CORTEX™
BY PALO ALTO NETWORKS

Cortex XSOAR for Managed Security Service Providers

Comprehensive Automation and Orchestration to Supercharge Managed Security Services

Managed security service providers (MSSPs) face many of the same problems as any other security operations team: disparate tools, siloed data sources, and inconsistent manual processes all create struggles for operationalizing security service offerings and growing services. Working across many different customers amplifies these headaches, inhibiting growth and cutting into both revenue and margins for your businesses.

Business Benefits

Cortex XSOAR helps your managed security services:

- **Reach peak productivity:** Playbook automation and orchestration help maximize margins by boosting analyst productivity and reducing costs.
- **Grow your business:** Easy point-and-click development of playbooks and processes expedites moves into high-margin services like managed detection and response (MDR).
- **Cut time to revenue:** Easily replicable automations, playbooks, and extensive out-of-the-box (OOTB) integrations accelerate customer onboarding.

Myriad Security Tools, Data Sources, and Processes

Customers bring a variety of tools looking to get incorporated into managed services, making onboarding difficult and costly. Consequently, as onboarding time increases, so does time to revenue.

In addition, MSSP analysts must work with these disparate tools to create their customers' security service outcomes. Bringing together data sources and processes from automated tools is critical in order to hit service-level agreements (SLAs) for incident investigation and response.

Analyst Productivity and Churn

Security analysts struggle with alert fatigue from the security tools they use, creating problems with churn due to unsatisfying and overwhelming workloads. MSSPs need to automate alert management to give analysts more time for high-value tasks.

Cortex XSOAR

Cortex™ XSOAR supercharges MSSP efficiency by unifying case management, automation, real-time collaboration, and native Threat Intel Management in the industry's first extended security orchestration, automation, and response (SOAR) offering. MSSPs can manage alerts across all sources, standardize processes with playbooks, take action on threat intelligence, and automate response for any security service, resulting in up to 90% faster response times and as much as a 95% reduction in alerts requiring human intervention.

Reduction of MTTR with Workflow Automation

Cortex XSOAR codifies analyst actions across tools into visual, task-based workflows called playbooks. You can leverage hundreds of OOTB playbooks or build custom workflows through a visual drag-and-drop playbook editor with thousands of executable actions to address simple use cases as well as complex, custom ones. 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.

Standardize actions and reduce mean time to respond (MTTR) with Cortex XSOAR, enforcing processes across use cases and personnel with ease.

