DEMISTO | tufin

Automated Security Policy Management and Incident Response

Benefits

- Harness rich network visibility data from Tufin SecureTrack for automated, playbook-driven response in Demisto.
- Use Demisto's orchestration to unify the network intelligence of SecureTrack with data from other security tools on a central console.
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation.
- Shorten decision-making cycle by automating key tasks with analyst review.

Compatibility

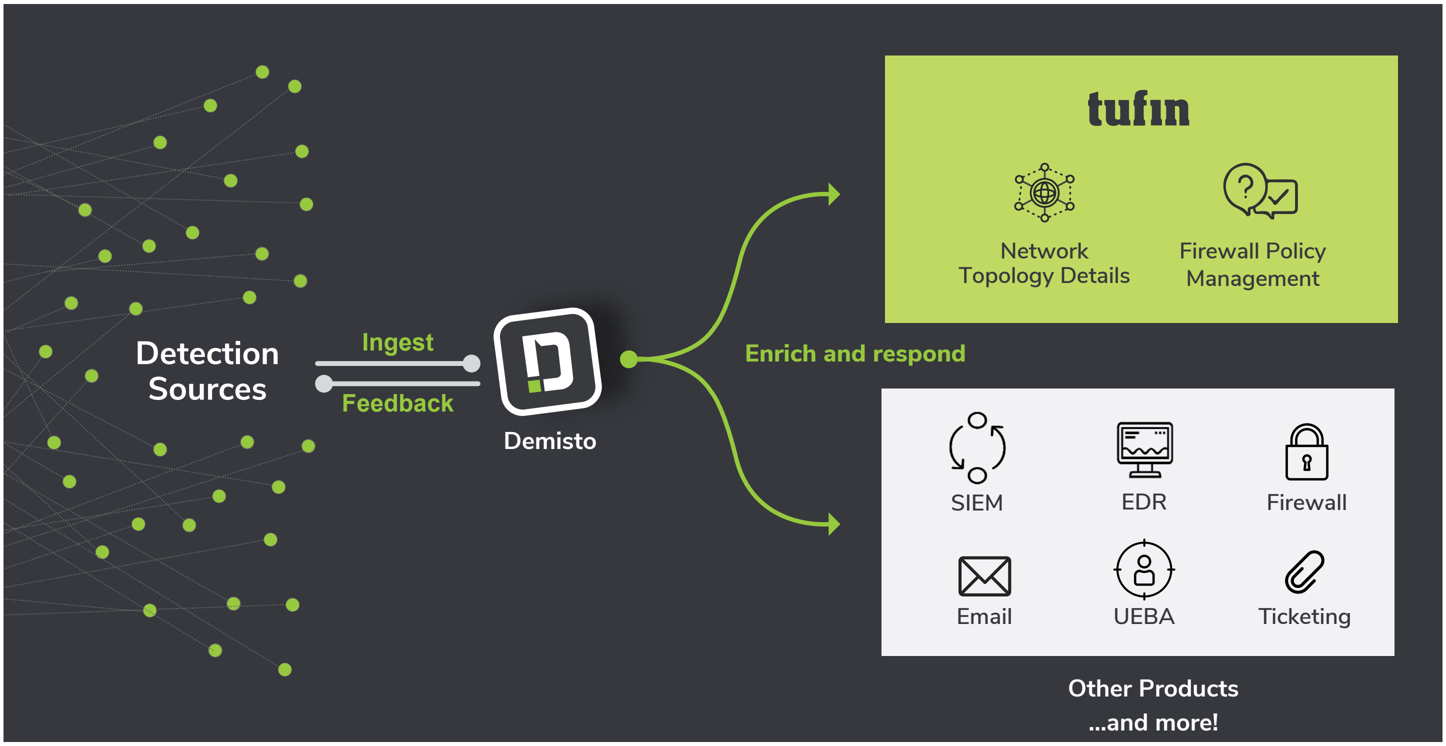
- Products: Demisto Enterprise, Tufin Orchestration Suite SecureTrack

In today's ever-changing security landscape, teams struggle to coordinate across disparate environments for their day-to-day operations as well as during incident response. Organizations often need heterogenous physical networks and hybrid cloud platforms to conduct business in an agile manner, but this leads to a lack of visibility and piecemeal security processes. Security teams need a platform that can provide deep, real-time network visibility and harness that information to drive automated action across security environments.

To meet these challenges, users can combine the security policy management capabilities of Tufin Orchestration Suite SecureTrack with the security orchestration and automation features of Demisto to improve end-to-end enterprise visibility and accelerate incident response.

Integration features:

- Get lists of monitored devices and network objects from SecureTrack in Demisto, either as automated playbook tasks or through real-time execution.
- Access network topology information, subnets, and pattern data for specific zones from SecureTrack within Demisto.
- Get granular policy rules, risk scores, and sub-policies from SecureTrack to enrich processes within Demisto.
- Leverage hundreds of Demisto product integrations to further enrich SecureTrack data and vice versa while coordinating response across security functions.
- Run thousands of commands (including for SecureTrack) interactively via a ChatOps interface while collaborating with other analysts and Demisto's chatbot.



USE CASE #1 AUTOMATED INCIDENT ENRICHMENT AND RESPONSE

Challenge: Due to a wide threat surface and disparate environments, it becomes time-consuming and repetitive for security analysts to cross-reference data across tools, get further policy context, and coordinate containment and response. Processes diverge depending on the analyst that handles the incident, leading to differing response quality.

Solution: Security teams can access granular policy, network topology, and object data from SecureTrack within Demisto through standardized and automatable playbook tasks. These playbooks can be triggered whenever an alert is detected on a relevant security tool (such as SIEMs, cloud security tools, and vulnerability scanners) and coordinate actions across the entire security product stack that an organization uses.

For instance, a playbook could query SecureTrack for NAT policies and rules for a particular device, cross-reference that data with intelligence from SIEMs and treat intelligence tools, and query SecureTrack again to determine whether policy changes are authorized.

Benefit: Leveraging SecureTrack's unique network security policy information along with data from other products through a common Demisto playbook helps minimize screen switching, manual reconciliation of data, and repetitive work for security teams. Unifying and automating response and compliance processes across cloud and on-premise infrastructures also helps security teams gain central oversight and coordinate actions at scale.

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, 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 SecureTrack commands in the Demisto War Room. For example, if playbook results throw up initial information, analysts can leverage the /topology/path and /topology/path_image APIs to access network topology paths and images to add to incident context.

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 Tufin

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2100 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

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.