INSIGHTS | **TECH BRIEF**

Written By Shawn Murphy
WEI Cybersecurity Senior Architect

Beyond SIEM: The Future Of Cyber Threat Management

Throughout modern history, we encounter situations where traditional methods plateau in effectiveness. Consider the evolution of personal computing. Initially, computers underwent incremental upgrades in processing power and storage capacity. However, as demands and technology progressed, there was a clear need for progression. This shift materialized in the form of cloud computing, moving away from the limitations of physical hardware to virtually unlimited resources accessible over the internet. That evolution has fundamentally altered how we access and store information.

The sudden adaptation to overcome natural barriers can be found in more industries than just information technology. Car manufacturers achieved gradual improvement in fuel efficiency for years. At some point however, they encountered a limit to what could be achieved with conventional technology, prompting the shift to a new paradigm. This led to the development of hybrid vehicles which marked a significant leap in efficiency, which subsequently gave way to electric cars whose performance is no longer gauged by miles per gallon.

Evolving Beyond Traditional Cybersecurity Tools

Today, we are witnessing similar evolutionary strides in cybersecurity technologies. The journey from antivirus (AV) solutions, endpoint detection and response (EDR), and extended detection and response (XDR) marks significant milestones in the evolution of endpoint protection. Similarly, network security has advanced from relying solely on perimeter defenses to embracing zero trust and secure access service edge (SASE) models. Finally, the shift from datacenter-focused to cloud-based data and workload security represents a pivotal change in how we protect digital assets.

The Persistent Use Of SIEM In The SOC

Despite the continual evolution of cybersecurity technologies, security operation centers (SOCs) have largely remained dependent on security information and event management (SIEM) solutions. Originating in the early 2000s, the SIEM model was developed for enterprises to meet the need

70%

of ransomware cases involving negotiation included **cybercriminals threatening to leak stolen data.**[1]

for centralized log collection and management. Since it offered unparalleled visibility at the time, SIEM became a cornerstone in the SOC.

However, the rapid pace of digital transformation, the expansion of threat landscapes, and the sophistication of cyberattack tactics have gradually outstripped the capabilities of traditional SIEM solutions. The requirements for protecting enterprises today demand a new approach to threat detection and remediation. As we move forward, the cybersecurity community is poised for the next significant leap in technology that will transcend the limitations of the SIEM model, ushering in a new era of cybersecurity readiness and resilience.

Exploring The Shortcomings Of SIEM Systems

Initially, when SIEM solutions were introduced, the volume of security alerts generated by enterprises was relatively manageable. However, in today's landscape, analysts are overwhelmed by the sheer quantity of alerts produced by a multitude of isolated and diverse security tools spread across the IT environment. With so many alerts from disconnected sources, SOC analysts must meticulously assemble pieces from multiple puzzles at the same time. This leads to missed threats and prolonged response times that fail to match the pace of cyberattacks.

Why Do SOCs Still Rely On SIEM Solutions?

Many SIEM solutions, having been developed more than ten years ago, rely on architectures now considered outdated, constraining their adaptability to contemporary security challenges. Frequently, organizations procure SIEM systems primarily to fulfill compliance mandates. However, the pace at which compliance and regulatory standards evolve is notoriously slow, leading to a situation in which having a SIEM is driven by the need to fill a checkbox requirement. Unfortunately, fulfilling these compliance requirements through SIEM adoption does not guarantee the cyber safety of an enterprise.

Reliance on legacy SIEM systems within SOCs can also be attributed to hesitancy. These systems are frequently integrated with a suite of security tools, including EDR, IDS and network traffic analysis tools.

In addition, many organizations have invested considerable time customizing their SIEM solutions to meet their specific needs. Also, abrupt alterations to the SIEM technology could necessitate expensive and complex reconfigurations, potentially leading to interruptions in security monitoring and operations. This underscores the cautious approach towards transitioning away from existing SIEM solutions.

