Cortex XSOAR Case Management

CORTEX XSOAR
BY PALO ALTO NETWORKS

- **Complete Case Management:** Multi-source alert ingestion, centralized incident queue, comprehensive SLA tracking and metrics, evidence collection and journaling, mobile application support.
- **Primed for Full Customization:** Custom flows and layouts for incident types and security personas, flexible playbooks for process workflows, widget-driven dashboards and reports.
- **Continuous Improvement and Learning:** Machine learning powered insights on incident owner/task assignment, related incidents, and commonly run security commands.

Security-Focused Case Management

In this landscape of ever-evolving and complex threats, SOC employees face challenges across the board. One major challenge is finding a balance between standardized incident response for high-quantity attacks and customized response for sophisticated, one-off attacks. There is also a lack of focus on continuous improvement and learning, with most of the time being spent fighting daily fires.

This is where Cortex XSOAR comes in. Our full case management capabilities weave in security orchestration and automation for quicker triage, response, and coordination in the face of rising attack numbers. A high focus on customization – from granular metrics and response workflows to incident flows and fields – allows users to tailor response to attack types. Machine learning insights also prime users for continuous learning, with suggestions for incident ownership, task assignment, related incidents, and commonly run commands. Integrated threat intel management automates the ingestion, aggregation and tuning of threat feed data for added context during investigations.

Key Benefits

Consistent, transparent, and documented processes

- Playbook-driven response actions and investigation queries.
- Auto-documentation of all investigations and historical searches.
- Search across investigations, indicators, and evidence.
- Granular tracking of incident and analyst metrics.

Tailored incident visibility and monitoring

- Custom incident ingestion rule sets and sources.
- Unique incident-specific fields, views, and response workflows.
- Analyst-level tracking of task assignment and response actions.
- Quick pivot searches and queries to focus on incident subsets.

Improved analyst productivity and enhanced team learning

- Visual maps of related incidents for quick detection of duplicates.
- Real-time collaboration and unstructured investigation support.
- ML-powered insights for task-analyst matching, ownership, and response actions.
- Mobile application for on-the-go case management.

Flexible and scalable deployment

- Solution available as cloud-hosted or on-premise deployment.
- Supports full multi-tenancy with data segregation and scalable architecture.
- Engine proxy to handle segmented networks.
- Multi-tier configurations for improved load management.

paloalto NETWORKS

Complete Case Management

Cortex XSOAR's platform manages all aspects of the incident lifecycle:

- Multi-source alert ingestion with centralized incident queue and playbook-driven response for every attack type.
- Intuitive drag-and-drop playbooks to automate SOC processes and standardize workflows.
- Auto-documentation of all incidents and investigations for comprehensive SLA tracking.
- Central indicator repository that enables pivoted searches around indicators and threat hunting exercises.
- Mobile application providing personalized dashboards, task lists, and executable incident actions on the go.
- Dissolvable agents across Windows/Mac/Linux OS to collect data from endpoints.

End-to-end Customization

Cortex XSOAR's flexibility lets users tailor response to attacks:

- Custom incident types, streamlined data classification and mapping for centralized alert visibility.
- Tailored incident flows and layouts with full access control for every incident type and security persona.
- Strong search and query capabilities that enable quick drill-down into incident subsets.
- Comprehensive dashboards and customizable reports to quantify performance and archive results.

Intelligent Automation and Orchestration

Cortex XSOAR's case management dovetails with playbook orchestration that spans across people, process, and technology:

- Hundreds of open and extensible integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more.
- Dynamic playbooks that engage analysts through manual tasks and end users through mail response and analysis.
- Flexibility to create new playbook tasks/blocks and carry them over across playbooks.
- Live visualization of playbook runs for task management and troubleshooting.

Continuous Learning

Cortex XSOAR's machine learning increases SOC efficiencies and enables teams to get smarter with each attack:

- ChatOps-powered virtual 'War Room' where analysts can collaborate in real-time and run security actions.
- Related Incidents investigative toolkit that provides a customizable map of related incidents across time.
- In-house security bot (DBot) that helps run commands, suggests incident ownership, and task assignment.
- Externally installable chatbot that allows mirroring investigations on Slack.
- Evidence gathering and auto-documentation with rich text markdown and highlightable notes.

CORTEX XSOAR
BY PALO ALTO NETWORKS

Cortex Xsoar For Incident Management

Unified Platform

Complete platform unifying case management, security orchestration, collaboration and threat intel management.

Full Customizability

Flexibility in ingestion sources, incident types, incident layouts, response playbooks, and reports

Continuous Learning

ML-powered insights for incident ownership, analyst-task matching, and analyst actions

Flexible Deployment

On-premise and cloud-hosted deployments with full multi-tenancy and three layers of isolation

Intelligent Automation

Interweaving automated and manual tasks through playbooks with 100s of integrations and 1000s of actions

SLA Confidence

Auto-documentation with full SLA tracking, granular analyst and incident metrics, dashboards and reports

Cortex XSOAR Community Edition

To experience the capabilities of Cortex XSOAR, try the free Community Edition. With its included 30-day enterprise license, it's the perfect way to test-drive Cortex XSOAR. Sign up for our free Community Edition

About Cortex XSOAR

Cortex XSOAR is the industry leading Security Orchestration, Automation, and Response platform that unifies case management, automation, real-time collaboration and threat intel management to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks and manage incidents across their security product stack to improve response times and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/xsoar

paloalto NETWORKS