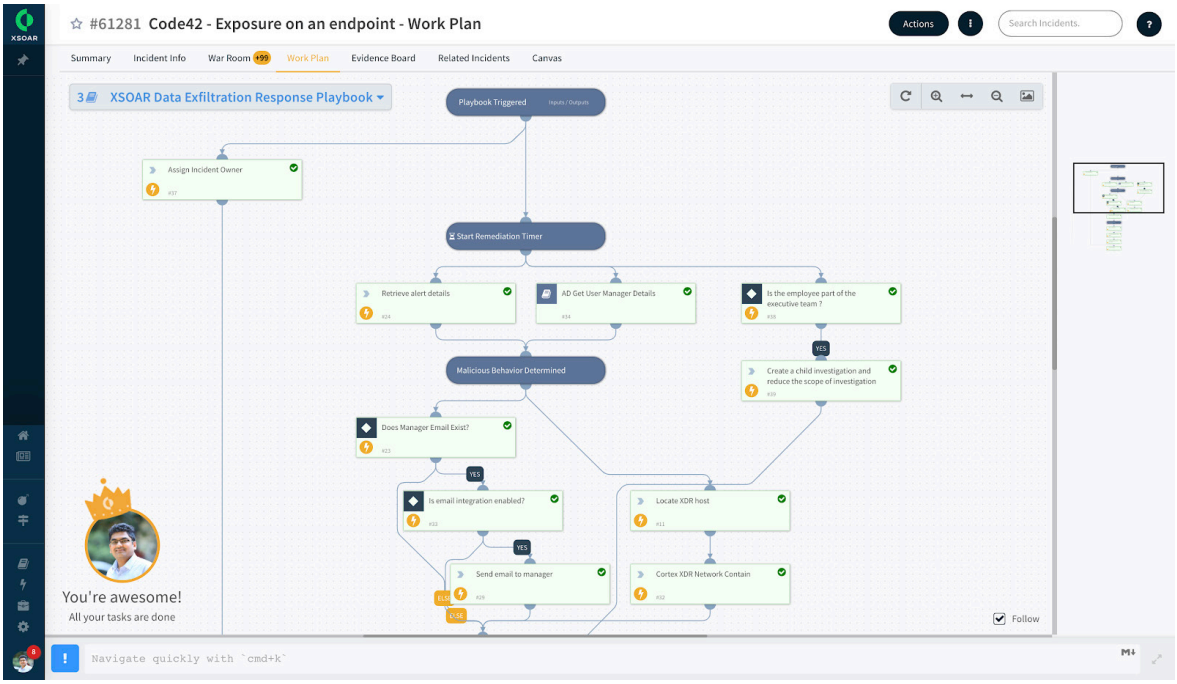

Figure 1: Cortex XSOAR playbook workflow visualization

Automation and Orchestration Across Hundreds of Tools

Orchestrate actions with Cortex XSOAR by bringing together disparate tools in analyst workflows for alert management, investigation, enrichment, response, threat hunting, and more. Thousands of automated actions are powered by hundreds of extensive product integrations across all types of security use cases, from incident response and threat hunting to network and cloud security. With Cortex XSOAR, security services can move at machine speed, automating incident resolution across tools with accuracy and scale while being flexible enough to codify where human interaction is required.

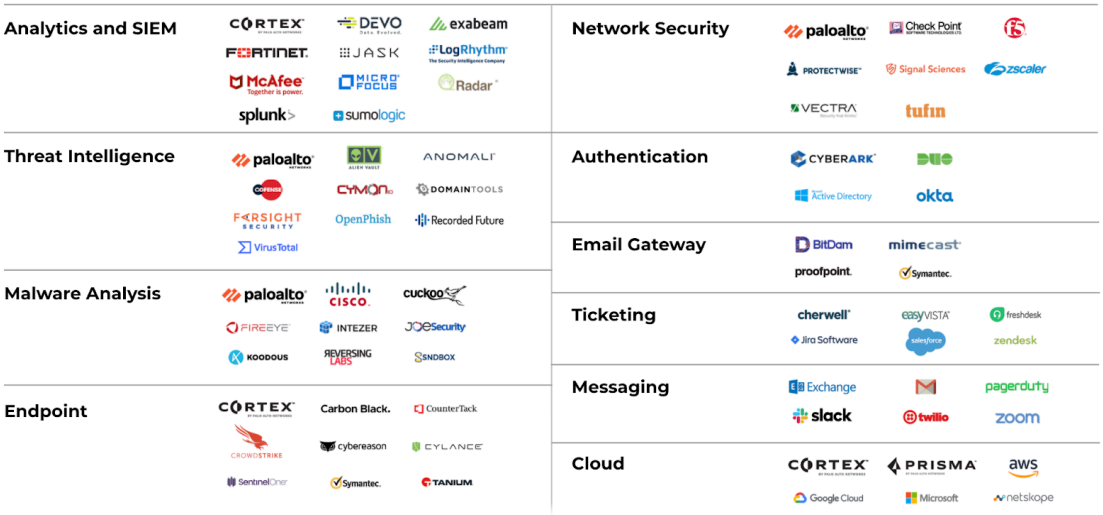

Figure 2: Some of the 370+ solutions integrated with Cortex XSOAR

Case Management

Cortex XSOAR has extensive security-focused case management capabilities built in for you to utilize when investigating and responding to incidents. For your pool of analysts, this makes managing incidents—from triage to investigation and response—easier than ever. Any analyst working an incident on behalf of a customer can quickly identify where the incident is in the investigation and response process so as not to miss or repeat crucial steps.

Collaboration and Learning

Collaboration among your analysts is key to effective incident management. Cortex XSOAR has built-in War Rooms for each incident created, providing a shared workspace where security analysts can chat with one another and conduct joint investigations. The War Room also enables third-party product actions to be executed in real time through a command-line interface (CLI), ensuring that you take advantage of your security product stack with minimal screen-switching and dead time.

All actions and commands are automatically documented in the War Room, preventing the need for manual post-incident documentation, where important information can fall through the cracks. The Cortex XSOAR War Room feature helps your analysts improve investigation quality and speed by working the way humans are meant to work: together. This ability is even more critical when you have large, globally dispersed teams of analysts working across dozens, hundreds, or even thousands of customers.

