paloalto NETWORKS

CORTEX™
BY PALO ALTO NETWORKS

Cortex XSOAR

Redefining Security Orchestration, Automation, and Response

Security teams lack the 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 manual, repetitive tasks throughout the lifecycle of an incident. As they face a growing skills shortage, security leaders deserve more time to make decisions that matter, rather than drown in reactive, piecemeal responses.

An Industry First

Cortex™ XSOAR supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native Threat Intel Management in the industry's first extended security orchestration, automation, and response (SOAR) offering. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case, resulting in up to 90% faster response times and as much as a 95% reduction in alerts requiring human intervention.

Business Benefits

- 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

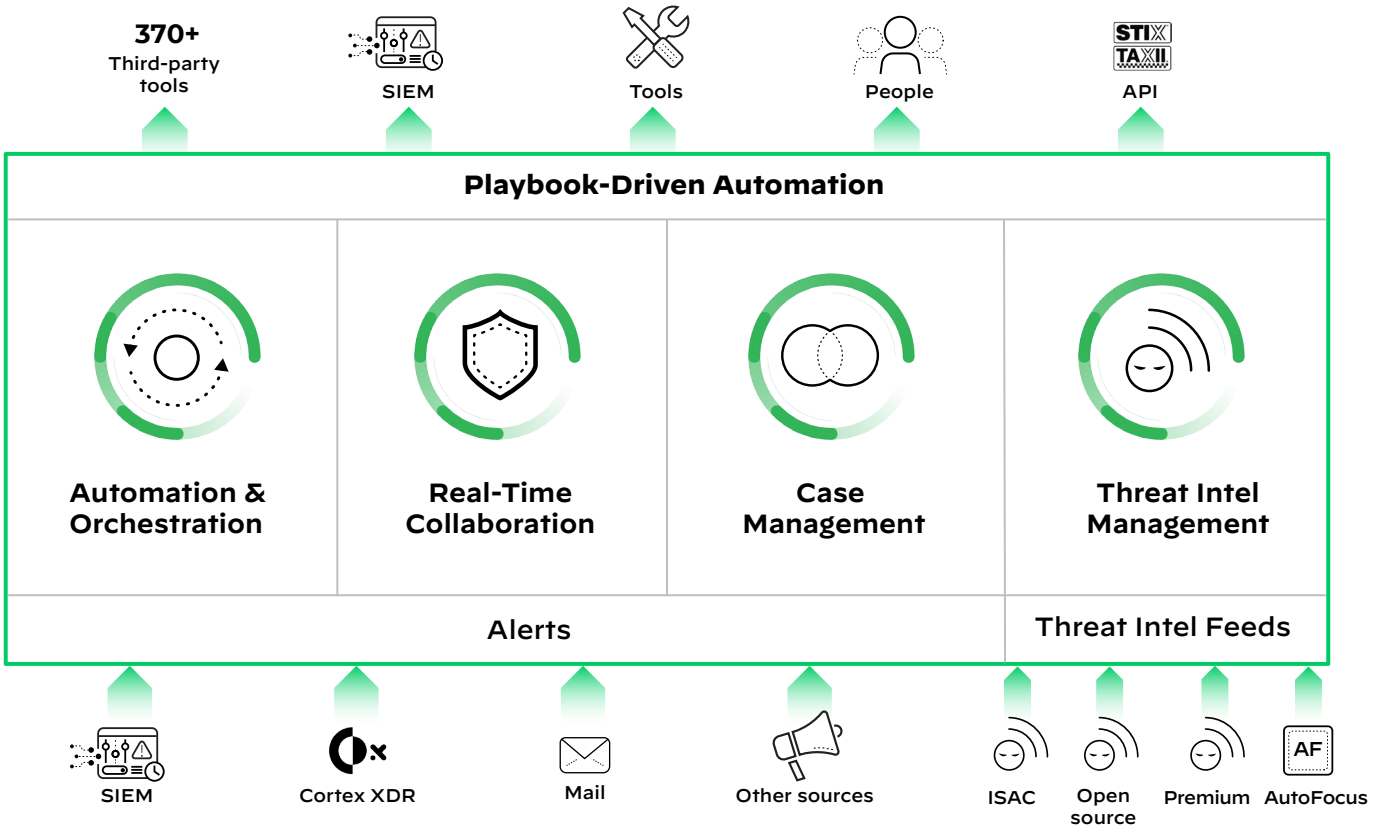

Figure 1: Cortex XSOAR inputs and outputs

Table 1: Standardize and Automate Processes for Any Security Use Case	
Scalable, consistent incident response	Hundreds of out-of-the-box playbooks covering a wide range of security use cases (e.g., phishing, IOC enrichment, vulnerability management, cloud security) speed up deployment. A powerful SDK allows you to build your own integrations.
Modular, customizable playbooks	A visual drag-and-drop playbook editor with thousands of executable actions addresses simple use cases and complex, custom workflows. Playbook blocks/tasks can be nested and reused across playbooks. Real-time editing, a playground for testing playbooks, and YAML-based sharing make playbook creation quick and easy.
Perfect balance of automation and human response	Maintain control over automated processes with manual approval tasks available as part of any playbook.