Making Better Use Of Your Data

In the hours, days, and months following a cyber incident or data breach, cybersecurity teams often resort to their data sources to identify how the cyber event transpired and why it happened. Of course, this information paints a clearer picture of what happened, which is important. But a bigger question must be asked – if your environment already had access to this data before detection occurs, then what prevented your personnel from stopping the cyberattack in real time? Ultimately, it is about making better use of the data that is at your disposal. Prevention is your first line of defense, it is time to leverage its power and potential.

Introducing Cortex XSIAM By Palo Alto Networks

As a cybersecurity pioneer for nearly two decades, Palo Alto Networks has recognized the imperative for a revolutionary leap forward. This advancement, as you might anticipate, leverages the power of artificial intelligence (AI) and machine learning (ML). Just as AI is revolutionizing roles from programming to clerical tasks, it is now poised to make a significant impact in cybersecurity. Palo Alto Networks' commitment to developing a groundbreaking solution for modern SOCs has culminated in the creation of a new security platform, Cortex XSIAM. This next-gen platform is designed to propel SOCs beyond the capabilities of traditional SIEM systems, setting a new standard in the industry.

XSIAM stands for Extended Security Intelligence and Automation Management and its concept is simple. In today's cybersecurity landscape, the sheer volume and complexity of attacks make it impossible for security analysts to scrutinize every minor incident. XSIAM represents a cybersecurity approach that aims to

transform security operations by integrating data across various sources at an unprecedented scale.

By harnessing advanced analytics and automation, XSIAM is crafted to outperform traditional SIEMs, enhancing the efficiency and effectiveness of threat detection and response. The goal is to eradicate alert fatigue, expedite investigations, and ensure attackers can no longer lurk undetected in networks for extended periods.

XSIAM is a cloud-based, integrated SOC platform that includes best-in-class functions including EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM. By consolidating multiple products into a cohesive platform, XSIAM not only reduces expenses and enhances operational efficiency but also significantly boosts analyst productivity. This is achieved by ensuring that only the most critical incidents are escalated to human operators while the rest are efficiently managed through AI automation. As XSIAM continually learns from network behaviors and data from every incident, it progressively improves its functionality, further alleviating the workload on your valued analysts and streamlining security operations.

Empower IT Security Analysts With Automated Intelligence

SIEM was designed to provide vast amounts of data about your cybersecurity environment. XSIAM takes that starting point and then automates incident detection, automation, and response. This powerful combination of automated intelligence then empowers your analysts, allowing for your security posture to become more proactive.

But don't just take the technical claims of Palo Alto as a validation of XSIAM, as it also powers Palo Alto Network's own SOC. Considering the scale at which a leading cybersecurity company operates, the volume of incidents it must manage is vast. Yet, XSIAM's efficiency is such that only a minimal number of the nearly one trillion monthly events require escalation to Palo Alto Networks' highly skilled, but relatively small, team of human analysts. This testament to XSIAM's capabilities showcases its potential to transform and elevate SOC operations.

