DEMISTO | CROWDSTRIKE

Automated Endpoint Protection, Threat Intelligence, and Malware Analysis

Benefits

- Unify endpoint protection, threat intelligence, and malware analysis processes through task-based playbooks.
- Eliminate dead time by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

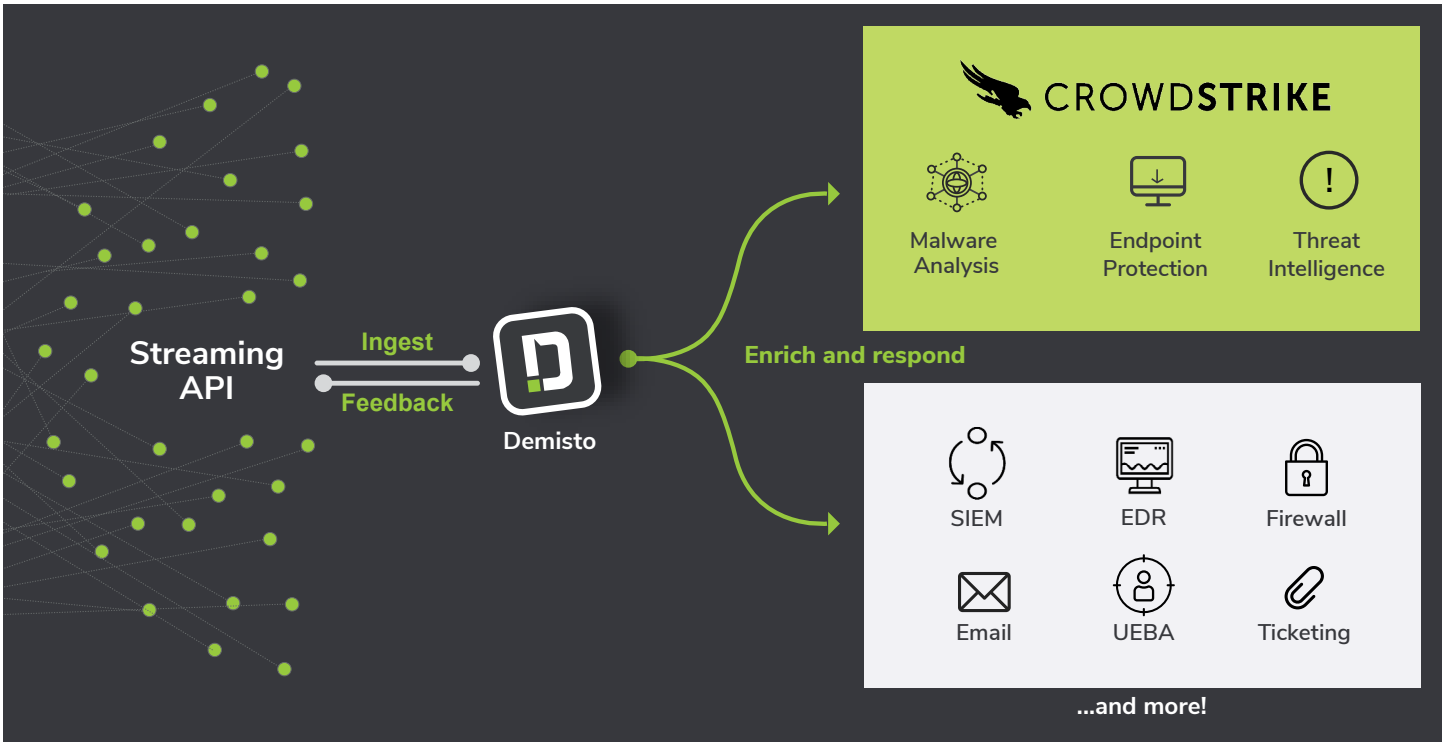
- Products: Demisto Enterprise, CrowdStrike Falcon X, Crowd Strike Falcon Sandbox, Crowd Strike Falcon Endpoint Protection
- Platform: Platform independent

New forms of sophisticated cybersecurity threats continually emerge to target enterprises utilizing multiple attack vectors. In this environment, understanding attack components, responding quickly, monitoring endpoint vitals, and ensuring continuous compliance become vital. Analysts need a tool stack that enables complete visibility over critical systems and endpoints and also drives scalable response that straddles across security functions.

