CORTEX XSOAR
BY PALO ALTO NETWORKS

Redefining Security Orchestration and Automation

Cortex™ XSOAR is a comprehensive security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration, and threat intelligence management to serve security teams across the incident lifecycle.

The New Pillars of a SOAR Platform

Security Orchestration

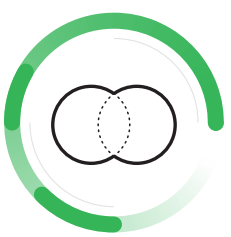
Respond to incidents with speed and scale

- Hundreds of integrations
- Thousands of automatable actions
- Visual playbook editor

Case Management

Ingest, search, and query ALL security alerts

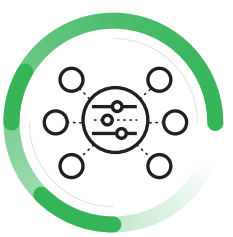
- Custom incident layouts
- Auto-documentation
- Dashboards and reports



Collaboration and Learning

Improve investigation quality by working together

- Virtual War Room
- Investigation canvas
- Machine learning



Threat Intel Management

Parse, manage, and act on threat intelligence

- Threat feed aggregation
- Granular indicator view
- Intel sharing and response

Select Customers

25% of the Fortune 500

Top worldwide online payment system

Fortune 50 healthcare organization

Fortune 100 athletic wear retailer

Online streaming and entertainment giant

SOAR Ecosystem

Platform
370+ integrations
Open, extensible platform

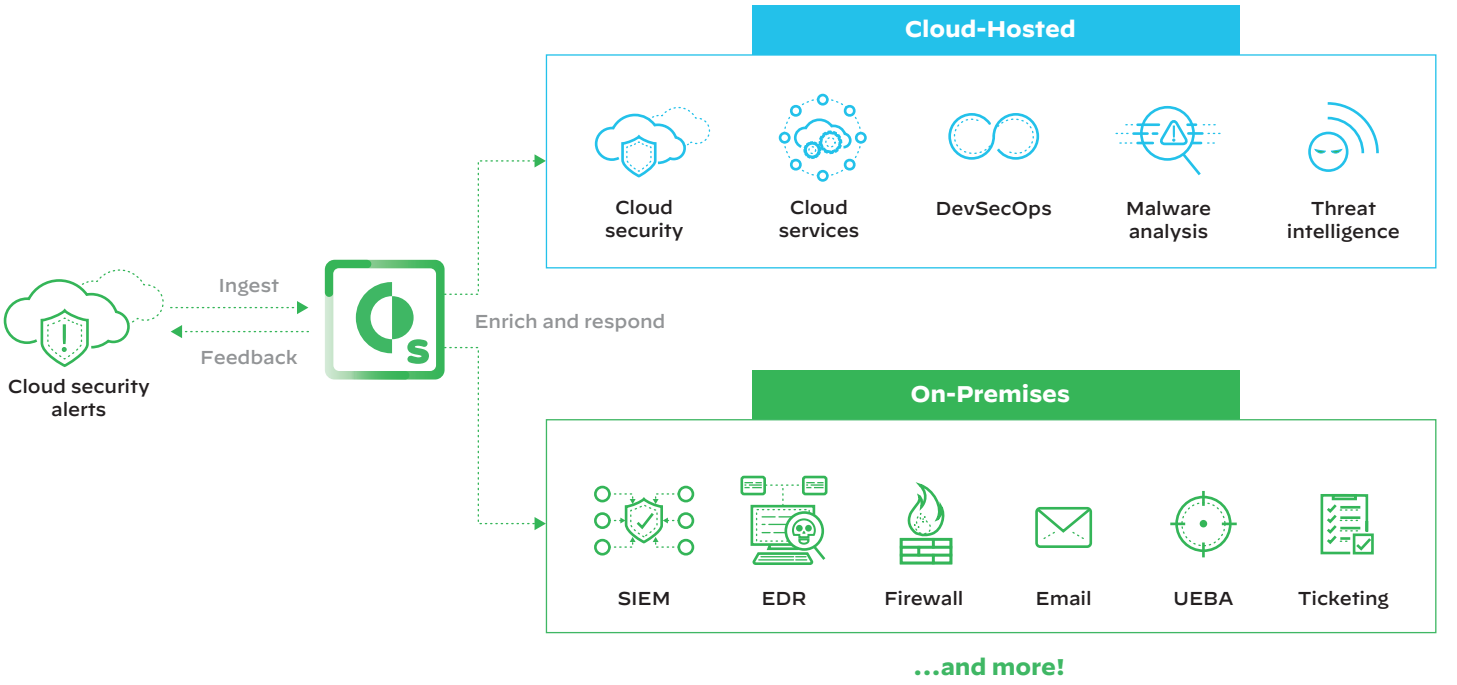
Community
13,000+ members (largest IR community in the industry)