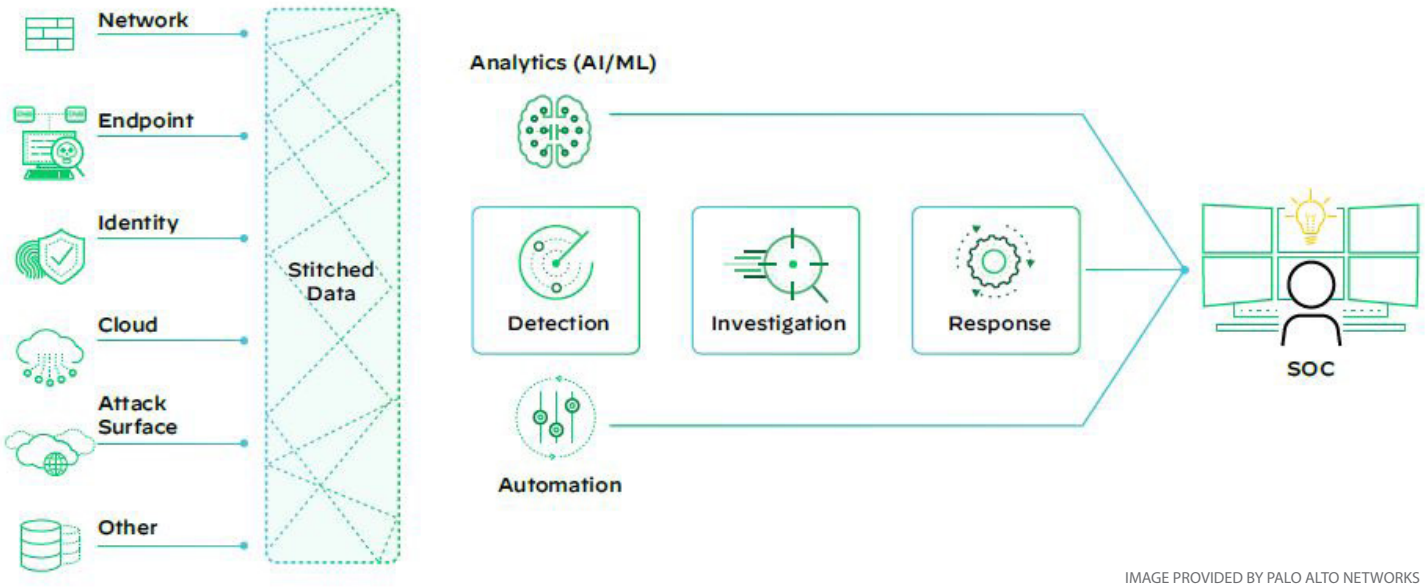

IMAGE PROVIDED BY PALO ALTO NETWORKS

A transformed SOC

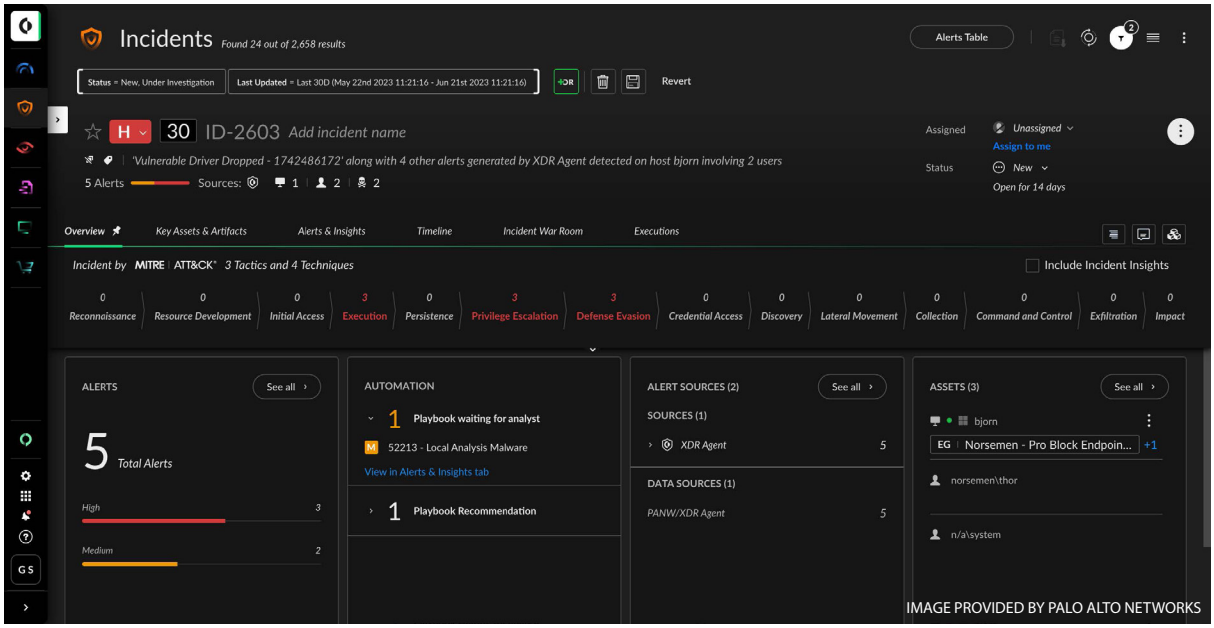

IMAGE PROVIDED BY PALO ALTO NETWORKS

Gain deeper context around incidents with MITRE ATT&CK mapping, associated alerts, playbook status, alert sources, and artifacts.

