Cortex XSOAR

Redefining Security Orchestration, Automation, and Response

Security teams need more people and scalable processes to keep pace with an overwhelming volume of alerts and endless security tasks. Analysts waste time pivoting across consoles for data collection, determining false positives, and performing repetitive, manual tasks throughout the lifecycle of an incident. Faced with a growing skills shortage, security leaders deserve more time to make decisions that matter rather than drown in reactive, fragmented, manual responses. This is not the way.

Transform Security Operations

Your SOC teams can simplify security operations by unifying automation, case management, real-time collaboration, and threat intelligence management. This means you can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response options for virtually any use case, all with the help of Cortex XSOAR.

Experience Better Performance, Reliability, and Scalability

Cortex XSOAR now offers cloud-native SOAR that autoscales to support future growth, with rapid deployment to accelerate your return on investment (ROI). Fully integrated into the Cortex platform, Cortex XSOAR is delivered through a unified user interface for ease of use and consistency in workflow management.

Business Benefits

With automation, your organization will be able to:

- Scale and standardize incident response processes.
- Speed up resolution times and boost SOC efficiency.
- Improve analyst productivity and enhance team learning.
- Gain immediate ROI from existing threat intelligence investments.

Why Cortex XSOAR?

Improve SOC Efficiency by Automating Incident Response

Automate incident response workflows and repetitive tasks to free up analysts to focus on the most critical incidents with Cortex XSOAR. Use predefined playbooks or easily customize your own to automate SOC use cases, such as indicator enrichment, alert deduplication, phishing response, ransomware response, threat intelligence feed management, malware investigation, and even IT operations, such as employee onboarding and offboarding.

Respond to Incidents with Speed and Scale

Efficiently carry out security operations and incident response by streamlining security processes, connecting disparate security tools, and maintaining the right balance of machine-powered security automation and human intervention.

Ingest, Search, and Query All Security Alerts

When complex, real-time investigations require analyst intervention, ensure they have access to lightning-quick search, query, and investigation to accelerate incident response by unifying alerts, incidents, and indicators from any source on a single platform with Cortex XSOAR.

Improve Investigation Quality by Working Together

Collaborative investigation features provide a potent toolkit to help analysts assist each other, run real-time security commands, and learn from each incident with autodocumentation of all actions. An ML-driven assistant learns from actions taken in the platform and offers guidance on analyst assignments and commands to execute actions.

Act on Threat Intelligence with Agility and Confidence

Unify aggregation, scoring, and sharing threat intelligence with playbook-driven automation with native threat intelligence management. The built-in, high-fidelity threat intelligence can be boosted by layering additional third-party threat intel to better reveal and prioritize critical threats.

Figure 1: The value of Cortex XSOAR

How Cortex XSOAR Works

Cortex® XSOAR™ ingests aggregated alerts and indicators of compromise (IoCs) from detection sources, such as security information and event management (SIEM) solutions, network security tools, threat intelligence feeds, and mailboxes, before executing automatable, process-driven playbooks to enrich and respond to these incidents. These playbooks coordinate across technologies, security teams, and external users for centralized data visibility and action.