Partners
100% Channel-friendly
MSSP and cloud ready

CORTEX XSOAR
BY PALO ALTO NETWORKS

Cortex XSOAR for Cloud Security

Cloud security demands agility and flexibility in the face of an expanded threat surface and disparate teams. Cortex XSOAR primes users for fast and standardized cloud security through multi-source ingestion of cloud data and playbooks that coordinate and automate incident response actions across cloud and on-premises environments.



Automate Repeatable Steps

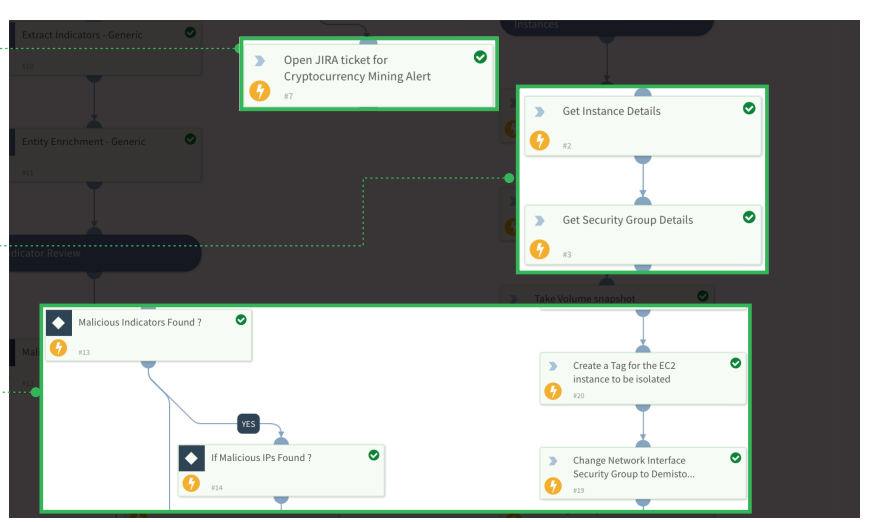
Automate actions to standardize and scale incident response

Unify Security Functions

Gather intelligence from multiple products on a single console

Orchestrate Cloud Security

Ingest alerts from your cloud environment and trigger automated workflows that span products



