Cortex XSOAR Threat Intelligence Management

Threat intelligence is at the core of every security operation. It applies to every security use case. Unfortunately, security teams are too overtaxed to truly take advantage of their threat intelligence, with thousands of alerts and millions of indicators coming at them daily. They require additional context, collaboration, and automation to extract true value. They need a solution that gives them the confidence to do their jobs effectively and shore up their defenses against the attacker's next move.

Cortex® XSOAR Threat Intelligence Management (TIM) takes a unique approach to native threat intelligence management, unifying aggregation, scoring, and sharing of threat intelligence with playbook-driven automation.

Features and Capabilities

Powerful, native centralized threat intel: Supercharge investigations with instant access to the massive repository of built-in, high-fidelity Palo Alto Networks threat intelligence crowdsourced from the largest footprint of network, endpoint, and cloud intel sources (Tens of millions of malware samples collected and firewall sessions analyzed daily).

Indicator relationships: Indicator connections enable structured relationships to be created between threat intelligence sources and incidents. These relationships surface important context for security analysts on new threat actors and attack techniques.

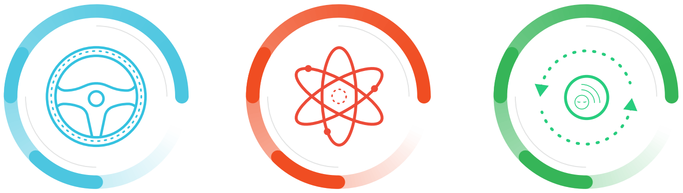
Hands-free automated playbooks with extensible integrations: Take automated action to shut down threats across more than 600 third-party products with purpose-built playbooks based on proven SOAR capabilities.

Granular indicator scoring and management: Take charge of your threat intel with playbook-based indicator lifecycle management and transparent scoring that can be extended and customized with ease.

Automated, multi-source feed aggregation: Eliminate manual tasks with automated playbooks to aggregate, parse, prioritize, and distribute relevant indicators in real time to security controls for continuous protection.

Most comprehensive marketplace: The largest community of integrations with content packs that are prebuilt bundles of integrations, playbooks, dashboards, field subscription services, and all the dependencies needed to support specific security orchestration use cases. With 680+ prebuilt content packs of which 700+ are product integrations, you can buy intel on the go using Marketplace points.

Business Value

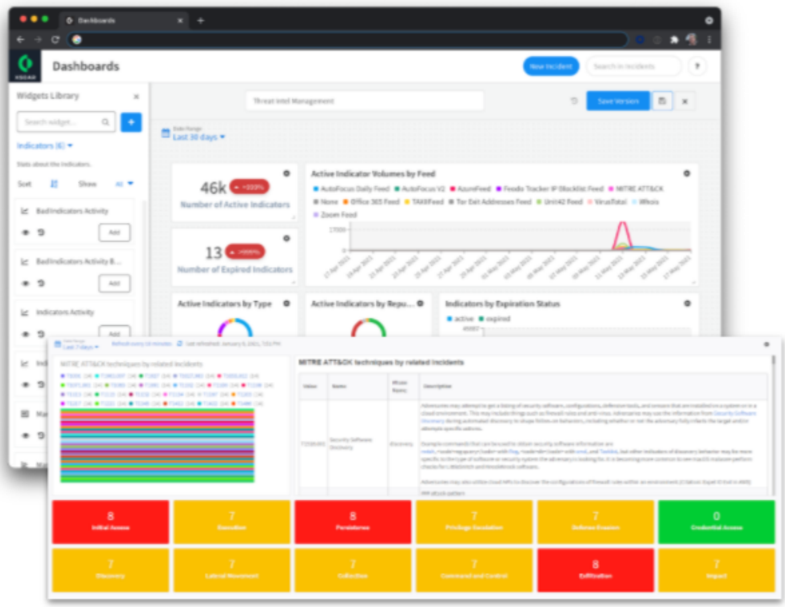


Take Full Control
Take complete control of your threat intelligence feeds

Enrich Incident Response
Make smarter incident response decisions by enriching every tool and process

Actionable Intel
Close the loop between intelligence and action with playbook-driven automation

