Cortex—a Holistic Ecosystem for Proactive Security Operations

Security operations centers (SOCs) have been around for approximately 15 years, yet operate with technology that hasn't helped them advance past their fundamental challenges, such as alert overload, lack of context, manual processes, and limited visibility. With a need to prevent cyberattacks and the adoption of centralized security operations (SecOps), security teams are challenged by a lack of qualified personnel (staff, skills, knowledge), budgetary constraints, and a barrage of complex solutions on the market.

Attacks are becoming more frequent, sophisticated, and costly, driven by the surge in ransomware.[1] Attackers are using automation to uncover vulnerabilities faster. In 2021, attackers started scanning for newly disclosed vulnerabilities within minutes.[2] Unfortunately, attacks can go undetected for too long, leading to increased dwell times and delayed investigation, mitigation, or remediation. While reasons for operational inefficiencies differ among organizations, common issues include:

- Limited visibility into their devices, applications, networks, and systems
- Not knowing which assets to protect
- Not understanding which tools to use and how to integrate them with the existing infrastructure
- Staff who is overwhelmed with triaging low-fidelity alerts and false positives generated by security controls

In order to address these challenges, security teams need some help. Palo Alto Networks Cortex solution is a web- and cloud-based platform that enables:

- Tighter control of security operations
- A holistic view of the security posture
- Centralized threat detection, behavioral monitoring, intelligence, asset discovery, and vulnerability assessment

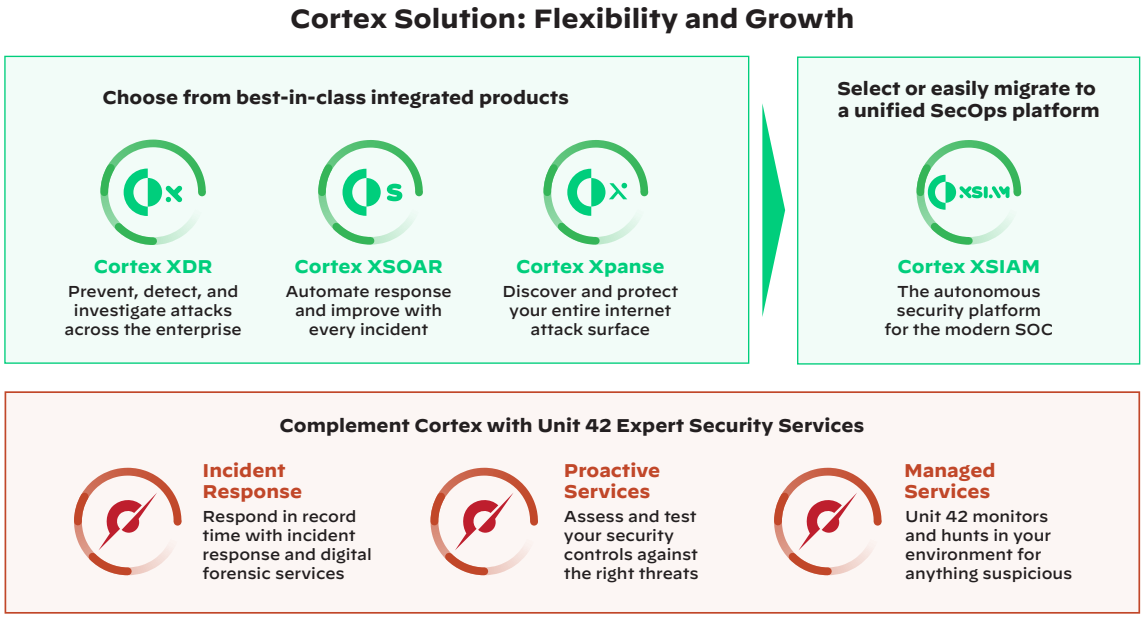

Figure 1: End-to-end workflow automation for security operations

With native end-to-end integration and interoperability within the Cortex portfolio, security teams can close the loop on threats across their ecosystem and technology stack. All of the Cortex solutions work in concert to monitor the threat landscape and provide the most robust prevention, detection, response, investigation capabilities, and automated response:

- Cortex XDR and Cortex Xpanse provide the ultimate visibility and detection across the internet-facing attack surface, endpoints, cloud, and network.
- Cortex XDR and Cortex Xpanse leverage Cortex XSOAR for full orchestration, automation, and response capabilities.
- Cortex XSOAR leverages Cortex XDR and Cortex Xpanse to provide high-fidelity detections and alerts to drive orchestrated workflows.

