DEMISTO | VECTRA

Automated Breach Detection and Response

Benefits

- Harness rich, aggregated network intelligence from Vectra Cognito in Demisto for automated, playbook-driven response.
- Further enrich Vectra Cognito data with intelligence from other security tools via Demisto's orchestration.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

- Products: Demisto Enterprise, Vectra Cognito

Security teams face unique challenges in today's data-heavy landscape with sophisticated attackers and vast threat surfaces. Separating insights from noise, battling a growing number of alerts sans enrichment, and coordinating between multiple security products all weigh heavily on the security analyst's mind.

Users can now leverage the **intrusion detection and response capabilities** of the Cognito Platform from Vectra with the **security orchestration and automation features** of Demisto Enterprise for repeatable and scalable threat response that dovetails with other organizational security measures.

Integration Features

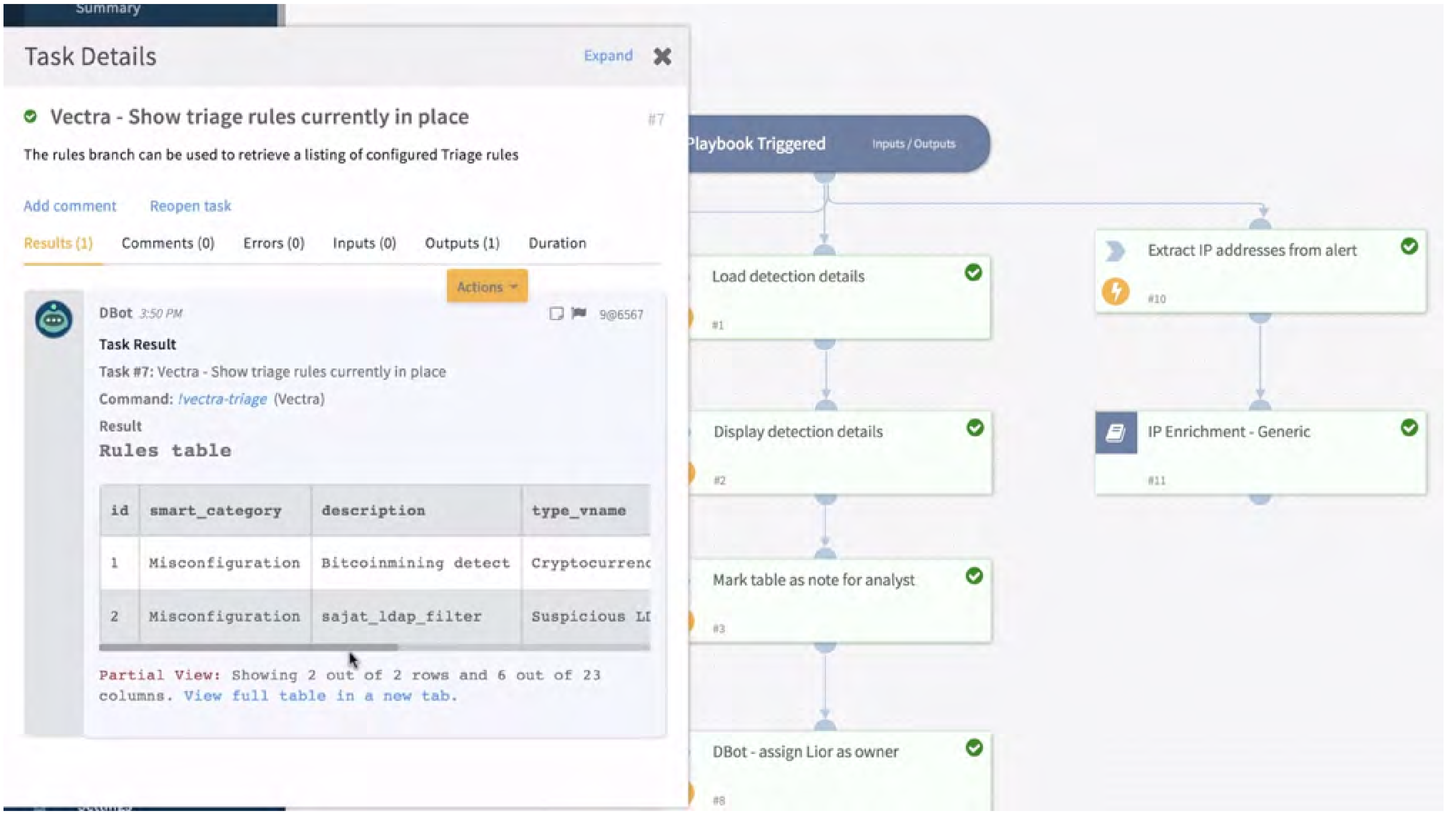
- Ingest Vectra Cognito alert data into Demisto to create incidents in Demisto and trigger playbooks tied to those incidents.
- Automate enrichment of alerts as playbook tasks: get associated sensors and health configuration with alerts, get detection and host details, retrieve listings of triage rules, and so on.
- Leverage hundreds of Demisto product integrations to further enrich Cognito alerts and coordinate response across security functions.
- Run 1000s of commands (including for Vectra Cognito) inter actively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.

USE CASE #1 AUTOMATED ENRICHMENT AND RESPONSE TO NETWORK SECURITY THREATS

Challenge: If threat detection 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 various 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 Vectra Cognito 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 details from Cognito as well as coordinate across other products to extract wider context without the need for screen switching and manual repetition.

For example, a playbook could check the detection details and health configurations tied to a Cognito alert, retrieve triage rules, extract indicator reputation using threat intelligence tools, and send automated mails to the affected users.



Vectra - Show triage rules currently in place #7

The rules branch can be used to retrieve a listing of configured Triage rules

DBot *3:50 PM* 9@6567

Task Result

Task #7: Vectra - Show triage rules currently in place

Command: *!vectra-triage* (Vectra)

Result

Rules table

id	smart_category	description	type_vname
1	Misconfiguration	Bitcoinmining detect	Cryptocurrenc
2	Misconfiguration	sajat_ldap_filter	Suspicious LI

Partial View: Showing 2 out of 2 rows and 6 out of 23 columns. View full table in a new tab.

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 Cognito queries and lookups can save screen switching time and orchestrating other product actions in the same window can help analysts look across security functions for richer, 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 then can gain greater visibility and new actionable information about the attack by running Vectra Cognito commands in the Demisto War Room. For example, if playbook results throw up an alert and associated details, analysts can get the list of hosts and sensors exposed by that alert in real-time by running the respective Cognito commands. 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 real-life analyst interactions and past investigations to help SOC teams with analyst assignment suggestions, playbook enhancements, and the 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.