DEMISTO | ANOMALI

Automated Threat Intelligence and Incident Response

Benefits

- Harness rich, aggregated threat intelligence from Anomali Threat Stream in Demisto for automated, playbook-driven response.
- Further enrich Anomali ThreatStream 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

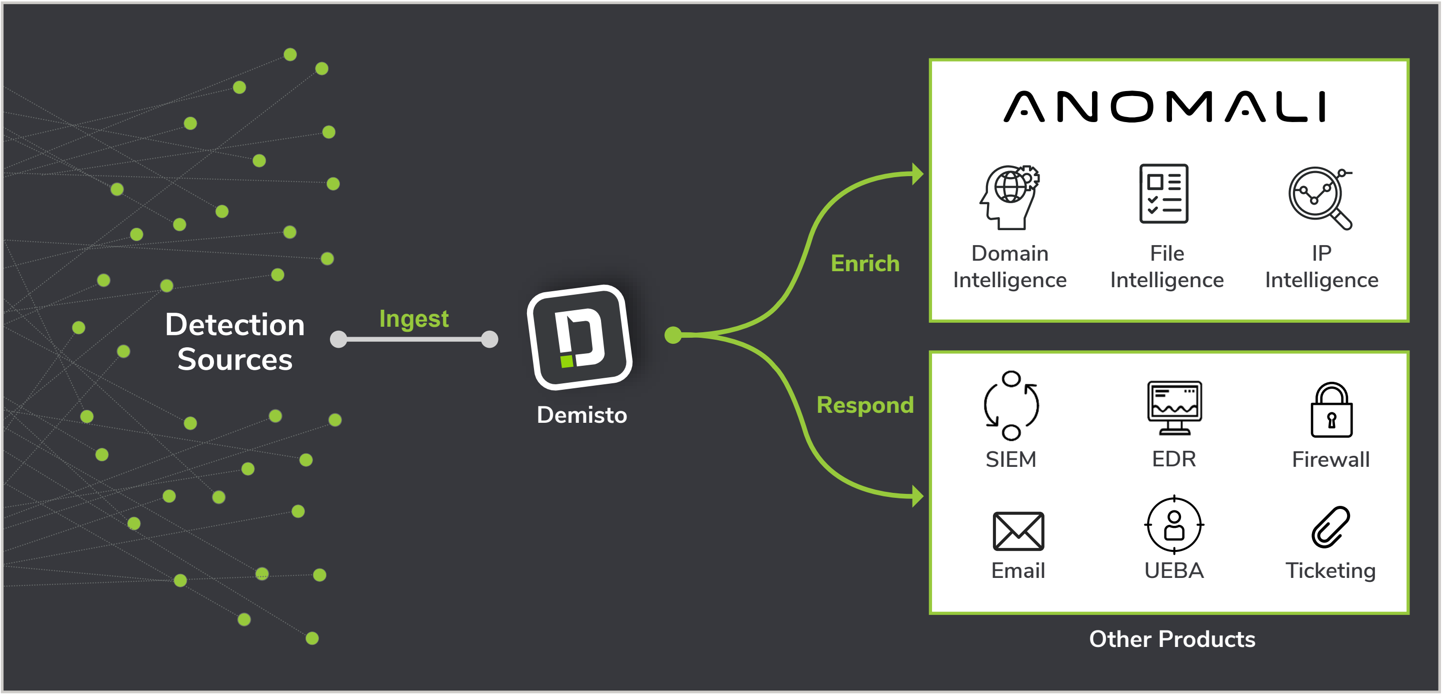
- Products: Demisto Enterprise, Anomali ThreatStream

In today's ever-changing security landscape, incident response teams often miss out on potential threats that can impact their organization because they're time-strapped by manual processes and high alert volume. They're unable to take advantage of the breadth of external threat intelligence available and instead focus only on internal logs and data. Security teams need a platform that can centralize threat intelligence across sources and harness that information to drive action across security environments.

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

Integration Features

- Automate Anomali ThreatStream enrichment of IPs, domains, and file hashes as playbook-driven tasks within Demisto.
- Access reputation of an email in Anomali ThreatStream from Demisto in real-time.
- Search for threat intelligence details in ThreatStream Cloud from within Demisto.
- Leverage hundreds of Demisto product integrations to further enrich Anomali ThreatStream data and coordinate response across security functions.
- Run thousands of commands (including for Anomali Threat Stream) 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, leaving them time-strapped for actual problem-solving and decision-making.

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

For example, analysts can leverage Anomali ThreatStream to enrich domains, IPs, and file hashes as automatable playbook tasks.

Benefit: Demisto playbooks coupled with Anomali ThreatStream 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: 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 Anomali ThreatStream commands in the Demisto War Room. For example, if playbook results throw up indicator information, analysts can get additional context from Anomali ThreatStream in real time by running the **threatstream-intelligence** command with relevant arguments.

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 Anomali

Anomali® detects adversaries and tells you who they are. Organizations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com and follow us on Twitter @Anomali.

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 the 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. Demisto is backed by Accel with offices in Silicon Valley and Tel Aviv. For more information, visit www.demisto.com or email info@demisto.com.