Orchestration across the product stack	Automate incident enrichment and response across more than 370 integrations with data enrichment tools, threat intelligence feeds, SIEMs, firewalls, EDRs, sandboxes, forensic tools, messaging systems, and more.

Security Orchestration

Cortex XSOAR empowers security professionals to 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.

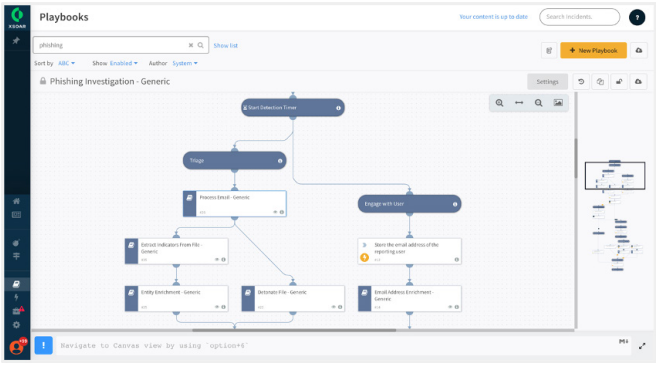

Figure 2: Cortex XSOAR phishing playbook

Table 2: Adapt to Any Alert with Security-Focused Case Management	
Custom views for security incident types	Fully customize incident views, layouts, and flows with access control specific to security personas/roles.
Indicator and incident correlation	A central indicator repository enables searches and automated indicator correlation across incidents from multiple sources to spot trends and patterns.
Flexible reports customizable to the needs of your organization	Widget-driven dashboards and reports offer unparalleled visibility into metrics.
On-the-go incident monitoring	The Cortex XSOAR mobile application provides dashboards, task lists, and incident actions on the go.
Automated ticketing process	Out-of-the-box integrations with case management platforms such as ServiceNow, Jira, Zendesk, Remedy, Slack, and more enable full automation of the ticketing process.

Case Management

Automation of incident response needs to be complemented by real-time investigations for complex use cases when human intervention is required. Cortex XSOAR accelerates incident response by unifying alerts, incidents, and indicators from any source on a single platform for lightning-quick search, query, and investigation.

