
Cortex XSIAM
EXTENDED SECURITY INTELLIGENCE AND AUTOMATION MANAGEMENT
The Machine-Led, Human-Empowered Security Platform
paloalto NETWORKS
CORTEX XSIAM
BY PALO ALTO NETWORKS

A Look into the Past in Order to Move Forward

In the last few years, the needs of the security operations center (SOC) have changed, but the designs of the SIEM and SOC have not. The security information and event management (SIEM) category has served security operations for years with significant manual overhead and slow incremental improvement in security outcomes. Most other key pieces of the security architecture have been modernized: The endpoint moved from antivirus (AV) to endpoint detection and response (EDR) to extended detection and response (XDR); the network moved from a "hard shell" perimeter to Zero Trust and SASE; runtime moved from the data center to the cloud. In contrast, the SOC still operates on a SIEM model designed 20 years ago.

To that end, the SIEM market has been slow to evolve, with limited incentive for vendors to invest in significant changes to their products and solutions. There are several reasons for this technological inertia, including:

- **Legacy technology**: Many SIEMs were developed over a decade ago and are often based on outdated architectures, limiting their ability to adapt to new security challenges.

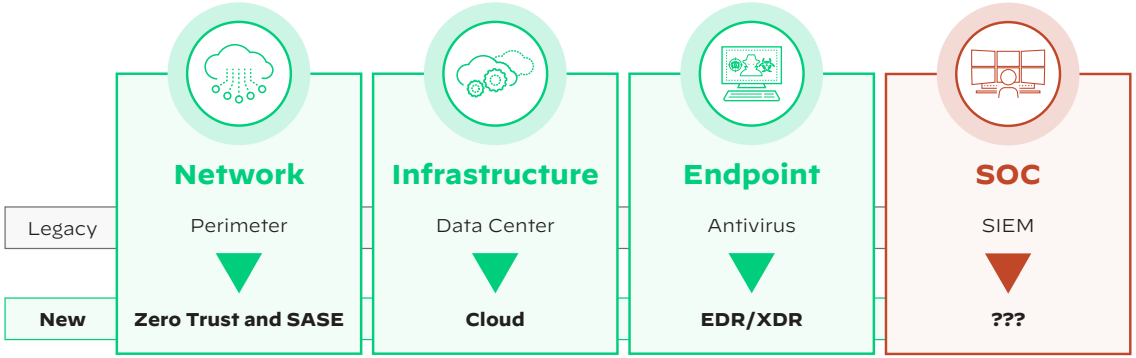


Figure 1: It's time for the SOC to evolve past legacy SIEMs

- **Complexity**: SIEMs are often complex to implement and manage, including the need for continuous tuning to prevent issues such as false positives or missing critical security events. As a result, vendors may be reluctant to make significant changes that could disrupt their customers' operations.
- **Lack of innovation**: The SIEM market is relatively mature, and there may be limited incentive for vendors to invest in innovations.
- **Integration challenges**: SIEM solutions often integrate with other security tools, such as EDR systems, intrusion detection systems (IDS), and network traffic analysis (NTA) tools. Changing the underlying technology of a SIEM solution could potentially break these integrations, making it difficult for customers to manage their security operations.
- **Customization requirements**: Many organizations have customized their SIEM solutions to meet their specific needs. Making significant changes to the underlying technology could require customers to reconfigure their systems, which can be time-consuming and costly.

- **Regulatory compliance**: Many organizations use SIEM solutions to meet regulatory compliance requirements so changes to a SIEM could potentially impact its ability to meet these requirements.

"Security analytics platforms have over a decade of experience in data aggregation they apply to these challenges but have yet to provide IR capabilities that are sufficient at enterprise scale, forcing enterprises to prioritize alternate solutions."[1]

– Allie Mellen, Senior Analyst, Forrester

Radically Reimagined Cybersecurity

Cybersecurity has an urgent threat remediation problem. With the rapid proliferation of applications, workloads, microservices, and users, our collective digital attack surface has expanded faster than we can protect it. A byproduct of this reality is detection and prevention tools end up generating potentially thousands of alerts every day—far exceeding the volume that security teams are staffed to effectively handle. These alerts come from many disconnected sources, leaving security analysts to piece the puzzle together.