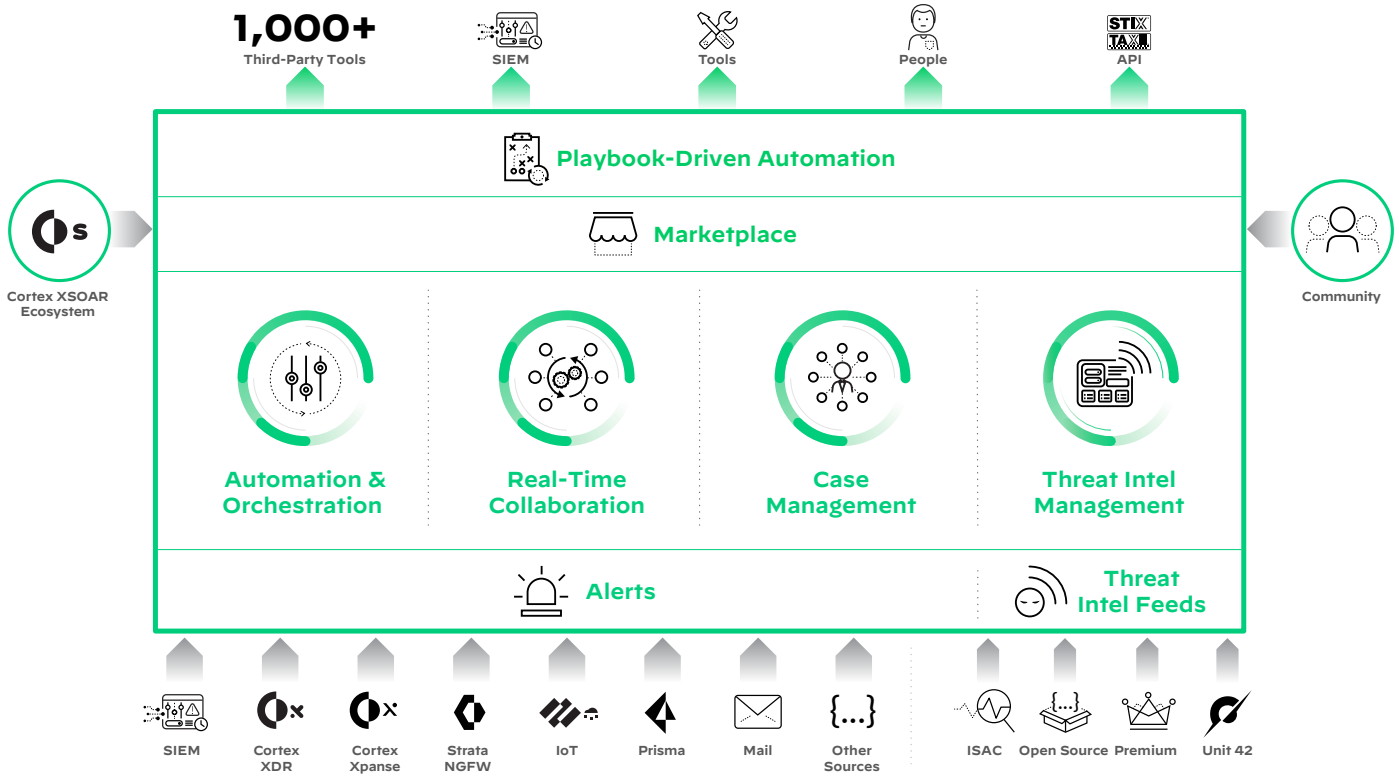

Figure 2: Cortex XSOAR platform

Simple, Scalable Deployment

Cortex XSOAR's cloud-native SaaS environment can be rapidly deployed for instant ROI, supporting customers of any size. We also offer on-premises deployment.

For managed security services providers (MSSPs), Cortex XSOAR supports full multitenancy with data segmentation and scalable architecture. MSSPs can build their managed service operations on Cortex XSOAR to provide best-in-class offerings for their customers and optimize internal team productivity. For existing Cortex users, XSOAR is easily integrated into other Cortex solutions and is delivered from the same platform.

Setting You Up for Success

Our industry-leading Customer Success Team is dedicated to helping you continuously optimize your security posture and get the most out of your Cortex XSOAR implementation.

Standard Success is included with every Cortex XSOAR subscription and gives you self-guided materials and online support tools to get you up and running quickly. An optional upgrade to Premium Success provides guided onboarding, custom workshops, 24/7 technical phone support, and access to the Customer Success Team for a personalized experience to ensure optimal ROI.

What Makes Cortex XSOAR Unique?

Enterprise Ready

With thousands of customer deployments of all sizes worldwide, XSOAR has a proven track record supporting security operation teams that range from several people to global service providers serving hundreds of clients.

Orchestrate Across Your Security Operations

With over 1,000 integrations, you get quick value out-of-the-box when it comes to deploying automation and orchestrating incident response across your SOC, network security, SASE, endpoint security, and cloud security solutions.

Integrated Case Management

Built-in collaborative functions, such as a War Room for every incident, real-time Chatbot, tight integrations with case management/ticketing tools, such as ServiceNow, Jira, Remedy, and Slack, promote teamwork across departments and help security teams speed remediation.

Integrated Threat Intel Management

Cortex XSOAR weaves native threat intelligence into a unified workflow, matching alerts to their sources and to compiled threat intelligence data to automatically execute an appropriate response.

Start your 30-day free trial of Cortex XSOAR. Begin your security automation journey by automating your security operations with a single use case.

Try it now: https://start.paloaltonetworks.com/sign-up-for-community-edition.html.

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