UNIFIED THREAT MANAGEMENT: WHY SIEM AND CISCO XDR ARE BETTER TOGETHER

Enhancing Security Through Integration

By Robert Keblusek, Sentinel Chief Innovation & Technology Officer

Contents:

Strengths of SIEM Technology

Answering Complex Questions

SIEM technology excels in aggregating and analyzing log data from various sources within an organization's IT ecosystem. One of its primary strengths lies in its ability to answer complex questions that require historical data analysis. For instance, if an organization needs to determine who accessed a particular file six months ago, SIEM can efficiently sift through the logs to provide that information. This capability is invaluable for compliance, forensic investigations, and understanding the context of security incidents.

Complexity of Detecting Modern Threats

Many SIEM systems do not naturally correlate Tactics, Techniques, and Procedures (TTPs) as described in the MITRE ATT&CK framework, requiring complex and resource-intensive searches instead. This approach can be impractical, particularly in fast-evolving threat environments where prompt responses are essential. Additionally, it requires substantial development resources to create and sustain intricate searches while cross-correlating data from various security tools within an organization.

Rapid Automated Response

SIEM technology was initially conceived to detect security events and alert human operators, who would then manually respond to these incidents. This manual approach was sufficient during a period when cyber threats were less sophisticated, and the dwell times of bad actors within systems were measured in months. However, the modern cyber threat landscape, where adversaries can compromise systems within hours or even minutes creates a new challenge.

Originally, SIEM systems weren't built to offer near real-time response capabilities. As cyber threats advanced, it became clear that a faster and more automated reaction was essential. This necessity spurred the development of Security Orchestration, Automation, and Response (SOAR) platforms, which enhanced SIEM functionalities through automation. SOAR implemented scripting and integration with traditional SIEM detections, allowing for more effective handling of security incidents.

However, as of 2025, Gartner has declared that SOAR, as a standalone concept, is “obsolete.” (Gartner, 2024) This is evidenced by Gartner’s statement in their June 2024 cyber security hype cycle where Gartner has listed the “Time to Plateau” as “obsolete” instead recommending that users should consider “consuming automation features onboard larger security platforms first. Standalone SOAR platforms should be the exception for clients with generalized automation requirements and organizations with larger development capabilities.”

The industry has shifted towards integrating automation as an inherent capability within SIEM systems. Modern SIEM solutions now include automated response features natively, which are critical for disrupting contemporary attacks. This integration ensures that SIEM systems function not just as passive alerting tools but as active defenders capable of responding to threats in near real-time, thereby significantly enhancing organizational security postures.

SIEM Technology Remains Necessary

SIEM technology continues to have a number of strengths, which include but are not limited to:

- **Robust Integration via Applications (APIs) or Logs:** IT systems have, for years, accommodated logging, which is imperative to SIEM technologies for compliance requirements. This robust integration allows SIEM systems to collect and analyze data from diverse sources, providing a comprehensive view of the organization's security posture. Nearly anything can be integrated into a SIEM with detections created to search and identify the “needle in the haystack.”

- **Compliance Requirements:** Compliance needs such as HIPAA, PCI, CMMC, SOC II, ISO, and more require the collection and retention of log information from IT systems to meet audit requirements. SIEM systems are adept at ensuring these logs are managed in a manner that satisfies stringent regulatory mandates.

- **Forensics Investigation:** The ability to search through logs, ask complex questions, and expect accurate responses is crucial for forensic investigations. This necessitates the retention and indexing of billions and trillions of logs over time. Some compliance standards require the retention of logs for seven years or more to meet government mandates and avoid costly non-compliance fines and litigation.

SIEM technology continues to be a crucial element in the cybersecurity domain, offering indispensable functionalities in logging, compliance, and forensics that are unparalleled by other solutions. Over time, SIEM and XDR technologies are converging and will persist in integrating, combining the strengths of both environments to enhance the Security Operations Center (SOC) of the future.

The Need for Next Generation Advanced Detection

Identifying Known and Unknown Threats

To effectively identify known threats, organizations require robust detection mechanisms combined with strong threat intelligence. This approach aids in recognizing patterns and behaviors associated with known malicious activities. However, the challenge lies in identifying unknown threats, which necessitates a different approach—behavioral detection. Understanding the "day in the life" of devices and users becomes crucial. By learning normal behavior patterns, organizations can detect anomalies that may signify novel threats.

