DEMISTO | cisco Cisco Umbrella

Automated Threat Intelligence and Response

Benefits

- Harness rich, aggregated threat intelligence from Cisco Umbrella Investigate in Demisto for automated, playbook-driven response.
- Further enrich Cisco Umbrella Investigate 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, Cisco Umbrella Investigate

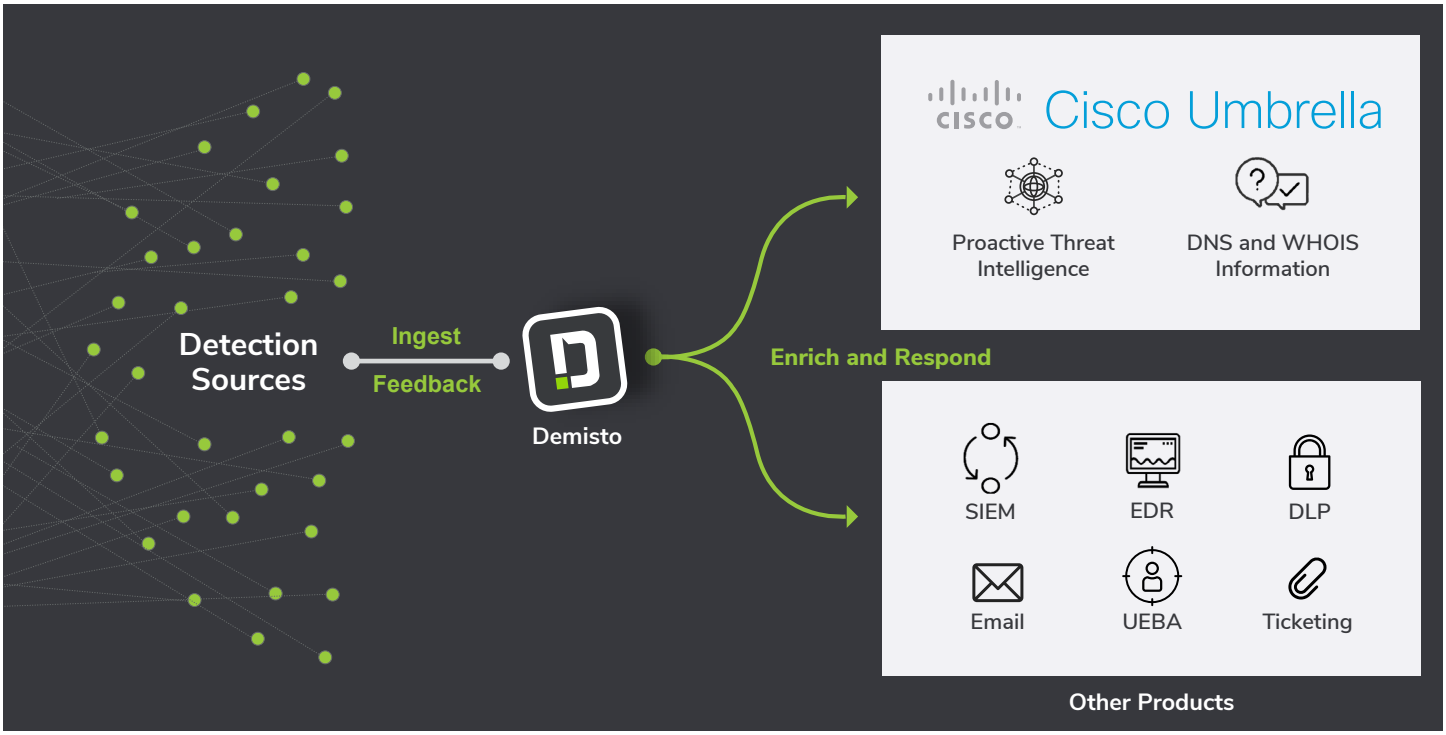
The agility and frequency of today's security attacks mean that security teams are too busy responding to the current threat to predict any future attacks that might occur. While attackers execute different malware and phishing emails with time, they often use the same underlying infrastructure (web servers and IPs), creating cyber fingerprints. Security teams can use these fingerprints for attacker identification, but don't have enough time because they're dealing with rising alert volumes, manual actions, and unconnected products. Security teams need a platform that can provide proactive threat intelligence across sources and harness that information to drive response across security environments.

To meet these challenges, users can combine the comprehensive threat intelligence of Cisco Umbrella Investigate with the security orchestration and automation features of Demisto to improve threat visibility and accelerate incident response.

Integration features

- Obtain domain reputation from Cisco Umbrella Investigate within Demisto as an automated task.
- Search for domain details in Cisco Umbrella Investigate using regular expressions within Demisto to access related domains, classifiers, DNS history, co-occurrences, and more.
- Get domain, IP, and URL timelines from Cisco Umbrella Investigate within Demisto.
- Get malicious domains and DNS information for an IP address from Cisco Umbrella Investigate within Demisto, either as an automated task or in real-time.
- Leverage hundreds of Demisto product integrations to further enrich Cisco Umbrella Investigate data and coordinate response across security functions.