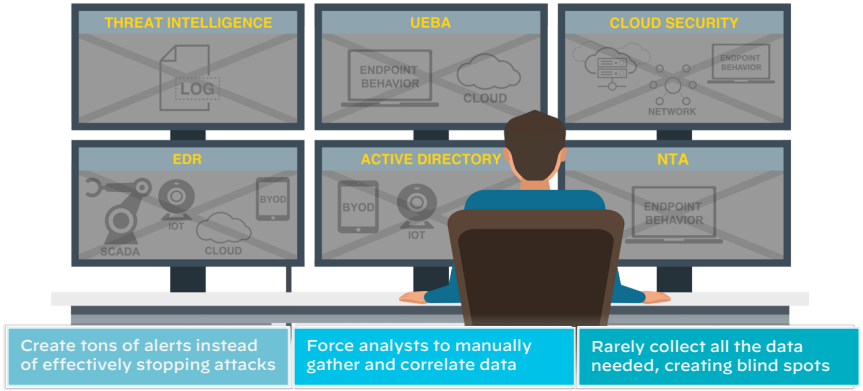


Figure 2: Siloed tools slow down investigation and response

Analyzing a potential threat generally requires many steps, including:

1. Reviewing available log data to start piecing together what may have occurred.
2. Manually comparing data against threat intelligence sources to determine if indicators are known to be malicious.
3. Finding information gaps and searching for available data that may indicate additional steps in an attack.
4. Checking if new information links to alerts are being handled by other team members to coordinate efforts.

1. Allie Mellen, *Adapt Or Die: XDR Is On A Collision Course With SIEM And SOAR*, Forrester, April 28, 2021.

5. Evaluating whether the alert needs to be escalated, discarded, or quickly remediated and closed out.

These steps take a lot of time and multiple tools to complete in a traditional SOC—and that's just triage. The net result is that analysts only have time to address the highest-priority alerts they come across each day. Meanwhile, a disconcerting number of lower-priority alerts aren't addressed at all. Historical incident investigations show that a collection of lower-priority alerts are actually part of a single attack, not realized by legacy threat detection platforms.

Further, security analysts responsible for alert triage are often left with insufficient context to determine the real risk that an attack presents to the organization. Thus, the alert is escalated to a higher-level group for further validation, requiring even more time, labor, and resources—creating inefficiencies at all levels. With that in mind, cyber adversaries are banking on our inability to act quickly, yet most organizations are still taking hours, or even days or months, to identify and remediate threats.

28 days

dwell time before ransomware is detected in environment[2]

7-48 days

typical dwell time before business email compromise (BEC) is detected and contained[3]

38 days

BEC median dwell time[4]

At the heart of our weakness lies our inability to fully leverage massive scales of data for our defense. SIEM solutions were built to facilitate alert and log management but have relied heavily on human-driven detection and remediation with bolt-on analytics and process automation only here and there. Combating today's threats requires us to radically reimagine how we run cybersecurity in our organizations using AI.

The modern SOC must be built on a new architecture designed to meet the evolving needs of modern IT environments. This architecture should be flexible, scalable, adaptable, and able to integrate with a wide range of security tools and technologies. Overall, the design should consider providing:

- Broad and automated data integration, analysis, and triage
- Unified workflows that enable analysts to be productive

2. *Incident Response Report 2022*, Unit 42, July 26, 2022.
3. Ibid.
4. Ibid.

- Embedded intelligence and automated response that can block attacks with minimal analyst assistance

Unlike legacy security operations, the modern SOC leads with data science over massive datasets rather than human judgment and rules designed to catch yesterday's threats.

Under the Hood of XSIAM

Palo Alto Networks has been working hard to address the above limitations from current security solutions. As such, our industry needs to continually innovate to stay ahead of the security curve. Cortex XSIAM, or extended security intelligence and automation management, is a pivot toward an AI-driven architecture, built from the ground up.

It's an inflection point in how we think about cybersecurity and lean into AI in areas where machines are simply built to perform better than us. It's the sum of a vision to create the autonomous security platform of the future, driving dramatically better security with near-real-time detection and response.

