DEMISTO
A PALO ALTO NETWORKS® COMPANY

DEVO

Automated SOC Operations

Benefits

- Detect, enrich and analyze threats with Devo and 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

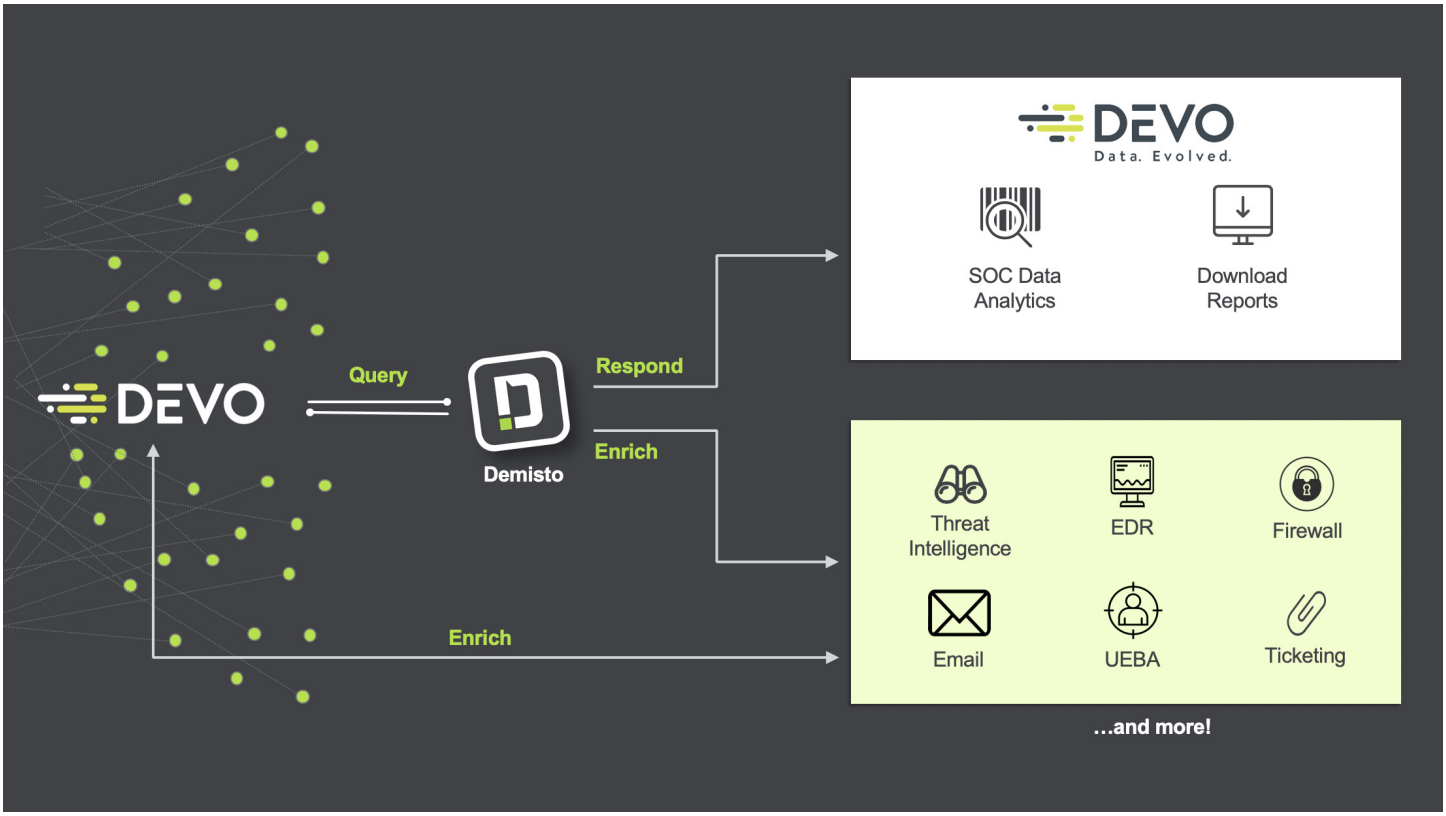
- Products: Demisto Enterprise, Devo Data Analytics Platform

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

Users can now leverage Demisto's security orchestration and automation capabilities with Devo's real-time, context-rich data insights for efficient incident response.

Integration Features:

- Hunt and investigate IOCs in Devo and leverage Demisto playbooks to automate and manage analyst response.
- Enrich all your security data and detect real-time threats with Devo and trigger automated workflows and response with Demisto.
- Leverage hundreds of Demisto third-party product integrations to coordinate response across security functions based on insights from Devo.
- Run 100s of commands (including for Devo) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED INCIDENT ENRICHMENT AND RESPONSE

Challenge: If SOCs use different solutions for security analytics and incident response, it can be tough to track the lifecycle of an incident due to fragmented information and lack of central documentation. Instead, analysts are stuck completing low-level tasks and manually building the workflow rather than quickly resolving an incident.

