Cortex XSIAM

The AI-Driven Security Operations Platform

Cortex® XSIAM™ (extended security intelligence and automation management) is the AI-driven security operations platform for the modern security operations center (SOC), harnessing the power of artificial intelligence and automation to radically improve security outcomes and transform security operations. Reduce risk and operational complexity by converging multiple products into a single platform purpose-built for security operations.

The Needs of the SOC Have Changed

The requirements of the SOC have evolved. Organizations are facing extended detection and remediation times for security incidents. When combined with recent regulatory breach notification mandates and the rapid execution of end-to-end attacks by threat actors within hours, this poses significant risks to organizations.

After every breach, the security team successfully investigates the incident, uncovering the methods of compromise, affected systems, and stolen data. The question arises: If you possess the information to understand post-incident details, why not take proactive measures to prevent or halt such incidents before they occur?

The answer to this question lies in the three primary challenges that SOCs face today:

1. Siloed Tools and Data

Too many tools to complete a job are not always helpful. Disparate cybersecurity tools lead to inefficient workflows—switching between multiple products and multiple consoles—resulting in increased cognitive load and potential oversight of threats. Lack of integration also hampers real-time threat detection and delays incident response, while maintaining multiple tools is resource-intensive and can add operational complexity. Most organizations have vast amounts of security and application data but there's too much of it and it exists in different places. Network data is stored in the firewall, endpoint data lives in endpoint detection and response (EDR), authentication data exists in a separate log, and other key information might never leave application-specific logs. Worse, about half of the organizations we speak to say they have not connected their cloud operations to the SOC—so everything remains a disconnected datapoint.

2. Weak Threat Defense

Relying solely on static correlation rules and extensive detection engineering, exacerbated by the sheer volume of data, poses significant challenges in identifying meaningful relationships between security events across the environment. In this scenario, alerts appear as disconnected data points, necessitating manual correlation efforts by the SOC team. Unfortunately, this approach often leads to inaccurate detections, characterized by high false positive rates. The disjointed nature of the process hampers the effectiveness of the security infrastructure, highlighting the need for more advanced and adaptive threat detection methodologies to mitigate false positives and enhance the overall security posture.

3. Heavy Reliance on Manual Work

Vast amounts of disconnected data and disparate tools result in an overwhelming number of alerts for SOCs to investigate and resolve. When handling these alerts, SOC analysts struggle to prioritize which alerts to handle first and often need to manually correlate events across various data sources and tools to figure out what they're dealing with. Oftentimes, they may be investigating several different alerts, without knowledge that the alerts are connected to a single incident. This results in redundancy and manual work that extends the mean time to detect and remediate security incidents.

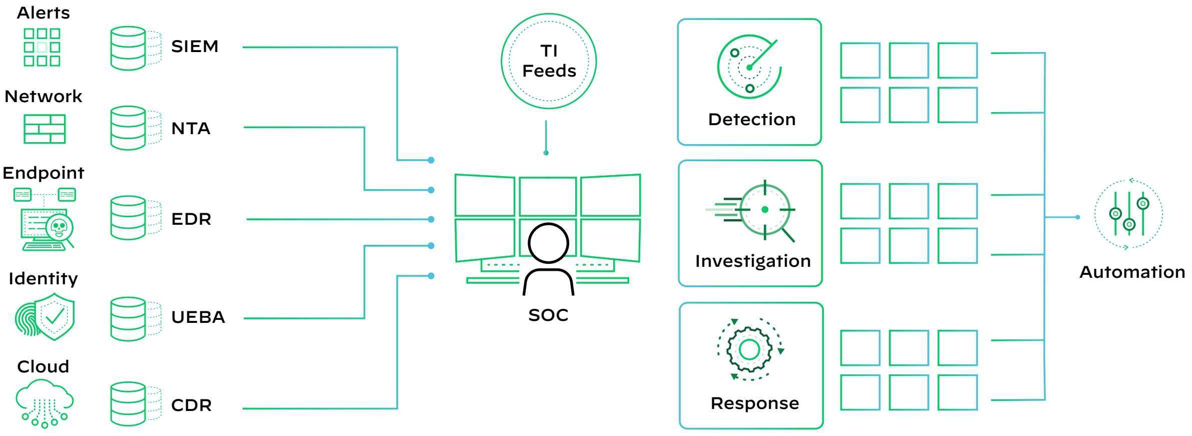


Figure 1: Siloed security operations

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. That's why a converged platform is essential to streamline processes and enhance efficiency. Simplifying operational complexity is crucial in today's fast-paced digital landscape. By integrating various systems and tools into one centralized solution, businesses can eliminate silos and achieve a unified view of their operations.

Additionally, stopping threats at scale is a top priority for organizations. With AI-driven outcomes, businesses can proactively detect and mitigate potential risks, ensuring the security of their data and systems.

