# Devo Security Operations

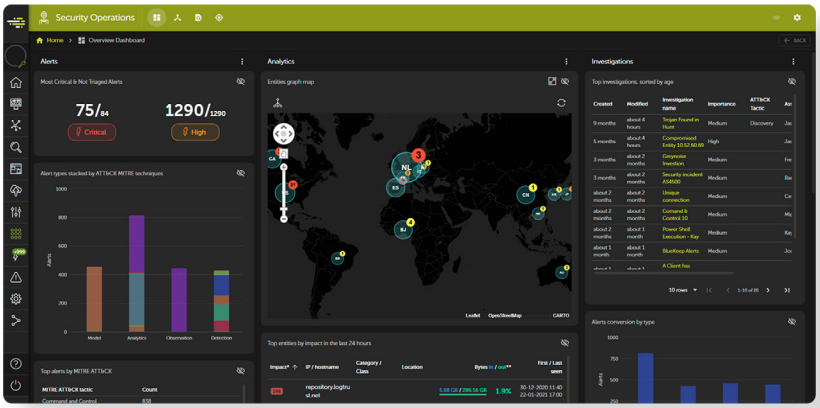
## Empower the SOC to detect, investigate and hunt in real time

SOLUTION BRIEF

### INTRODUCTION

As more workloads migrate to the cloud, the attack surface continues to grow, and cyberattackers become more sophisticated, security teams struggle to monitor and analyze an ever-increasing volume of data so they can quickly distinguish real threats from numerous false positives.

Legacy tools simply cannot address these security challenges. Fortunately, Devo Security Operations, a next-gen cloud SIEM, empowers your SOC team to defend your organization against cyberattacks by closing the visibility gap so analysts can detect and investigate cyberthreats more effectively and efficiently.




*At-a-glance security monitoring information available via the Overview Dashboard*

### BRING TOGETHER ALL SECURITY-RELEVANT DATA FOR FULL VISIBILITY — WITHOUT COMPROMISE

Security teams face the challenging dilemma of choosing which data to send to their SIEM. Data sources are abundant, but legacy SIEM capabilities and organizational budgets are limited. Organizations that cannot centralize all their data handicap their security analysts' ability to investigate and respond to cyberthreats swiftly and decisively.

Powered by the cloud-native Devo Platform, Devo Security Operations delivers the performance required for petabyte-scale data ingestion and analysis. The Devo Platform enables your team to ingest data in any format from all sources — on-cloud or on-prem — and retain it always hot for 400 days. This closes the visibility gap that puts your organization at risk. Devo's flexible, all-inclusive SaaS license enables your organization to ingest relevant security data to build more use cases without exceeding your budget.

### OVERCOME ALERT FATIGUE WITH HIGH-FIDELITY ALERTING

With Devo, your security team is well-positioned to detect threats fast and get ahead of adversaries. Alerts in Devo Security Operations monitor active queries on specific events and trigger real-time notifications when the alert conditions are met. From there, analysts can triage alerts efficiently with just one click to automatically group them according to entity or alert type, sort and filter alerts using their preferred method, and save their view for future use.

Security Operations is powered by the Devo Content Stream, Devo's content delivery service. The Content Stream arms security teams with continuously updating high-value content, including curated alerts and threat intelligence. With more than 100 out-of-the-box alerts, the Security Operations Content Manager makes it easy for analysts to select which alerts to install and deploy.


*Devo Content Stream provides instant access to threat intelligence and pre-built alerts*

When out-of-the-box won't cut it, your analysts can easily create complex chained alerts for advanced threat detection and configure them with the Alert Creation Wizard, an intuitively guided process that doesn't require code. With the wizard, analysts can create consistent, high-quality alerts and then see the related queries and test the alerts before deployment.

A combination of ready-to-deploy and customized alerts provides organizations with ample coverage against lesser-known or previously unseen threats, and several machine-learning models also help identify suspicious behaviors from unknown threats. With Devo Security Operations your SOC team will improve your security posture and continue to adapt quickly to the ever-evolving threat landscape.

## JUMP-START AND STREAMLINE THREAT INVESTIGATIONS TO MAXIMIZE SOC PRODUCTIVITY

Security is a team sport and Devo Security Operations enables security teams to collaborate and communicate effortlessly. Analysts receive notifications from tools such as email, Slack and Jira when they are assigned to an alert or an investigation. To ensure a smooth handoff from one analyst or team to the next, the comprehensive investigation timeline makes it easy for analysts to access a detailed list of actions, enrichments and comments that piece together an investigation story no matter who has worked on it.

Analysts also can recover valuable time to focus on high-priority security tasks by leveraging Security Operations' automation capabilities to triage alerts. Security Operations automatically triages alerts based on severity and the entities involved, which enables analysts to determine if they should create a new investigation or update a related existing investigation.

