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 repetitive, manual 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 is the industry's first extended security orchestration and automation platform that simplifies security operations by unifying automation, case management, real-time collaboration, and threat intelligence management. Teams can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security use case.

Business Benefits

With Cortex XSOAR, 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
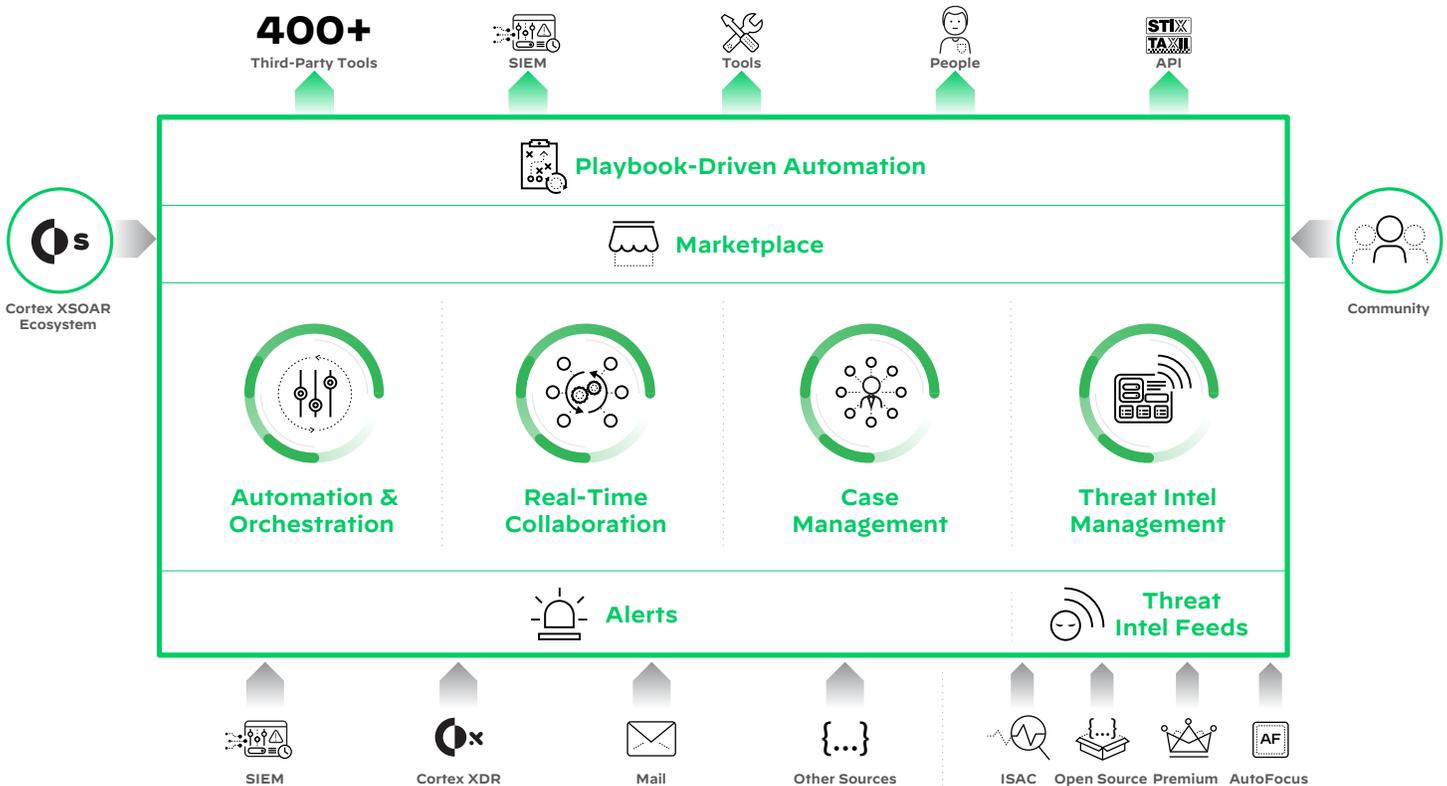- Gain immediate ROI from existing threat intelligence investments

Figure 1: Cortex XSOAR platform

Table 1: Standardize and Automate Processes for Any Security Use Case	
Scalable, consistent incident response	Speed up deployment with hundreds of out-of-the-box (OOTB) playbooks covering a wide range of security use cases (e.g., phishing prevention, IOC enrichment, vulnerability management, cloud security). A powerful software development kit allows you to build your own integrations.
Modular, customizable playbooks	Address simple use cases and complex, custom workflows using a visual drag-and-drop playbook editor with thousands of executable actions. 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 400 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.

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 2: Cortex XSOAR phishing playbook

Table 2: Adapt to Any Alert with Security-Focused Case Management	
Custom layouts for incidents and indicators	Fully customizable incident and indicator layouts help you quickly surface relevant information when responding to events.
Indicator and incident correlation	A central indicator repository enables searches and automated indicator correlation across incidents from multiple sources to spot duplicates, trends, and patterns.
Flexible, customizable reports and dashboards	Widget-driven dashboards and reports offer unparalleled visibility into metrics so you can cut and dice data for your reporting needs.
On-the-go incident monitoring	The Cortex XSOAR mobile application provides dashboards, task lists, and incident actions on the go.
Automated mapping across integrations	Mirrored connections can be created with other applications so incident updates in Cortex XSOAR will be pushed automatically to third-party applications (ServiceNow, Jira, Slack, etc.) for automated ticketing management.

