

# Cortex XSIAM

## The AI-Driven Security Operations Platform

The needs of the security operations center (SOC) have changed. It is taking organizations too long to detect security incidents, and when they detect them, too long to remediate. When combined with recent regulatory requirements and threat actors carrying out end-to-end attacks in a matter of hours, this introduces significant risk to organizations.

---

## The Challenge: The Needs of the SOC Have Changed

This core problem is a result of three fundamental challenges that SOCs are facing today.

### 1. Siloed Tools and Data

Organizations often store vast amounts of security and application data that never comes together in a single place, let alone in a normalized manner that makes it usable for threat detection and response. When analysts need to investigate threats, they spend too much time switching between tools to find the information they need. This leads to operational complexity in the SOC.

### 2. Weak Threat Defense

Vast amounts of siloed data combined with heavy detection engineering requirements make it difficult, if not impossible, to identify relationships between security events. Organizations often rely on static correlation rules to identify malicious activity, but this often leads to high false positive rates and missed threats. And since security alerts are disconnected data points in multiple tools, SOCs are forced to manually correlate events. This ultimately results in the inability to stop threats at scale.

### 3. Heavy Reliance on Manual Work

Disjointed data, separate tools, and lack of effective use of AI and automation lead to massive amounts of manual work and redundancy for the SOC. This scale problem means that SOCs cannot possibly respond to all incoming alerts, and they struggle to prioritize which alerts to handle first. This leads to impactful delays in detection and remediation of threats, in addition to analyst burnout and job dissatisfaction.

## The Solution: Rethink and Transform Security Operations

The modern SOC must be built on a new architecture: broad and automated data integration, analysis, and triage; unified workflows that enable analysts to be productive; and embedded intelligence and automated response that can block attacks with minimal analyst assistance. Unlike legacy security operations, the modern SOC leads with AI and automation to process massive datasets, rather than human judgment and rules designed to catch yesterday's threats.

### Simplified Security Operations with a Converged Platform

The convergence of SOC capabilities, such as XDR, CDR, SOAR, ASM, and SIEM, into a single platform—with a single frontend and backend—is a game-changer for security operations. It eliminates the hassle of console switching, providing a streamlined experience. The platform offers broad integration support, making it easier to onboard various data sources without the need for extensive engineering and infrastructure work. This enables SOCs to seamlessly incorporate additional security-related data, enhancing their ability to analyze and detect security threats with greater precision. Moreover, the platform ensures continuous collection, stitching, and normalization of raw data, going beyond just alerts. This empowers SOC teams with superior and simplified investigation, enabling them to identify and remediate threats faster and more effectively.

### AI-Powered Defense to Stop Threats

Out-of-the-box AI models go beyond traditional methods, connecting events across various data sources and offering a comprehensive overview of incidents and risks in a single location. This empowers organizations to enhance their detection, analysis, and response capabilities. XSIAM identifies threats and anomalous activity across data sources, alerting analysts to potential threats for investigation and remediation. XSIAM seamlessly connects low-confidence events, transforming them into high-confidence incidents, enabling security teams to prevent, detect, and respond more efficiently.

## Automated Operations to Accelerate SOC Outcomes

XSIAM uses native automation and built-in integrations for seamless orchestration and execution of tasks such as incident enrichment, threat analysis, and response actions. With hundreds of tried and tested content packs in the Cortex Marketplace, SOCs can optimize processes and interactions across their entire security program. By automating previously manual tasks, embedded automation saves time and effort in responding to incidents or managing risks, such as attack surface exposures. Moreover, users have the flexibility to add, customize, or modify automations according to their specific needs. The platform also features alert-specific playbooks that trigger automatically, ensuring security tasks are executed promptly, and risks are addressed, even before an analyst gets involved. Additionally, XSIAM learns from manual analyst actions and provides recommendations for future automation. This continuous learning process enhances the platform's ability to automatically resolve incidents, improving efficiency and accuracy over time.

