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 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 easily extended and customized.

Automated, multisource 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 550+ integrations and 500+ product integrations, you can buy intel on the go using Marketplace points.

Business Value

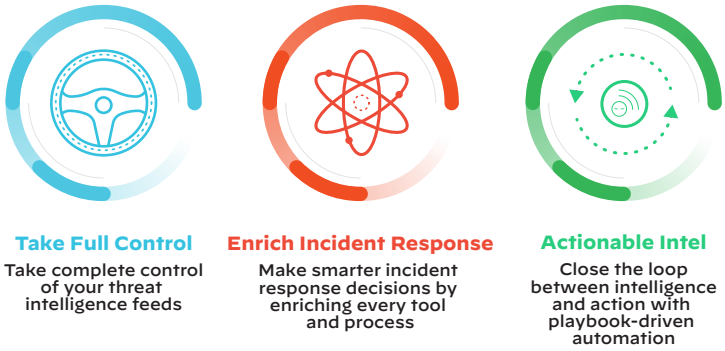


Figure 1: Control, enrich, and take action with playbook-driven automation

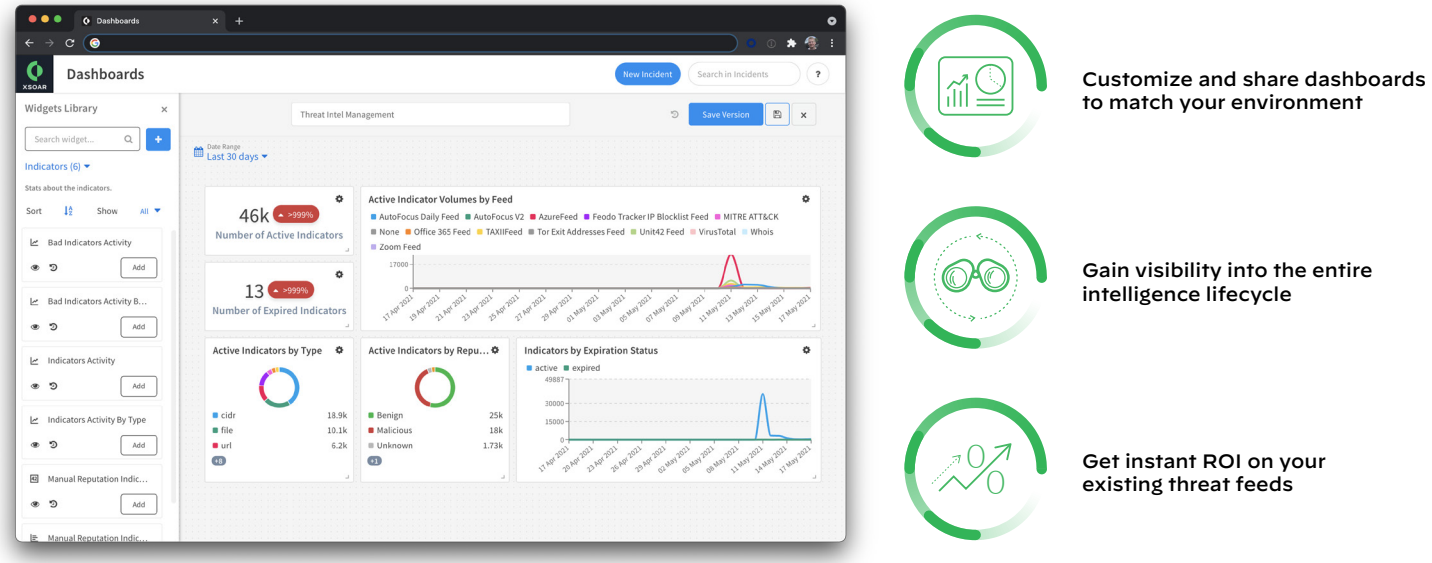
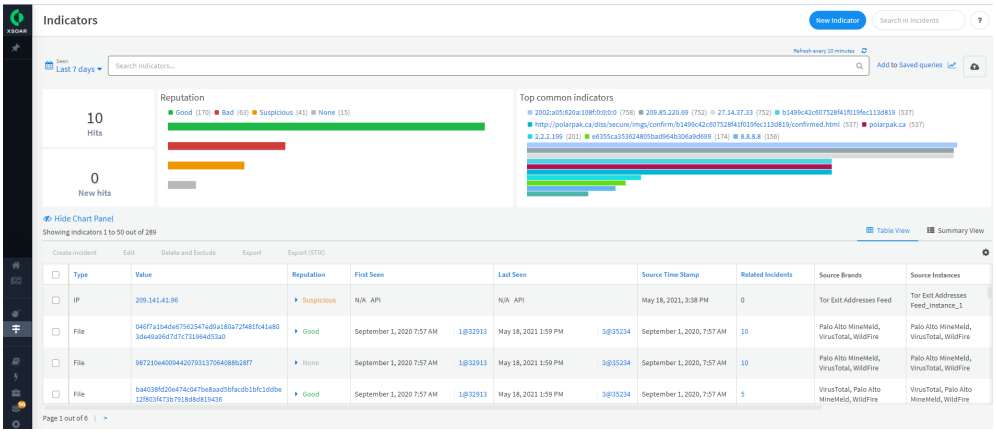