Collaboration and Learning

Cortex XSOAR offers interactive investigation features, providing a potent toolkit to help analysts collaborate, run real-time security commands, and learn from each incident.

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 Intelligence Management

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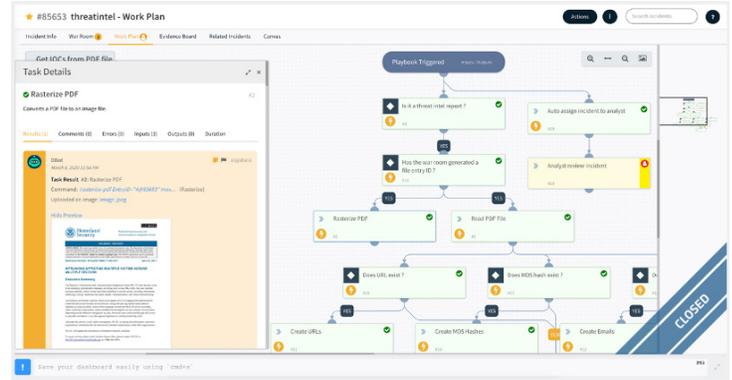

Figure 4: Intelligence-based automated playbook

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 400 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 security operations center (SOC) or security incident response team. The flexible platform can be adapted to any use case, with common ones including phishing, security operations, incident alert handling, cloud security orchestration, vulnerability management, and threat hunting.

Figure 5: Ingestion of alerts and IOCs in Cortex XSOAR

Cortex XSOAR Marketplace

Cortex XSOAR Marketplace is the industry's most comprehensive security orchestration marketplace. As a native extension of Cortex XSOAR, the Marketplace enables you to discover, share, and consume content packs contributed by the industry's largest SOAR community.

Content packs are pre-built bundles of integrations, playbooks, dashboards, fields, and subscription services designed to address specific security use cases. Packs can be deployed with a single click, simplifying and speeding up the adoption of automation.
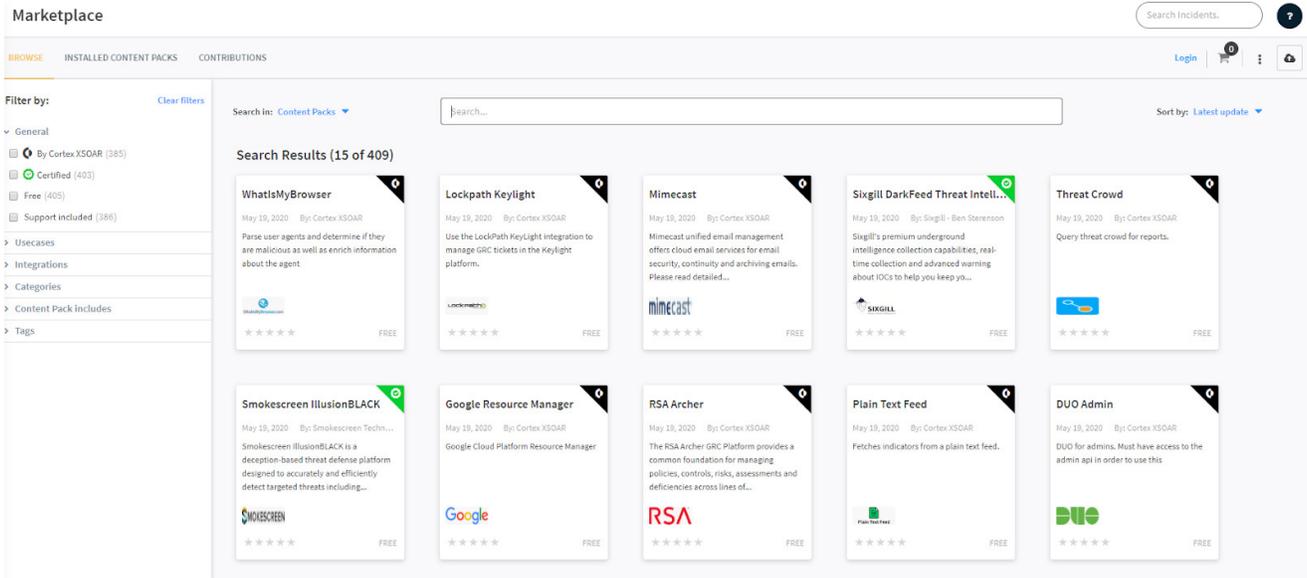
Figure 6: Highly rated, validated content to discover