1. *Ransomware and Extortion Report*, Unit 42, March 21, 2023.
2. *Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, May 10, 2021.

Cortex Xpanse: Internet-Connected Asset Discovery and Remediation

The rise of the cloud and remote work means that the attack surface is constantly moving, changing, and becoming more complex. Additionally, advancements in scanning technologies allow attackers to scan the entire internet quickly and easily to locate attack vectors along paths of least resistance, revealing abandoned, rogue, or misconfigured assets that can become backdoors for compromise. Deploying an attack surface management solution can provide a continuous assessment of an organization's external attack surface.

Cortex Xpanse helps your organization actively discover, learn about, and respond to unknown risks in exposed services. Large and distributed organizations like the Department of Defense turn to Xpanse to solve their visibility, context, and remediation challenges. With the introduction of the new Active Response Module, your teams can now benefit from Palo Alto Networks industry-leading automation, orchestration, and remediation expertise.

Figure 2: U.S. Department of Defense supercharges its cybersecurity programs with Cortex Xpanse

Fix Security Blind Spots
Automatically discover and eliminate risks from unmanaged IT infrastructure in your environments.

Prevent Ransomware
Actively shut the door on ransomware attacks with automation.

Eliminate Shadow Cloud
Eliminate unsanctioned, rogue cloud sprawl.

Improve Zero-Day Response
With just a click, assess and reduce your exposure to the latest CVE.

Improve M&A Evaluation
Achieve better due diligence on security posture pre- and postmergers and acquisitions.

Reduce Cyber Insurance
Eliminate unknown exposures to reduce insurance risk and premiums.

Cortex XSOAR: Security Orchestration, Automation, and Response, Plus Threat Intel Management

At the heart of any SOAR solution is the ability to set incident response priorities and build streamlined workflows for security events that require minimal human involvement. Improved efficiencies are the result of a SOAR platform that can automate processes and minimize complex incident investigations in a single platform.

Cortex XSOAR provides end-to-end incident and security operational process lifecycle management, helping companies accelerate security operations, reduce the time it takes to investigate and respond to security alerts and incidents and handle incidents at scale. Security teams of all sizes can orchestrate, automate, and speed up incident response for any security workflow or security process across their

environment by leveraging the extensive vendor integration and 900+ prebuilt content packs to maximize enterprise coverage.

With XSOAR, security teams gain access to a central threat repository for their threat intelligence feeds—including tactical (machine-readable-based) to strategic sources (report-based)—providing the ability to automatically map external threat information to incidents happening in their network.

Automation & Orchestration

Respond to security incidents with speed and scale:

- Hundreds of product integrations.
- Thousands of security actions.
- Intuitive, visual playbook editor.

Real-Time Collaboration

Improve investigation quality by working together:

- Virtual war room for every incident.
- ChatOps and real-time security actions.
- Autodocumentation of playbook and analyst actions.

Case Management

Standardize process across products, teams, and use cases:

- Ingest and query all security alerts.
- Custom views by incident type.
- Prebuilt integrations and mirroring with case management tools (ServiceNow, Jira, Remedy, Slack, etc.).
- Customizable dashboards and reporting.

Threat Intel Management

Take full control of your threat intel feeds:

- Automate repetitive daily indicator management tasks.
- Get instant ROI from existing threat intel feeds.
- Gain confidence in incident response decisions.

Cortex XDR: Endpoint Threat Prevention, Endpoint Detection and Response, Behavior Analytics, and Managed Detection and Response

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. Once you prevent everything you can at the endpoint, Cortex XDR provides detection and response that focuses on incidents by automating evidence gathering, groups of associated alerts, putting those alerts into a timeline, and revealing the root cause to speed triage and investigations for analysts of all skill levels.

Cortex XDR can stop attacks at the endpoint and host with world-class EDR for Windows and Linux hosts with:

- AI-driven local analysis and ML-based behavioral analysis that is updated regularly
- A suite of endpoint protection features, such as Device Control, host firewall, and disk encryption
- A range of protection modules to protect against preexecution and postexecution exploits

Cortex XDR brings tighter third-party integrations, better analytics, and faster response capabilities—a must when one considers that organizations may use up to 45 security tools while responding to an incident.[3]

Security teams can stop attacks more efficiently and effectively, eliminating blind spots, reducing investigation times, and ultimately improving security outcomes using Cortex XDR. With Cortex XDR's ability to stop attack sequences at critical stages, such as execution—before persistence techniques result in broader lateral damage—security teams finally have a solution to "head attacks off at the pass."

