POINT OF VIEW

Understanding the Security Operations Journey

The Pathway to Proactive and Resilient Cybersecurity

Executive Summary

In today's cybersecurity landscape, security teams grapple with sophisticated threats that challenge conventional security approaches. According to the Fortinet Cybersecurity Skills Gap Report, 53% of organizations reported that breaches cost them over $1 million in 2023, emphasizing the need for efficient and effective security solutions.[1]

Organizations must create a flexible cybersecurity strategy to meet their evolving security operations (SecOps) needs over time. For proactive and resilient security, the SecOps journey should start with foundational solutions, which can be enhanced and scaled over time to create a centralized, AI-driven security operations center (SOC) with adaptable incident response. This evolution is characterized by integrating unified security management, AI assistance, security automation, and continuous posture assessment, all of which are essential for tackling modern cyberthreats.

Attacks occur 43% faster than they did in the previous six months, as they're more targeted, more automated, and happen across more channels.[2]

Managing Cybersecurity Challenges with AI and Automation

When it comes to security technology, more isn't necessarily better. Trying to stitch together disparate point products often puts unnecessary strain on security staff and analysts. Organizations need integrated security management that enables their security and IT teams to comprehensively view the entire threat landscape.

A holistic view of an organization's security posture is crucial for identifying and addressing threats across diverse IT environments. Organizations also need to efficiently use their resources and enforce policies consistently. Streamlining security processes reduces the need to manage multiple disparate tools and makes for a more efficient use of resources. Organizations minimize exploitable gaps in their defenses by ensuring uniform security policy application.

Because threat actors are increasingly employing AI to advance their efforts, organizations need to combat these risks with AI-enabled solutions of their own. AI algorithms excel in analyzing large datasets to identify potential threats swiftly and accurately, which is critical for tackling sophisticated cyberthreats. AI's predictive capabilities can help organizations prepare for possible future threats, fostering a proactive defense stance. AI-driven automation of initial response measures also frees up human operators to work on more complex threat resolution tasks.

Security automation is also a critical element of a robust cybersecurity strategy, particularly given the shortage of skilled personnel. With the inundation of security alerts, automation helps manage them efficiently, sifting through false positives and prioritizing severe threats. Automation also helps ensure that response protocols are consistently executed, reducing human error. Using automated systems allows security operations to expand seamlessly alongside organizational growth. Continual security posture assessment enables organizations to rapidly adapt their security strategies in response to emerging threats, and regular evaluations provide essential data for informed resource allocation and strategic planning. These continuous assessments also help the business maintain compliance with evolving legal and regulatory standards, mitigating potential legal and financial risks.

More than 50% of IT leaders say a lack of essential cybersecurity products is a top cause of breaches.[3]

The Pathway to Proactive and Resilient Cybersecurity

One of the top priorities for security leaders should be to implement advanced technologies such as AI and ML that enable faster threat detection, followed by central monitoring to speed response. This structured pathway in SecOps development is essential for effectively combating evolving threats.

Addressing today's cybersecurity challenges won't happen overnight, but the first step is laying the foundation for a structured pathway that can grow alongside their security needs. This SecOps journey can be classified into three stages: essential, expanded, and advanced SecOps. Each stage offers capabilities to address specific pain points.

Essential security operations

The first foundational stage of this journey should provide the security and IT teams with central logging, security analytics, baseline automation, and AI assistance. This stage is crucial for teams beginning their security operations journey, focusing on centralizing log management and employing baseline security analytics and automation. Lean security teams lack the time and resources to build out use cases, maintain them, and create new ones. They need a way to get essential SecOps capabilities in place without disrupting their day-to-day operations. A tool that offers minimal configuration deployments that is ready to use out of the box can provide all the baseline functions without adding further complexity or stressing resources.

Expanded security operations

The second stage includes leveraging security information and event management (SIEM) and user and entity behavior analytics (UEBA) for enhanced analysis. As organizations evolve, the need for more advanced analytics emerges to gain a more granular view of the security landscape. SIEM solutions can help manage the complexity of diverse tools and data sources, offering better analysis through UEBA. This additional analytics layer detects subtle, sophisticated threats by monitoring user behavior and detecting anomalies that might indicate insider threats or compromised credentials. This stage is particularly beneficial for dedicated security teams that need to manage a diverse range of security tools and data sources.

Advanced security operations

For organizations with extensive security requirements, the third stage includes security orchestration, automation, and response (SOAR) integration. Integrating SOAR with the foundational and expanded security operations tools makes it possible to manage complex incidents and processes. It facilitates managing complex security scenarios and coordinating responses across a sophisticated security infrastructure. With automation for complex workflows, SOAR helps ensure swift and consistent responses to threats and facilitates collaboration across various security tools and teams at scale.

Enhancing SecOps with Generative AI

Integrating generative AI (GenAI) into the cybersecurity platform is a game-changer for enhancing security capabilities. GenAI can work with solutions to analyze vast datasets to identify patterns and anomalies, providing deeper insights into potential threats. It complements existing AI and ML tools by automating routine tasks, generating comprehensive threat reports, and suggesting proactive measures. This integration ensures that security operations are not reactive but predictive, enabling faster and more accurate threat detection and response. By leveraging GenAI, organizations can enhance their capabilities and uplevel skillsets, allowing their teams to focus on more complex threat resolution tasks.

Progressive SecOps Enhancement

The pathway from essential to advanced SecOps should be a strategic progression that aligns with an organization's evolving security requirements. This structured approach caters to establishing a secure environment and ensures readiness for complex, multifaceted threats, laying the groundwork for a resilient, AI-powered SOC over time. By continually enhancing and adapting their SecOps environment, organizations can more effectively navigate the complexities of today's cybersecurity landscape. This progression from basic automation to advanced orchestration, with integrated threat intelligence, AI, and GenAI capabilities, ensures that organizations can handle the growing threat landscape with agility and confidence.

Conclusion

Building an effective SecOps framework requires a tailored approach that considers team size, tool diversity, and process maturity. Organizations can identify the right capabilities to enhance their security posture by assessing these variables. Whether through central management and analytics for lean teams, SIEM for dedicated security teams, or SOAR for advanced operations, a strategic approach to SecOps can significantly improve an organization's ability to detect, respond to, and mitigate threats. This structured pathway ensures readiness for complex, multifaceted threats, laying the groundwork for a resilient, AI-powered SOC over time. By continually enhancing and adapting their SecOps environment, organizations can more effectively navigate the complexities of today's cybersecurity landscape.

[1] 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, June 20, 2024.

[2] Douglas Jose Pereira dos Santos, Key Findings from the 2H 2023 FortiGuard Labs Threat Report, Fortinet, May 6, 2024.

[3] 2024 Cybersecurity Skills Gap Global Research Report, Fortinet, June 20, 2024.

FORTINET

www.fortinet.com

August 24, 2024 6:47 PM / 2824932-0-0-EN