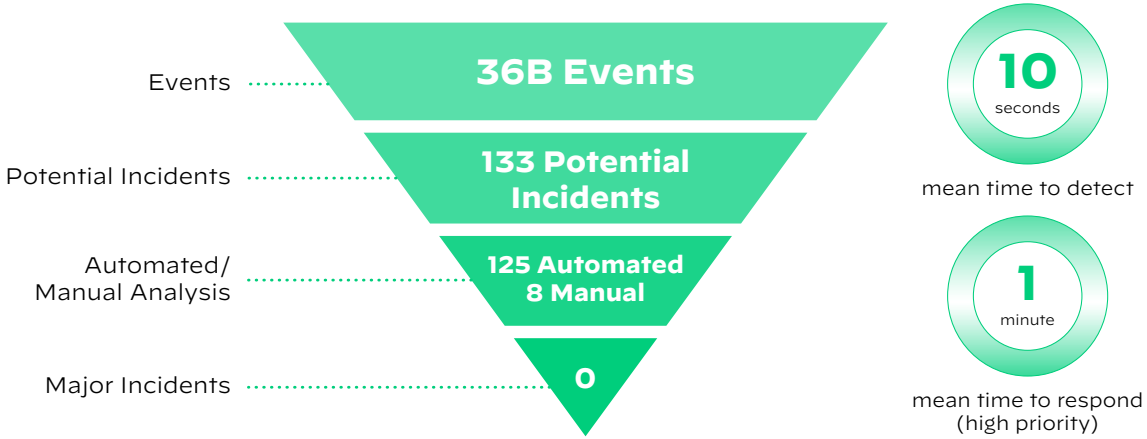


Figure 3: At Palo Alto Networks, we're our first customer

XSIAM unifies best-in-class functions, including EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM.

Built on a security-specific data model and updated continuously with Palo Alto Networks threat intelligence gathered globally across tens of thousands of customers, XSIAM uses an ML-led design to integrate massive amounts of security data. It then aggregates alerts into incidents for automated analysis and triage, and to respond to most incidents automatically, enabling analysts to focus on the few threats that require human intervention. XSIAM is already proven in production, powering Palo Alto Networks own SOC and turning over one trillion monthly events into a handful of analyst incidents daily.

A New Paradigm to Power the Modern SOC

Cortex XSIAM harnesses the power of machine intelligence and automation to radically improve security outcomes and transform the SecOps model. XSIAM puts the SOC in full control of enterprise security—endpoint to cloud—centralizing data and security functions to outpace threats, accelerate response, and dramatically streamline analyst and SOC team activities.

Today's hybrid enterprise generates many times the security data of a few years ago. Yet the typical SOC still operates on data silos, limited cloud visibility, aging SIEM technology, and manual, human-driven processes that invite attackers to exploit their advantage.

Incremental analyst headcount cannot stem the tide, and additional tooling only worsens today's complex SOC architecture and engineering maintenance burdens. The modern SOC must turn to an intelligent, machine-driven model that can block attacks from endpoint to cloud, at scale, with minimal analyst involvement and SOC engineering overhead.

Cortex XSIAM is designed to address the needs of the modern SOC by harnessing the power of machine intelligence and automation to dramatically improve security outcomes and transform the manual SecOps model. This model enables the SOC to be proactive instead of reactive by delivering on the promise of machine-triaged data so the analysts can focus on unusual behavior and anomalies.

XSIAM is uniquely designed to be the center of SOC activity, replacing SIEM and specialty products by unifying broad functionality into a holistic, task-oriented SecOps platform. Purpose-built with threat detection and response at its core, XSIAM centralizes, automates, and scales security operations that can fully protect the hybrid enterprise.

