tufin The Security Policy Company.

IBM

IBM Security SOAR and Tufin Orchestration Suite Network Intelligence

Incident Response in a Hybrid, Heterogeneous World

Today's security incidents are seldom contained to a single host; almost every incident involves a large set of controls at some phase of the attack lifecycle. Unfortunately, most incident response and security operations teams are blind to the configuration of access and connection points they are tasked to defend. The increasingly dynamic nature of today's networks means that the spreadsheets of network data incidents provided to the responders are almost immediately out-of-date and can lead to incorrect conclusions or incomplete investigations.

IBM Security SOAR enables incident response and security operations teams to codify their unique incident response processes into workflows, automating tasks which do not require human intervention, allowing teams to dedicate resources to tasks which require human action. The core of trusted automation lies in data which is both complete and accurate. Automation based on data which is incomplete or inaccurate can result in incidents which are incorrectly triaged, or worse, erroneous containment actions. When automating with IBM Security SOAR a comprehensive, reliable source of network security policy and topology data provides confidence in automated response that otherwise cannot be achieved.

Network Intelligence and Change Automation for Incident Response

Tufin has been the leader in security policy management for over a decade and excels at managing the most complicated heterogenous environments around the enterprise. The Tufin Orchestration Suite (TOS) is used by global security, cloud and network operations teams to provide accurate security policy administration, network topology information, compliance management, and change design and automation in multi-vendor, hybrid cloud environments. The same TOS features trusted to manage the complex connectivity of global enterprises can be used by incident response and security operations teams to gain deep insight into security controls and perform automated threat containment.

Benefits to Your Business:

- Improve the security posture of your organization by automatically gathering critical network intelligence during incident response workflows.
- Troubleshoot and assess complex network topologies and perform path analysis based on actual device configurations and security policies.
- Increase efficiency by automating changes from design to implementation across heterogeneous security controls.
- Maintain compliance and a complete audit trail of changes during the incident response process.

Access and Connectivity Insights for Informed Automation

Proper context is vital for reliable automated workflows and decision making. Unreliable or incomplete contextual information gathered during the triage and investigation stage of an incident can lead to weak decisions, resulting in loss of efficiency, or worse, a potential security incident remaining undetected. The dynamic nature of today's modern enterprises means that static network documentation, such as spreadsheets of configuration databases, are inefficient and obsolete by the time they are used in a production environment.