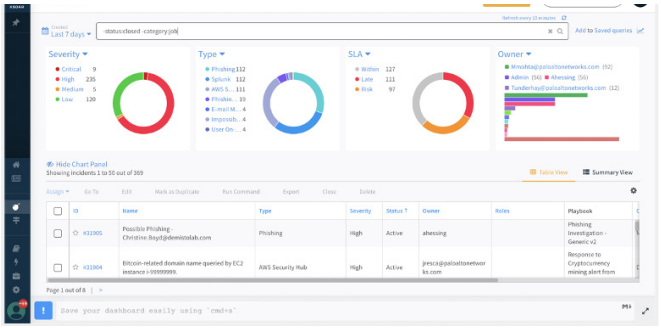

Figure 3: Customizable incident views

Table 3: Boost SecOps Efficiency with Real-Time Collaboration	
Real-time investigation and collaboration	Each incident has a virtual War Room with built-in ChatOps and command line interface (CLI) so analysts can collaborate and run security actions in real time.
Machine learning assistance	An ML-driven virtual assistant learns from actions taken in the platform and offers guidance on analyst assignments and commands to execute actions.
Continuous learning	Auto-documentation of all investigation actions aids analyst learning and development.
Streamlined, automated reporting	Flexible, widget-driven dashboards and reports eliminate manual reporting and can be fully customized to your organization's needs.

Threat Intel Management

Cortex XSOAR takes a new approach with native Threat Intel Management, unifying aggregation, scoring, and sharing of threat intelligence with playbook-driven automation.

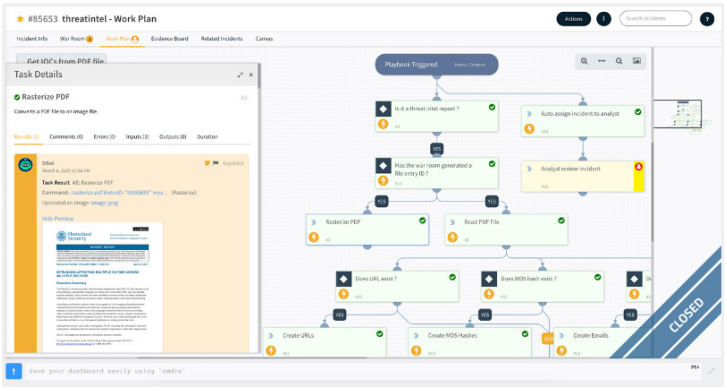

Figure 4: Intel-based automated playbook

Table 4: Act on Threat Intelligence with Confidence and Speed	
Automated multi-source feed aggregation	Eliminate manual tasks with automated playbooks to aggregate, parse, deduplicate, and manage millions of daily indicators across dozens of supported sources.
Granular indicator scoring and management	Take charge of your threat intelligence with playbook-based indicator lifecycle management and transparent scoring that can be extended and customized with ease.
Best-in-class operational efficiency	Boost collaboration and reveal critical threats by layering third-party threat intelligence with internal incidents to prioritize alerts and make smarter response decisions.
Powerful native threat intelligence	Supercharge investigations with built-in, high-fidelity threat intelligence from Palo Alto Networks AutoFocus™ contextual threat intelligence service.
Hands-free, automated playbooks with extensible integrations	Take automated action to shut down threats across more than 370 third-party products with purpose-built playbooks based on proven SOAR capabilities.

Breadth of Use Cases

Cortex XSOAR provides an open, extensible platform applicable to a wide range of use cases—even processes outside the purview of the SOC or security incident response team. Some of the most common use cases include phishing, security operations, incident alert handling, cloud security orchestration, vulnerability management, and threat hunting.

