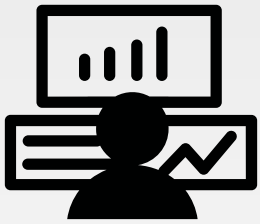
SOLUTION BRIEF

FortiGuard SOC Assessment Service



A security operations center (SOC) will lose its ability to perform over time unless it has a built-in growth plan that keeps its people, process, and technology aligned with the ever-changing threat landscape.[1]

Executive Summary

Today's security operations centers (SOCs) and teams must be effective and efficient, often despite limited resources, to maintain the organization's lowest possible cyber risk. This can be especially challenging given today's expanding attack surface, sophisticated threat landscape, evolving network infrastructure, and shifting business priorities.

To ensure you have the adaptive, agile, and successful security operations you need, every aspect of your SOC's people, process, and technologies needs to keep up with the demands of the day and anticipate those of the future. But to achieve this, you need to be able to answer some critical questions: How do you assess your SOC strategy? How do you know if your approach is the most effective? Are you optimizing your resources, retaining talent, and achieving the security efficacy you had hoped and that your business requires?

Your answers to these questions can mean the difference between a business that can successfully meet the demands of today's digital marketplace and a disaster waiting to happen. But that's easier said than done. FortiGuard's Security Operations Assessment can help.

Is your SOC set up for success? Does your SecOps function have a mature structure, process, and planning system?

Enterprises are continually evolving, from adopting new technologies, managing employee turnover, and supporting new business initiatives. The threat landscape is also changing, with sophisticated attacks designed to exploit your rapidly evolving ecosystem. As a result, your security operations functions—whether on-site, virtual, or hybrid (in location or ownership)—must be prepared for these changes. Ensuring you have a clear charter, appropriate governance and compliance processes, and a personnel strategy that ensures you have skills and resources available when needed are all critical to your SOC's success.

The first focus area of the FortiGuard SOC Assessment addresses the coherence of your structures inside and outside the SOC. This assessment reviews your SOC goals, organizational processes, people planning, and governance and compliance processes. For example, it checks that SOC positions are clearly defined and that staffing plans and talent requirements exist to ensure and optimize the personnel needed for your established goals. Cost management processes and budget forecasting are reviewed. And it ensures that appropriate regulatory compliance and privacy processes have been established and a privacy impact assessment is in place.

How comprehensive and effective are your SOC visibility and related processes? Can your SecOps team effectively and swiftly detect malicious activity?

Knowing that your SOC has solid security technology and tools and a sound hiring plan with requisite talent in place is essential. But how do you know if the systems and personnel you have in place are adequate? The second phase of our SOC Assessment focuses on baselining your SOC's tools and processes to determine their ability to effectively and quickly detect malicious activity.

Fortinet assessors consider the existence and maturity of your existing SOC tools and processes, including:

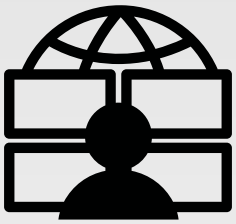
- The range and selection of use cases and their relevance
- MITRE adoption and usage
- The selection, maturity, and processes around SIEM, log aggregation, and XDR tools
- The selection and use of detection tools
- Threat intelligence sources and the maturity of processes
- SOC logging scenarios and usage
- Vulnerability and patch management processes
- Threat hunting criteria, processes, and use

SOC response planning: Can your SecOps team respond swiftly and effectively to incidents?

It is vital for every business to monitor for and protect against today's growing threat landscape, safeguard critical digital assets, and enable secure connectivity for employees regardless of where they choose to work. Given today's dynamic networking environments, a complete cybersecurity solution, continuously updated with real-time information and able to span on-premises, cloud, and remote resources and users, is crucial. Fortinet's suite of essential cybersecurity services can enable, enhance, and extend protection across your environment, creating a solid foundation of security that allows you to compete effectively and securely in today's digital marketplace.

SOC maturity: Can you substantiate the value of, sustain, and future-proof your SOC?

An effective SOC must be agile and able to adapt continually to change. New technologies and automation are developed, threats evolve, and your network will inevitably change. Our final SOC Assessment category addresses these challenges by exploring the activities that sustain your SOC's efficacy, helping to improve responsiveness and adapt to new threats and technologies over time.



"To fight a continuously growing enemy… many SOC metrics—focused on people, process, and technology—are needed for consistent improvement. CISOs should focus on bringing automated, repeatable, and consistent processes to detection engineering."[2]

Key SOC Assessment Services

- Document review: Reviews relevant documents and plans
- Workshops: Focuses discussions to gauge maturity in your various practices, discovers reinforceable strengths, and identifies areas that can be improved
- Report: Provides maturity scoring and prioritized, actionable recommendations to return the most value for effort and resources

Every SOC should have its key performance indicators (KPIs) defined and the ability to generate and share reports substantiating its value and efficacy. Vital to this are metrics that help SOC leaders understand the state of daily operations and trends, from event counts and false positive rates to service requests and availability to the overall time to detect, contain, and resolve threats against expected SLAs. This assessment addresses the SOC strategic plan and its long-term vision, metrics, staff training, exercises, and the processes related to security tool assessment and acquisition.

The SOC assessment output: Measuring efficacy and improving sustainability

With these four assessment areas in place, the FortiGuard SOC Assessment can provide your organization with objective maturity scoring aligned to your SOC's goals. It also provides a realistic roadmap for areas needing fortification or improvement. With these insights and guidance, your SOC has a path toward achieving its highest potential, creating and maintaining the most value for your business investment and having the greatest probability of *sustained* success.

Assessment Benefits, Output, and Value

Regardless of how the threat landscape unfolds, a successful SOC must align with business priorities and reduce organizationwide cyber risk while adapting to the ever-changing threat landscape and business needs. The FortiGuard SOC Assessment helps optimize SOC investments, from tools and talent to staff time, aligns the SOC to business priorities, identifies gaps or areas for advancement, helps the SOC retain valuable, scarce talent, and returns the most value for the business. Doing so provides your security leaders with a path to evolving and sustaining the most valuable security operations function possible to protect your business.

[1] Gartner, "How to Build and Operate a Modern Security Operations Center," 2021.

[2] SC Magazine, "What CISOs don't know about their SOCs," January 11, 2023.

March 10, 2023 10:13 AM

2002866-0-0-EN