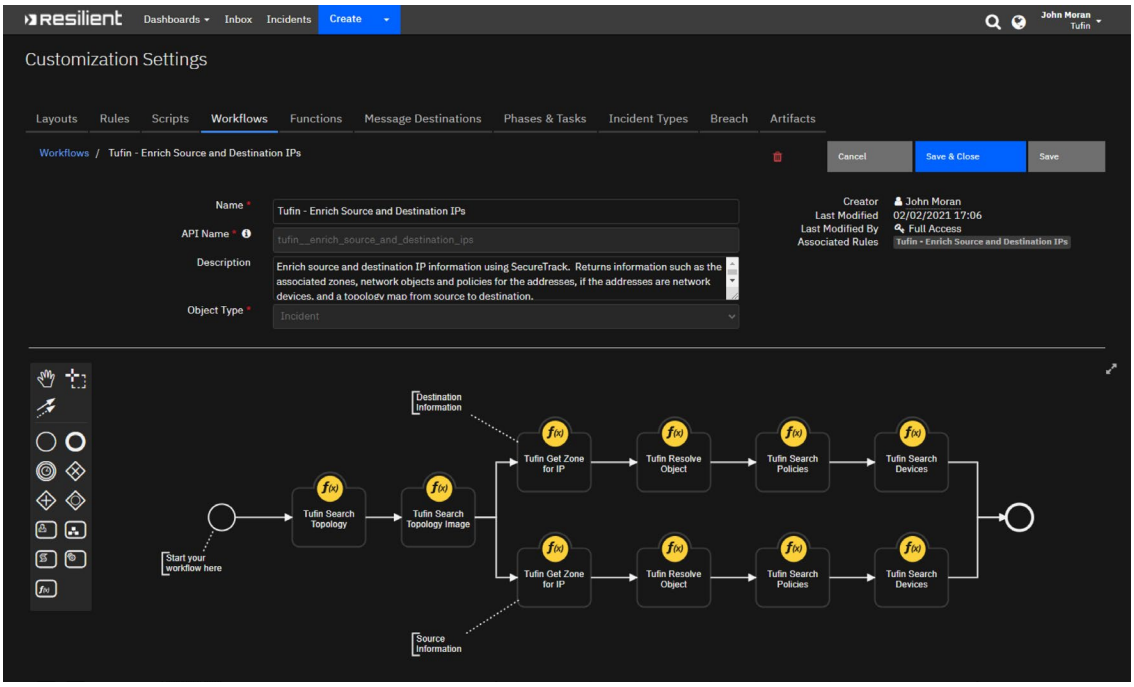

Figure 1. Sample Workflow - IP Enrichment

Tufin's rich topology mapping and security policy information provides incident response teams with unparalleled visibility into the enterprise's network. Providing insight into what can talk to what and who can talk to whom allows analysts and automated workflows to make accurate triage decisions based on the most up-to-date topology, quickly determining the actual risk posed by the security event, vulnerability, or other initiating event.

Centralized Visualization and Path Analysis

Understanding connectivity and services access across enterprise assets is critical to properly scope a potential security incident. This simple task can be extremely challenging in a hybrid world with many different vendor solutions in use, and different teams managing different control points. Often, this involves manually querying different vendor tools and databases, and correlating the information by hand, wasting critical time and analyst cycles.

Using knowledge of the current security controls and associated policies, Tufin can build an accurate, interactive topology map, detailing connectivity across the entire hybrid network. This topology map can be automatically queried from IBM Security SOAR, showing the route traffic would take from source to destination, quickly identifying additional sources of potential log information. More importantly, Tufin can immediately determine if traffic would be permitted by policy, allowing automated workflows to escalate events which pose a greater likelihood of risk to the enterprise.

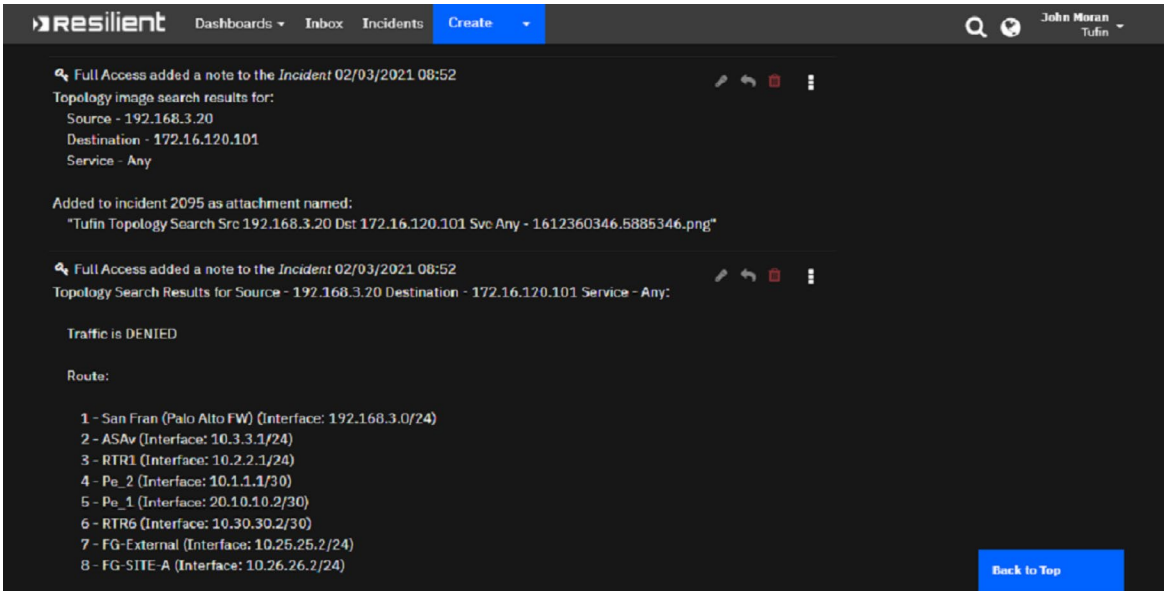

Figure 2. Tufin Topology Results

Automated Multi-vendor Change Design and Provisioning

Designing security policy changes in a complex, hybrid, multi-vendor environment can be a time-consuming process, requiring manual review of the current topology and existing security policies. This process can be difficult, if not impossible, to script accurately using workflow logic and individual vendor integrations.