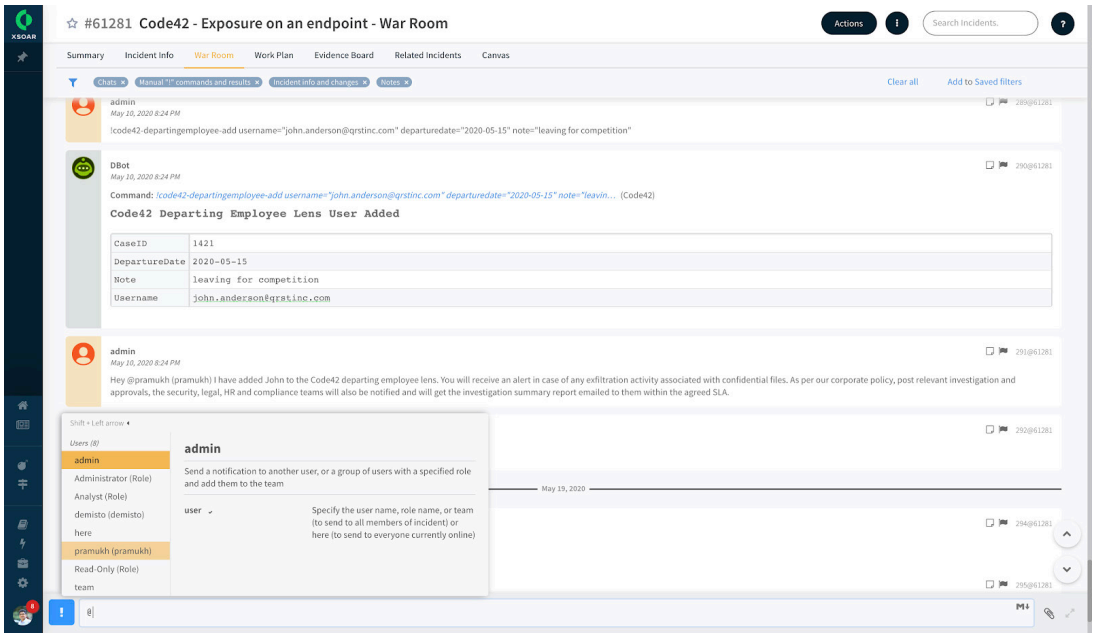

Figure 3: Collaboration and auto-documentation in a Cortex XSOAR War Room

The Cortex XSOAR Platform, Purpose-Built for MSSPs

Full Multitenancy

Cortex XSOAR offers complete data segmentation between customers in a single deployment. Customer data can be separated into individual hosts and tenants while you get a bird's-eye view of every tenant in a single master view. Full tenant separation—both data and processes—and extensive role-based access control (RBAC) provides granular control over customer data, ensuring ironclad security and privacy. You 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.