## Cortex XSIAM

Cortex XSIAM® is the AI-driven platform that transforms the SOC, harnessing the power of AI and automation to simplify operations, stop threats at scale, and accelerate incident remediation.

Reduce risk and operational complexity by centralizing multiple products into a single, converged platform purpose-built for security operations.

XSIAM unifies best-in-class security operations functions, including SIEM, EDR, XDR, SOAR, CDR, ASM, UEBA, and TIP. XSIAM centralizes all of your security data and uses AI models designed specifically for security. With XSIAM, organizations can automate data integration, analysis, and response actions, enabling analysts to focus on the incidents that matter.

### A new design for security operations that:

- **Redefines** SOC architecture into an automation-first approach
- **Unifies** best-in-class SOC functions to improve analyst experience
- **Consolidates** multiple products into a single platform
- **Extends** the SOC to the cloud for complete visibility
- **Increases** analyst productivity by focusing on the incidents that matter

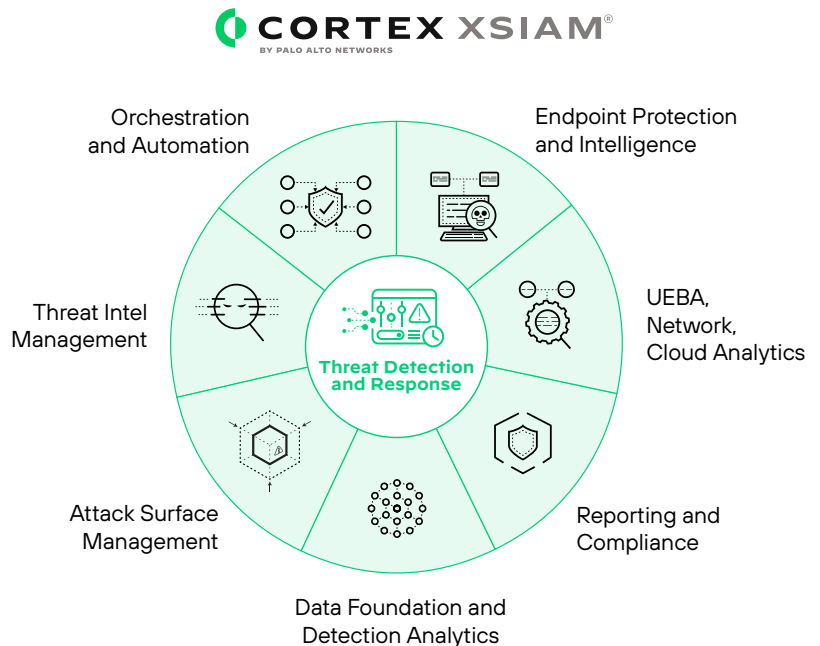


Figure 1: Cortex XSIAM

---

A streamlined data onboarding process lets SecOps teams easily add new data sources while an extended data model normalizes and correlates data for schema on-read data access. Cortex XSIAM also automatically stitches together endpoint, network, cloud, identity, and other data so it can detect advanced threats with precision and simplify investigations with cross-data insights.

Cortex XSIAM lets analysts swiftly investigate incidents by providing a complete picture of every attack with intelligent alert grouping and root cause analysis. Embedded automation enriches alerts, responds to malicious activity, and closes low-risk alerts before they reach the queue—enabling analysts to focus on the few threats that require human intervention. Cortex XSIAM is powering Palo Alto Networks own SOC and turning over a trillion events per month into a handful of analyst incidents per day.

Unlike legacy SOC solutions, where operationalizing and optimizing the product is an exercise left to the customer, Cortex XSIAM benefits from continuous updates from the Palo Alto Networks Unit 42 research team. Palo Alto Networks experts collect threat intel from more than 90,000 customers, update machine learning (ML) detection models, and automatically distribute the latest protections to Cortex XSIAM deployments. Insights from across the threat landscape help safeguard customers from the latest advanced and fast-moving threats. By fusing leading technology with shared intelligence and research, Palo Alto Networks shares the responsibility of protecting our customers' ongoing operations.