Figure 2: Take control of your threat intel feed

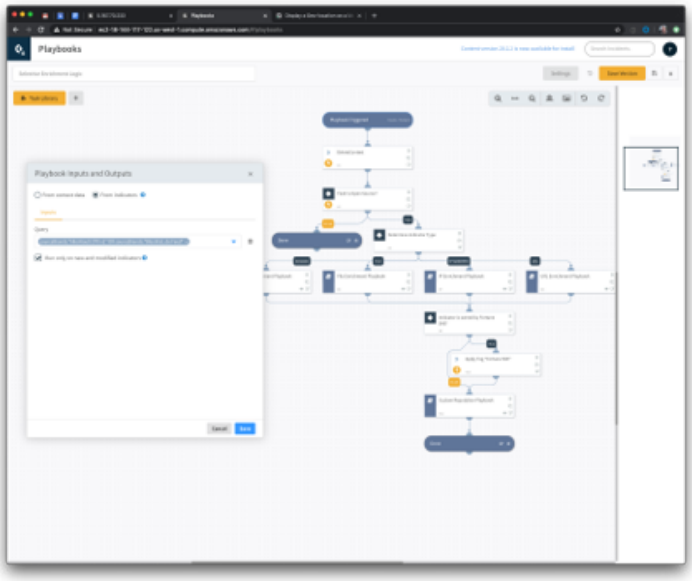


Supercharge investigations with high-fidelity threat intel feed built-in

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

Approx. 50M+ samples collected and analyzed daily and over 26B malware samples from real-world attacks sourced from more than 82K enterprise customers

Figure 3: Make smarter decisions by enriching and prioritizing indicators



Enforce automated action to immediately shut down 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 can automatically execute an appropriate response.

As part of the extensible Cortex XSOAR platform, TIM 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.

