EXTENDED SECURITY INTELLIGENCE
AND AUTOMATION MANAGEMENT

Cortex XSIAM

The AI-Driven SecOps Platform That Goes Beyond Reactive Security

paloalto NETWORKS | CORTEX XSIAM®

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 security information and event management (SIEM) and SOC have not. The 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, including:

- 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. Several reasons for this technological inertia include:

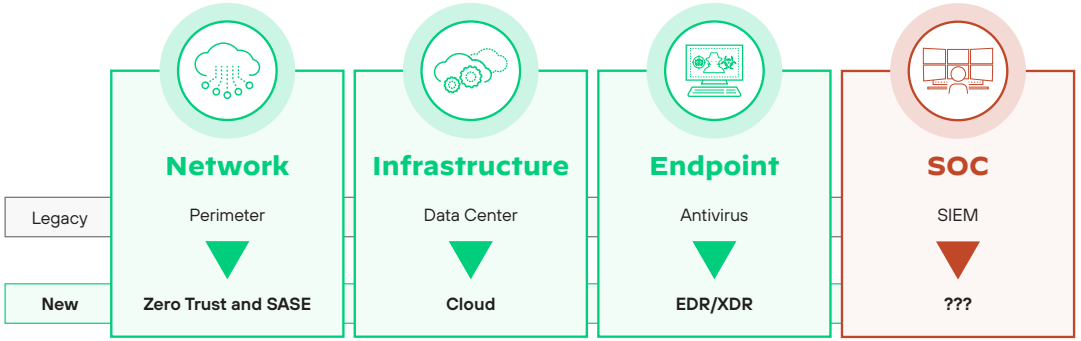


Figure 1. It's time for the SOC to evolve past legacy SIEMs

- **Legacy technology:** Many SIEMs were developed over a decade ago and are often based on outdated architectures, limiting their ability to adapt to new security challenges.
- **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 might be reluctant to make significant changes that could disrupt their customers' operations.
- **Lack of innovation:** The SIEM market is relatively mature, and there might 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 organizations 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 them to reconfigure their systems, which can be time-consuming and costly.
- **Regulatory compliance:** For organizations that use SIEM solutions to meet regulatory compliance requirements, changing 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."**
>
> – Allie Mellen, Senior Analyst, Forrester

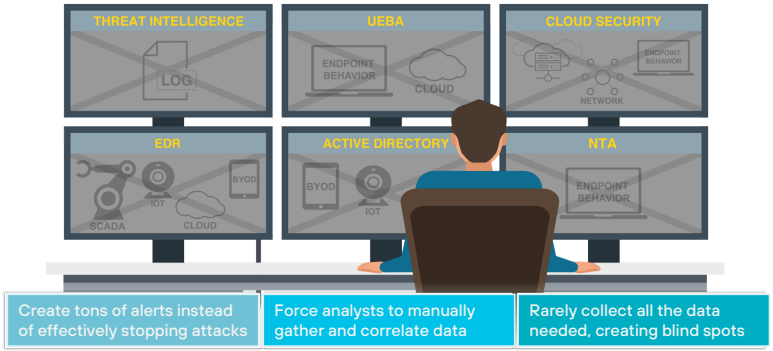


Figure 2. Siloed tools slow down investigation and response

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 that 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 together the puzzle.

Analyzing a potential threat generally requires many steps, such as:

1. Review the available log data to start piecing together what might have occurred.
2. Manually compare the data against threat intelligence sources to determine if indicators are known to be malicious.
3. Find information gaps and search for available data that could indicate additional steps in an attack.

4. To coordinate efforts, check whether other team members are handling new information links to alerts.
5. Evaluate 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 an environment[1]

7–48 days

typical dwell time before a business email compromise (BEC) is detected and contained[2]

38 days

BEC median dwell time[3]

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 provide:

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

1. *Unit 42 Incident Response Report 2022*, Palo Alto Networks, July 26, 2022.
2. Ibid.
3. 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 Cortex XSIAM

Our industry needs to continually innovate to stay ahead of the security curve. Cortex XSIAM®, or extended security intelligence and automation management (XSIAM), is a pivot toward an AI-driven architecture, built from the ground up.