3. *Cyber Resilient Organization Report*, IBM Security, June 30, 2020.

Detect Advanced Attacks with Analytics
Uncover threats with AI, behavioral analytics, and custom detection rules.

Focus on Incidents, Not Alerts
Avoid alert fatigue with a game-changing unified incident engine that intelligently groups related alerts into incidents.

Investigate Eight Times Faster
Verify threats quickly by getting a complete picture of attacks with root cause analysis.

Stop Attacks Without Degrading Performance
Obtain the most effective endpoint protection available with a lightweight agent.

Maximize ROI
Use existing infrastructure for data collection and control to lower costs by 44%.

Cortex XSIAM: Intelligent Data and Analytics with Automation-First Proactive Security

Cortex XSIAM unifies best-in-class functions, including EDR, XDR, SOAR, ASM, UBA, TIP, and SIEM. Using a security-specific data model and applying machine learning, XSIAM automates data integration, analysis, and triage to respond to most alerts, enabling you to focus on the incidents that require human intervention.

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 centralization, intelligent stitching, analytics-based detection, incident management, threat intelligence, automation, attack surface management, and more—all delivered within an intuitive, automation-first user experience.

Massive volumes of security data are integrated by XSIAM using an ML-led design, which also groups alerts into incidents for automated analysis and triage and handles the bulk of incidents automatically. It is constructed using a security-specific data model and is regularly updated with threat intelligence received by Palo Alto Networks from tens of thousands of customers across the world.

Security information and event management (SIEM) solutions were built to facilitate alert and log management but have relied heavily on human-driven detection and remediation with bolt-on analytics and automation only here and there. The SIEM category has served security operations for years with significant manual overhead and slow incremental improvement in security outcomes. Combating today's threats requires us to radically reimagine how we run cybersecurity in our organizations using AI.

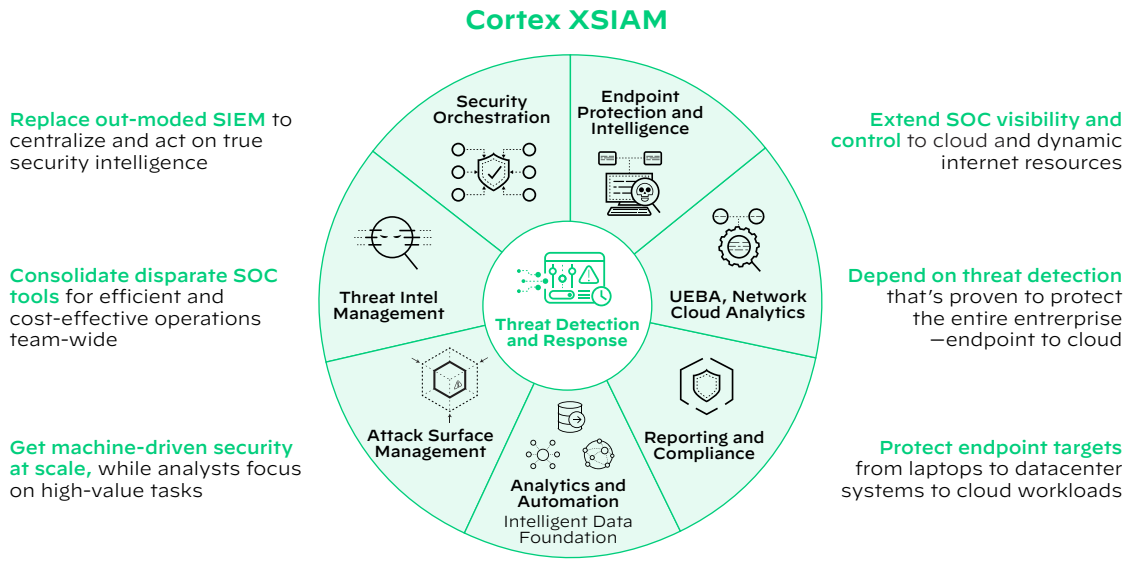

Figure 2: Centralize, automate, and scale operations to protect your organization

Great on Their Own, Yet Better Together

The Cortex portfolio offers an end-to-end security solution that ensures every step of security processes is covered.

Cortex is the industry's most comprehensive security operations product portfolio to ensure enterprises are being proactive with security, not reactive. This begins with attack surface management for complete visibility of assets and risks to best-in-class prevention, detection, and response on endpoints, and powerful automation capabilities to reduce human effort. By taking a portfolio approach, teams benefit from integrated solutions for continuous protection with uninterrupted monitoring.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087