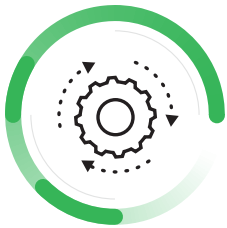


Redefining Security Orchestration and Automation

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

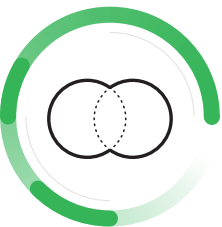
Custom incident layouts



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



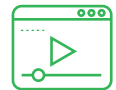
Fortune 50
healthcare organization



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)



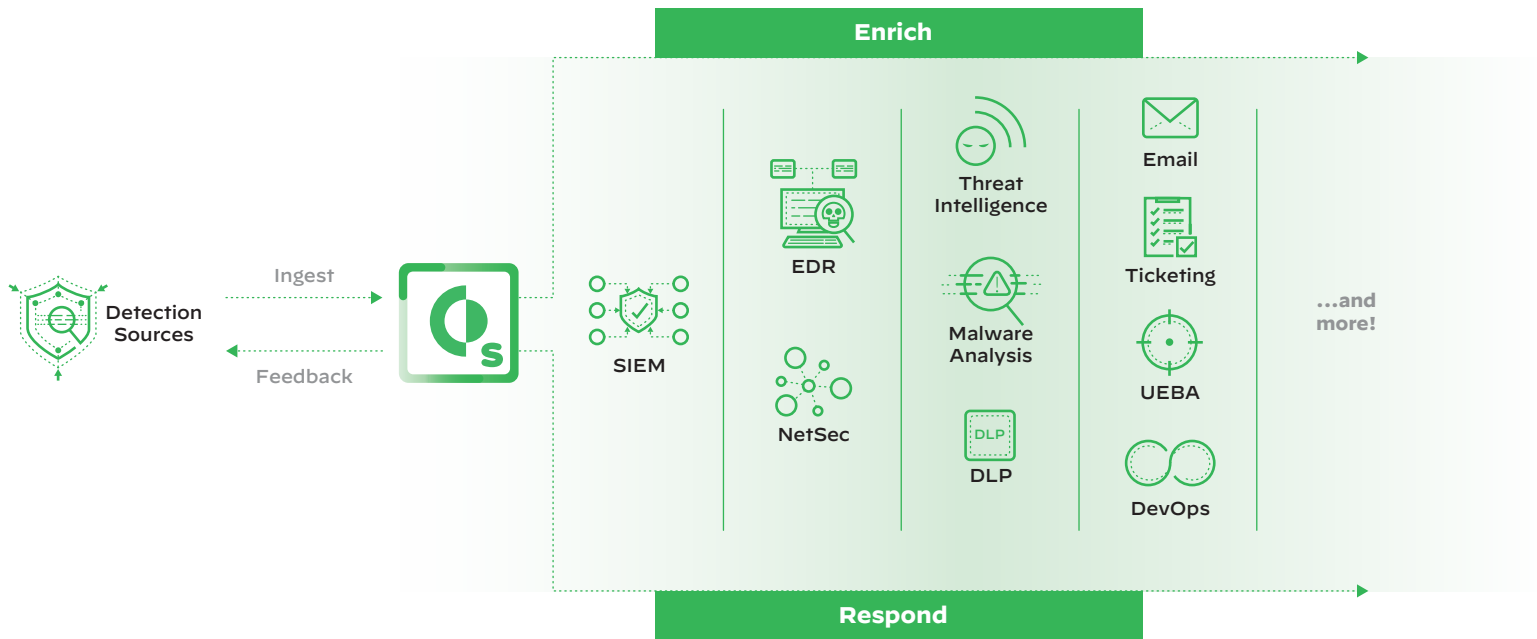
Partners 100%
Channel-friendly

MSSP and cloud ready





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.



How Cortex XSOAR Helps

- 

Improve Investigation Quality •
Use a collaborative workspace, machine learning and cross-correlations
- 

Automate Repeatable Steps •
Automate actions to standardize and scale incident response
- 

Unify Security Functions •
Gather intelligence from multiple products on a single console

