SOLUTION BRIEF

Enhance Your Security Operations Center with the FortiGuard SOC Development Service

Executive Summary

In an age when digital threats are constantly evolving and becoming increasingly sophisticated, organizations face a daunting challenge in protecting their sensitive data and critical infrastructure. Cyber adversaries, equipped with advanced tools and techniques, continually seek to exploit vulnerabilities and breach security measures. In response to this escalating cyber-arms race, Fortinet, a trusted name in cybersecurity, offers a comprehensive Security Operations Center (SOC) Development Service to empower businesses to stay ahead of these relentless attackers.

The landscape of cybersecurity has evolved dramatically over the years. As a result, the traditional, reactive approach to security is no longer sufficient. With attacks ranging from commonplace malware and ransomware delivered by Ransomware-as-a-Service groups and their affiliates to advanced persistent threat (APT) techniques, businesses must shift away from sole reliance on perimeter defenses. They require proactive, dynamic, automated, and threat-informed defenses that can help them detect and respond to threats and adapt to emerging risks. This is precisely where the FortiGuard SOC Development Service comes into play, offering an advanced solution tailored to each organization's unique security needs while reducing the complexities of their response processes.

The top two contributing factors to breaches are inadequate incident response (IR) procedures and a lack of network and system logging processes.[1]

Our Approach

With years of hands-on experience in observing threat actors and disrupting their tactics, techniques, and procedures (TTPs), our experts collaborate with your organization to establish a resilient and proficient SOC. We focus on four fundamental pillars crucial to any successful SOC: organization, visibility, response, and evolution.

- **Organization:** This area of focus addresses the cohesion of structures both outside and inside the SOC, encompassing the alignment of the SOC with the business, the internal organization of the SOC itself, and its integration into the organization's broader IR framework.
- **Visibility:** Detecting malicious activities within the organization is a pivotal aspect of the SOC, which requires appropriate tools, logging mechanisms, use cases, and defined approaches that the organization utilizes to detect and mitigate a threat. Practitioners should also have ongoing access to threat intelligence, which helps provide indicators of compromise and other insights on the latest threats.
- **Response:** An effective SOC requires well-defined processes, playbooks, workflows, data-sharing mechanisms, communication protocols, and skilled personnel. Adequate visibility is also important but not valuable if these other protocols aren't in place.
- **Evolution:** The SOC necessitates continuous maturation and development, requiring ongoing meticulous planning, sound metrics, training programs, educational exercises, and assessments. A SOC that attains a certain level of maturity but stagnates will rapidly lose its efficacy, given that attackers evolve their methods daily. The ability to quickly adapt and evolve is vital to a successful SOC.

How the FortiGuard SOC Development Service Works

The FortiGuard SOC Development Service offers a step-by-step, vendor-neutral approach to assist teams with building a SOC from the ground up. Fortinet recognizes that every organization is different and has unique needs. Our team can help with:

- Assessing your organization's current maturity level via our SOC Assessment
- Creating processes and procedures, including an incident response plan and playbooks
- Alignment with the goals of the business, as well as industry standards
- Defining existing and future roles and responsibilities of the SOC
- Ensuring appropriate tools are in place, monitored, and responded to in a timely fashion
- Establishing detection and response capabilities that are aligned with the latest adversary TTPs
- Measuring improvement

Why Organizations Choose the FortiGuard SOC Development Service

The FortiGuard SOC Development Service offers a myriad of advantages to your organization, including:

- Elevated security posture: By crafting comprehensive plans, processes, and procedures, the service enhances your organization's overall security stance.
- Enhanced workflows and communication: Critical to addressing any threat, the service improves workflows and communication, ensuring a more effective response to potential incidents.
- Minimized downtime and business impact: Through expedited response to events and incidents, the service helps reduce downtime and mitigates the overall impact of a breach on business operations.
- Prioritized threat detection and response: The service aligns threat detection and response strategies with the threats most pertinent to your organization, ensuring you have a focused and proactive approach to cybersecurity.

Conclusion

Whether you're just starting to develop a SOC capability or already have a skilled team of analysts on staff, the FortiGuard SOC Development Service can help enhance the organization's capabilities and design a robust and integrated SOC. Together, we assess your unique needs and decide what is required and where the organization's priorities lie so that we enhance your SOC operations as quickly as possible.

Contact us to learn more about the FortiGuard SOC Development Service.

[1] FortiGuard Incident Response Report—1H 2023, Fortinet, October 17, 2023.

FORTINET

www.fortinet.com

January 21, 2024 2:13 PM

2474768-0-0-EN