Figure 1: Control, enrich, and take action with playbook-driven automation

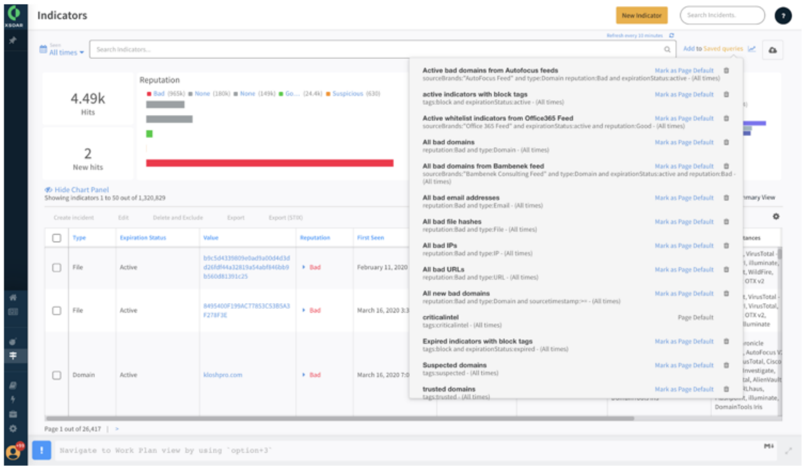

Dashboards
46k
Number of Active Indicators
13
Number of Expired Indicators
Active Indicator Volumes by Feed
Active Indicators by Type
Indicators by Expiration Status
MITRE ATT&CK techniques by related incidents

Customize and share dashboards to match your environment

Gain visibility into the entire intelligence lifecycle

Get instant ROI on your existing threat feeds

Figure 2: Take control of your threat intel feed

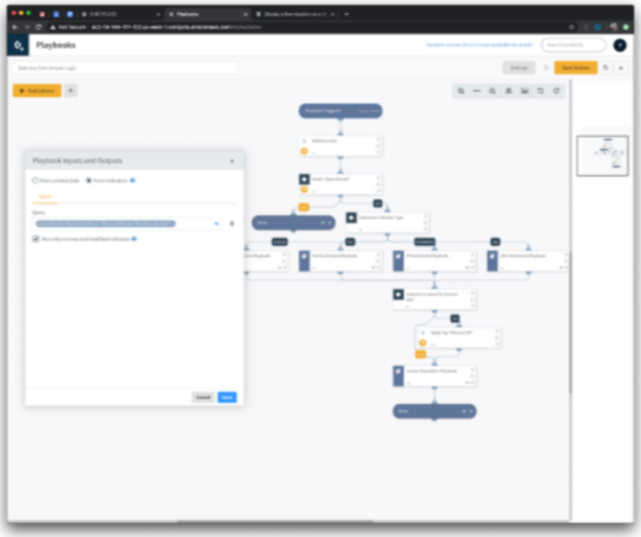


Supercharge investigations with high-fidelity threat intel feed built in

Take charge of your threat data with easy-to-edit IOC scoring and by adding new indicator types

Approx. 50+ million samples collected and analyzed daily and over 26 billion malware samples from real-world attacks sourced from more than 82,000 enterprise customers

Figure 3: Make smarter decisions by enriching and prioritizing indicators



Enforce automated action to immediately shutdown threats across your enterprise with purpose-built playbooks

Expand the scope of your investigations by easily sharing threat intelligence across internal teams and trusted organizations

Gain confidence in your actions by enriching any detection, monitoring, or response tools via playbooks

Figure 4: Close the loop between intel and action with automation

Threat Intelligence Combined with SOAR

Security orchestration, automation, and response (SOAR) solutions have been developed to more seamlessly weave threat intelligence management into workflows by combining TIM capabilities with incident management, orchestration, and automation capabilities. Organizations looking for a threat intelligence platform often look for SOAR solutions that can weave threat intelligence into a more unified and automated workflow—one that matches alerts both to their sources and to compiled threat intelligence data and that can automatically execute an appropriate response.

As part of the extensible Cortex XSOAR platform, threat intel management unifies threat intelligence aggregation, scoring, and sharing with playbook-driven automation. It empowers security leaders with instant clarity into high-priority threats to drive the right response, in the right way, across the entire enterprise.