## **The AI-Driven Security Operations Platform**











Cortex XSIAM harnesses the power of artificial intelligence (AI) and automation to simplify security operations, stop threats at scale, and accelerate incident remediation.

Applying AI to drive better security outcomes relies on having good data. Cortex XSIAM puts the SOC in full control of enterprise security—from endpoint to cloud—by centralizing, stitching, and optimizing data, specifically for detecting and preventing security incidents.

Cortex XSIAM uses artificial intelligence, which leverages thousands of mature ML data models designed to quickly and accurately identify malicious security events. These models are built based on learned behavior from tens of thousands of environments, which help to differentiate between anomalous vs. malicious activities. This significantly reduces false positives and improves detection and prevention capabilities, stopping attacks before they become security incidents. Cortex XSIAM analytics provide technique-based intelligence, allowing multiple alerts to be stitched and grouped into a smaller number of incidents. These incidents are fully enriched with relevant context and are either resolved with automation or presented to an analyst with an appropriate severity classification (critical, high, low, etc.) that is defined leveraging an AI SmartScoring system.

# Key Integrated Capabilities

Cortex XSIAM combines these key SOC product capabilities into a single unified platform.

 <p><b>Security Information and Event Management (SIEM)</b> Includes log management, correlation and alerting, compliance reporting,* and other common SIEM functions.</p>	 <p><b>Threat Intelligence Platform (TIP)*</b> Provides full TIP capabilities to manage Palo Alto Networks and third-party feeds, and to automatically map them to alerts and incidents.</p>	 <p><b>Extended Detection and Response (XDR)</b> Integrates endpoint, cloud, network, and third-party telemetry for automated detection and response.</p>	 <p><b>Endpoint Detection and Response (EDR)</b> 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.</p>	 <p><b>Attack Surface Management (ASM)*</b> Includes embedded ASM capabilities that provide a holistic view of the asset inventory, including internal endpoints and vulnerability alerting for discovered internet-facing assets.</p>
 <p><b>Identity Threat Detection and Response (ITDR)*</b> Combine UEBA capabilities with enhanced identity threat modules to effectively detect, prevent, and respond to threats like insider threats, data exfiltration, suspicious lateral movement, and more.</p>	 <p><b>User and Entity Behavior Analytics (UEBA)</b> Uses machine learning and behavioral analysis to profile users and entities and alert on behaviors that may indicate a compromised account or malicious insider.</p>	 <p><b>Security Orchestration, Automation, and Response (SOAR)</b> Includes a robust SOAR module and marketplace to create and orchestrate playbooks for use with Cortex XSIAM.</p>	 <p><b>Cloud Detection and Response (CDR)</b> The Cortex 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.</p>	 <p><b>Management, Reporting, and Compliance</b> Centralized management functions simplify operations. Powerful graphical reporting capabilities support reporting for compliance, data ingestion, incident trends, SOC performance metrics, and more.</p>

\* Available through additional licensing and modules.

## Cortex XSIAM Delivers Real Outcomes

While Cortex XSIAM is delivering exponential improvements in the Palo Alto Networks SOC, our primary objective is to innovate to outpace cyberthreats so customers can embrace and deploy our technology with confidence. Recent customer success metrics provide evidence that Cortex XSIAM is doing just that.