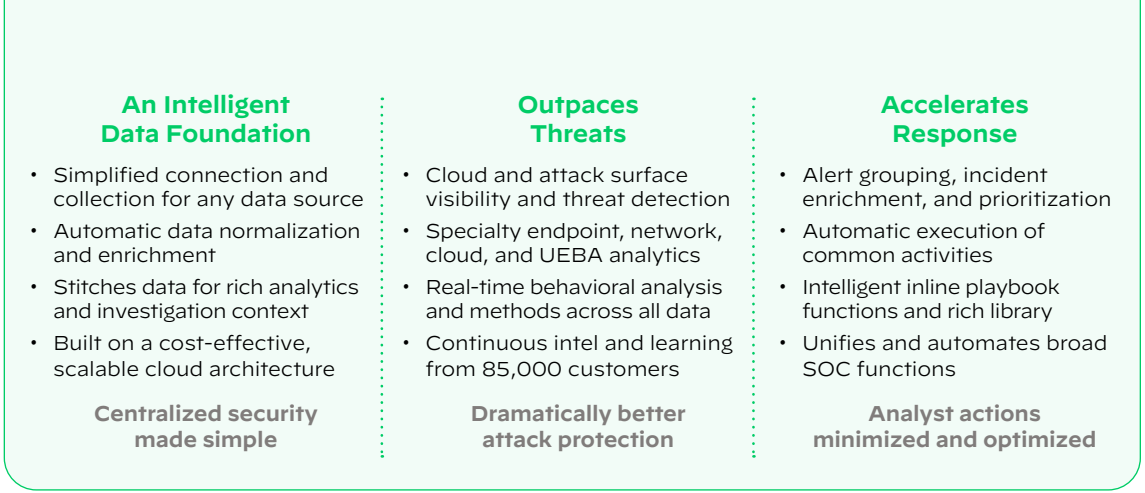


Figure 4: Cortex XSIAM highlights: a single platform does it all

The human-first approach to SecOps has long since hit a wall. The modern SOC must turn to an intelligent, machine-led, human-empowered security system that delivers dramatically better protection at unprecedented scale and efficiency.

How It Works

XSIAM is the central operations platform for the modern SOC, providing the best-in-class capabilities of EDR, XDR, SOAR, attack surface management (ASM), threat intelligence management (TIM), UEBA, SIEM, and more. But XSIAM is not a collection of disparate tools. Instead, XSIAM weaves together functions and intelligence in a task-oriented user experience and a rich incident management flow that minimizes activities and context switching to power rapid and accurate attack response.

XSIAM is revolutionary in the way it operates, using intelligent automation to break from the analyst-driven model of today's security products. From data onboarding to incident management, XSIAM helps minimize the tasks of analysts and all SOC personnel so they can focus on valuable activities that the system cannot perform.

SOC Controls for Cloud and the Hybrid Enterprise

Today, most SOC teams operate on limited and siloed data, including woefully inadequate visibility to fluid cloud and internet-facing resources that are already involved in over one-third of breach cases.[5] Cloud security products provide essential protections but are typically operated independently and outside the SOC. Yet the SOC team must be able to centrally monitor complete end-to-end security and conduct investigations of the many incidents involving cloud assets.

XSIAM builds an intelligent data foundation across all enterprise security sources, from endpoints to specialized cloud feeds from providers, dynamic workloads, and cloud security products. The system continually collects deep telemetry alerts and events from these sources, automatically prepares and enriches the data, and uniquely stitches it into security intelligence tuned to support rich machine learning analytics specialized for both specific sources and kill chain-wide behavioral detection.

Rearchitecting the SOC

SIEM's aging database architecture, management complexity, and limited evolution have forced innovation to come from surrounding specialized tools. The result is a SOC architecture that is a complex and brittle maze of data pipelines, product integrations, and constant management headaches.

XSIAM consolidates multiple tools and scales, centralizes, and automates data collection to streamline SOC infrastructure and significantly reduce engineering and operations costs.

Snapshot: Augment Analysts with ML-Driven Intelligence

A key component in a modern SOC transformation is to ensure that security teams are using machine learning to its full potential to augment and complement humans in security. Advanced analytics and AI can significantly reduce the time teams spend processing massive amounts of data in the enterprise to develop critical security insights. As a subset of AI, machine learning uses

5. *Incident Response Report 2022*, Unit 42, July 26, 2022.

training data from a client environment to enable machines to learn and improve their knowledge about the environment and performance on a task.

By automatically detecting anomalous patterns across multiple data sources and automatically providing alerts with context, machine learning today can deliver on its promise of speeding investigations and removing blind spots in the enterprise.

This works by training ML models with quality security-relevant data, using them to detect patterns among and across the data, and testing and refining the processes. ML techniques can gather, integrate, and analyze data and interrogate the data to reduce the amount of time and knowledge needed for a human to perform these tasks. This also minimizes the challenge for a SOC team trying to find threat context and evidence across multiple security layers embedded in data.