Furthermore, an automation-first approach expedites incident remediation, reducing manual efforts and response times. By leveraging automation, businesses can quickly resolve issues, minimize downtime, and optimize their overall operational performance.

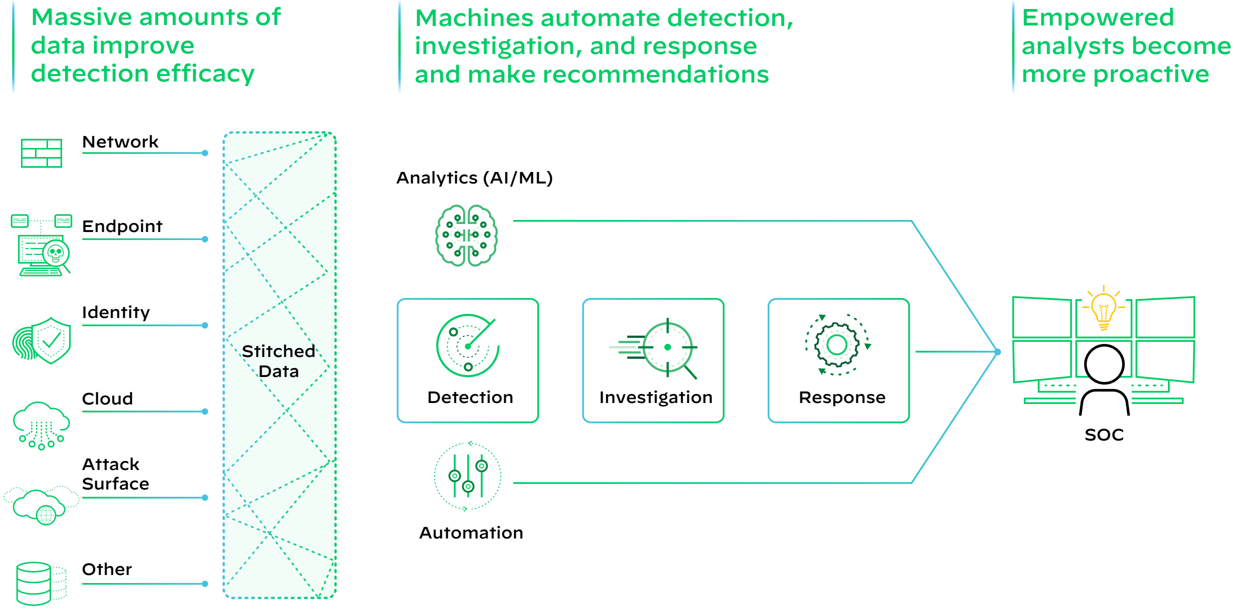

Massive amounts of data improve detection efficacy
Machines automate detection, investigation, and response and make recommendations
Empowered analysts become more proactive
Network
Endpoint
Identity
Cloud
Attack Surface
Other
Stitched Data
Analytics (AI/ML)
Detection
Investigation
Response
Automation
SOC

Figure 2: A transformed SOC

Cortex XSIAM

Cortex® XSIAM™ is the AI-driven security operations platform for the modern SOC, harnessing the power of artificial intelligence and automation to to simplify security operations, stop threats at scale, and accelerate incident remediation. Reduce risk and operational complexity by converging multiple products into a single, coherent platform purpose-built for security operations.

Cortex XSIAM was built to address the unique challenges that SOCs face today and into the future. By consolidating data and tools into a single AI-driven platform, SOCs can simplify security operations, stop threats at scale, and significantly accelerate security outcomes.

Built with three goals in mind, Cortex XSIAM makes the unsolvable solvable in the SOC:

1. Simplify Security Operations with a Converged Platform

The convergence of SOC capabilities, such as XDR, SOAR, ASM, and SIEM, into a single platform 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 allows SOCs to effortlessly ingest more security-relevant data, enhancing their analytical capabilities. 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.

2. Stop Threats at Scale with AI-Driven Outcomes

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. By leveraging alert grouping and AI-driven incident scoring, Cortex XSIAM seamlessly connects low confidence events, transforming them into high confidence incidents. This prioritization is based on the overall risk, enabling security teams to focus their efforts efficiently.

3. Accelerate Incident Remediation with an Automation-First Approach

With hundreds of tried and tested content packs in the Cortex Marketplace, SOCs can optimize processes and interaction 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 automations. This continuous learning process enhances the platform's ability to automatically resolve incidents, improving efficiency and accuracy over time.

