DEMISTO | JASK

Automate Security Operations

Benefits

- Ingest rich, correlated data from JASK into Demisto for automated playbook-driven response.
- Enrich JASK data with intelligence from other security products with Demisto's orchestration.
- Lessen dead time by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

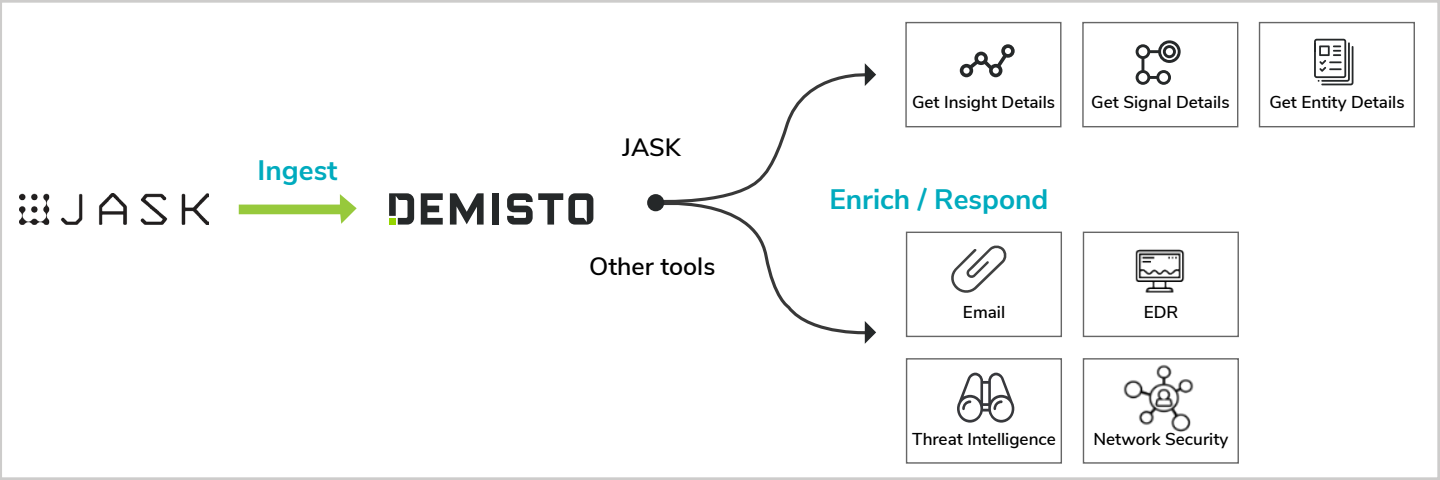
- Products: Demisto Enterprise, JASK
- Platform: Platform independent

New forms of sophisticated cybersecurity threats are continually emerging to target enterprises by utilizing multiple attack vectors and entry points. In this environment, security teams often waste time collecting data from disparate sources and performing repeatable tasks while the attack continues to engulf the system. SOCs need security tools that enable analysts with rich, correlated data, and automate repeatable tasks so that analysts have the time and energy they need for incident resolution.

Users can now leverage Demisto's security orchestration and automation capabilities with JASK's AI-driven security operations capabilities for efficient and accelerated incident response.

Integration Features

- Ingest insights from JASK to create incidents in Demisto and trigger automated triage, enrichment, and response.
- Search for specific JASK insights, signals, and entities from within Demisto.
- Access JASK entity whitelists, related entities, and riskiest entity details for deeper investigations in Demisto.
- Leverage hundreds of Demisto product integrations to enrich insights from JASK and coordinate response across security functions.
- Run 1000s of commands (including for JASK) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