Supervised ML techniques can be used to read the digital markers from devices, such as desktop computers, mail servers, or file servers, and then learn the behavior of different types of devices and detect anomalous behavior. The promise of machine learning is having the ability to determine causal inferences around what is happening in an environment and letting the software direct next steps instead of relying on human interaction. For instance, flagging bad actions based purely on behavior and interactions within the joined datasets so it can then propagate a decision to the rest of the network with explicit instructions such as instructing an agent to contain it or a firewall not to communicate with it.

Machine learning in XSIAM can provide:

- **Behavioral analysis**: XSIAM uses AI and ML algorithms to analyze the behavior of endpoints and detect anomalies that may indicate the presence of a threat.
- **Threat intelligence**: The platform applies ML algorithms to analyze large volumes of threat intelligence data and identify patterns and trends that may indicate an emerging threat.
- **Automated response**: XSIAM uses AI-powered automation to respond to threats in real time, without the need for human intervention.
- **Predictive analytics**: The platform leverages ML algorithms to analyze historical data and predict potential threats, helping organizations proactively protect against future attacks.
- **Continuous learning**: XSIAM's ML algorithms continuously learn from new data and adjust their models, improving the platform's accuracy and effectiveness over time.

Built for Threat Detection and Response

The heart of XSIAM is threat detection and response, and XSIAM is unique in its automation of the incident management flow. XSIAM analytics provide technique-based intelligence, allowing alerts to be grouped to incidents, fully enriched with relevant context. Embedded automation and inline playbooks apply analytic results for intelligent execution—fully processing and closing alerts or incidents whenever possible.

The analyst incident management view provides a full summary of actions automatically taken, the results, and suggested actions that remain. When further investigation and response activities are required, the analyst is presented with a drill-down incident timeline and broad XSIAM intelligence from all analytics and functions. Remediation and response actions can leverage inline playbooks, and for managed endpoints, XSIAM provides one-click remediation action options along with powerful Live Terminal access and forensics tools.

