# Cortex XSOAR and Devo

## Automated SOC Operations

### Benefits

Together, Cortex XSOAR and the Devo Data Analytics Platform enable you to:

- Quickly detect, enrich, and analyze threats with Devo, and then react with playbook-driven response
- Shorten investigation time and increase decision-making efficacy by automating key tasks in the analyst review cycle
- Reduce unnecessary churn with a single platform for triage, investigation, collaboration, and incident documentation

### Compatibility

Cortex XSOAR, Devo Data Analytics Platform

## Overview

Security operations teams often deploy a multitude of security tools to keep pace with constantly changing threat and data landscapes. With so many tools, teams often waste time chasing data from disparate sources and performing repetitive tasks. Security operations centers (SOCs) need to equip their teams with rich, correlated data and automate repeatable tasks so their analysts have the time and energy they need for incident resolution.

SOC teams can now leverage the security orchestration and automation capabilities of Cortex™ XSOAR with the Devo Data Analytics Platform.

## Integration Features

The integration between Cortex XSOAR and the Devo Data Analytics Platform lets you:

- Hunt and investigate indicators of compromise (IOCs) in Devo and leverage Cortex XSOAR playbooks to automate and manage analyst response.
- Automatically enrich all your security data and detect threats in real time with Devo, and trigger automated workflows and response with Cortex XSOAR.
- Leverage hundreds of Cortex XSOAR third-party product integrations to coordinate response across security functions based on insights from Devo.
- Run hundreds of commands (including for Devo) interactively via a ChatOps interface while collaborating with other analysts and the Cortex XSOAR chatbot.

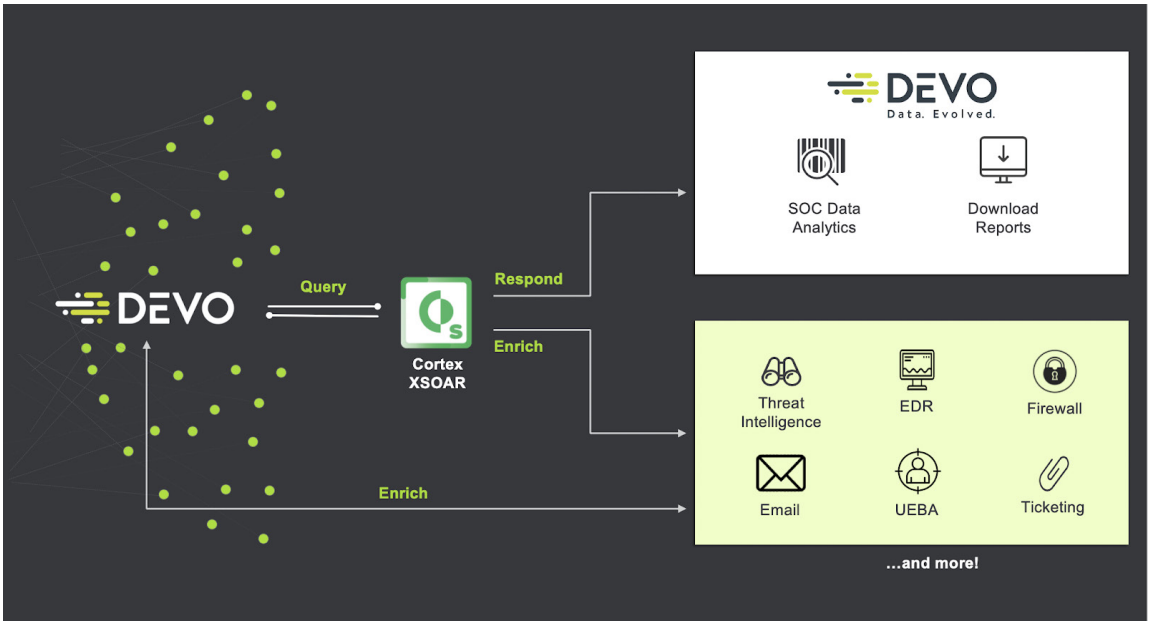


**Figure 1:** Cortex XSOAR and Devo Data Analytics Platform

## Use Case No. 1: Automate Incident Enrichment and Response

### Challenge

If a SOC uses different solutions for security analytics and incident response, fragmented information and lack of central documentation can make it difficult to track the lifecycle of an incident. Instead, analysts are stuck completing low-level tasks and manually building workflows rather than quickly resolving incidents.

