having full visibility and control is key. This allows them to build a complete map of all available assets on the networks and be able to manage any weak or blind spots. With a complete view of all the endpoints, software, servers, and services, SOCs can stay on top of the nature of traffic flowing between these assets and monitor for anomalies.

- [ ] **Activity Log Collection:** As SOCs collect, maintain, and review all network activity for an organization, it allows them to acquire a baseline snapshot of what normal network operations look like. This is significant for the SOC as it allows the team to better locate threats, malicious files, and changes to assets. Compiling activity logs is also useful for remediation and forensic analysis in the aftermath of a security event.
- [ ] **Compliance Strategy:** Compliance audits ensure that organizations handling sensitive information are held to a standard set of rules and regulations. Should a breach occur, being compliant can shield the organization from reputational damage as well as severe legal and financial ramifications.

Summary

Though cyber adversaries move fast, you can stay ahead of them with the right security stack in place. Investing in a SOC is the next best step for those who want to build a robust security framework backed by security experts with experience dealing with ever-evolving cyber adversaries. Streamline how you and your clients face modern, advanced cyberthreats with the assurance that real-time identification and prevention are taken care of. Elevate your strategy by augmenting the SOC services with an MDR's capability for advanced threat hunting and network analysis. This will ensure a comprehensive and optimized security strategy for those looking to stay ahead of cyberthreats today.

LEARN ABOUT THE BLACKPOINT SOC