CHECKLIST

5 Reasons for a Security Operations Center Checkup

It's no secret that today's security operations centers (SOCs) have a mountain of challenges and pressures. Between the constantly changing threat environment and the evolving enterprise, everyone in your SOC is like a juggler—on a tightrope—and knows that there's a great deal at stake if they drop any ball.

How do you know it's time for a sanity check to ensure your SOC is working smarter against this sea of change? If you're struggling in any of the following areas, it could be time for an independent assessment. With the evolution of the enterprise and increasing sophistication of threats, it's important to continually test and update your SOC processes and strategy. One way to do that is with an independent SOC assessment. Such an assessment can help you create a practical plan that's aligned to your specific goals to optimize your SOC.

☑ Turnover, analyst burnout, and other personnel-related concerns

According to a recent study, there is currently a cybersecurity workforce gap of 3.4 million people.[1] So when you're able to secure the right expertise for your team, you obviously want to retain that talent. Beyond the usual disruption that turnover causes, that "seat" may sit vacant for far longer than a SOC can afford. According to a blog post published by the SANS Institute, "When there's this constant turnover of staff, it inevitably disrupts the SOC workflow and, ultimately, the effectiveness of the SOC."[2] But with burnout as a part of the day-to-day reality, it may be time to revisit your personnel plan. This means examining who and how you hire and what you can do to optimize skills, processes, and tools to improve job satisfaction and retain talent.

☑ Insufficient or partial visibility of detection capabilities and processes

Without optimized detection processes and capabilities, a SOC is operating somewhat blindly, unable to respond effectively to threats impacting the organization. Enterprises know they take a great risk if they don't have optimum visibility and detection capabilities. It may be time to revisit all your logging processes, alerting on all key functions. It may also be time to reexamine the tools and processes you're using for log aggregation or your security information and event management (SIEM) and extended detection and response (XDR) technologies. Are you able to easily identify changes in systems, applications, and your network that may indicate malicious activity or a stability issue? Can you identify intrusions in transit? Is there cooperation across all roles—including SOC analysts, detection analysts, threat intelligence analysts, and malware or reverse engineers—for creating use cases and rules?

☑ Slow or ineffective response

If you have good visibility but can't act swiftly on what you're seeing, the consequences can be dire. In the SANS 2022 SOC Survey, the second greatest challenge SOCs identified to using SOC capabilities is a lack of automation and orchestration.[3] Consider whether your team can quickly take response actions generated by automated processes, such as blocking and removing processes and files or isolating a device. Do you have all communications protocols established for different scenarios, and is your team well-versed in them? Do you have an effective incident response plan that you test at least once a year?

☑ Disparate or partial threat insights, intelligence, and hunting

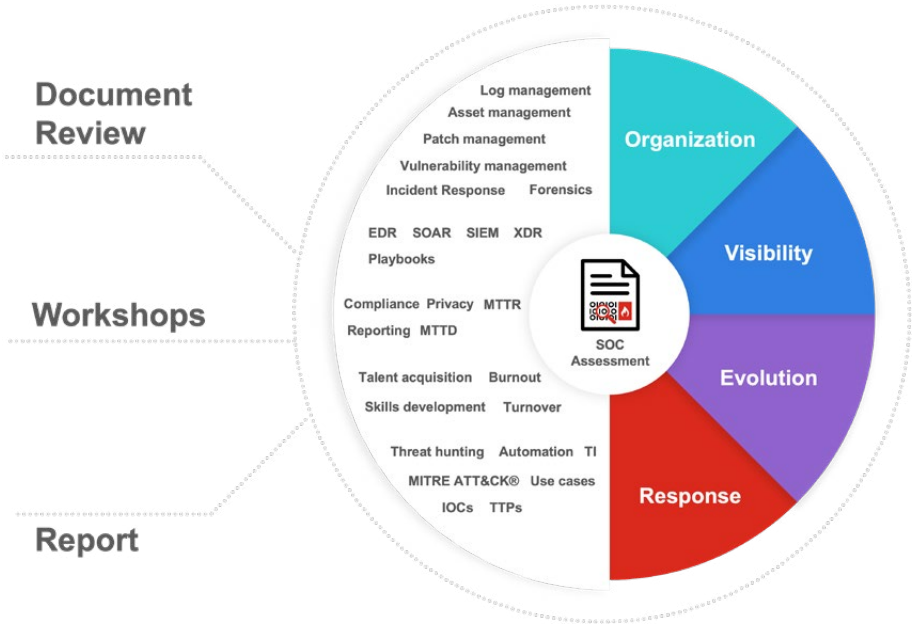
Without good processes and sources for threat intelligence, a SOC can't effectively utilize the feeds they're getting, much less act when warranted. Tactics, techniques, and procedures (TTPs) may get lost in a sea of information as opposed to being surfaced as intelligence. Sound processes and sources can enable the SOC to use incoming, evolving TTPs to identify potential indicators of compromise (IOCs) and inform the decision-making process.

In terms of sources, are you getting regular insights from open-source intelligence (OSINT), closed communities and underground forums, business partners, internal sources, and threat intelligence providers? Can your SOC collect, compare, prioritize, and triage threat data to yield intelligence to use in real time? Can you retroactively search to discover missed incidents with newly acquired IOCs? Can you easily track threat actors and identify new TTPs and campaigns?

☑ Limited management visibility and support

Another major challenge SOCs identified to using SOC capabilities is lack of support from management.[4] If executive leadership still isn't convinced of the SOC's value, it can be difficult to develop better processes, hire more skilled professionals, and improve your tooling. If you haven't established key performance indicators (KPIs) and don't continually measure or report on them, there's an opportunity for improvement. This is a chance to establish a clearer strategy, better align to corporate expectations, and establish or improve organizational access to metrics, tracking, dashboards, and reporting. These activities can help demonstrate the SOC's value and help you better identify areas for improvement.

Optimize Your Security Operations and SOC with the FortiGuard SOC Assessment



If you have concerns about your SOC and its efficacy, evolution, or future, our FortiGuard Readiness and Response team can help. Our FortiGuard SOC Assessment was developed for SOC organizations that have expressed concerns about challenges across four primary categories: the organization, their visibility, response capabilities, and their SOC's evolution. The assessment also leverages insights from recent and ongoing incident investigations, as knowing where and why failures happen can mean the difference between averting and succumbing to a cyber incident.

The assessment also looks at areas such as SOC cost management and budget forecasting, executive sponsorship and representation, dashboards and reporting, metrics, processes (use cases, playbooks, and logging), the efficacy of tools, automation, and threat data, talent recruitment, planning, and career development, as well as many other common SOC challenges.

Contact Fortinet to learn more about how we can help take your SOC to the next level, improving your processes and response time to better protect your organization.

[1] "(ISC)2 Cybersecurity Workforce Study 2022," (ISC)2, October 20, 2022.
[2] Kayla Williams, "It's Time to Break the SOC Analyst Burnout Cycle," SANS Blog, October 12, 2022.
[3] Christopher Crowley and Barbara Filkins, "SANS 2022 SOC Survey," SANS, May 16, 2022.
[4] Ibid.

March 18, 2023 4:48 PM
2018305-0-0-EN