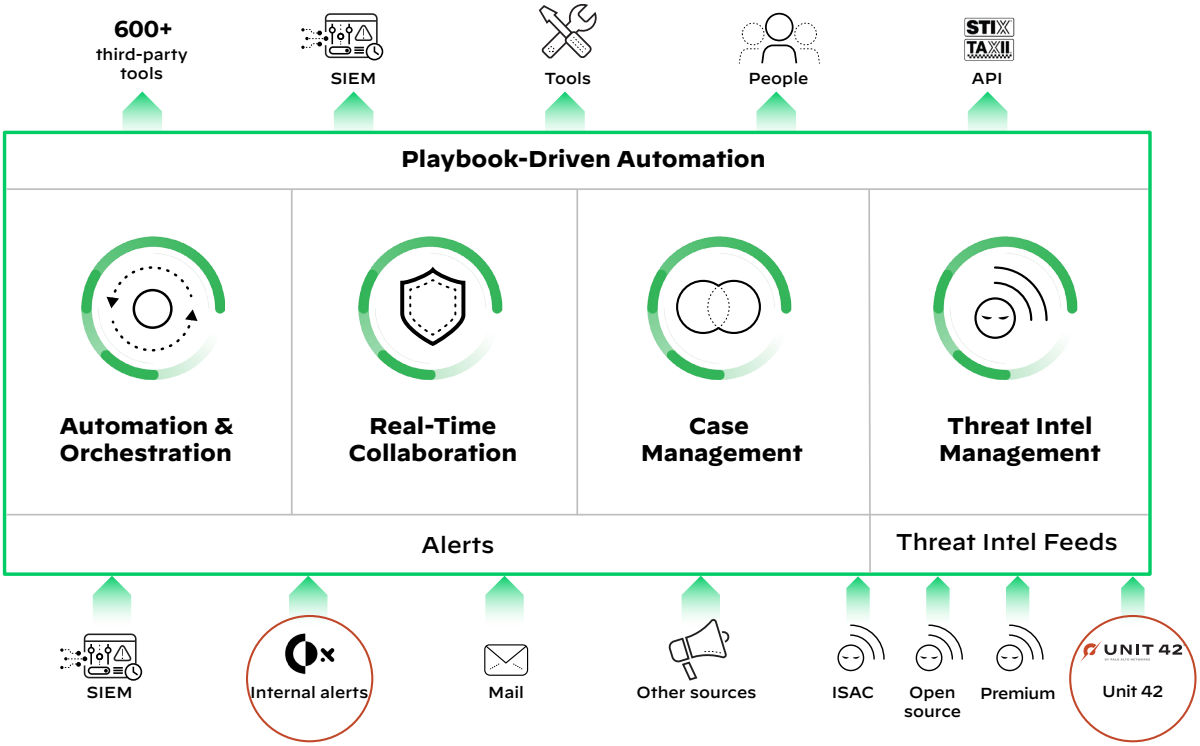


Figure 5: SOAR + TIP playbook-driven automation

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, boosts operational efficiencies across teams, and automates playbooks to 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: Incident Enrichment Using Threat Intel Data

Challenge

Most tools that Security Operations Centers and Incident Response (IR) teams use to respond to alerts are very generic. There is not much of a correlation between network data and understanding of threats and attacker movements. There is often a dump of information, including bad IP addresses or domains, and someone has to be assigned to manually resolve to figure out false positives. There is also a lack of understanding of malicious families, hacking tools, and their patterns of attacks. The process is cumbersome, takes up a lot of time, and is impractical. It's especially so in the present security scenario where hundreds if not thousands of indicators are collected on a daily basis.

Solution

Accelerate incident response with Cortex TIM and alert enrichment using threat intelligence data.

The incident enrichment workflow in Cortex XSOAR Threat Intelligence Management leverages threat intelligence from our very own high-fidelity, centralized threat intelligence library, including information on:

- Data from Unit 42 to learn about known malware campaigns or families
- IPs and domains with WHOIS data
- Passive DNS data
- Web categorization data

Use Case 3: External Threat Landscape Modeling

Challenge

Threat Intelligence teams need to understand attack details and how their organization may be vulnerable. The foundational element of understanding risk/impact to an organization begins when threat analysts start profiling the attacks.

Solution

Threat modeling to prevent or mitigate the effects of threats to the system. The intel team builds profiles of threat actors, identifies if there are related attacks, and then identifies which techniques and tools the threat actor used. This information is shared with stakeholders, including security operations and leadership.

Use Case 4: Intelligence Reporting and Distribution

Challenge

Threat Intelligence programs have a growing set of responsibilities. One of the key responsibilities is the production and dissemination of threat intelligence reports which keep employees up to date on the latest threats targeting their industry. Most intelligence is still shared via unstructured formats such as email, blogs, etc. Sharing information about indicators of compromise is not enough. Additional context is required for the shared intelligence to have value. Analysts go through hours of manual work aggregating and digging for known malware families, curated news, threats related to the company or the vertical for an industry, and why the story is relevant to the company. They need to send this report out to a large audience for security awareness and alert other stakeholders to facilitate better in the future.

Solution

Workflows and a central repository for intelligence analysts to create, collaborate, and share finished intelligence products with stakeholders via PDF reports. Intel analysts will be able to understand trends within threat intelligence using their local/curated intel and Unit 42 threat intelligence. Consume RSS feeds to collect all the news sources.

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, this plan 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**: This is the recommended plan, and it 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 that will help you realize an 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