It's time to rethink cybersecurity and lean into AI in areas where machines are simply built to perform better than us. XSIAM is 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.

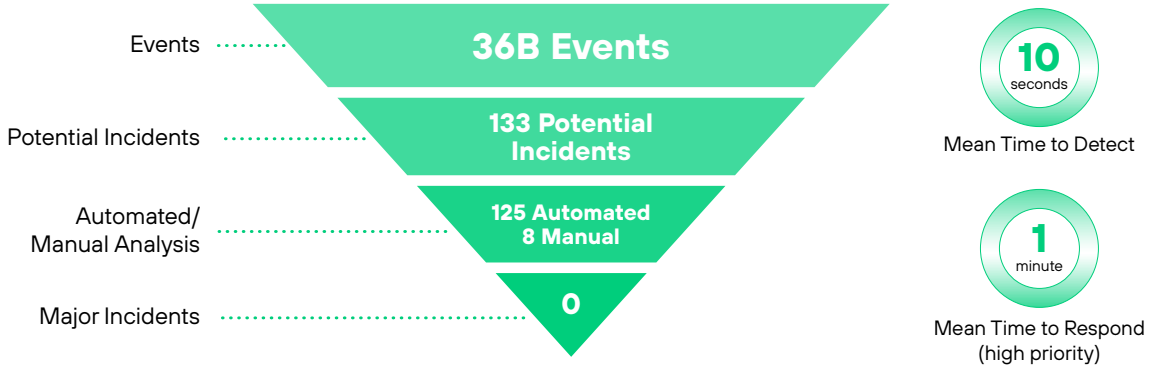


Figure 3. At Palo Alto Networks, we're our first customer

XSIAM unifies best-in-class functions, including EDR, XDR, security orchestration, automation, and response (SOAR), cloud detection and response (CDR), attack surface management (ASM), user and entity behavior analytics (UEBA), Threat Intel Management (TIM), threat intelligence platform (TIP), and SIEM. Built on a security-specific data model and updated continuously with our threat intelligence gathered globally across tens of thousands of our customers, XSIAM uses machine learning (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 our own SOC and turning over one trillion monthly events into a handful of analyst incidents daily.

A New Paradigm to Power the Modern SOC

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 much more security data than 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 tools only worsen 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.

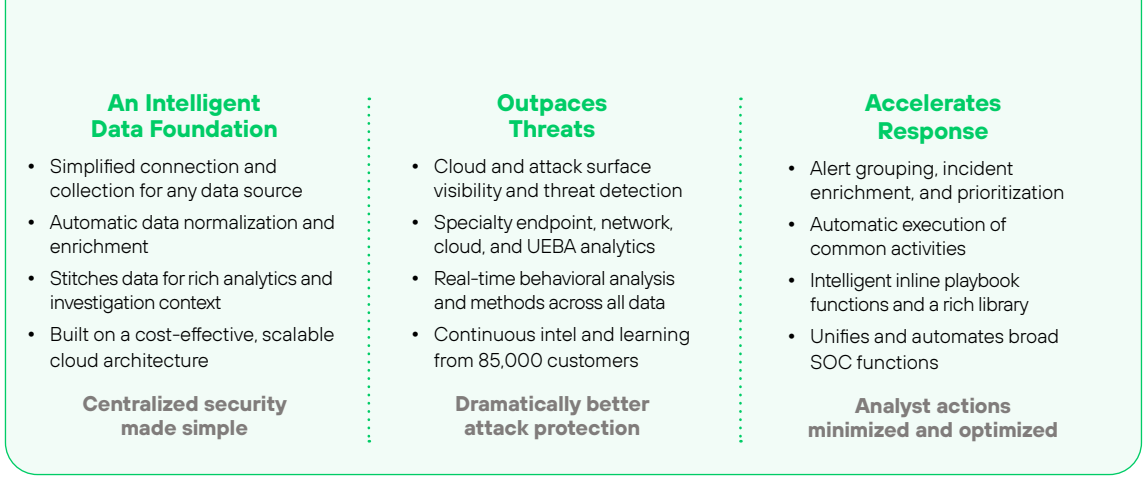


Figure 4. Cortex XSIAM highlights: A single platform does it all

XSIAM harnesses 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 analysts can focus on unusual behavior and anomalies.