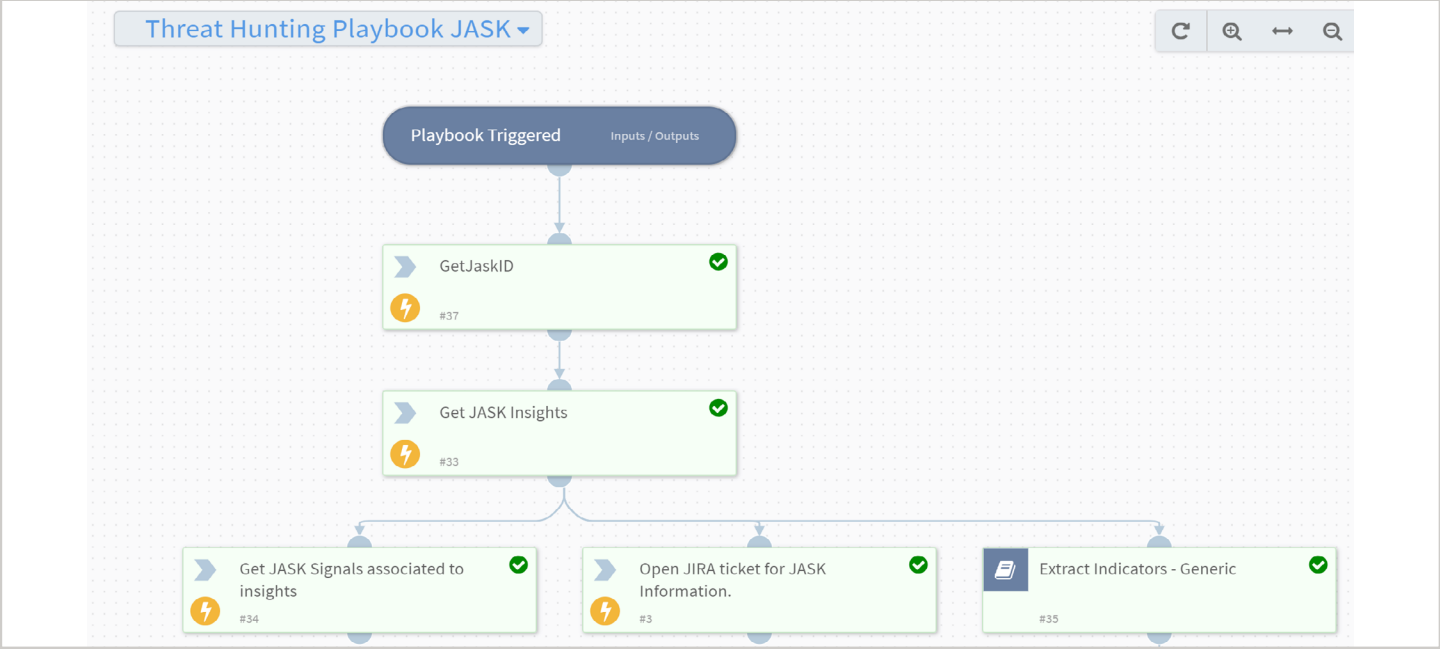


USE CASE #1 AUTOMATED INSIGHT INGESTION, ENRICHMENT, AND RESPONSE

Challenge: If SOCs use different solutions for data/log enrichment and incident response, it can be tough to track the lifecycle of an incident due to flitting between screens, fragmented information, and lack of single-window documentation. Analysts spend time completing low-level tasks that can be better spent resolving the incident.

Solution: If SOCs use JASK for data enrichment and Demisto Enterprise for security orchestration and automation respectively, they can automate incident creation in Demisto for each insight type in JASK. They can also trigger playbooks to execute upon incident creation. These playbooks will orchestrate enrichment and response actions across the entire stack of products that a SOC uses in a single screen and seamless workflow.

For example, analysts can create tickets, quarantine endpoints, retrieve pcaps, and send emails as automatable playbook tasks.

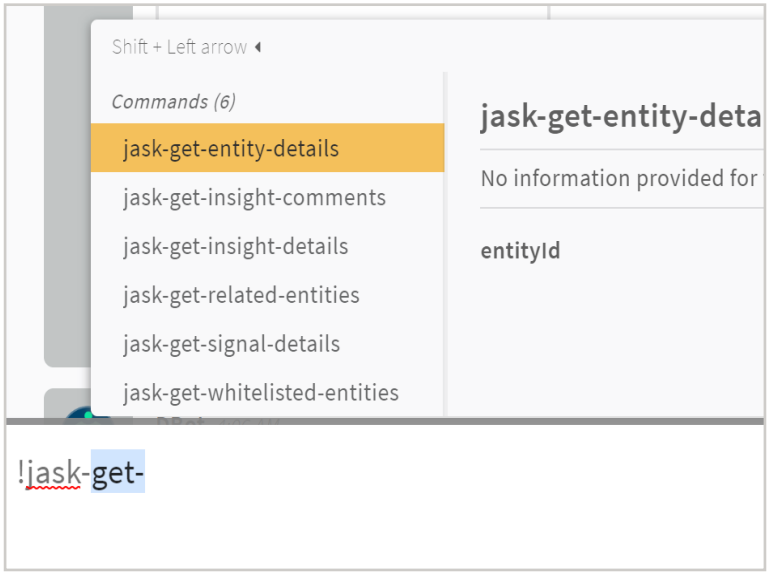


Benefit: JASK's rich data coupled with Demisto playbooks can speed up incident triage and resolution. Analysts can get a comprehensive view of the incident's lifecycle, access documentation from a single source, and forego the need to switch between screens while performing investigation actions.

USE CASE #2 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: While standardized, repeatable playbooks can automate commonly performed tasks to ease analyst load, an attack investigation usually requires additional tasks such as pivoting from one suspicious indicator to another to gather critical evidence, drawing relations between incidents, and finalizing resolution. Running these commands traps analysts in a screen-switching cycle during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts can then gain greater visibility and new actionable information about the attack by running JASK commands in the Demisto War Room. For example, if playbook results throw up signal details from JASK, analysts can get a list of records related to that signal and access entity whitelists by running the respective JASK command. Analysts can also run commands from other security tools in real-time using the War Room, ensuring a single-console view for end-to-end investigation.



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 and run unique commands relevant to incidents in their network from a common window. All participating analysts will have full task-level visibility of the process and be able to run and document commands from the same window. They will also prevent the need for collating information from multiple sources for documentation.

About Demisto

Demisto is the only Security Orchestration, Automation and Response (SOAR) Platform that combines orchestration, incident management and interactive investigation into a seamless experience. Demisto's orchestration engine automates security product tasks and weaves in human analyst tasks and workflows. Demisto Enterprise, powered by its machine learning technology, acquires knowledge from the real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and best next steps for investigations. The platform (and you) get smarter with every analyst action. For more information, visit www.demisto.com or email info@demisto.com.

About JASK

JASK is modernizing security operations to reduce organizational risk and improve human efficiency. Through technology consolidation, enhanced AI and machine learning, the JASK Autonomous Security Operations Center (ASOC) platform automates the correlation and analysis of threat alerts, helping SOC analysts focus on highest-priority threats, streamlining investigations and delivering faster response times. To learn more,visit https://jask.com.