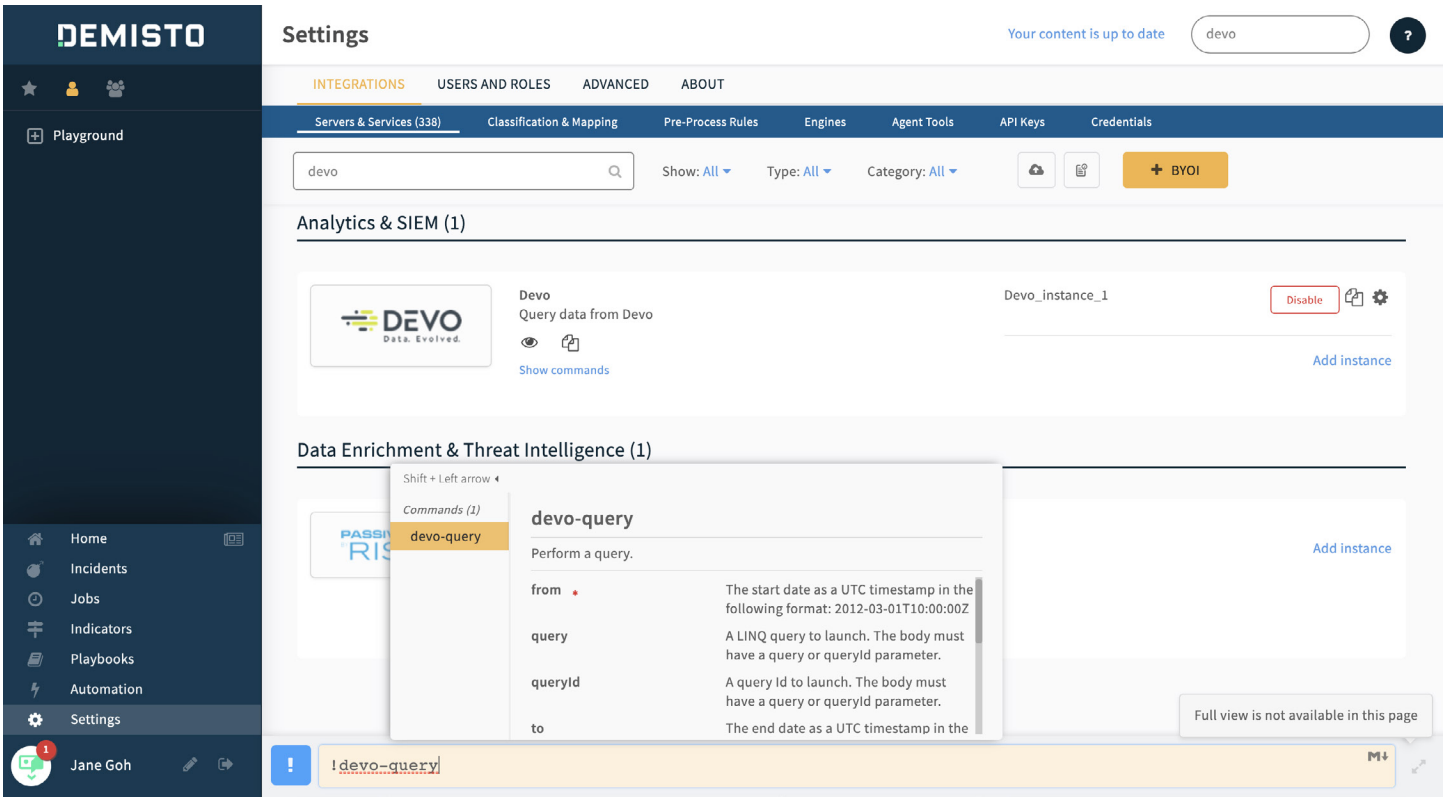
Solution: SOCs can use Devo for high-volume, high-velocity data correlation, enrichment and visualization, and Demisto Enterprise for security task orchestration and automation to trigger playbooks at incident creation. These playbooks will orchestrate response actions across the entire stack of products for a single 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 Demisto playbooks speed incident triage and resolution. The seamless workflow enables analysts to gain a comprehensive view of the incident's lifecycle, access all documentation in a single platform and speed investigative and response actions through automated insight.

USE CASE #2 INTERACTIVE, REAL-TIME FORENSICS OF 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 of their security data, with context, to enable them to make accurate and rapid decisions.

Solution: After running playbooks, analysts can then gain greater visibility and new, actionable insights into the attack by running Devo commands in the Demisto 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, from a single window. All participating analysts will have full task-level visibility into the process and be able to run and document commands from the same window.
Auto-documentation of all automation and analyst actions allow for reports to be generated quickly for executive review or post-investigation debriefs.

About Devo

Devo unlocks the full value of machine data for the world's most instrumented enterprises, putting more data to work now. Only the Devo data analytics platform addresses both the explosion in volume of machine data and the new, crushing demands of algorithms and automation, enabling enterprises to realize the full transformational promise of machine data to move the business forward. Visit www.devo.com to learn more.

About Demisto

Demisto, a Palo Alto Networks company, 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 Demisto, 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 www.demisto.com.