tufin **DEMISTO**

Tufin Technology Alliance Partner (TAP) Program

Partner Brief

Business Challenge

Tufin Orchestration Suite takes a policy-centric approach to cybersecurity to provide visibility across heterogeneous and hybrid IT environments, enable end-to-end change automation for network and application connectivity and orchestrate a unified policy baseline across the next generation network. The result is that organizations can make changes in minutes, reduce the attack surface and provide continuous compliance with internal and external/industry regulations. The ultimate effect is greater business continuity, improved agility and reduced exposure to cybersecurity risk and non-compliance.

As an open and extensible platform, Tufin Orchestration Suite allows you to make the most of your existing technology and security investment and use best of breed products for security operations, incident response, vulnerability management, compliance, ticketing systems and more. There is a distinct advantage in focusing on our partners' core competencies integrated with Tufin Orchestration Suite to provide solutions that are better together.

Tufin is committed to partners with best-in-class products, to bring the most value to our mutual customers.

Solution: Tufin SecureTrack and Demisto Enterprise

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.

The combination of Tufin SecureTrack together with Demisto's security orchestration and automation capabilities enables security teams to improve end-to-end enterprise visibility and accelerate incident response.

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.

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, which is a shared space for real-time analyst collaboration. 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.

This joint solution helps security teams minimize visibility confusion, process variance, and alert fatigue by aggregating vital context, automating high-quantity actions, and providing teams with the right data for decision-making at scale.

Partner: Demisto
Partner Product: Demisto Enterprise
Product Integration Benefits:

- Accelerate incident response

- Unify data across security infrastructures

- Realize process repeatability

- Increase analyst productivity by reducing time spent on executing high-quantity tasks

- Improve return on existing security investments

- Improve investigation quality through indicator cross-correlation, machine learning insights, and real-time collaboration

tufin Ready

How it Works

The diagram below demonstrates how Tufin SecureTrack and Demisto work together to provide automated policy visibility, unified context, and accelerated response.
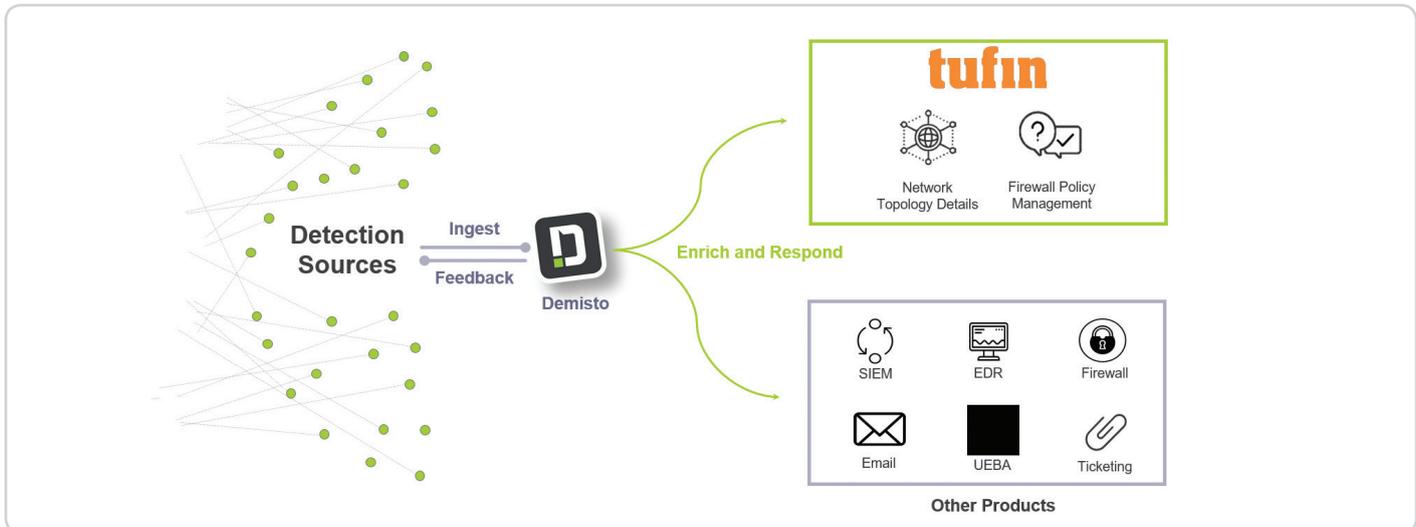
Security teams can use Tufin SecureTrack along with Demisto to deploy a central, actionable hub that ingests data across sources and executes standardized playbooks that automate repeatable tasks. These playbooks can query SecureTrack for policy rules, topology details, and other vital context to enrich incidents and provide security teams with the information they need to remediate threats.

Benefits

The combined Tufin Orchestration Suite and Demisto solution enables teams to:

- 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.

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.

To learn more, please visit: https://www.demisto.com for more information.

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 2,100 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.

Learn more about Tufin technology partners on our website.