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

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 Cortex XSIAM Works

XSIAM is the central operations platform for the modern SOC, providing EDR, XDR, SOAR, ASM, TIM, TIP, UEBA, and SIEM capabilities, and more. But XSIAM is not a collection of disparate tools. Instead, it 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, it helps minimize analyst and SOC personnel tasks 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. 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 and automatically prepares and enriches the data. It also uniquely stitches it into security intelligence tuned to support rich ML analytics specialized for both specific sources and attack lifecycle-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 security teams use ML 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, ML uses 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, ML 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 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 ML 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, ML flags bad actions based purely on behavior and interactions within the joined datasets. Then, it can 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 might 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 might 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:** The XSIAM 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, with its automation of the incident management flow making it unique. XSIAM analytics provide technique-based intelligence, allowing the grouping of alerts into 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 Incidents management view provides a full summary of actions automatically taken, the results, and remaining suggested actions. When further investigation and response activities are required, an 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.

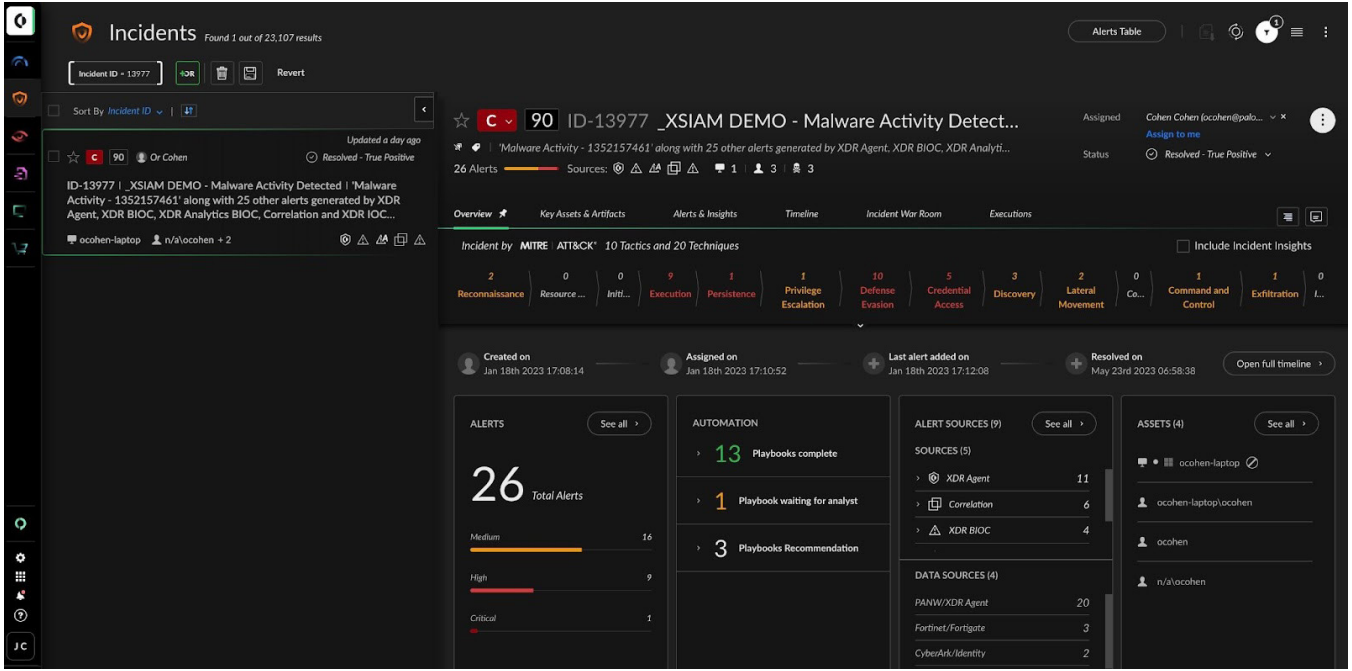


Figure 5. Analyst Incidents management view

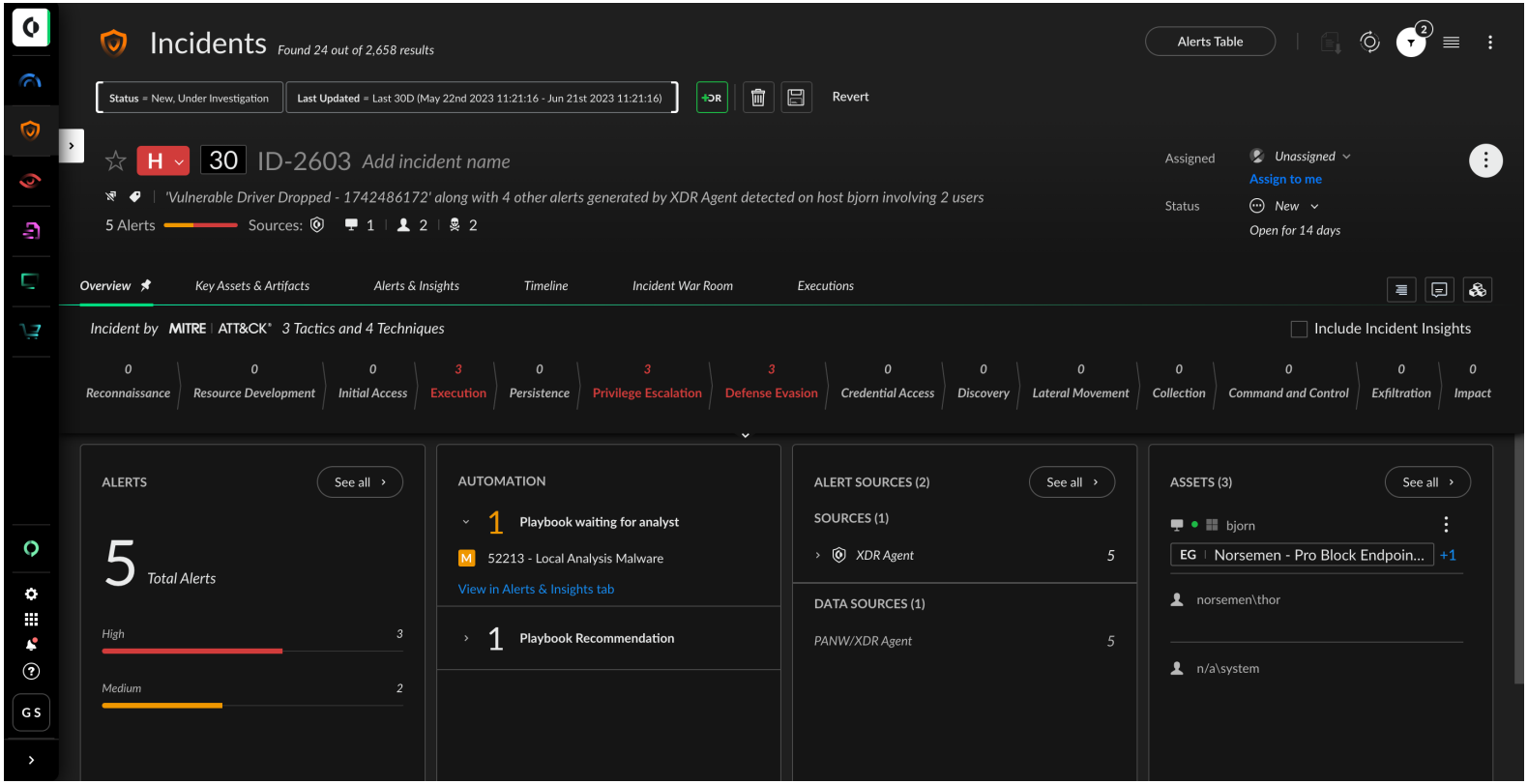


Figure 6. Gain deeper context around incidents with MITRE ATT&CK mapping, associated alerts, playbook status, alert sources, and artifacts