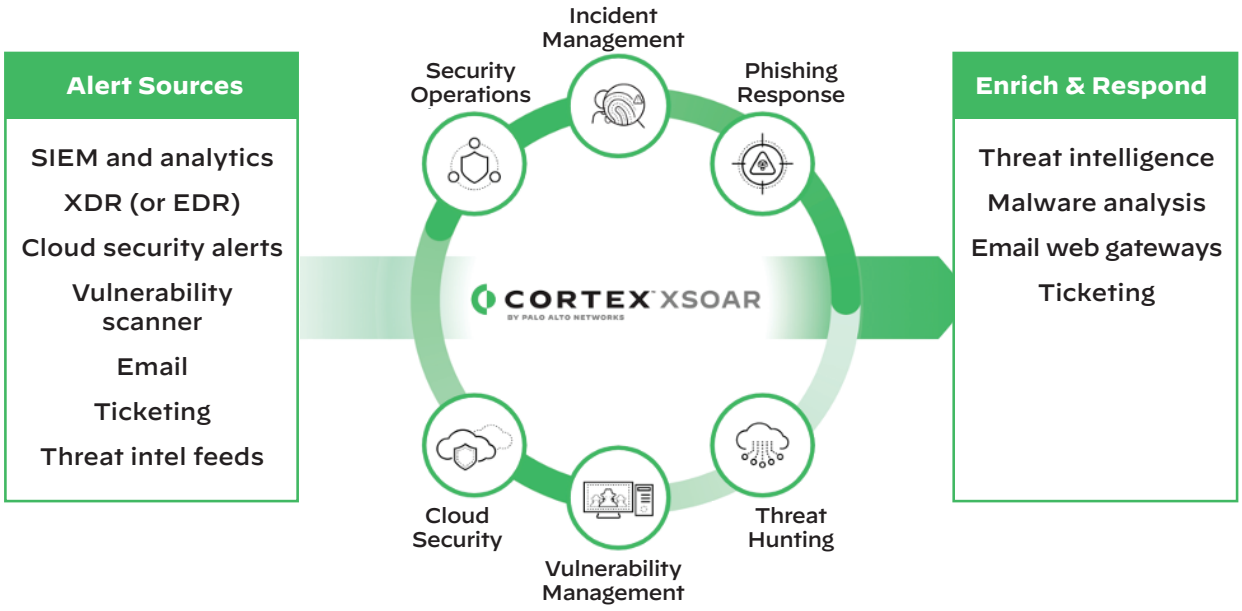

Figure 5: Ingestion of alerts in Cortex XSOAR

Breadth of Integrations

Cortex XSOAR has the industry's most extensive and in-depth out-of-the-box (OOTB) integrations with security and non-security tools used by security teams. New integrations are added every two weeks to facilitate quick and seamless deployments for our customers.

Benefits of Our Extensive Integration Ecosystem

- Promote your platform and solution offerings
- Develop a strategic partnership with Palo Alto Networks
- Take advantage of co-marketing activities and lead generation
- Gain brand recognition in the security industry