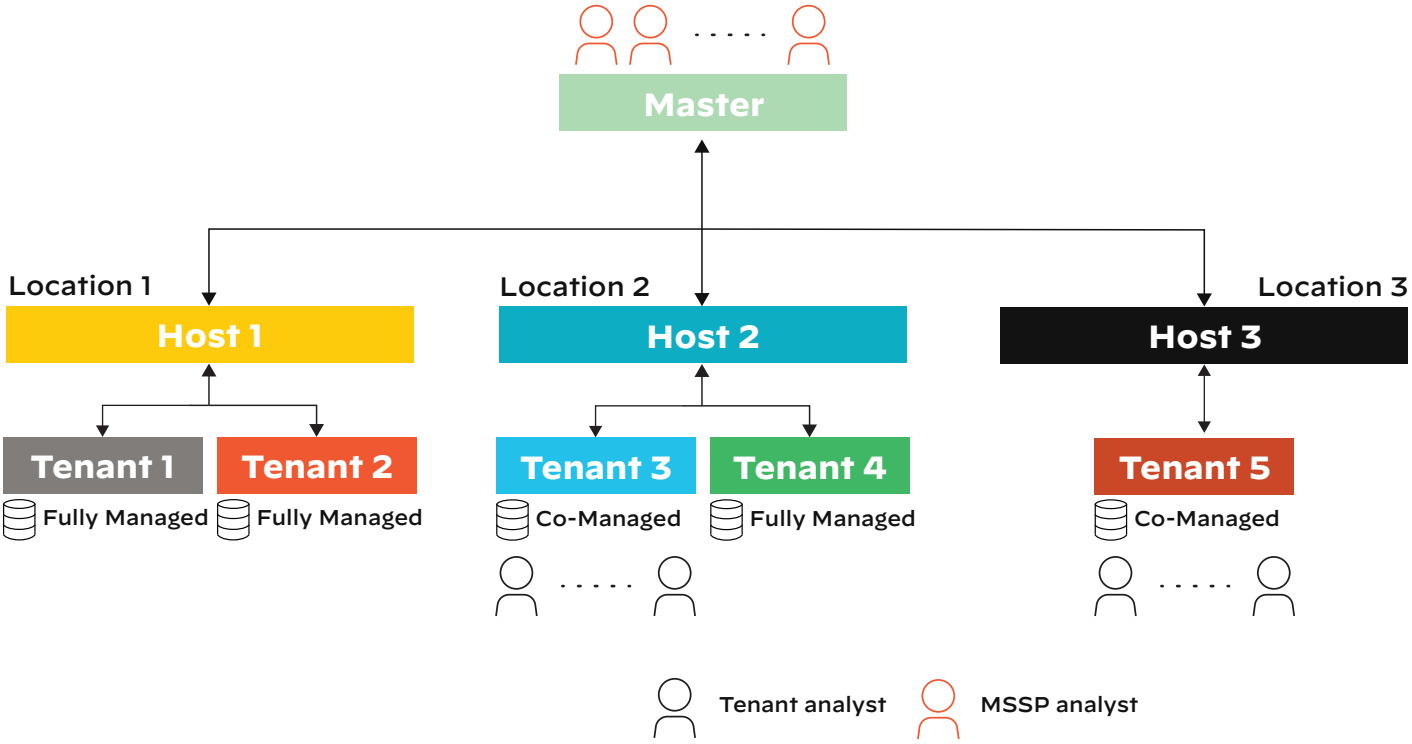

Figure 4: Cortex XSOAR multitenant architecture

Modular Playbooks

Cortex XSOAR has an easy-to-use visual playbook editor with numerous OOTB playbooks for specific use cases (e.g., vulnerability management). You can also build custom playbooks for specific services and service levels. Inside each playbook, analysts can "copy" tool actions for reuse in other playbooks at both the master and tenant levels for efficient scaling with new customer additions.

SLA and Team Performance Tracking

Customers demand reliable SLAs in the security services they purchase. Cortex XSOAR offers built-in SLA tracking capabilities to help you guarantee timely service outcomes to your customers. For example, you can trigger a notification—via Slack®, email, etc.—to your analyst team to handle a timely incident before an SLA breach.

Using machine learning, Cortex XSOAR can selectively place incidents with specific analysts based on previous performance for that alert or incident type. The virtual assistant learns from actions taken in the platform so that it can offer guidance on analyst assignments and commands to execute actions.

Extensive APIs

Many MSSPs have their own customer-facing portals for their services. Some such portals even have SOAR-like capabilities to aggregate data and facilitate analyst collaboration. You can leverage all the capabilities of Cortex XSOAR as a powerful backend automation and orchestration enabler for your services while maintaining existing customer-facing portals.

Threat Intel Management

Cortex XSOAR takes a new approach with native Threat Intel Management capabilities, unifying aggregation, scoring, and sharing of threat intelligence with playbook-driven automation. This vastly simplifies adding threat intelligence to any service to increase customer value. Threat intelligence feeds can be compiled at the master and tenant levels to cater to different customer types and use cases.

Cortex XSOAR Deployment

You can deploy Cortex XSOAR in one of two ways depending on your service delivery model.

One-to-One Model

In this model, you manage each customer separately. Both fully managed and co-managed are supported:

- Hosted by the customer, managed by the MSSP (on-premises)
- Hosted and managed by the MSSP (on-premises or cloud-delivered)

One-to-Many Model

In this model, you manage SOCs for many customers. This could represent a SOC shared by many customers or a dedicated SOC per customer. This model can also support fully managed vs. co-managed SOCs.

Table 1: Cortex XSOAR Managed Service Deployment Models

	Fully Managed		Co-Managed	
	Customer-Hosted	MSSP-Hosted	Customer-Hosted	MSSP-Hosted
One-to-One	Yes	Yes	Yes	Yes
One-to-Many	No	Yes	No	Yes

Horizontal Scalability for MSSPs

Cortex XSOAR multitenancy functionality enables you to run a single Cortex XSOAR instance on multiple hosts, with each host serving multiple tenants. This enables a single Cortex XSOAR multitenant server to serve many customers. Horizontal scalability allows your service to cater to large enterprise-grade environments, where additional hosts can be added to manage numerous tenants while keeping all functionality of the master instance intact.

Multitenancy deployment is also helpful for scenarios in which you are required to separate your customers into different groups, because you can manage access and deploy content centrally to the entire Cortex XSOAR deployment. As an example, for compliance reasons, you may host certain customers on a server that resides in a specific geographic location.

Cortex XSOAR Community Edition

To experience the capabilities of Cortex XSOAR, try the free Community Edition. With its included 30-day 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

cortex-xsoar-for-managed-security-service-providers-ds-071420