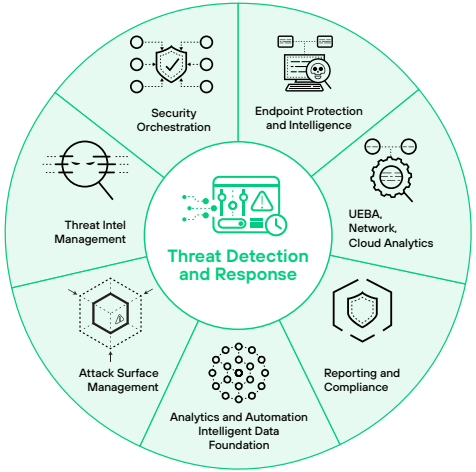
Unique Benefits of Cortex XSIAM

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 experience a similar pain from their existing security architecture and management. XSIAM was built by security practitioners who have lived through these pains. Its development was influenced by our 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 Integrated Capabilities	
Security Information and Event Management (SIEM) Includes all common SIEM functions, including log management, correlation and alerting, and compliance reporting.	**Endpoint Detection and Response (EDR)** Includes a complete endpoint agent and cloud analytics backend to provide endpoint threat prevention, automated response, and in-depth telemetry useful for any threat investigation.
Extended Detection and Response (XDR) Integrates endpoint, cloud, network, and third-party telemetry for automated detection and response.	**Security Orchestration, Automation, and Response (SOAR)** Includes a robust SOAR module and marketplace to create and orchestrate playbooks for use with XSIAM.
Cloud Detection and Response (CDR) The XSIAM analytics array includes specialty analytics designed to detect and alert on anomalies in cloud data such as cloud service provider logs and cloud security product alerts.	**Cortex Exposure Management*** Cuts vulnerability noise by up to 99% with AI-driven prioritization and automated remediation spanning the entire enterprise.
Identity Threat Detection and Response (ITDR)* Includes specialized identity analytics that 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.	**Cortex Advanced Email Security*** Stop sophisticated email-based attacks missed by other solutions with advanced AI and automation.
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.	**Attack Surface Management (ASM)*** Includes embedded ASM capabilities that provide a holistic view of the asset inventory, including internal endpoints and vulnerability alerting for discovered internet-facing assets.
Threat Intelligence Platform (TIP)* Provides full TIP capabilities to manage Palo Alto Networks and third-party feeds, and to automatically map them to alerts and incidents.	

* Available through additional licensing and modules.

CBTS resolves incidents in seconds with platformization, featuring Cortex XSIAM

Determined to strengthen security, reduce complexity and inefficiency, boost visibility, and embrace automation, CBTS turned to Cortex XSIAM.

> We needed a cohesive, supported platform—essentially one place, one screen, one data source—and we needed an opportunity to truly automate within that platform.
>
> **— Chris DeBrunner, Vice President of Security Operations, CBTS**

Customer Needs

- Minimize customer data exposure risk.
- Consolidate disparate security solutions to increase effectiveness and automation.

Solution

- Cortex XSIAM

Outcomes

- Cortex XSIAM dramatically improved efficiency, reducing incident resolution time from days to just 13 seconds.
- Automation capabilities from over 108 playbooks eliminated manual alert handling, allowing the security team to maintain headcount while focusing on strategic initiatives.
- A unified SOC platform now provides a single source of truth through stitched and normalized data.

Bridging Proactive and Reactive Security with Cortex XSIAM 3.0

The latest evolution of XSIAM takes a revolutionary step forward by unifying reactive incident response with proactive security posture management. Cortex XSIAM 3.0 expands its capabilities to address two of the most critical risk areas impacting enterprises today.

Cortex Exposure Management

Cut vulnerability noise by up to 99% with AI-driven prioritization and automated remediation spanning enterprise and cloud. This disruptive approach to vulnerability management focuses on the vulnerabilities with active weaponized exploits and no compensating controls, allowing you to prioritize the threats that matter.

With Cortex Exposure Management, you can:

- Reduce noise across the enterprise and cloud by 99% by prioritizing vulnerabilities with weaponized exploits and no compensating controls.
- Accelerate remediation with industry-leading automation through AI-powered plain language summaries and native playbook automation.
- Close the loop to prevent future attacks by seamlessly creating new protections for critical risks directly in our industry-leading security platforms.

