DEMISTO | netskope

Automated Cloud Security Incident Response

Benefits

- Orchestrate cloud security ingestion, enrichment, and response actions through playbooks.
- Reduce time to resolution by using one platform to collaborate, investigate, and document.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

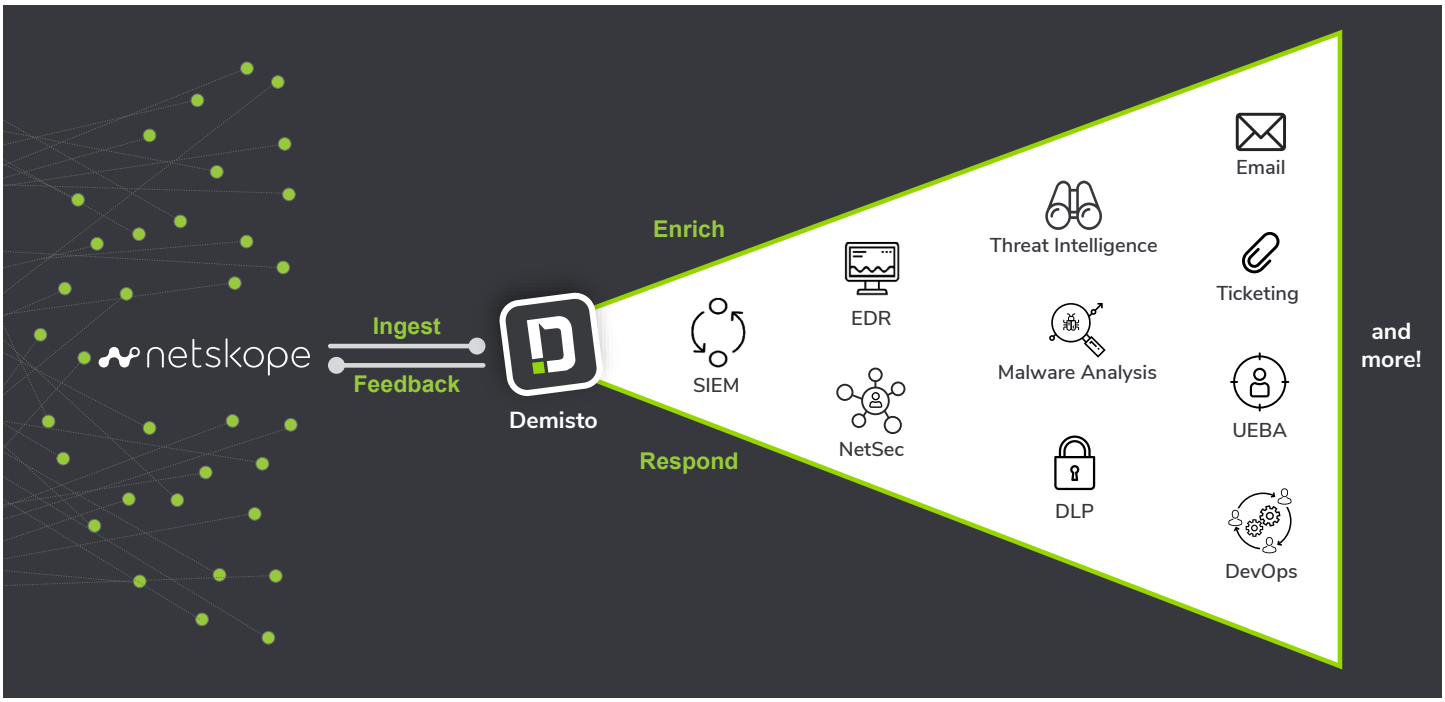
- Products: Demisto Enterprise, Netskope Security Cloud
- Platform: Platform independent

Mobile and cloud have changed the way organizations work, making it easier to collaborate, manage projects, and develop products at scale. However, this decentralization of computing power has brought with it security challenges. Mobile apps and cloud tools often use APIs to bypass organizational perimeters, which can have a profound impact on information integrity and confidentiality. There's a need to standardize cloud security procedures and interweave them with other security processes to curtail new-age attacks.

Users can now leverage the cloud visibility, data security, and threat protection capabilities of Netskope with the security orchestration and automation features of Demisto Enterprise for repeatable and scalable cloud security incident response that dovetails with other organizational security measures.