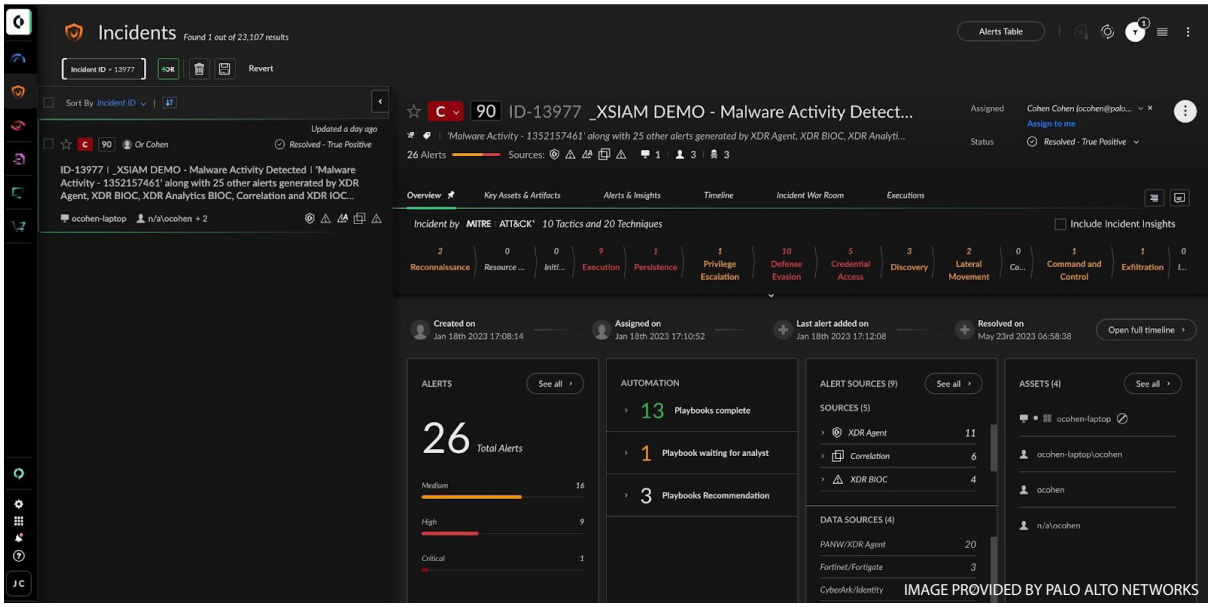

IMAGE PROVIDED BY PALO ALTO NETWORKS

The analyst incident management view provides a full summary of actions automatically taken, the results, and all remaining suggested actions. A drill-down incident timeline is presented to the analyst if further investigation and response is required. This is also complemented by broad XSIAM intelligence from all analytics and functions.

Talk to WEI today

At the inception of SIEM technology, conveying its full technological scope, capabilities, and potential benefits to organizations was a formidable challenge. Similarly, detailing the transformative impact of XSIAM on your SOC's capabilities within the confines of this document is a tall order. This is precisely why we invite you to engage with a WEI SOC specialist. Through a scheduled discussion, you can gain insights into how XSIAM can be tailored to into your unique environment and revolutionize your SOC to address the security challenges of today and tomorrow.

Sources:

1. Palo Alto Networks Unit 42, Ransomware and Extortion Report 2023: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2023-unit42-ransomware-extortion-report.pdf

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.