Cortex Email Security

Stop advanced phishing attempts and email-based threats with large language model (LLM)-driven analytics merged with industry-leading detection and response. With email remaining a primary communication tool—projected to reach 5 billion users by 2030[4]—and accounting for a quarter of all security incidents, this capability provides:

- Identity attacker-behavior detection and advanced phishing protection with LLM-powered analytics that continuously learn from emerging threats.
- Automatic removal of malicious emails, disabling of compromised accounts, and isolation of affected endpoints in real time.
- Correlation of email, identity, endpoint, and cloud data for unparalleled visibility into the full attack path for effective incident response.

We've brought these capabilities into the same unified data, AI, and automation platform that has successfully protected hundreds of the most demanding SOC environments globally. In doing so, XSIAM 3.0 combines reactive incident response and proactive cyberdefense, making SecOps capable of handling any current and future threat vectors.

4. *Email Statistics Report 2025-2030*, cloudHQ, April 24, 2025.

Cortex XSIAM Services You Can Count On

Drive Successful XSIAM Outcomes with Global Customer Services

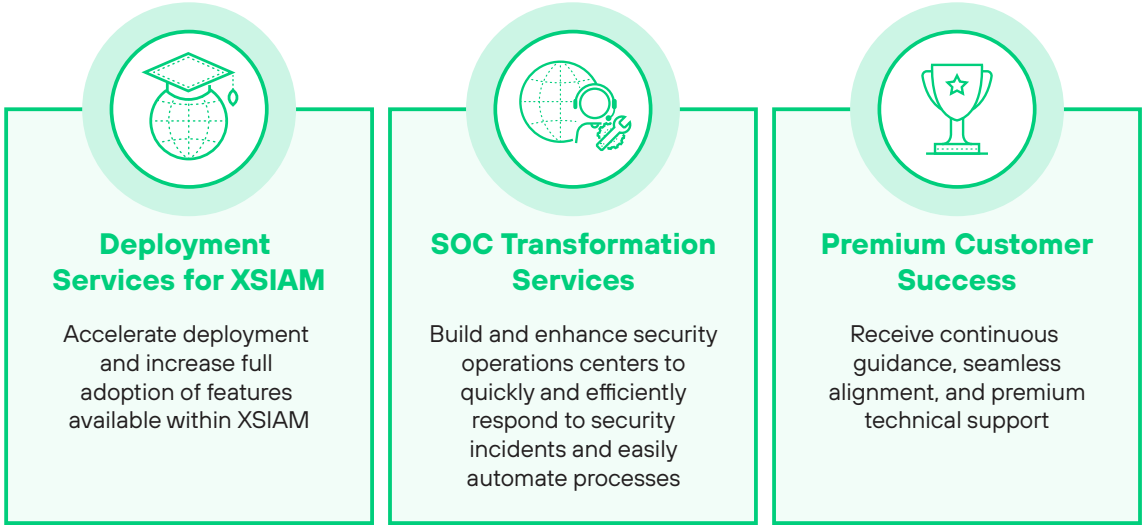


Figure 8. Global Customer Services provides a number of support and service options for XSIAM

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

Deployment Services for Cortex XSIAM

These Deployment Services enable greater adoption of XSIAM features and accelerates time to value. Key benefits include:

- 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 by 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

These Deployment 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 include:

- 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 XSIAM efficiently.
- Build advanced SOC features for threat hunting and intelligence using the Cortex platform.

Premium Customer Success

You get continuous guidance, seamless alignment, and premium technical support.

Key benefits include:

- Access to Customer Success experts who provide strategic guidance throughout the lifetime of your XSIAM investment.
- Tailored strategies to ensure you realize an optimal return on investment.
- 24/7 technical phone support that 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.

Check out our latest XSIAM resources:

- Explore Cortex XSIAM Security Analytics
- What is Cortex XSIAM?
- Request a Cortex XSIAM personal demo
- Watch Cortex XSIAM in action (5-min video)
- Listen on demand to Cortex XSIAM customer success stories

About Palo Alto Networks

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AI-powered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Explore more at www.paloaltonetworks.com.

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

cortex_eb_xsiam_052925