Cortex XSIAM

The Autonomous Platform Powering the Modern SOC

Cortex XSIAM harnesses the power of machine intelligence and automation to radically improve security outcomes and transform the manual SecOps model. From enterprise to cloud, XSIAM centralizes, automates, and scales security operations to protect organizations from advanced attacks.

Be a Defender, Not Just a Detective

Cyberattacks continue to rise, and stopping an attack is as difficult as ever. Every time an attack happens, the target's security team is able to perform forensics quite well. Security quickly figures out what happened, how the attackers got in, which systems were affected, and what data was taken. So, the key question is: if the organization has the information needed to solve the puzzle after the fact, why couldn't it prevent the attack in the first place?

The answer is the difference between data analysis and data analytics. Security organizations have too much information to manage in too many silos. This data can be pulled together after the fact for data analysis to determine what happened. But that siloed data doesn't work as well for data analytics and being able to anticipate and prepare for the future. It's not the security operations center (SOC) team's fault. Most SOCs are built for a different era.

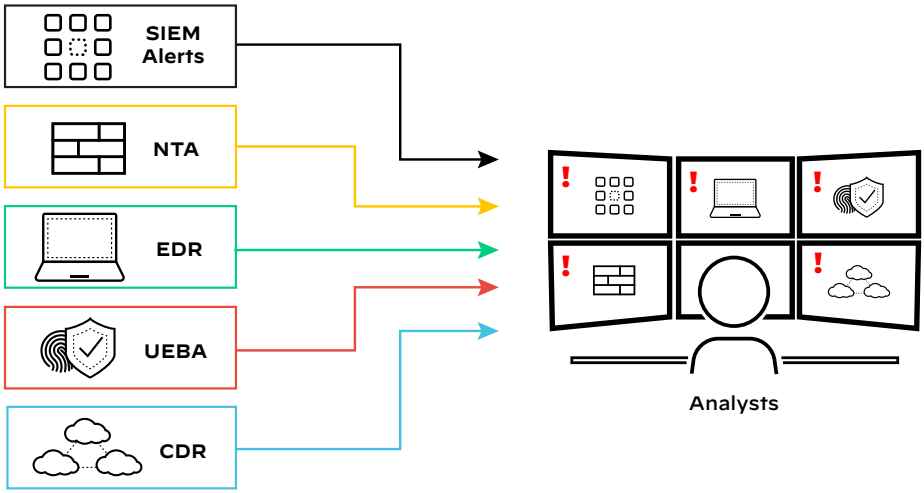
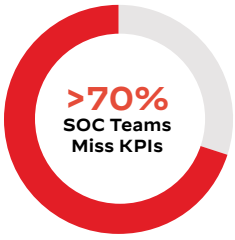


Figure 1: Siloed security operations

Today's expanded enterprise attack surface generates much more security data, that is both more complex and siloed, than only a few years ago. Network, endpoint, identity, and cloud data remain in separate systems. Endpoint telemetry is locked in an endpoint detection and response (EDR) system, cloud data is in a separate cloud security tool, and more—with only a subset of logs but a flood of alerts going to the SIEM. As a result, SOC analysts must manually analyze data to triage alerts and take effective action. Alerts overload analysts, so threats are missed, and dwell times remain long. At the same time, security engineers struggle to integrate new data streams and create new detection rules and playbooks, while security architects integrate the latest new point product. The results are predictable: alert fatigue, slow investigations, and attackers who hide in networks for months.



~11K
Alerts per day

4+
Days to investigate

212
Days of dwell time

SOCs Need to Evolve Beyond SIEM

In short, the needs of the SOC have changed, but the design of the SIEM and SOC have not. Most other key pieces of the security architecture have been modernized. The endpoint moved from antivirus to EDR and to 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.

