DEMISTO | AWAKE

Automated Network Detection And Response

Benefits

- Detect malicious intent from insiders and external actors in Awake and respond through Demisto.
- Harness rich, aggregated AI-based network context from Awake Security in Demisto for automated, playbook-driven response.
- Use Demisto's orchestration to enrich other security tools with network intelligence from Awake and enrich the Awake platform with data from other security tools.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

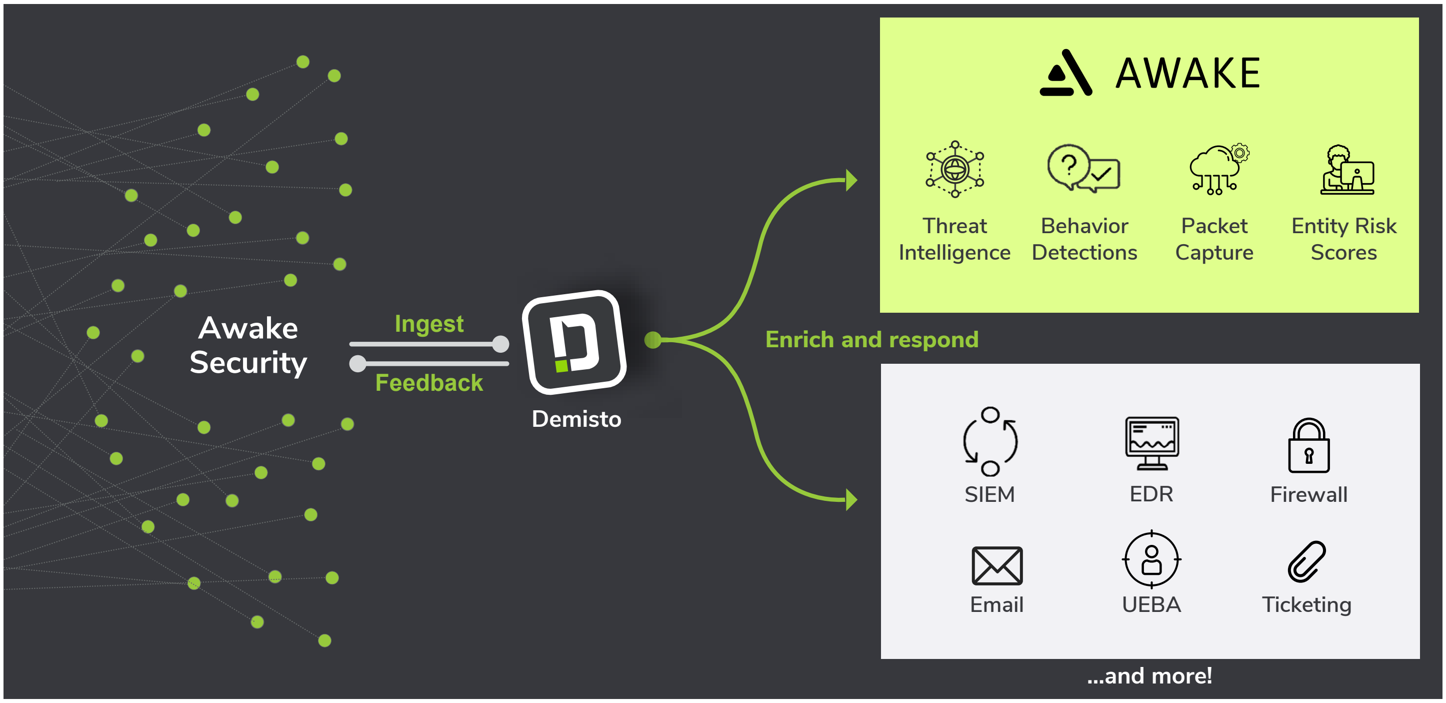
- Products: Demisto Enterprise, Awake Security Network Detection and Response Platform

In today's ever-changing security landscape, incident response teams often miss out on potential threats that can impact their organization because of evolved attacker techniques. By abusing insider credentials, using existing tools in target environments, and leveraging SSL to legitimize malicious sites, attackers can deceive traditional security products and launch large-scale compromises. Security teams need a platform that can provide deep, real-time network intelligence and harness that information to drive action across security environments.