- Run thousands of commands (including for Cisco Umbrella Investigate) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED THREAT ENRICHMENT AND RESPONSE

Challenge: The disparate nature of threat intelligence and incident response tools can make it tough for SOC teams to track the lifecycle of an incident due to moving between screens, fragmented information, and the lack of single-window documentation. Incident response will also often involve a host of important but repetitive actions that analysts need to perform, not leaving them with enough time for actual problem-solving and decision-making.

Solution: SOCs using Cisco Umbrella Investigate for threat intelligence and Demisto Enterprise for security orchestration and incident response respectively can automate alert enrichment through Demisto playbooks. These playbooks will receive indicator intelligence from Cisco Umbrella Investigate and use that information to execute actions across the entire stack of products that a SOC uses.

For example, analysts can leverage the Cisco Umbrella Investigate integration to get domain reputation, DNS information, WHOIS data, and IP timelines as automatable playbook tasks within Demisto.

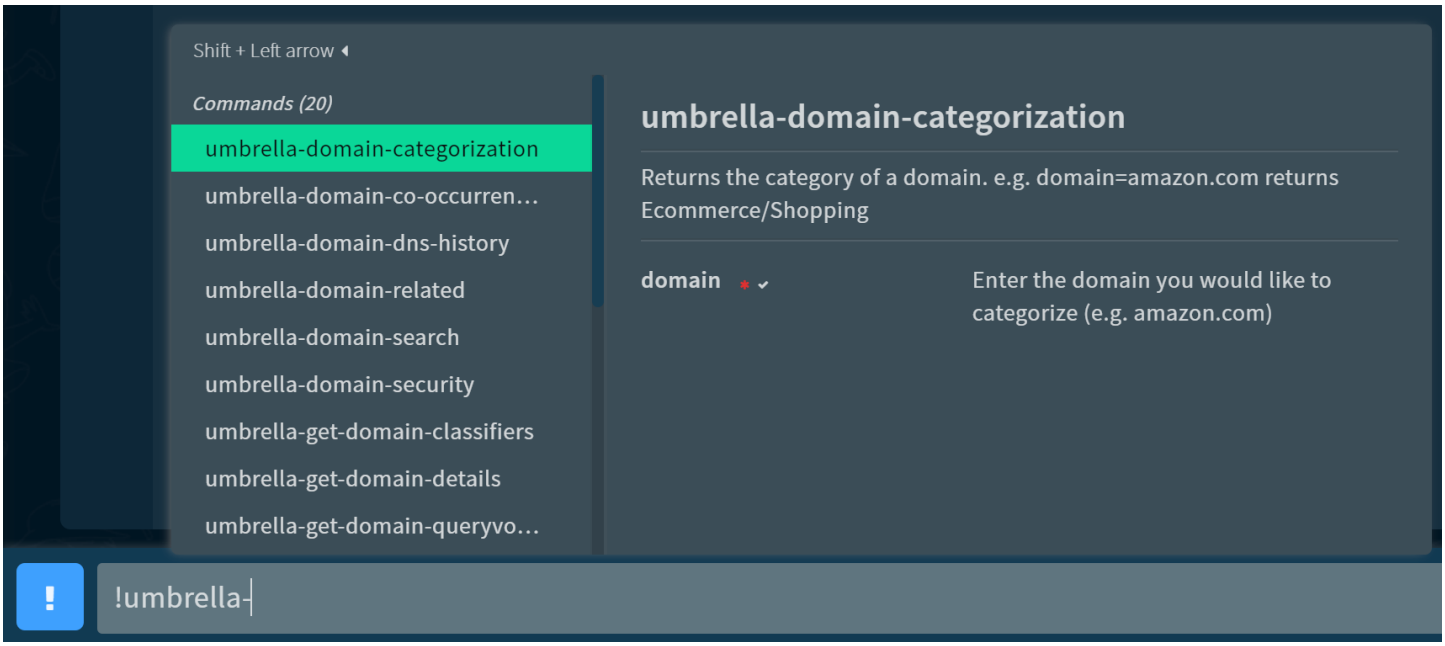
Benefit: Demisto playbooks coupled with Cisco Umbrella Investigate actions can standardize and speed up triage and resolution of security alerts. Analysts get a comprehensive view of the response workflow on a single screen. With repeatable tasks now automated, analyst time is freed up for deeper investigation and strategic action.

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 Cisco Umbrella Investigate commands in the Demisto War Room. For example, after a Demisto playbook has finished execution, analysts can get additional context in real time by running commands such as **umbrella-get-domain-details and umbrella-get-whois-for-domain** with relevant arguments to get domain details and WHOIS data for a particular domain 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 Cisco Umbrella Investigate
Cisco Umbrella Investigate provides the most complete view of an attacker's infrastructure and enables security teams to discover malicious domains, IPs, file hashes, and even predict emergent threats.

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.