Integration features:

- Ingest Netskope alert data into Demisto to create incidents in Demisto and trigger playbooks tied to those incidents.
- Automate enrichment of alerts as playbook tasks: get associated events and logs with an alert, get indicator reputation, perform file analysis, and so on.
- Leverage hundreds of Demisto product integrations to further enrich Netskope alerts and coordinate response across security functions.
- Run thousands of commands (including for Netskope) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED ENRICHMENT AND RESPONSE TO CLOUD SECURITY INCIDENTS

Challenge: If cloud security consoles are isolated from other functions such as EDR, malware analysis, and threat intelligence, it becomes time-consuming and repetitive for security analysts to cross-reference alerts from cloud security tools, get further context, and coordinate containment and response. Processes diverge depending on the analyst that handles the incident, and this leads to differing response quality.

Solution: Analysts can use the Netskope integration to ingest alert data, create incidents in Demisto, and trigger standard, automated playbooks for that incident. These playbooks can enrich the alert with more event detail from Netskope as well as coordinate across other products to extract wider context without the need for screen switching and manual repetition.

Analysts can use the Netskope integration to ingest alert data, create incidents in Demisto, and trigger standard, automated playbooks for that incident. These playbooks can enrich the alert with more event detail from Netskope as well as coordinate across other products to extract wider context without the need for screen switching and manual repetition.

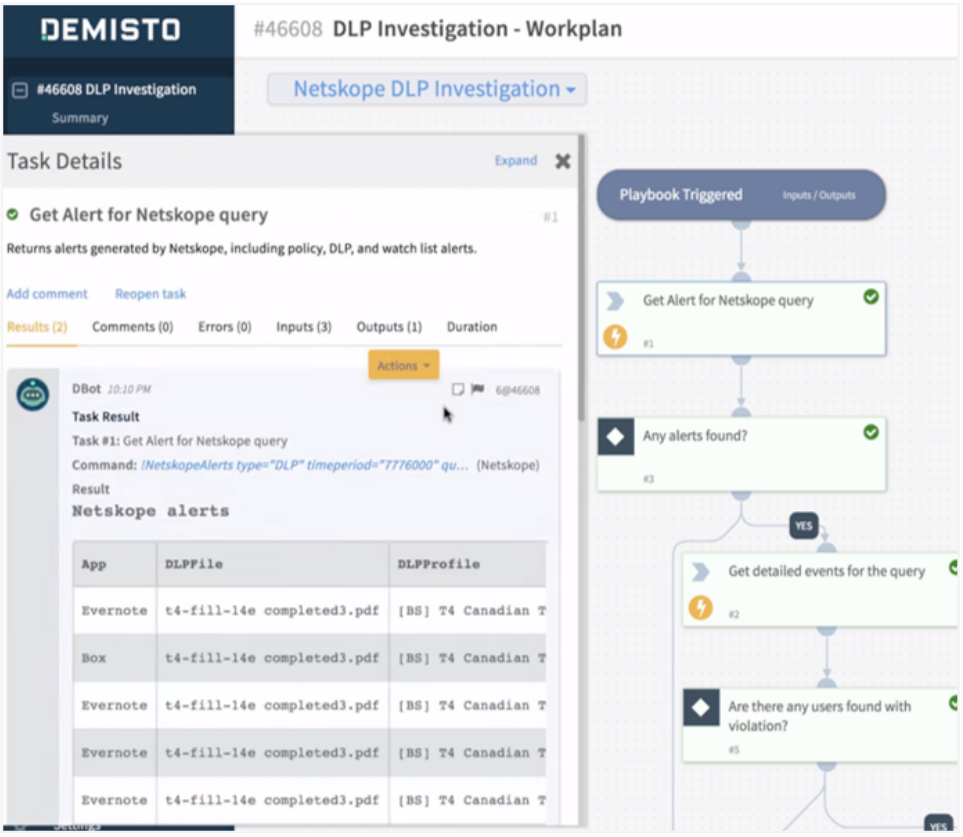
Benefit: Enrichment playbooks automate a host of actions across products so that analysts have a wealth of information at their fingertips while starting incident investigation. Automating Netskope lookups can save screen switching time and orchestrating other product actions in the same window can help analysts look across security functions for richer and deeper incident context.

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 Netskope commands in the Demisto War Room. For example, if playbook results throw up an alert and associated details, analysts can get the list of applications exposed by that alert in real-time by running the respective Netskope 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 Netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

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 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.