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 and escalate several sophisticated threats that challenge conventional security approaches, so 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 security operations solutions, which can be enhanced and scaled over time to a centralized, AI-driven security operations center with multivector incident response. This evolution is characterized by integrating unified security management, AI assistance, security automation, and continuous posture assessment, which all are essential for tackling modern cyberthreats.

A Multifaceted Approach

In today's intricate cybersecurity environment, organizations must take a multifaceted approach to security management and SecOps. This necessity stems from the escalating complexity of cyberthreats and the growing interconnectivity of modern IT infrastructures. To meet cybersecurity needs, organizations must create a strategy that includes unified security management, AI assistance, security automation, and continuous assessment.

According to a recent survey, "Security leaders' top priority is to implement advanced technologies such as artificial intelligence (AI) and machine learning (ML) that enable faster threat detection, followed by central monitoring to speed response."[1]

Managing Cybersecurity Challenges

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 provides a comprehensive view into 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, 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. The predictive capabilities of AI 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 for more complex threat resolution tasks.

Security automation is also a critical element of a robust cybersecurity strategy, particularly given the difficulty many organizations have in hiring skilled personnel. With the inundation of security alerts, automation helps manage this flow efficiently, sifting through false positives and prioritizing severe threats. Automation 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 organization maintain compliance with evolving legal and regulatory standards, mitigating potential legal and financial risks.

A Structured Pathway in SecOps Development

Addressing today's cybersecurity challenges doesn't happen overnight, and many organizations can benefit from a structured pathway that evolves 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 challenges.

Essential SecOps

The first foundational stage should provide 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. AI assistance at this level helps interpret vast amounts of data, offering actionable insights. The threat detection, streamlined incident investigation, and effective management of routine tasks help pave the way for lean teams to develop robust security protocols.

Expanded SecOps

The second stage includes security information and event management (SIEM) with 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. UEBA adds an extra analytics layer to detect 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 SecOps

For organizations with extensive security requirements, the third advanced SecOps stage includes security orchestration, automation, and response (SOAR) integration. Integrating SOAR with the foundational and expanded security operations 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.

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.

[1] Fortinet, The 2023 Global Ransomware Report.

www.fortinet.com

March 28, 2024 1:43 PM

2624075-0-0-EN