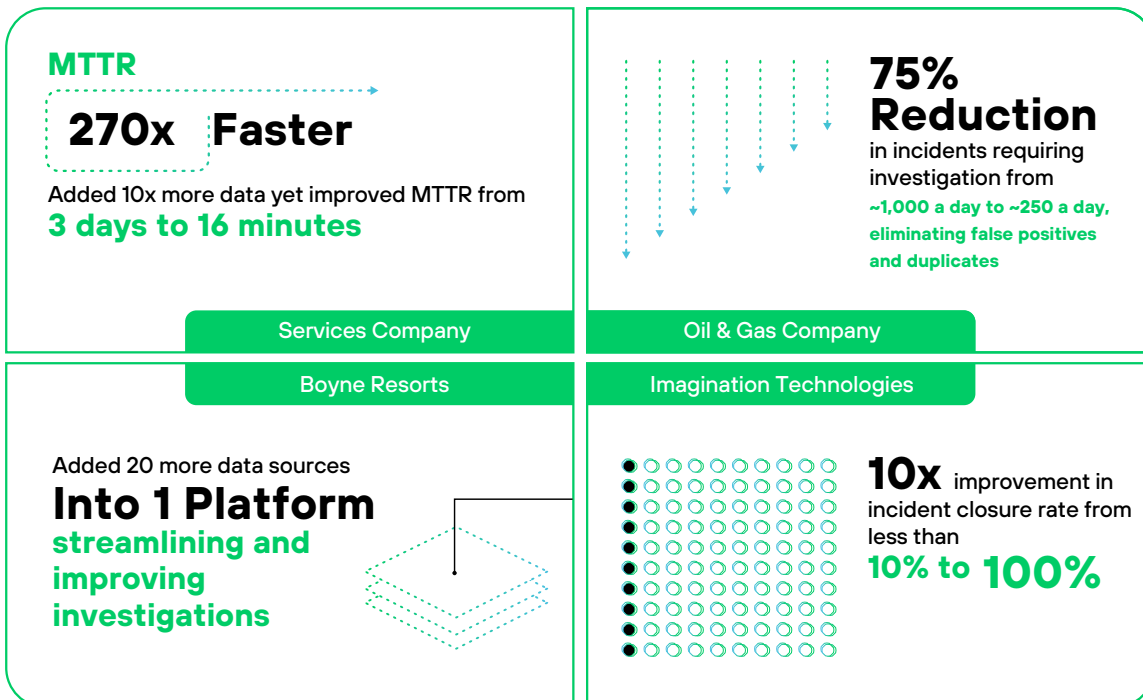


Figure 2: Cortex XSIAM customers have improved SOC efficiency while increasing overall visibility

Benefits of Cortex XSIAM:

- Improves detection and prevention capabilities, **stopping attacks before they become incidents**
- Enables SOCs to ingest more data sources, while still **improving response times from days to minutes**
- **Improves incident closure rates and minimizes the number of incidents** requiring manual investigation and remediation
- Simplifies data onboarding and **reduces infrastructure complexities**
- Provides security practitioners with the knowledge and capabilities they need to **shift from reactive to proactive security**

## Enlist Experts for Managed Services

The Unit 42® team applies years of experience protecting businesses and governments around the globe to monitor your environment 24/7 and hunt for suspicious activity. Armed with industry-leading threat intelligence from over 10 years of malware analysis, augmented every day by over 30 million new malware samples and 500 billion events, our Unit 42 experts ensure you stay ahead of emerging threats. Unit 42 Managed Detection and Response (MDR) and Managed Threat Hunting (MTH) services can be easily added to your Cortex XSIAM subscription.

### Unit 42 Managed Detection and Response

The Palo Alto Networks Unit 42 Managed Detection and Response ([Unit 42 MDR](#)) service provides a team of world-class analysts, threat hunters, and researchers who work for you to investigate and respond to attacks, allowing your team to scale fast and focus on more strategic tasks. Unit 42 MDR includes Managed Threat Hunting.

### Unit 42 Managed Threat Hunting

The Palo Alto Networks Unit 42 Managed Threat Hunting ([Unit 42 MTH](#)) service provides a team of world-class analysts, hunters, and researchers who will proactively hunt for advanced threats and provide detailed reporting, giving you peace of mind.

## Resources

- [Cortex XSIAM e-book](#)
- [Cortex XSIAM Help Center](#)
- [Customer Story: Imagination Technologies transforms SOC operations with Cortex XSIAM](#)
- [Customer Story: Oil and gas company deploys AI-driven SOC with Cortex XSIAM](#)



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](http://www.paloaltonetworks.com)

© 2024 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

cortex\_ds\_cortex-xsiam\_090324