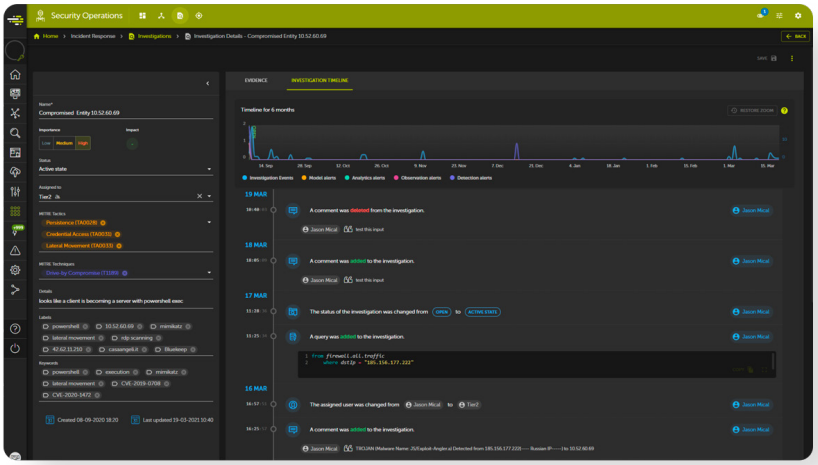
Another key feature of Security Operation is Entity Analytics, which provides valuable context for analysts. One Entity Analytics capability is the Entity Battlecard that ties together valuable data points, such as entity impact score and the alerts, investigations and enrichments associated with the entity. It also provides visual representations that show the connectedness between entities and the outcomes of several machine-learning models.

Once the investigation is completed and it's time to respond, Security Operations' bidirectional integration with your SOAR of choice enables SOAR playbook execution to complete and the investigation status to remain in sync in Security Operations.

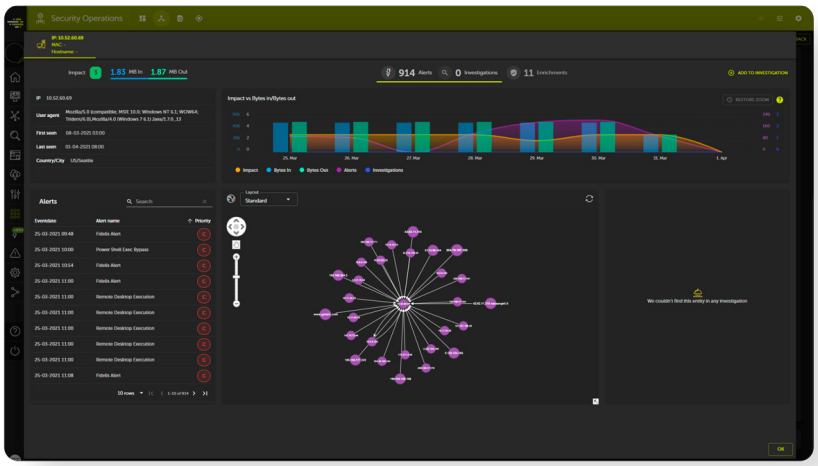
## MAKE CONFIDENT DECISIONS WITH THE NECESSARY CONTEXT, WHILE ELIMINATING REPETITIVE TASKS

An indicator of compromise is only a small piece of the threat puzzle. You need relevant context on threats that target your company, industry and geography to see the bigger picture and enable fast, effective mitigation. To make that possible, Security Operations automatically enriches your data with threat intelligence in the Content Stream or using third-party threat-intelligence feeds.

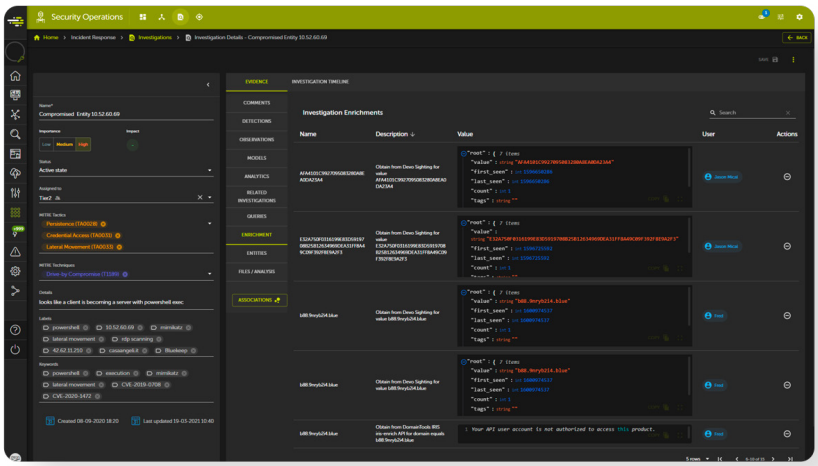
Additionally, Devo Security Operations eliminates manual and repetitive tasks with automatic enrichments from other common data sources including, but not limited to, EDR, NTA, identity context, active directory, configuration management database, access privileges, and vulnerability context. Other enrichments include priority scoring, MITRE ATT&CK labels, custom SOC taxonomy, and entity impact. With Devo's open ecosystem and agnostic approach to integrations, you can use our API to integrate your existing security tools and achieve unified security while maximizing your investments.