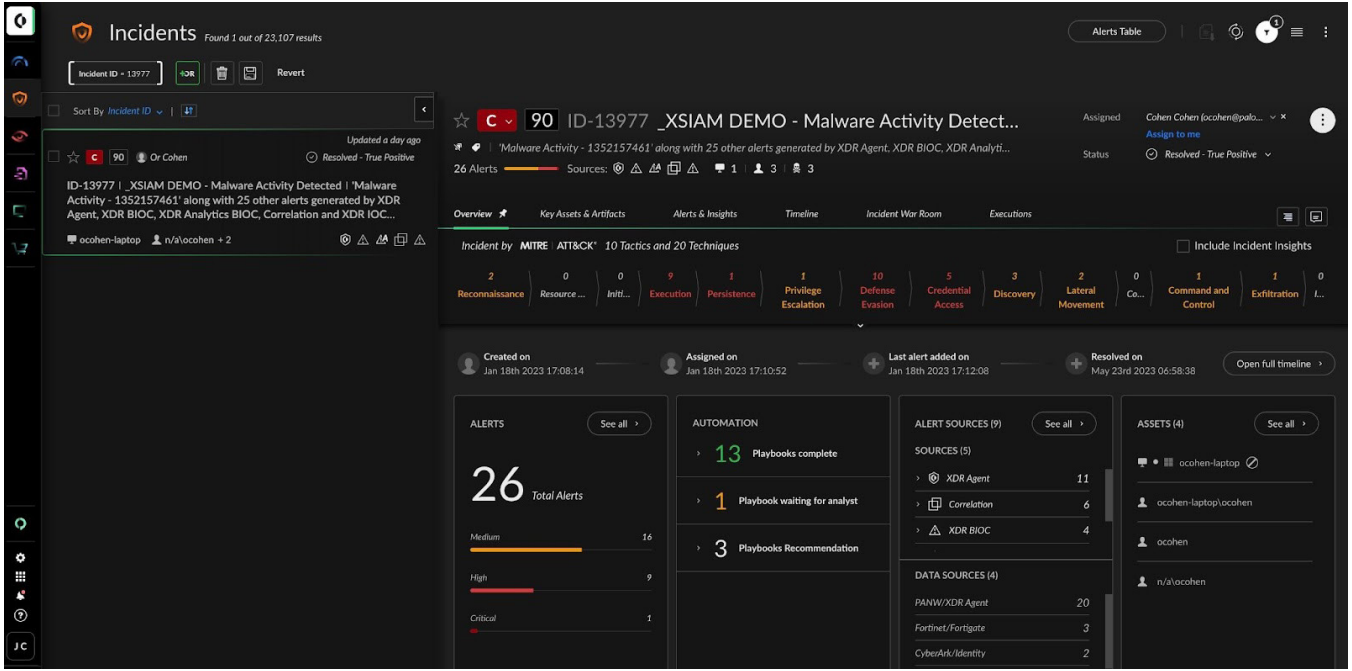


Figure 5: Analyst incident management view

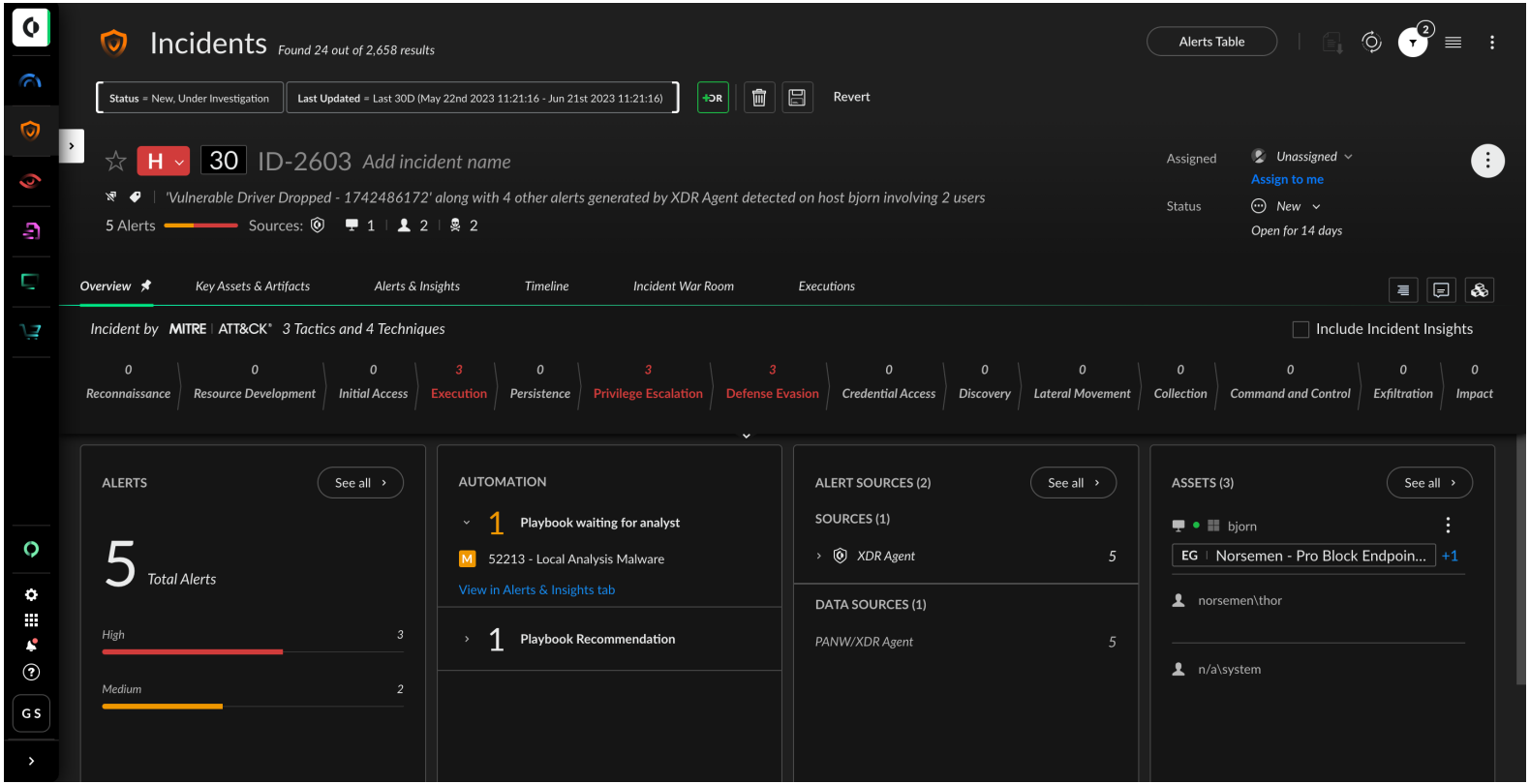


Figure 6: Gain deeper context around incidents with MITRE ATT&CK mapping, associated alerts, playbook status, alert sources, and artifacts

