tufin The Security Policy Company. + CORTEX XSOAR BY PALO ALTO NETWORKS

Solution Brief

Automated Security Policy Management and Context -enriched Incident Response

Overview

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 Orchestration Suite with Cortex XSOAR'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 Cortex XSOAR through standardized and automatable playbook tasks. Whether the change process is instigated directly through SecureChange or through Cortex XSOAR, enterprises can initiate automated threat containment while maintaining compliance with existing change control processes and full auditability.

Integration Features:

- Visualize network topology and application connectivity to provide investigators with enhanced visibility to assess the possible scope of an incident quickly and accurately
- Automatically initiate, design and implement network access changes using playbooks and Tufin workflows (e.g. to contain potentially infected systems)
- Maintain compliance and adherence to established change control processes throughout the incident, with full auditability
- Leverage hundreds of Cortex XSOAR product integrations to further enrich Tufin SecureTrack data and vice versa while coordinating response across security functions.
- Run thousands of commands including Tufin Orchestration Suite playbooks, supported via a ChatOps interface while collaborating with other analysts and Cortex XSOAR chatbots

Use Case #1: Automated incident enrichment and response

Challenge: Due to a wide threat surface and multi-vendor disparate environments, it becomes time-consuming and repetitive for security analysts to cross-reference data across tools, acquire 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 Tufin SecureTrack within Cortex XSOAR 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 can coordinate actions across the entire security product stack.

Benefits:

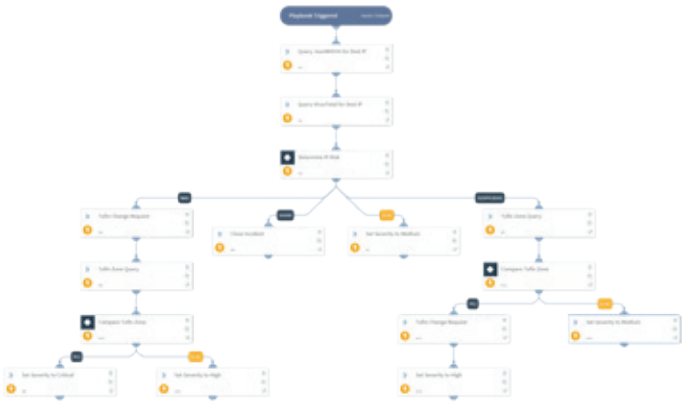
- Harness rich network visibility data from Tufin SecureTrack for automated, playbook-driven response in Cortex XSOAR
- Use Cortex XSOAR's orchestration to unify the network intelligence of Tufin SecureTrack and application context from Tufin SecureApp with data from other security tools on a central console
- Ensure secure, auditable, and compliant change management through response actions initiated in Cortex XSOAR and implemented through Tufin SecureChange
- Improve analyst efficiency by centralizing collaboration, investigation, and documentation and implementing changes in moments instead of days and months
- Shorten decision-making cycle by automating key tasks and proactive risk analysis with analyst review

Compatibility:

- Cortex XSOAR
- Tufin SecureTrack
- Tufin SecureChange
- Tufin SecureApp

For instance, a playbook could query Tufin 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 Cortex XSOAR playbook promotes increased efficiency, minimizes manual reconciliation of data, and avoids repetitive work for security teams.



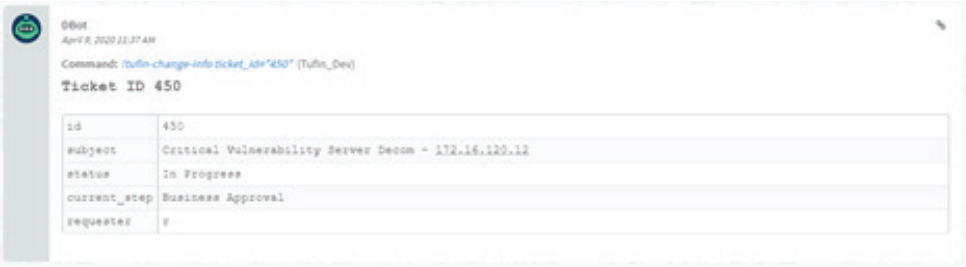
Cortex XSOAR playbook to enrich and streamline incident management and response

Use Case #2: Interactive, real-time forensics of 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 initiating remedial actions. Running these commands traps analysts in a screen-switching cycle between various security vendor management dashboards, during investigation and a documentation-chasing cycle after investigations end.

Solution: After running enrichment playbooks, analysts gain greater visibility and new actionable information about the attack by running SecureTrack commands in the Cortex XSOAR War Room. For example, if playbook results throw up initial information, analysts can leverage the tufin-policy-search and tufin-search-topology commands to search policy and topology details respectively, adding vital information to incident context. Analysts can also run commands to initiate change on the security devices through automation playbooks for Tufin SecureChange after proactive analysis of the impact and 'what-if' scenarios.

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 can be assured that the changes are accomplished through a well-established workflow instead of ad-hoc unauthorized changes, leading to compliance, audit and security complexities after the investigation ends.



Command issued to create a ticket in Tufin SecureChange to start server decommissioning

tufin The Security Policy Company.

Tufin (NYSE: TUFN) 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 company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.

CORTEX XSOAR BY PALO ALTO NETWORKS

Cortex XSOAR, a Palo Alto Networks company, 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. With Cortex XSOAR, security teams can standardize processes, automate repeatable tasks, and manage incidents across their security product stack to improve response time and analyst productivity. For more information, visit https://www.paloaltonetworks.com/cortex/xsoar