### Solution

SOCs can use the Devo Data Analytics Platform for high-volume and high-velocity data correlation, enrichment, and visualization alongside Cortex XSOAR Enterprise for security task orchestration and automation to trigger playbooks at incident creation. These playbooks will orchestrate response actions across the entire stack of products for a single, analyst-focused, seamless workflow. For example, analysts can create tickets, quarantine endpoints, retrieve PCAPs, and send emails as automated playbook tasks.

### Benefit

Devo's context-rich, real-time security data analytics coupled with Cortex XSOAR playbooks speed up incident triage and resolution. A seamless workflow enables analysts to gain a comprehensive view of an incident's lifecycle, access all documentation in a single platform, and more rapidly take investigative and response actions with automated insight.

## Use Case No. 2: Conduct Interactive, Real-Time Forensics for Complex Threats

### Challenge

While automated playbooks can reduce analyst workloads, a forensic investigation usually requires additional tasks, such as pivoting across multiple data views to gather critical evidence, drawing relationships between different incidents, and defining remediation steps. Analysts need full access to all their security data, with context, to make accurate and rapid decisions.

### Solution

After running playbooks, analysts can gain greater visibility and new, actionable insights into the attack by running Devo commands in the Cortex XSOAR War Room to draw on all security data, context, and threat intelligence. The War Room will document all analyst actions and suggest the most effective analysts and command sets with time.

### Benefit

The War Room allows analysts to quickly pivot on all security data in Devo and run unique commands relevant to incidents in their network, all from a single window. All participating analysts have full task-level visibility into the process and can run as well as document commands from the same window. Auto-documentation of all automation and analyst actions allows reports to be generated quickly for executive review or post-investigation debriefs.

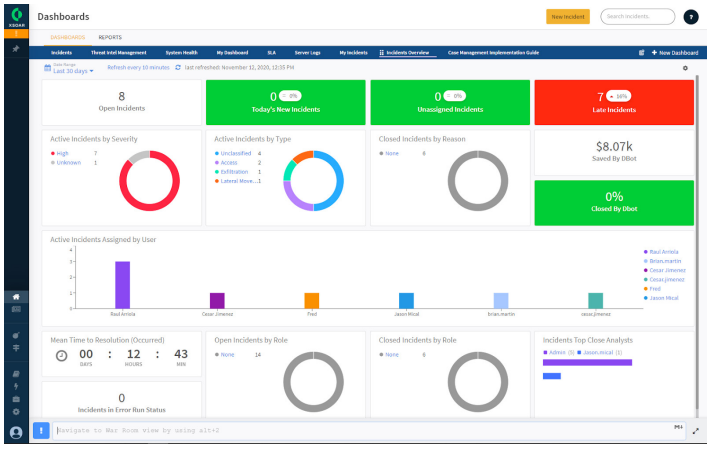


**Figure 2:** Devo securely passes data and analytics to Cortex XSOAR to facilitate automated responses

## About Devo Security

Devo unlocks the full value of machine data for the world's most instrumented enterprises, putting more data to work—now. Only the cloud-native Devo Data Analytics Platform addresses both the explosion in volume of machine data and the new, crushing demands of algorithms and automation. This enables IT operations and security teams to realize the full transformational promise of machine data to move businesses forward. Learn more at devo.com/siem.

## About Cortex XSOAR

Cortex XSOAR is the only security orchestration, automation, and response (SOAR) platform that combines security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit paloaltonetworks.com/cortex/xsoar.

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