CORTEX XSOAR
BY PALO ALTO NETWORKS

Case Study: The Pokémon Company International

Goals

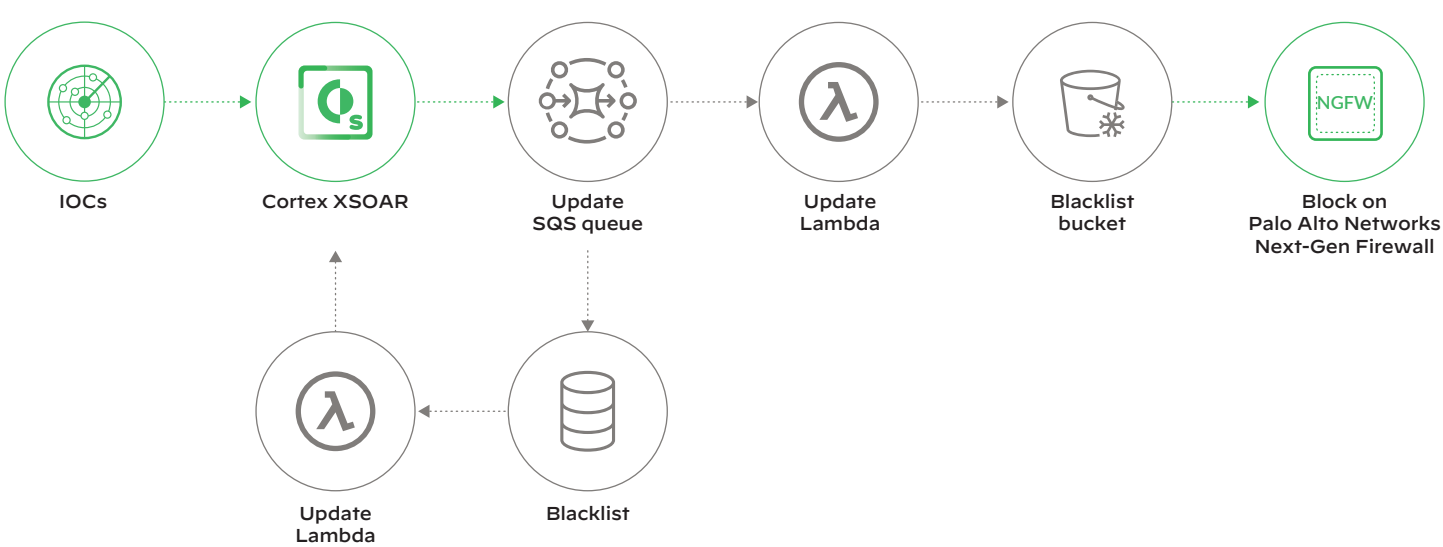
- Keep pace with rapidly scaling cloud environment
- Automate everything that humans don't need to do
- Provide value to other technology departments

Use Cases

- EC2 and account compromise
- Phishing enrichment and response
- Employee offboarding

Use Case Deep Dive

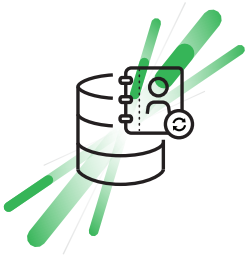
As part of the phishing response playbook that The Pokémon Company deployed, Cortex XSOAR automated extraction of IOCs before pushing those IOCs to blacklists across both cloud and on-premises environments.



CORTEX XSOAR
BY PALO ALTO NETWORKS

How Cortex XSOAR Deploys

Cortex XSOAR can be deployed both on-premises and as a cloud-hosted offering, adapting to customer requirements as the need arises. The platform is also primed with native multitenancy for managed security service providers (MSSPs) that scales horizontally, provides three layers of isolation, and maintains data integrity while simplifying communication across tenants.

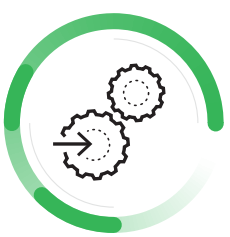


Customer on-premises server

Customer virtual or cloud

Hosted SaaS

Illustrative Integrations: Cloud Security



Hundreds of integrations

Thousands of actions

Open and extensible platform

Amazon/AWS

- Amazon Athena
- Amazon CloudWatch Logs
- Amazon DynamoDB
- Amazon EC2
- Amazon GuardDuty
- Amazon Route 53
- Amazon S3
- AWS Access Analyzer
- AWS ACM
- AWS CloudTrail
- AWS IAM
- AWS Lambda
- AWS Security Hub

Microsoft/Azure

- Azure Compute
- Azure Feed
- Azure Security Center
- Microsoft Active Directory
- Exchange Web Services
- Microsoft Graph Calendar
- Microsoft Graph Groups
- Microsoft Graph Mail
- Microsoft Graph Security
- Microsoft Teams
- Microsoft Server

Google Cloud

- Google Apps API
- Google BigQuery
- Google Chronicle
- Google Cloud Compute
- Google Cloud Storage
- Google Cloud Translate
- Google Docs
- Google Gmail
- Google Key Management
- Google Resource Manager
- Google Safe Browsing
- Google Vault
- Google Vision AI

Other

- Prisma Cloud by Palo Alto Networks
- Cisco CloudLock
- Cisco Stealthwatch Cloud
- CloudShark
- Mimecast
- Netskope
- Okta
- Skyformation
- Zscaler