The Dual-Edged Sword of AI in Cybersecurity

Adversaries are increasingly leveraging artificial intelligence (AI) to enhance their attack strategies. They use AI to profile organizations and their users, collecting information and crafting tailored attacks that can bypass traditional security measures, deceive users, and compromise data. Consequently, defensive measures must evolve to incorporate AI and machine learning (ML) to counter these sophisticated threats.

Similar to how Large Language Models (LLMs) have delivered significant benefits in productivity and advancements in health and wellbeing, artificial intelligence (AI) has also empowered malicious actors to monetize their attacks and impact businesses adversely. Prominent LLMs such as ChatGPT have captivated audiences, accelerated market trends, and transformed nearly every business and institution globally. However, less recognized LLMs, such as WormGPT, have provided cybercriminals with a strategic advantage in the cybersecurity landscape. The advent of malware and attacks-as-a-service has enabled even novice attackers to swiftly and efficiently venture into cybercrime, thereby expanding the risk landscape and targeting a broader range of organizations beyond just large financial and medical institutions with valuable data and private information.

AI has facilitated the acceleration of cyberattacks, improved the ability to profile users, and generated precise and deceptive emails that compel users to take action. These developments allow cybercriminals to infiltrate organizations, cloud applications, and data systems, enabling lateral movement within the network and your systems at will.

The Imperative of Data Recovery

In recent years, the risk of ransomware has motivated most organizations to acknowledge the importance of having data backup solutions that are immutable and recoverable. The capability to recover data has transitioned from a best practice to an absolute requirement. However, adversaries have adapted their tactics accordingly. They not only hold data hostage via ransomware but also exfiltrate sensitive information to threaten public exposure—commonly known as extortionware. This dual-pronged approach significantly increases the stakes and potential damage to organizations.

Organizations must now adopt a proactive stance that includes not only robust backup solutions but also sophisticated detection and response mechanisms that can swiftly address data exfiltration. The ability to restore data to a previous state is indeed fundamental, but the landscape of cyber threats demands more nuanced and agile responses. IT managers can no longer rely solely on manual interventions due to the speed and complexity of modern cyberattacks.

This shift underscores the necessity for advanced technologies like AI and ML to be integrated into cybersecurity strategies. These technologies can automatically detect and respond to threats in real time, significantly reducing the window of opportunity for cybercriminals. Leveraging AI and ML enables organizations to not only restore compromised data but also prevent the initial breach from causing significant harm.

Furthermore, business continuity now hinges on the ability to maintain operations amidst cyber disruptions. Unlike traditional disaster recovery scenarios, where incidents were relatively rare and often predictable, cybercrime introduces an element of unpredictability and frequency that demands continual preparedness. Thus, the resilience of an organization, in today's context, is measured by its ability to anticipate, detect, and neutralize threats swiftly and effectively.

Comprehensive Detection and Response with Cisco XDR

Behavioral Detection Across Endpoints and Identities

In the current threat landscape, it is essential to have behavioral detection mechanisms for endpoints, user identities, and data. Cisco XDR excels in this regard by providing detection capabilities that baseline the behavior of users and devices, regardless of where they work or what they do. This continuous monitoring and analysis help identify deviations from normal behavior, which could indicate potential security incidents.

Some organizations have invested in network segmentation and network traffic behavioral detection. Although these techniques are effective, they are no longer sufficient in today's business environment where work-from-anywhere is commonplace. Behavioral baselining and detection must extend beyond the network to include endpoints and identity services in order to effectively detect and respond to modern cyber threats.

Chaining Together Complex Attacks

Modern cyberattacks often span multiple vectors, including email, identity, network, cloud, devices, and data. Detecting such intricate attacks requires the ability to correlate activities across these different domains. Cisco XDR provides this capability by integrating data from various sources and correlating it to identify multi-faceted threats that might otherwise go unnoticed.

Leveraging the MITRE ATT&CK framework and chaining attack techniques and procedures is crucial for identifying contemporary cyberattacks and automating responses at the pace of cyber adversaries. Cisco XDR utilizes machine learning (ML) and artificial intelligence (AI) within a massive data lake to enable the chaining of TTPs, which enhances detection accuracy. By correlating related techniques, chaining allows security systems to recognize patterns of activity that might otherwise appear benign in isolation. This process increases the accuracy of detection systems and reduces false positives.