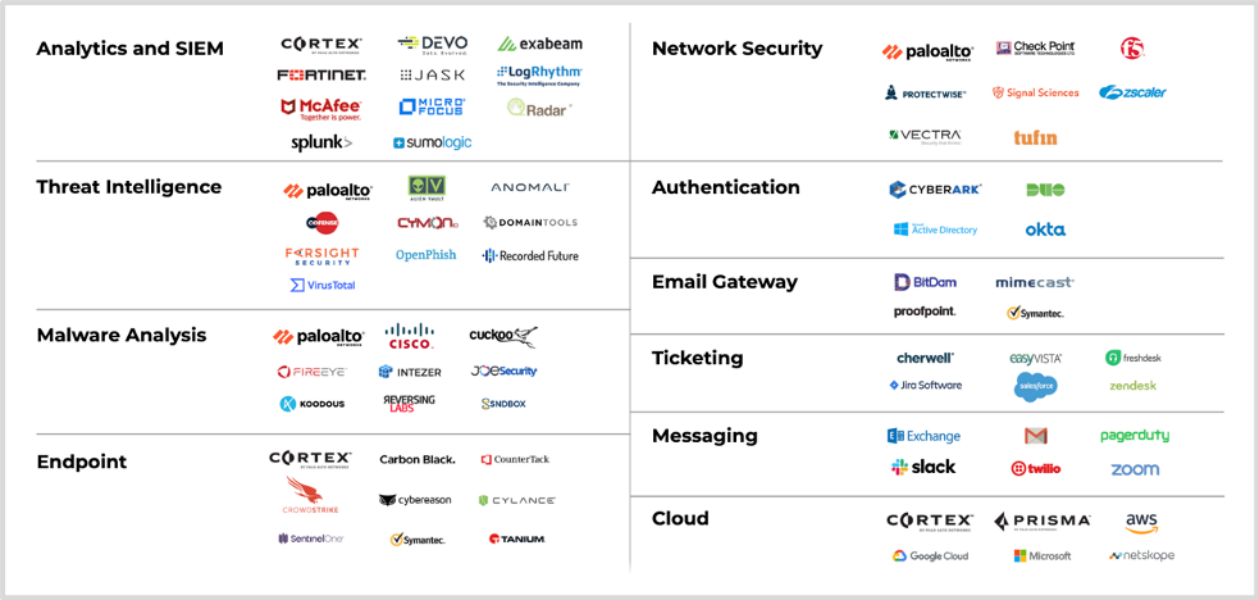

Figure 6: Some of our 370+ OOTB integrations

Designed for MSSPs

Cortex XSOAR supports full multitenancy with data segmentation and scalable architecture for managed security service providers (MSSPs). MSSPs can build their managed service operations on Cortex XSOAR to provide best-in-class offerings for their customers and optimize internal team productivity.

Table 5: The Connective Fabric for Your Security Infrastructure and Teams	
Ironclad security and privacy	Take advantage of data isolation with master-tenant separation and execution isolation with each tenant running as a separate process, as well as network isolation with engine (proxy) for segmented networks without firewall changes.
Role-based visibility and control	Update playbooks, reports, automation, and more for all tenants from the master (MSSP) account. Customers can be granted access to their environments only. Third-party integrations can be done at the master or tenant level.
Increased customer trust and response agility	Collaborate with customers in real time via War Room for joint investigations. Enjoy quick customer onboarding and scalability.
Flexible deployment	Integrate with cloud-based services, MSSP systems, and customers' on-premises systems.

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.

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).

		Standard	Premium
	Summary Value	Self-Help	Optimized Experience
Onboarding Assistance	Customer journey kickoff	●	●
	Onboarding assistance		●
	First use case definition assistance		●
Technical Support	Access to support community	●	●
	Access to Support Portal	●	●
	Telephone support		24/7
	Slack DFIR private channel		●
Education Training	Access to online documentation	●	●
	Access to online training	●	●
	Custom workshop		●
Optimized Experience	Annual health check	●	●
	Customized success plans		●
	Periodic operation reviews		●
	Prioritized integration development		●

Figure 7: Key aspects of Standard and Premium Success plans

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.

Table 6: Cortex XSOAR Service Tiers

Cortex XSOAR	Cortex XSOAR Community Edition
Unlimited automation	166 daily automation commands
Unlimited incident history	Rolling 30-day incident history
Unlimited threat intelligence feeds	5 active feeds/100 indicators per feed
Native threat intelligence with AutoFocus	Native threat intelligence with AutoFocus not included
Full enterprise reports package	Incident closure report
24/7 Customer Support	Slack DFIR community
Multitenant	Single tenant

System Requirements: On-Premises

Table 7: Cortex XSOAR Server		
Component	**Minimum**	**Recommended**
CPU	8 CPU cores	16 CPU cores
Memory	16 GB RAM	32 GB RAM
Storage	500 GB SSD	1 TB SSD with minimum 3K dedicated IPOS
Physical or virtual server	Linux OS: Ubuntu 14.04, 16.04, 18.04, 18.10; RHEL 7.x; Oracle Linux 7.x; Amazon Linux 2; Fedora; Centos 7.x	

Table 8: Cortex XSOAR Engine		
Component	**Minimum**	**Recommended**
CPU	8 CPU cores	16 CPU cores
Memory	16 GB RAM	32 GB RAM
Storage	500 GB SSD	1 TB SSD with minimum 3K dedicated IPOS
Operating system	macOS, Windows, Linux	

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.

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