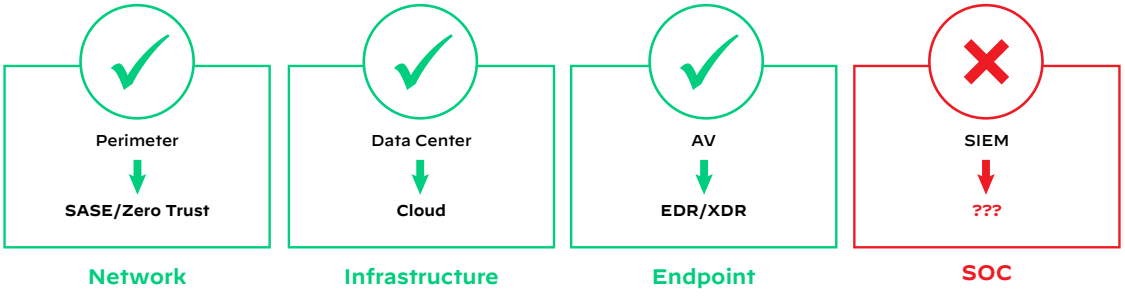


Figure 2: The evolution of IT and security

Transforming the Manual SOC Model

That model, whether delivered as on-premises software or forklifted to the cloud, was built around the human analyst. SOC analysts pored through hundreds of alerts per day, triaged manually by collecting contextual data, and spent the bulk of their time on false positives and manual effort. As alert volumes grew and data became harder to integrate from more systems, the human-led approach broke down.

Instead, the modern way to scale an effective SOC is with automation as the foundation and with analysts working on a small set of high-risk incidents. Just as flying a commercial airplane no longer requires constant, hands-on control by the pilot, an automation-led SOC handles the bulk of low-risk, repeated alerts, analysis tasks, and mitigations. This frees the analysts to work on urgent, high-impact incidents while the underlying platform autopilots the SOC to safe outcomes, learning from each activity and offering information and effective recommendations to the captain at the wheel. This is our vision for the autonomous SOC.

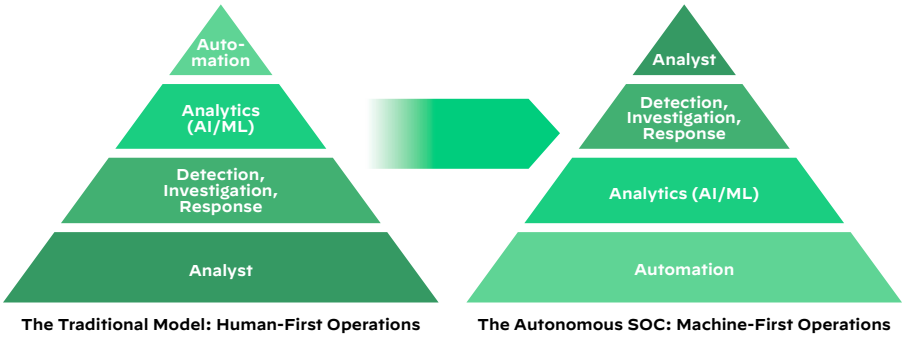


Figure 3: Machine-driven security operations

Ultimately, better data modeling and integration combined with automated analytics and detection, ease the burden on security engineers, who no longer need to build custom correlation rules to integrate data and detect threats. Unlike legacy security operations, the modern SOC leads with data science applied to massive data sets rather than human judgment and rules designed to catch yesterday's threats.

The modern SOC must be built on a new architecture with:

- 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

The Solution: Cortex XSIAM —Transform the SOC by Rethinking the SIEM

Cortex XSIAM, or extended security intelligence and automation management, is a cloud-delivered, integrated SOC platform that unifies key functions, including EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM. XSIAM customers can consolidate multiple products into a single, integrated platform, cutting costs, improving operations, and increasing analyst productivity. XSIAM delivers an intelligent data foundation that can easily integrate telemetry from any source, providing unified security operations across any hybrid IT architecture.

CORTEX XSIAM
BY PALO ALTO NETWORKS

- **Architects** data strategy using stitching to improve analytics outcomes as opposed to traditional human approaches
- **Unifies** best-in-class SOC functions to improve analyst experience (AX)
- **Consolidates** multiple capabilities into a single platform to alleviate integration pain and reduce vendor management
- **Enhances** the SOC by rethinking telemetry sources to include information **about** the environment itself as opposed to just information **from** the environment
- **Extends** the SOC to cloud operations for full visibility