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

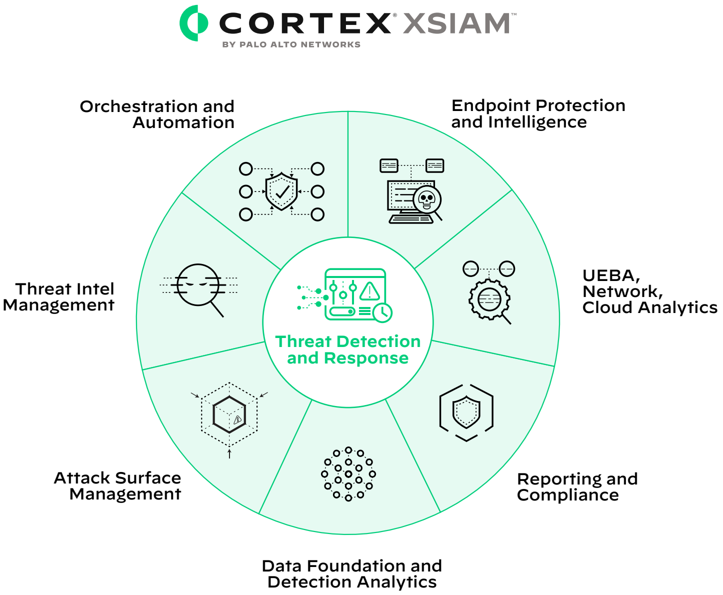

CORTEX XSIAM
BY PALO ALTO NETWORKS
Orchestration and Automation
Endpoint Protection and Intelligence
Threat Intel Management
Threat Detection and Response
UEBA, Network, Cloud Analytics
Attack Surface Management
Reporting and Compliance
Data Foundation and Detection Analytics

Figure 3: Cortex XSIAM

Key Integrated Capabilities

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

Security Information and Event Management (SIEM)

Includes log management, correlation and alerting, compliance reporting,* and other common SIEM functions.

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.

Extended Detection and Response (XDR)

Integrates endpoint, cloud, network, and third-party telemetry for automated detection and response.

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.

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.

Identity Threat Detection and Response (ITDR)*

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.

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)

Includes a robust SOAR module and marketplace to create and orchestrate playbooks for use with Cortex XSIAM.

Cloud Detection and Response (CDR)

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.

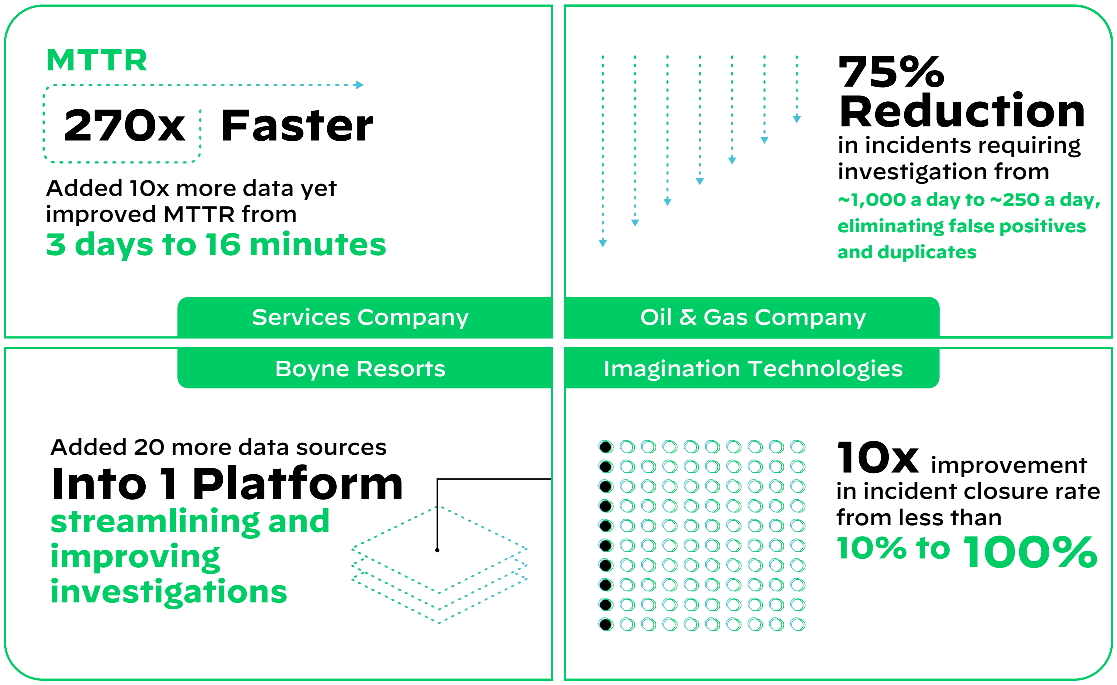
Management, Reporting, and Compliance

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.

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.



MTTR

270x Faster

Added 10x more data yet improved MTTR from **3 days to 16 minutes**

Services Company

75% Reduction

in incidents requiring investigation from **~1,000 a day to ~250 a day, eliminating false positives and duplicates**

Oil & Gas Company

Boyne Resorts

Added 20 more data sources

Into 1 Platform

streamlining and improving investigations

Imagination Technologies

10x improvement in incident closure rate from less than **10% to 100%**

Figure 4: 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.

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