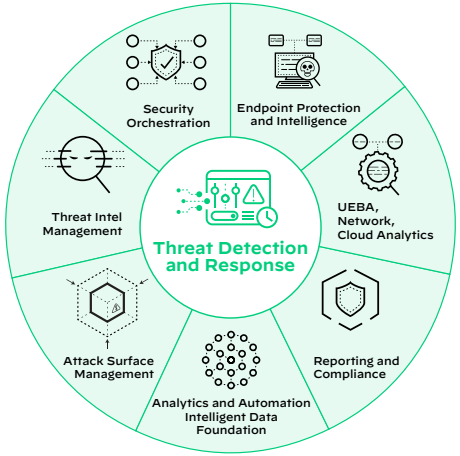
Cortex XSIAM's Unique Benefits

Cortex XSIAM is a true SOC platform and a game-changer for the traditional, multitool, human-driven SOC operating model. Overwhelmingly, organizations using a legacy SOC model all have similar pain about their existing security architecture and management. Cortex XSIAM was built by security practitioners who have lived through these pains. Its development was influenced by Palo Alto Networks clients seeking a way to solve their security outcome challenges.

Replace outmoded SIEM to centralize and act on true security intelligence

Consolidate disparate SOC tools for efficient and cost-effective operations teamwide

Get machine-driven security at scale, while analysts focus on high-value tasks



Extend SOC visibility and control to cloud and dynamic internet resources

Depend on threat detection that's proven to protect the entire enterprise, endpoint to cloud

Protect endpoint targets from laptops to data center systems to cloud workloads

Figure 7: Centralize, automate, and scale operations to protect your organization

Key Features Summary	
Data Onboarding The cloud architecture makes onboarding, monitoring, and reporting simple with hundreds of prebuilt data packs, standard connector types, and simple, automated steps for configuration.	**Threat Intelligence Management** Manage Palo Alto Networks and third-party threat intelligence feeds and automatically map them to alerts and incidents.
Intelligent Data Foundation Continually collect deep telemetry, alerts and events from any source, automatically enrich and map it to a unified data model, and stitch events into intelligence tuned for machine learning analytics.	**Endpoint Protection and Intelligence** Consolidate SIEM and EPP/EDR spend into a unified and integrated solution, with a complete endpoint agent and cloud analytics backend to provide endpoint threat prevention, automated response, and in-depth telemetry useful for any threat investigation.
Threat Detection Analytics Apply specialized analytics and behavior-based detections across all collected data with technique-based analytics.	**Attack Surface Visibility and Action** Gain a holistic view of your asset inventory, including internal endpoints and vulnerability alerting for discovered internet-facing assets, with embedded ASM capabilities.
Automated Investigation and Response Autoexecute many tasks and provide your analysts the intelligence and guidance necessary to complete actions that require human actions with automated functions and intelligent inline playbooks.	**User and Entity Behavior Analytics** Use machine learning and behavioral analysis to profile users, machines, and entities to identify and alert on behavior that may indicate a compromised account or malicious insider.
Playbooks and Orchestration Create and orchestrate playbooks for use with a robust SOAR (security orchestration, automation, and response) module and marketplace.	**Network and Cloud Analytics** Detect and alert on anomalies in network and cloud data, such as firewall events, cloud service provider logs, and cloud security product alerts with specialty analytics.
Management, Reporting, and Compliance Centralized management functions simplify operations. Powerful graphical reporting capabilities support reporting for compliance, data ingestion, incident trends, SOC performance metrics, and more.	

Imagination Technologies Group: An XSIAM Customer Story

Imagination Technologies Group standardized on Palo Alto Networks Cortex XSIAM in their SOC to deliver automated, end-to-end threat management, wherever the threats originate.

Imagination

> Cortex XSIAM is a single, tightly integrated suite of tools. It's easy to commission, easy to use, and delivers the trusted answers a modern SecOps team need.

— Paul Alexander, Director of IT Operations, Imagination Technologies Group

Customer Needs

- Automate repetitive data analysis tasks to improve productivity, allowing more time for value-add security operations.
- Unite endpoint, network, cloud, and identity data to detect advanced threats with precision and simplify investigations.