*Comprehensive investigation timeline for improved team collaboration*




*Detailed Entity Analytics displayed in the Entity Battlecard for analysis*




*Automated enrichments from third-party integrations for context*

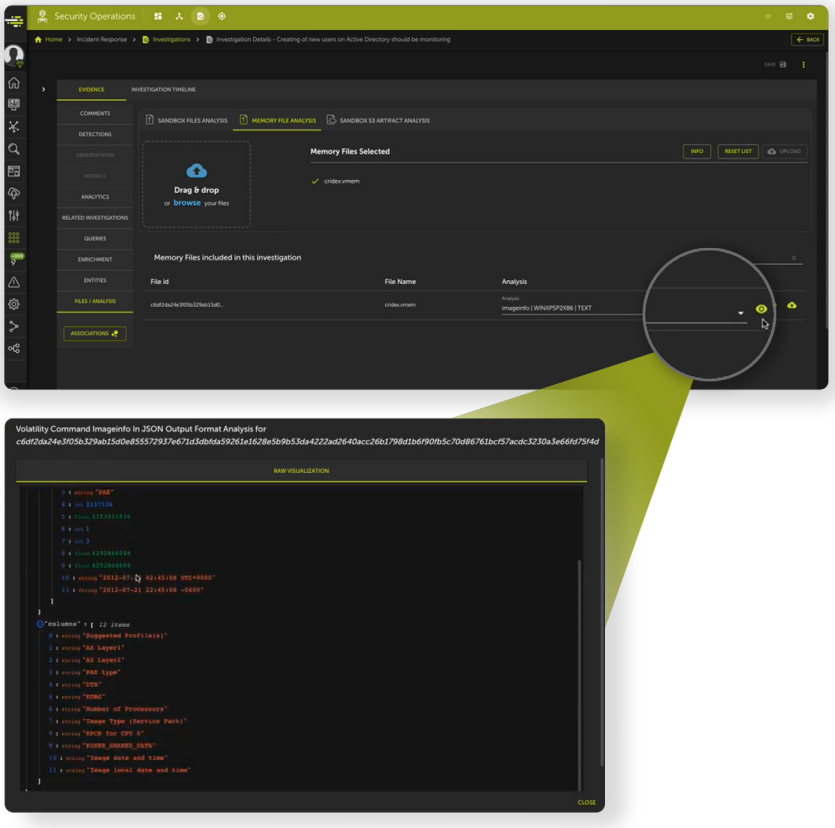
With automated enrichments, Devo Security Operations simplifies and accelerates investigations by adding context to alerts and investigations to give analysts the full picture of the situation so they can make confident triage and response decisions to reduce attacker dwell time and minimize impact.

## PROACTIVELY HUNT FOR THREATS ACROSS ALL DATA AND IDENTIFY ADVANCED THREATS WITH FORENSIC ANALYSIS

The Devo Hunting Workbench enables threat hunters to run queries across any volume of data, any number of sources, and any time horizon, applying multiple filter criteria to proactively identify threats. The Hunting Workbench offers different modes of hunting including multi-table search, query replay, and an expert mode.

Threat-hunting teams also can automate investigation retrospection to search for indicators of compromise that have been associated with a specific threat. This capability parses and matches indicators of compromise against threat intelligence; if a match is found, Security Operations automatically runs queries across additional data sources to check if the indicator exists elsewhere. Any new information uncovered during these searches is added to a new or existing investigation.

Security Operations also enables experienced analysts to conduct sophisticated forensic analyses and add the results as evidence to investigations, these include packet capture (pcap) analysis and malware sandbox analysis. The newest capability, memory forensic analysis, enables analysts to upload memory files to a new or ongoing investigation and initiate forensic analysis to detect sophisticated file-less malware, all from a single, easy-to-use UI.




*Memory forensic analysis from the Devo UI*

As threat actors and their attack methods become increasingly intricate, the demand for more sophisticated threat-hunting and analysis tools will increase. With Devo Security Operations the most experienced analysts in your SOC will have the tools and resources they need to expedite the investigation and analysis of those suspicious indicators of compromise and help mitigate the risk advanced threats pose to your organization.

**Are you ready to learn more about Devo Security Operations?**
**Contact your sales representative to schedule a demo or visit Devo.com.**

**Devo**
255 Main Street
Suite 702
Cambridge, MA 02142



Devo is the only cloud-native logging and security analytics platform that releases the full potential of your data to empower bold, confident action. With unrivaled scale to collect all of your data without compromise, speed to give you immediate access and answers, and clarity to focus on the signals that matter most, Devo is your ally in protecting your organization today and tomorrow. Devo is headquartered in Cambridge, Mass. Learn more at **www.devo.com**.