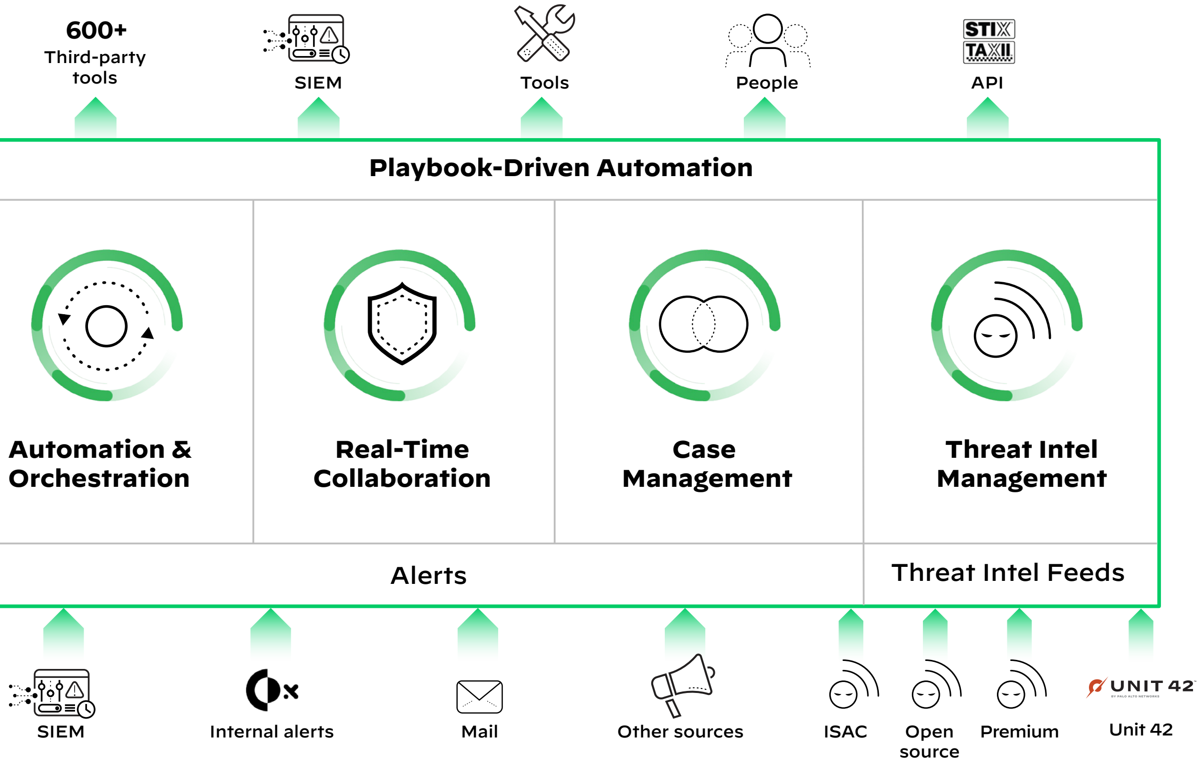


Figure 5: SOAR + TIP playbook-driven automation

Cortex XSOAR TIM provides a common platform for incidents and threat information, where there is no disconnect between external threat data and your environment, as we believe your incident data is the most relevant source of threat intelligence available to your organization and we help you treat it that way. Automated data enrichment of indicators provides analysts with relevant threat data to make smarter decisions.

Integrated case management allows for real-time collaboration, boosting operational efficiencies across teams, and automated playbooks speed response across security use cases.

Key Use Cases

Use Case 1: Proactive Blocking of Known Threats

Challenge

The security team needs to leverage threat intelligence to block or alert on known bad domains, IPs, hashes, etc. (indicators). The indicators are being collected from many different sources, which need to be normalized, scored, and analyzed before the customer can push to security devices such as SIEM and firewall for alerting. Detection tools can only handle limited amounts of threat intelligence data and need to constantly re-prioritize indicators.

Solution

Indicator prioritization. Palo Alto Networks Threat Intelligence Management can ingest phishing alerts from email inboxes through integrations. Once an alert is ingested, a playbook is triggered and can have any combination of automated or manual actions that users desire. The playbooks can have filters and conditions that execute different branches depending on certain values.

Use Case 2: Dynamic Allow/Deny List Administration

Challenge

Manual process for allow/deny lists. Managing a single allow list and updating across the enterprise can involve updating dozens of network devices. Security teams often have to liaise with firewall admins, IT teams, DevOps, and other teams to execute some parts of incident response.

Solution

Eliminate downtime by using automated playbooks to extract valid IP addresses and URLs to exclude from enforcement point EDLs, ensuring employees have access to these business-critical applications at all times.

Use Case 3: Cross-Functional Intelligence Sharing

Challenge

Intelligence sharing is unstructured. Most intelligence is still shared via unstructured formats such as email, PDF, blogs, etc. Sharing indicators of compromise is not enough. Additional context is required for the shared intelligence to have value.

Solution

Indicator connections enable structured relationships to be created between threat intelligence sources. These relationships surface important context for security analysts, threat analysts, and other incident response teams, who can collaborate and resolve incidents via a single platform.

Industry-Leading Customer Success

Our Customer Success team is dedicated to helping you get the best value from your Cortex XSOAR investments and giving you the utmost confidence that your business is safe. Here are our plans:

- **Standard Success**, included with every Cortex XSOAR subscription, makes it easy for you to get started. You'll have access to self-guided materials and online support tools to get you up and running quickly.
- **Premium Success**, the recommended plan, includes everything in the Standard plan plus guided onboarding, custom workshops, 24/7 technical phone support, and access to the Customer Success team to give you a personalized experience to help you realize optimal return on investment (ROI).

Flexible Deployment

Cortex XSOAR can be deployed on-premises, in a private cloud, or as a fully hosted solution. We offer the platform in multiple tiers to fit your needs.

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