Solution

Palo Alto Networks Cortex XSIAM

Outcomes

- Easier to ingest data and normalize it.
- All of the threat vector information and insights are centralized.
- More confidence in security decisions.
- Frees up time to focus on other tasks.

XSIAM Services You Can Count On

Drive Successful XSIAM Outcomes with Global Customer Services

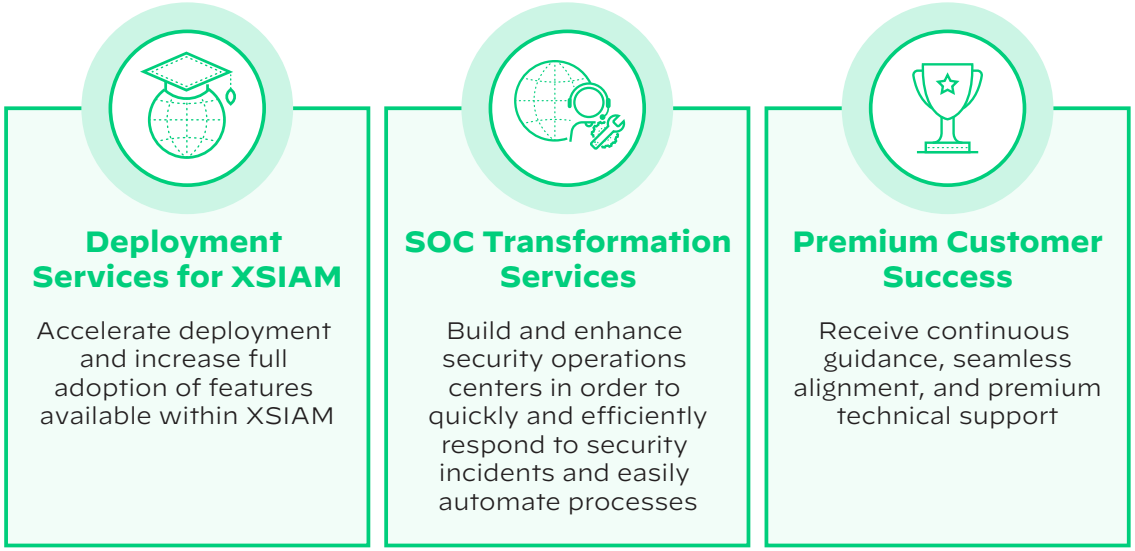


Figure 8: Global Customer Services provides a number of support and service options for XSIAM

Our industry-leading cybersecurity experts help you optimize your deployments by applying technical expertise, professional services, and operational processes to maximize your security investment.

XSIAM Deployment Services enable greater adoption of Cortex XSIAM features and accelerates time to value.

Key benefits:

- Accelerate protection for sophisticated threats across all enforcement points, endpoint policy tuning, correlation creation, security operations best practices, incident management methodologies, and playbook creation.
- Reduce deployment risks using best practices with assistance from our experts.
- Ensure ongoing effective operations, administration, and management with knowledge transfer to your team.
- Achieve dramatically faster, better, and more measurable security outcomes.

SOC Transformation Services provide a framework for organizations to build and enhance security operations centers to quickly and efficiently respond to security incidents and easily automate processes.

Key benefits:

- Develop a custom strategy to operationalize Cortex platforms in your environment.
- Establish modular processes and procedures to increase automation opportunities.
- Showcase security operations success through robust metrics and reporting frameworks.
- Enable analysts to use Cortex XSIAM efficiently.
- Build advanced SOC features for threat hunting and intelligence utilizing the Cortex platform.

Premium Customer Success provides continuous guidance, seamless alignment, and premium technical support.

Key benefits:

- Access to Customer Success experts who provide strategic guidance throughout the lifetime of your Cortex XSIAM investment.
- Provide tailored strategies to ensure you realize an optimal return on investment (ROI).
- 24/7 technical phone support helps solve any challenges you come across.
- Always-on digital support and knowledge tools.

For more information on these services, contact our Services Sales Team.

Access the latest XSIAM resources:

Visit the XSIAM product page

What is XSIAM?

Request a personal demo of XSIAM

See XSIAM in action in a 15-minute video

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com