Joint users can use Demisto's deep integrations with multiple CrowdStrike solutions – Falcon Sandbox, Falcon X, Falcon Streaming, and Falcon Endpoint Protection – to coordinate and automate actions through standardized task-based workflows. Users can unify context and activate response procedures across security functions, reduce response times through automation, and improve investigation quality through central collection and correlation of data.

Integration features:

- Ingest CrowdStrike events into Demisto through the Streaming API and trigger playbooks for standardized response.
- Obtain threat intelligence from CrowdStrike Falcon X within Demisto, either as automated playbook tasks or through real-time execution.
- Get IOC and device information from CrowdStrike Falcon Endpoint Protection within Demisto, either as automated playbook tasks or through real-time execution.
- Execute CrowdStrike Sandbox malware analysis and obtain reports within Demisto.
- Leverage hundreds of Demisto product integrations to enrich CrowdStrike events and coordinate response across security functions.
- Run thousands of commands (including for CrowdStrike) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

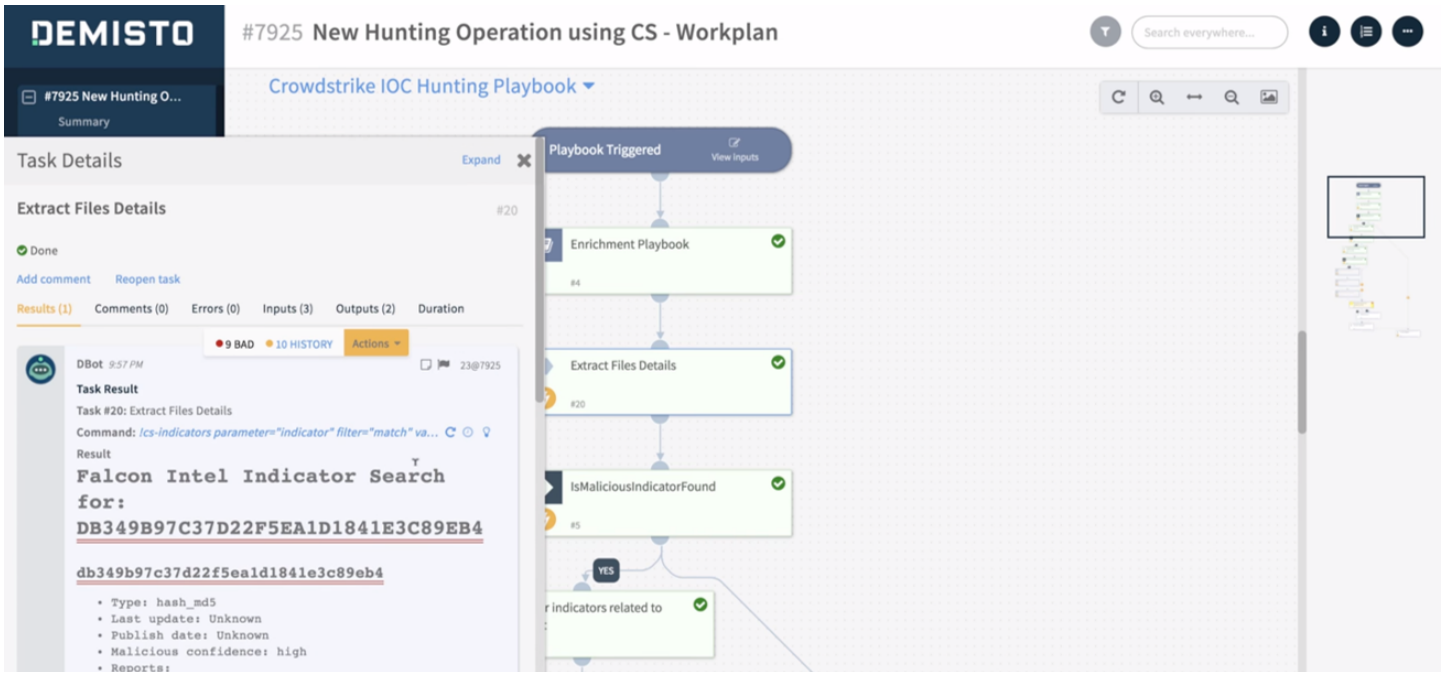


USE CASE #1 AUTOMATED ENDPOINT PROTECTION AND INCIDENT RESPONSE

Challenge: If SOCs use different solutions for endpoint protection, malware analysis, and threat intelligence, it can be tough to track the lifecycle of incident response due to flitting between screens, fragmented information, and lack of single-window documentation.

Solution: SOCs that use the CrowdStrike Falcon platform and Demisto Enterprise can automate incident creation and trigger playbooks in Demisto after ingesting events via the CrowdStrike Streaming API. This playbook can orchestrate enrichment and enforcement actions across the entire stack of products that a SOC uses in a single screen and seamless workflow.

For example, analysts can leverage Falcon X to obtain threat intelligence, Falcon Sandbox to perform malware analysis, and Falcon Endpoint Protection to search for device and IOC details as automatable playbook tasks.

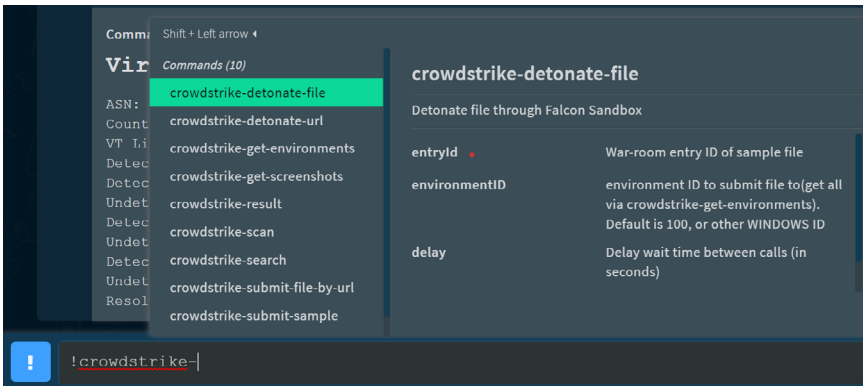