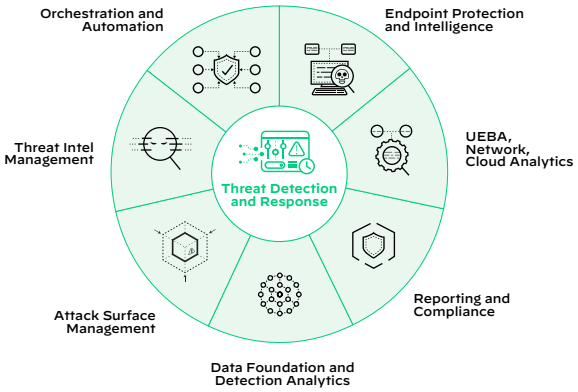


Figure 4: Cortex XSIAM

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, and identity 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, including intelligent alert grouping and collected information about the root cause. Embedded automation can enrich alerts, respond to malicious activity, and close low-risk alerts before they reach the queue—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 reducing over one 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, XSIAM benefits from continuous updates from Palo Alto Networks Unit 42 research team. Palo Alto Networks experts collect threat intel from more than 85,000 customers, update machine learning (ML) detection models, and automatically distribute the latest protections to XSIAM deployments to safeguard customers from 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.

Key Integrated Capabilities

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

Security Information and Event Management (SIEM) Delivers all common SIEM functions, including log management, correlation and alerting, reporting, and long-term data retention.	**Threat Intelligence Platform (TIP)** Aggregates, scores, and distributes threat intelligence data, including the industry-leading Unit 42 threat feed, to third-party tools and enriches alerts for context and attribution.
Extended Detection and Response (XDR) Gathers telemetry from any source for unrivaled detection coverage and accuracy, with the highest number of technique-level detections in the 2022 MITRE ATT&CK evaluations.	**Endpoint Protection Platform (EPP)** Prevents endpoint attacks with a proven endpoint agent that blocks exploits, malware, and fileless attacks and collects full telemetry for detection and response.
Attack Surface Management (ASM) Provides embedded attack surface management (ASM) capabilities for an attacker's view of your organization, with asset discovery, vulnerability assessment, and risk management.	**User and Entity Behavior Analytics (UEBA)** Uses machine learning and behavioral analysis to profile users and entities and alert on behaviors that may indicate a compromised account or malicious insider.
Security Orchestration, Automation, and Response (SOAR) Automates nearly any use case with hundreds of built-in playbooks and offers customization with a visual drag-and-drop playbook editor.	**Cloud Detection and Response (CDR)** Analyzes cloud audit, flow, and container host logs together with data from other sources for holistic detection and response across your hybrid enterprise.
Management, Reporting, and Compliance Simplifies operations, centralizing all configuration, monitoring, and reporting functions, including endpoint policy management, orchestration, and response.	

Cortex XSIAM Customer Outcomes

Improve analyst experience and increase productivity by eliminating security silos	The typical SOC relies on a mix of screens from multiple products. In contrast, XSIAM delivers all functionality in the same console with the same workflows, operating on fully-integrated data.
Uncover advanced attacks with behavioral analytics and industry-leading threat intelligence	Palo Alto Networks experts collect indicators across customers, process, and update models to ensure up-to-date protection.
Easily onboard new data sources	Unlike existing SIEMs, adding a new data source to XSIAM is fast and easy. Onboarding takes only a few clicks, and the new data is automatically integrated into the XSIAM data model, into models and correlations, and into playbooks and dashboards. The result is an ever-growing foundation for machine learning and analytics.
Connect tools and orchestrate response with 600+ product integrations	The Cortex Marketplace includes hundreds of SOAR playbook integrations and automation packs for XSIAM that can be deployed out of the box.
Speed up investigations with intelligent alert grouping and SmartScore	XSIAM automatically groups multiple alerts into a single incident, automating the scoping process and cutting investigation time. SmartScore incident scoring uses machine learning to identify high-risk incidents, helping analysts focus on the threats that matter most.
Lower risk with attack surface management and internal asset discovery	XSIAM displays all known data about a given internal or internet-facing asset using various data sources, including Cortex agents, network traffic, attack surface analysis, Active Directory, and more. Embedded attack surface discovery and response proactively identifies and shuts down new vulnerabilities, while integrating vulnerability data into incidents and analytics.
Take the guesswork out of response with remediation suggestions	XSIAM will automatically suggest response actions to the analyst based on the information in a given incident.
Extend detection, monitoring, and investigation to the cloud	For many organizations, new cloud systems are not integrated into their SOC. XSIAM is designed to analyze multicloud data and operations, ensuring true enterprise-wide visibility and security operations.

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