Tufin's SecureChange utilizes in-depth security policy and topology visibility to automatically identify target assets and design new security policies to enact the desired change. SecureChange allows administrators to design custom workflows based on existing change control processes, utilizing varying levels of automation based on the preference of the organization. Tufin can automatically provision the change across vendor technologies, and automatically verify that the change was provisioned correctly.

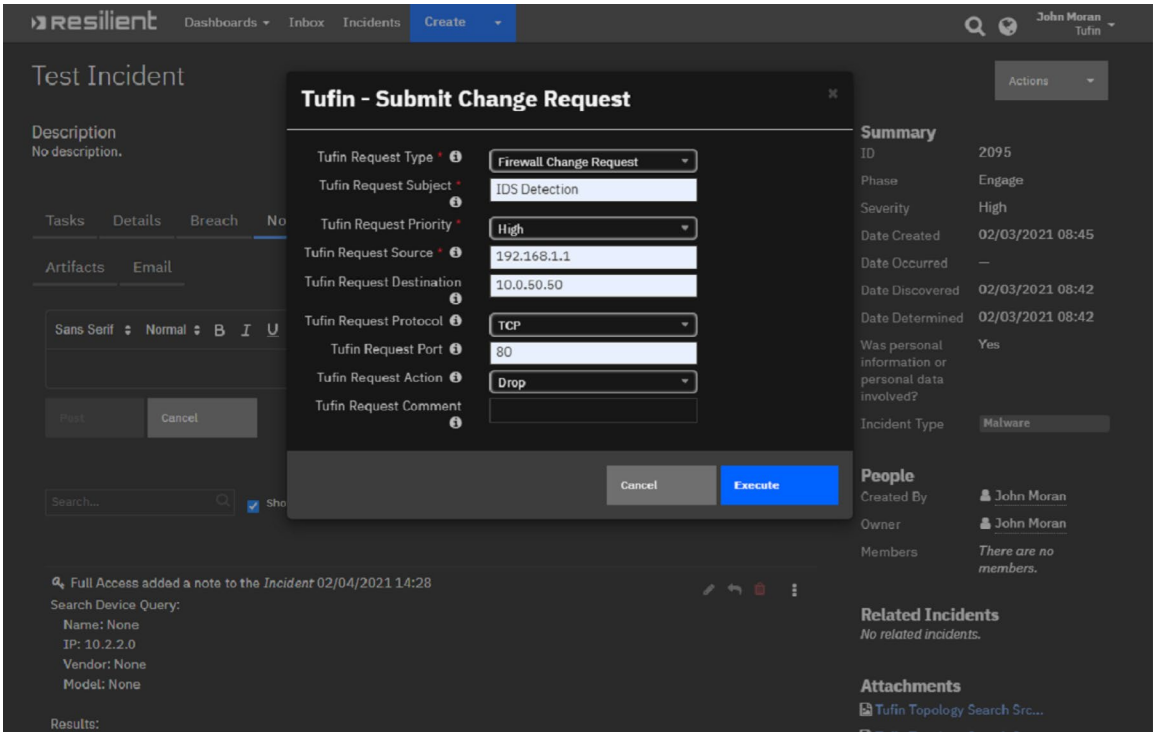

Figure 3. Change Request Submission

Continuous Compliance and Auditability

A security incident can be a chaotic event, with priority given to containing the potential threat and mitigating risk. Manual documentation and normal change control processes are often circumvented for the sake of swift action. While the result may or may not be a faster resolution, a side effect is often a lack of change auditability or changes which result in non-compliance.

Tufin's Unified Security Policy provides security policy guardrails which are applied uniformly across all security controls. In addition to detecting policy violations in existing security policies, Tufin also proactively assesses each change request for potential policy violations, ensuring any potential risk is identified before it is provisioned. Designing and provisioning policy changes through Tufin also provides an automatic audit trail, documenting when changes were made, by whom, and the justification for the change.

Summary

The integration of Tufin with IBM Security SOAR provides incident response and security operations teams with unparalleled visibility into security policies and topology. Integrating with Tufin allows workflows to make more accurate automated decisions based on the current state of access and connectivity, reducing analyst workload and the mean time to respond. The industry-leading change management solution from Tufin allows enterprises to perform rapid threat containment across a hybrid, heterogeneous environment, while ensuring auditability and compliance is maintained throughout the event.

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.

DP20210518