Cortex XSIAM
At a Glance

The AI-Driven Security Operations Platform

The needs of the 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 modern SOC must be built on a new architecture:

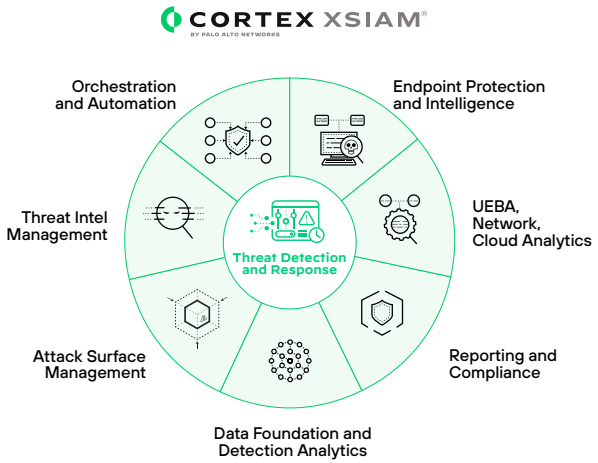
- Broad and automated data integration, analysis, and triage
- Unified workflows that enable analysts to be productive
- Embedded intelligence and automated response that can block attacks with minimal analyst assistance

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

Cortex XSIAM® (extended security intelligence and automation management) unifies best-in-class functions, including endpoint detection and response (EDR); extended detection and response (XDR); security orchestration, automation, and response (SOAR); attack surface management (ASM); user and entity behavior analytics (UEBA); threat intelligence platform (TIP); and security information and event management (SIEM). Using a security-specific data model and applying machine learning, XSIAM automates data integration, analysis, and triage to respond to most alerts. This enables you to focus on the incidents that require human intervention.

The data model is 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, aggregate alerts into incidents for automated analysis and triage, and respond to most incidents automatically.

XSIAM is already proven in production, powering Palo Alto Networks own SOC and turning over a trillion events per month into a handful of analyst incidents per day.



XSIAM Delivers Integrated Capabilities

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

SIEM* Includes all common SIEM functions, including log management, correlation and alerting, and compliance reporting.*	**TIP*** Provides full TIP capabilities to manage Palo Alto Networks and third-party feeds, and to automatically map them to alerts and incidents.
XDR Integrates endpoint, cloud, and network telemetry for automated 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.
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.	**UEBA** 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.
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.
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.	

* Available through additional licensing and modules.

Visit the Cortex XSIAM page or connect with your account manager today to set up a demo and see XSIAM in action.