To meet these challenges, users can combine the network detection and response capabilities of Awake Security with the security orchestration and automation features of Demisto to improve network intelligence and accelerate incident response.

Integration Features

- Automate the enrichment of IPs, domains, email addresses and devices with Awake Security's automated context as playbook-driven tasks within Demisto.
- Access Awake Security risk score of a device, a comprehensive threat timeline, and evidence of risky behavior from Demisto in real-time.
- Access Awake Security domain risk scores from Demisto to discover previously unknown malicious and suspect domains.
- Access Awake's Threat behavior detections, that uncover malicious intent by insiders or external actors, from Demisto.
- Retrieve network full packet capture data stored in Awake as required during an investigation in Demisto.
- Leverage hundreds of Demisto product integrations to further enrich Awake Security data and vice versa while coordinating response across security functions.
- Run thousands of commands (including for Awake Security) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 — DETECT AND RESPOND TO MAL-INTENT FROM INSIDE AND OUTSIDE ACTORS

Challenge: Sophisticated attackers have adapted their tactics, techniques, and procedures to avoid malware, instead relying on credential theft and the use of legitimate privileges. Security teams are therefore being asked to look for mal-intent that blends in with business-justified activity. Unfortunately, traditional security solutions struggle to detect this activity and then respond in a rapid and consistent fashion. Only the most sophisticated threat hunters stand a chance at detection but even that involves time-consuming efforts.

Solution: Awake detects mal-intent using a combination of artificial intelligence based behavioral analytics as well as through detection rules that identify known attacker tactics, techniques, and procedures. Threat behaviors triggered using Awake DetectIQ™ will automatically create incidents within Demisto. Analysts can then instantly respond and remediate using orchestration playbooks and the broader set of Demisto integrations within the enterprise.

For instance, the identification of a command and control domain can trigger the automated blocking of that domain at the perimeter as well as the creation of service tickets to remediate the endpoint. Similarly, when Awake detects a compromised credential, Demisto can automatically trigger the suspension of that account while any breach is investigated.

Benefit: The detection of non-malware activity by Awake Security and the rapid response through Demisto playbooks helps flush out both malicious insiders and outside attackers that have breached the perimeter. Moreover, reduced detection and response times lowers the impact to the organization.

USE CASE #2 AUTOMATED NETWORK DETECTION AND RESPONSE

Challenge: The disparate nature of network 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 source of truth. Incident response will also often involve a host of important but repetitive actions that analysts need to perform, leaving them time-strapped for actual problem-solving and decision-making.

Solution: SOCs using Awake Security for network detection and Demisto Enterprise for security orchestration and incident response respectively can automate threat enrichment through Demisto playbooks. These playbooks will harness Awake Security EntityIQ™ for rich context and risk profiles of devices, users, domains and use that information to execute actions across the entire stack of products that a SOC uses.

For example, analysts can create automatable playbook tasks that pivot from an IP address to contextual information such as device name, type, associated users, threat profile and timeline from Awake Security.

Benefit: Demisto playbooks coupled with Awake Security 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 #3 INTERACTIVE, REAL-TIME INVESTIGATION FOR COMPLEX THREATS

Challenge: 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, grabbing and archiving evidence, 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 Awake Security commands in the Demisto War Room. For example, if playbook results throw up a set of artifacts, analysts can run the **awake-query-devices** command to access other devices that match the same set of artifacts for a specific time interval. The analyst can use a rich set of queries supported by Awake QueryIQ™ to view the set of matching devices, domains or activities. Analysts can also grab full packet capture data from Awake Security as necessary.

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. This helps with elimination of false positives while improving response times by collating information from multiple sources of documentation.