Breadth of Integrations

Cortex XSOAR has the industry's most extensive and in-depth OOTB integrations with security and non-security tools used by security teams. New integrations and content packs are continuously added to the Cortex XSOAR Marketplace 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
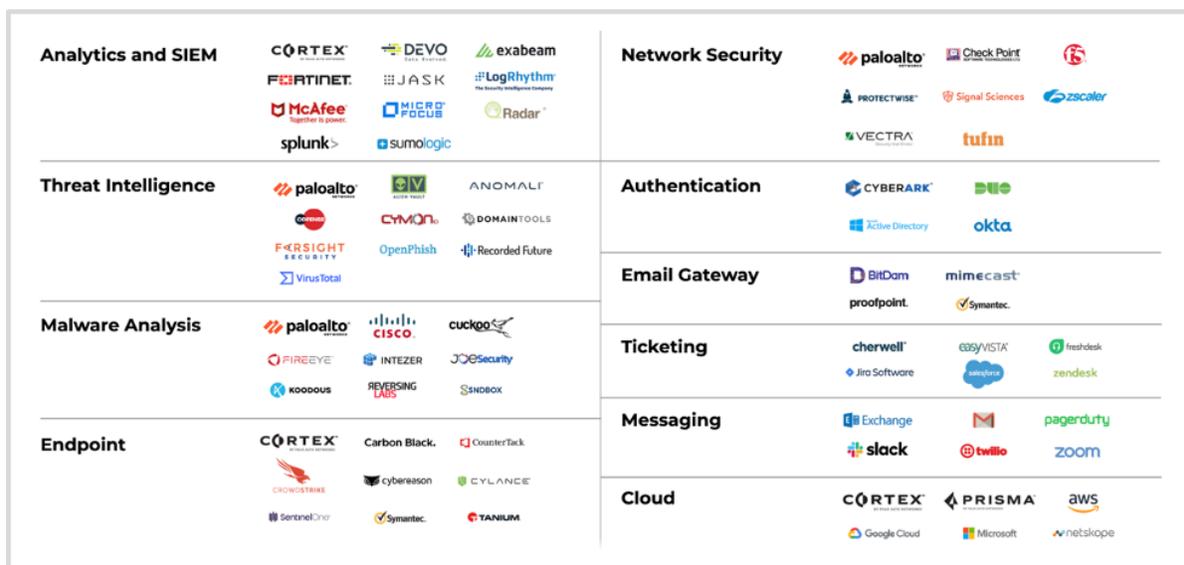- Gain brand recognition in the security industry

Join the Marketplace today.

Figure 7: Some of our 400+ OOTB integrations

Industry-Leading Customer Success

Our 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, 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		●
	Initial service configuration		●
	Use case assistance		●
Technical Support	Access to support community	●	●
	Access to Support Portal	●	●
	Telephone support		24/7
	Response time (S1)		< 1 hour
	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		●
	Executive business reviews		●
	Prioritized integration development		●

Figure 8: Key aspects of Standard and Premium Customer Success plans

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.

Cortex XSOAR Mobile App

Use Cortex XSOAR to track and respond to security incidents on the go with a mobile-first experience for iOS and Android®. Create and access personalized dashboards, assign and complete tasks from any device, and improve investigation quality by working together.

Get the app from the App Store® and Google Play®.

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	
Feature	**Value**
True multitenancy	MSSPs can create playbooks and enforce policy at both the master and tenant levels, creating flexibility to quickly onboard new customers, offer different levels of service, and expand into additional management options.
Modular playbooks	MSSPs can also build custom playbooks for specific services and service levels. Inside each playbook, tool actions can be simply "copied" and reused in other playbooks at both the master and tenant levels for efficient scaling with new customer additions.
SLA and team performance tracking	Cortex XSOAR features built-in SLA tracking capabilities to help MSSPs guarantee timely service outcomes to their customers. An MSSP can trigger a notification—via Slack, email, etc.—to the analyst team to handle a timely incident before an SLA breach.

Table 5: The Connective Fabric for Your Security Infrastructure and Teams (continued)	
Feature	**Value**
Extensive APIs	MSSPs can leverage all Cortex XSOAR capabilities as a powerful backend automation and orchestration enabler for their services while maintaining existing customer-facing portals.
Threat intelligence management	For MSSPs, adding threat intelligence to any service to increase customer value is vastly simplified. Threat intelligence feeds can be compiled at the master and tenant levels to cater to different customer types and use cases.

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.

Cortex XSOAR Hosted Solution

With our hosted solution, security teams can improve response times and efficiencies without having to devote dedicated resources for infrastructure, maintenance, and storage. Cortex XSOAR will manage and maintain the infrastructure and platform layer, enabling SOCs to focus on the critical aspects of incident response.

Benefits of a Hosted Solution
- Reliable, flexible, and scalable technology
- Ironclad security and privacy
- Lower total cost of ownership
- Accelerated, standardized incident response

Table 6: Cortex XSOAR Server—System Requirements for On-Premises Deployment		
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 IOPS
Physical or virtual server	Linux OS: Ubuntu 16.04, 18.04; RHEL 7.x & 8; Oracle Linux 7.x; Amazon Linux 2; CentOS 7.x & 8	

Table 7: Cortex XSOAR Engine—System Requirements for On-Premises Deployment		
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 IOPS
Operating system	macOS, Windows, Linux	