Contextual awareness is another significant advantage. Chaining provides Security Operations Center (SOC) teams with a clearer understanding of the context behind detected activities. For instance, observing a phishing attempt (initial access) followed by process injection (execution) offers a more evident indication of a malicious campaign than viewing these events independently.

Furthermore, chaining TTPs across the attack lifecycle aids in detecting threats earlier by recognizing patterns indicative of advanced persistent threats (APTs). This reduces the attacker's dwell time—the duration an attacker remains undetected within a system—thus improving incident response times.

Prioritization of alerts is also considerably improved. By linking related attack techniques, SOC analysts can prioritize responses more effectively. A chain of TTPs indicating that an attacker is advancing toward critical objectives, such as data exfiltration, is given higher priority compared to isolated, unrelated events.

Enhanced automation is a pivotal benefit. Many modern detection and response platforms, such as XDR and SIEM systems, employ MITRE ATT&CK chaining to automate the identification of complex attack sequences. This capability allows for automated responses to threats based on recognized patterns, thereby streamlining and fortifying the cybersecurity posture of organizations.

Asset Visibility and Risk Identification

Not all assets are equal. For example, blocking a known bad executable that a user clicked on may indicate a lapse in user awareness training, but it also demonstrates that your investment in a quality endpoint detection and response (EDR) solution is effective. However, detecting the same threat on a server, which should never have end-user interaction, especially clicking on a bad executable, warrants a thorough investigation. Today's detection and response technologies must be capable of differentiating assets based on their priority and associated risk.

Effective security necessitates comprehensive asset visibility. Organizations need to distinguish between different types of assets, such as desktops versus servers, and standard users versus administrators. Cisco XDR enhances visibility into these assets, allowing for better risk assessment and management. Additionally, the integration of AI and ML enables continuous analysis of a massive data lake, persistently searching for and identifying risks, enriched by threat intelligence.

The Power of AI and ML

Turning the Tables on Adversaries

To counter the AI-driven tactics of adversaries, organizations must employ AI and ML in their security operations. These technologies can process vast amounts of data in real-time, identifying patterns and anomalies that human analysts will miss. Cisco XDR leverages AI to turn the tables on adversaries, providing organizations with advanced detection and response capabilities.

Cisco XDR employs artificial intelligence within Cisco's extensive data lake to continuously monitor for anomalies in your IT systems. This multi-billion-dollar investment in AI allows you to effectively counteract malicious actors. By leveraging AI, Cisco XDR can analyze vast amounts of data and enrich it with threat intelligence from Cisco Talos, the world's largest threat intelligence organization. This ensures constant vigilance over risks in your IT environment.

Through the power of AI, Cisco XDR maps incidents to the MITRE ATT&CK framework, chains TTPs, and alerts your Security Operations Center (SOC) to potential risks. The AI assistant generates a root cause report for every incident, regardless of its risk level. What traditionally would require hours or even days of human effort, often with a high degree of inaccuracy, is now completed within seconds. This information can be readily reported and exported for analysis, summarization, and board-level reporting.

Nevertheless, even with XDR or XDR + SIEM, it is essential to employ high-quality endpoint, identity, email, network, and edge security technologies. XDR and SIEM are only as effective as the tools providing data to them and their configurations in identifying attack tactics, techniques, and procedures (TTPs). Without robust protection and detection tools, or even with leading tools that are poorly configured and maintained, XDR, SIEM, or any type of detection system will remain ineffective. As a result, malicious actors can successfully penetrate and navigate through your systems, launch business email compromise and phishing attacks, and ultimately monetize their efforts at your expense. Sentinel offers a series of workshops designed to help you assess your readiness for protection and detection, identifying strengths and weaknesses within your security landscape.

XDR AI Assistant – SOC Investigations Accelerated

Cisco XDR now includes a new AI assistant, poised to become an indispensable tool for SOC analysts. This advanced AI assistant enables analysts to investigate incidents with unparalleled speed, precision, and accuracy, surpassing any other tool currently available on the market.

Leveraging the power of generative AI, SOC analysts can:

· Investigate incidents using natural language, conversing with the AI assistant as they would with another human.

· Utilize Cisco’s extensive data lake and robust generative AI capabilities to enhance incident investigations within seconds, irrespective of the analyst's experience level.

· Specify details and ask multiple questions to gather comprehensive information, thereby enabling the assistant to provide the most useful responses.

