paloalto | CORTEX

THE CORTEX PLATFORM

A Force Multiplier for Your SOC

Reimagine your approach to security where your data makes the difference. Stay one step ahead with a machine-led, human-empowered platform that utilizes advanced analytics to give you the upper hand.

Cortex XDR: Extended Detection and Response

Cortex XDR stops attacks at the endpoint and host with world-class EDR, providing detection and response that focus on incidents by automating evidence gathering and associated groups of alerts. Those alerts are put into a timeline, revealing the root cause to speed triage and investigations for analysts of **all** skill levels.

Advanced Threat Prevention, Detection and Response

Cortex XDR

- Endpoint Analytics
- Network Analytics
- Cloud Analytics
- Identity Analytics
- Global Analytics

All Data Stitched and Normalized

- Endpoints
- Network
- Cloud
- Identity
- Additional Sources

Data Sources

Takeaway: Cortex XDR is a viable alternative approach to SIEM solutions by providing threat detection, investigation, response, and hunting rooted in endpoint threat detection and response with the ability to scale to cloud environments which is where enterprise data is moving.

Cortex Xpanse: Active Attack Surface Management

Xpanse is an active attack surface management solution that helps your organization actively discover, learn about and respond to unknown risks in all connected systems and exposed services.

Active Discovery

Automated continuous scans to index the entire internet and actively discover your unknown risks in all connected systems and exposed services.

Active Learning

Use supervised machine learning models to continuously map your attack surface and prioritize remediation efforts without additional analysts.

Active Response

Immediately reduce your attack surface risks with built-in automated playbooks instead of merely raising IT tickets.

How ASM Benefits the Broader Security Team

- Threat hunters gain historical records for retrospective investigations
- NetSec teams have visibility into all internet assets to find anomalous/suspicious network behavior
- Vulnerability managers and security analysts can bolster the effectiveness of their tools and technologies with a complete asset inventory
- Executives and board members get cyber risk reports that align with business processes and initiatives
- Pentesters can use ASM in the reconnaissance phase
- IT operations gain a clear list of high priorities

Remote Work and the Move to the Cloud Have Scattered Your IT Infrastructure

- Development Infrastructure
- Remote Access Services
- File-Sharing Systems
- Networking & Security Systems
- Database Storage & Analysis Systems
- Building Control Systems
- Web Frameworks
- M&A IT Infrastructure

While Attackers Use Automation to Quickly Find and Exploit Them

Organizations average a new serious public exposure **every 12 hours**

In 2022, attackers started scanning for vulnerabilities **within minutes** of newly published remote code execution exploits

On average, Xpanse prospects did not know about **30-40%** of their publicly accessible attack surfaces

Takeaway: Attackers scan for exposures within minutes of a new CVE but defenders are responding in weeks on account of a lack of visibility and backlogged repairs. Active Attack Surface Management helps defenders fight back!

Cortex XSOAR: Security Orchestration, Automation, and Response

Cortex XSOAR unlocks security operations efficiency with a comprehensive SOAR solution for managing incident response. SecOps teams of all sizes can use XSOAR to automate response workflows, collaborate in real-time investigations, and manage their threat feeds.

Automate

Automate repetitive tasks and dedup alerts to reduce incidents requiring human touch by up to 95%. 900+ out-of-the-box integrations and playbooks ease deployment.

Investigate

Single place for incidents, IoCs, and threat intel for lightning-quick search and query. Virtual war rooms for multiteam investigations. Manage and act on your threat intel feeds.

Respond

Speed up MTTR. Reduce up to 90% of manual steps, automate data enrichment, auto-distribute indicators to enforcement points, and automate response actions.

Cortex XSOAR

- 900+ integrations & playbooks
- SIEM
- Tools
- People
- STIX TAXII API
- Playbook-Driven Automation
- Marketplace
- Cortex XSOAR Ecosystem
- Community
- Automation & Orchestration
- Real-Time Collaboration
- Case Management
- Threat Intel Management
- Alerts
- Threat Intel Feeds
- SIEM
- Cortex XDR
- Cortex Xpanse
- Illusive NGFW
- IoT
- Prisma
- Mail
- Other Sources
- ISAC
- Open Source
- Premium
- Unit 42

Takeaway: At the heart of any SOAR solution is the ability to set priorities and build streamlined workflows for security teams that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes, as well as provide a single platform for minimizing complex incident investigations.

Our Approach: Comprehensive End-to-End Security

Cortex XDR

Detect and investigate threats in real time

Cortex XSOAR

Automate attack response actions

Cortex Xpanse

Shift from a reactive to a proactive stance

NEW RULES CALL FOR NEW TOOLS

Cortex XSIAM: Extended Security Intelligence and Automation Management

XSIAM is designed to be the center of SOC activity, augmenting SIEM and specialty products by unifying broad functionality into a holistic solution. XSIAM capabilities include data normalization, intelligent stitching, analytics-based detection, incident management, threat intelligence, automation, attack surface management, and more—all delivered within an intuitive, automation-first user experience.

Intelligent Data Foundation

Accelerate Response

Outpace Threats

Natively Integrates XDR, SOAR, Threat Intel, ASM, and SIEM Capabilities to Power the Autonomous SOC

Cortex Portfolio

- Orchestration & Automation
- Endpoint Protection & Intelligence
- Threat Intel Management
- UEBA, Network & Cloud Analytics
- Threat Detection & Response
- Attack Surface Management
- Reporting & Compliance
- Data Foundation & Detection Analytics

Takeaway: Cortex XSIAM is the automation-first platform for the modern SOC, harnessing the power of machine intelligence to radically improve security outcomes and transform security operations. XSIAM customers can consolidate multiple products into a single coherent platform, cutting costs and improving analyst experience and productivity.

BETTER TOGETHER

With end-to-end native integration and interoperability, SOC teams can close the loop on threats with continual synergies across the Cortex ecosystem. These products work in concert to monitor the threat landscape and provide the most robust detection, response, and investigation capabilities.

Get started today on your SOC transformation journey

paloalto | © 2023 PALO ALTO NETWORKS | 3000 Tannery Way Santa Clara, CA 95054 Support: +1.866.898.9087 www.paloaltonetworks.com