Benefit: Demisto playbooks help unify the capabilities of multiple CrowdStrike products in a single workflow, standardizing and speeding up triage and resolution of alerts. Analysts get a comprehensive view of the incident's lifecycle, access documentation from a single source, and forego the need to switch between screens while performing investigation actions.

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

Challenge: Standardized processes are not enough for responding to every security alert. Apart from running automated actions, attack investigations usually require additional real-time 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 gain greater visibility and new actionable information about the attack by running CrowdStrike commands in the Demisto War Room. For example, after a Demisto playbook gets an event through the Streaming API, analysts can get additional context in real time by running commands such as **cs-device-details** and **crowdstrike-submit-url** with relevant arguments to get device details and submit URLs for analysis respectively.



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 that coordinates across the product stack. 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 environment 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 a unified console. 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 security orchestration, incident management, and interactive investigation to serve security teams across the incident lifecycle. Our orchestration engine coordinates and automates tasks across 100s of partner products, resulting in an increased return on existing security investments. Demisto enables security teams to reduce Mean Time to Response (MTTR), create consistent incident management processes, and increase analyst productivity. For more information, visit www.demisto.com or follow @demistoinc on Twitter.

About CrowdStrike

CrowdStrike is the leader in next-generation endpoint protection, threat intelligence and response services. The CrowdStrike Falcon™ platform stops breaches by preventing and responding to all attacks type – both malware and malware-free. Only Crowdstrike unifies next-generation antivirus with EDR (endpoint detection and response), backed by 24/7 proactive threat hunting – all delivered via the cloud.