· Receive immediate feedback powered by Cisco's security-optimized generative AI large language model.

· Provide feedback to the AI assistant to facilitate continuous improvement and learning.

Your information remains secure as the AI assistant adheres to Cisco’s Responsible AI Framework, which emphasizes transparency by citing information sources where applicable and ensuring that your PII is not shared with any external services.

With the new AI assistant included in Cisco XDR, analysts swiftly determine the root cause details of incidents within your enterprise. The context of each incident is presented in clear and comprehensible human language. The efficiency of responding to and mitigating attacks is significantly enhanced with this innovative AI assistant.

Why Cisco XDR Complements SIEM

The integration of Cisco XDR with SIEM technology offers a comprehensive security solution that addresses both the strengths and limitations of traditional SIEM systems. While SIEM provides foundational capabilities for log analysis and answering complex queries, Cisco XDR enhances detection, response, and threat intelligence. Together, they offer a robust defense against modern cyber threats.

A distinguishing feature of Cisco XDR is its unparalleled detection and automated response capabilities, powered by AI. Unlike competing vendors, Cisco does not impose additional charges for AI utilization, nor does it charge for unpredictable consumption of AI. Instead, Cisco has made AI an integral and foundational aspect of their advanced XDR technology, ensuring that all users benefit from its capabilities without incurring extra costs.

An example of the integration between Cisco XDR and SIEM is the recently introduced Cisco Security Cloud application for Splunk, offered at no cost. This application enables the connection of multiple Cisco products, including Cisco XDR, to Splunk. As a result, Cisco XDR can escalate identified incidents to Splunk Enterprise Security notables. Soon this integration will also allow identified risks from Splunk to be integrated into Cisco XDR's data lake, enabling bi-directional integration between Cisco XDR and Splunk. It is worth noting that Cisco XDR does not solely support Splunk, now a Cisco company. Instead, Cisco has adopted an open approach to supporting SIEM technologies, with XDR accommodating several popular platforms including, but not limited to, Elastic, Exabeam, Google Chronicle, Graylog, LogRhythm, Sumo Logic Cloud SIEM, and Sumo Logic Log Management.

Conclusion

The combination of SIEM and Cisco XDR represents a powerful synergy in the realm of cybersecurity. By leveraging the strengths of both technologies, organizations can achieve a more comprehensive and effective security posture. As the threat landscape continues to evolve, this integrated approach will be essential in protecting critical assets and data from sophisticated cyber adversaries.

Combining SIEM and XDR technologies is no small feat for any organization. If your organization has extensive IT and development resources, embarking on this journey yourself may make sense. However for most organizations without unlimited budget and resources, partnering with a service such as Fortis by Sentinel’s ActiveDefense™ MDR makes the most sense. By investing in this service, Sentinel combines the best capabilities of our own Security Insights SIEM technology powered by Splunk with Cisco XDR to advance your protection, protect your users, as well as detect and disrupt emerging threats.

Fortis by Sentinel’s ActiveDefense™ MDR offers a comprehensive managed detection and response service that integrates seamlessly with existing IT infrastructures. This partnership leverages Sentinel's expertise in SIEM technology and Cisco's advanced XDR capabilities, providing a dual-layered defense mechanism against cyber threats. With Fortis, organizations benefit from 24x7x365 monitoring, rapid incident response, and continuous threat hunting, ensuring that no malicious activity goes unnoticed.

Fortis by Sentinel's MDR service includes tailored security strategies that align with your organization's specific needs, allowing for a customized approach to cybersecurity. This flexibility ensures that the combined SIEM and XDR technologies are utilized to their full potential, providing maximum protection against sophisticated cyber adversaries.

In a rapidly evolving threat landscape, the collaboration between SIEM and XDR technologies through Fortis by Sentinel’s ActiveDefense™ MDR represents a strategic investment. It allows organizations to stay ahead of emerging threats, safeguard critical assets, and maintain a resilient security posture without the need for extensive in-house resources.

Choosing to partner with a managed service provider like Sentinel not only enhances your security capabilities but also optimizes operational efficiency. It empowers your organization to focus on core business objectives while ensuring that your cybersecurity measures are robust, up-to-date, and capable of countering the latest threats in real-time.

Contact Sentinel if you are interested in exploring how the combination of SIEM and XDR can advance the protection of your organization no matter its size or industry.