Tufin Technology Alliance Partner (TAP) Program

Partner Brief

Business Challenge

Tufin Orchestration Suite's policy-centric approach to cybersecurity provides visibility across multi-vendor and multi-platform networks, supports zero-touch change automation to ensure network and application connectivity, and enables organizations to realize a state of both security and business agility. The policy-centric approach enables organizations to make changes in minutes, reduce their attack surface, and achieve continuous compliance. Companies leverage Tufin to achieve greater business continuity, improve agility, and ingrain security policy throughout the networks evolution to include next generation networkingplatforms.

As an open and extensible platform, Tufin Orchestration Suite empowers you to make the most of your existing technology and security investments. The Tufin API enables extending the Tufin automation features to further the realized value of best-of-breed products for security operations, incident response, vulnerability management, compliance, ticketing systems, and more. The distinct advantage in focusing on complementing our partners core competencies with Tufin provides solutions that enable IT and security to consistently operate better together.

A policy-centric platform is the ideal choice to tightly integrate with solutions that can share data and ensure that the intent of the enterprise security policy is met and carried across the whole infrastructure regardless of the complexity and vendor-diversity of the network.

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

Partner: Splunk

Partner Product: Splunk Phantom

Product Integration Benefits:

- Automate repetitive tasks to force multiply your team's efforts
- Reduce dwell times with automated detection and investigation
- Shorten response times with playbooks that execute at machine speed
- Drive efficient communications across your team with integrated collaboration tools
- Bring event data and SOC tools together into one consolidated view through Mission Control
- Implement, configure, and maintain easily

Solution: Tufin Orchestration Suite and Splunk Phantom

The combination of Tufin's Orchestration Suite together with Splunk Phantom's security orchestration, automation and response (SOAR) capabilities ensures faster and more accurate incident response processes.

Tufin's real-time visibility into network policy and changes deliver critical context to security analysts directly within Splunk Phantom. This allows analysts to more accurately automate the response process to network threats at machine speeds. When automated response isn't viable, Tufin delivers analysts the network policy detail required to understand the threat and respond quickly, creating strong cross-organizational alignment.

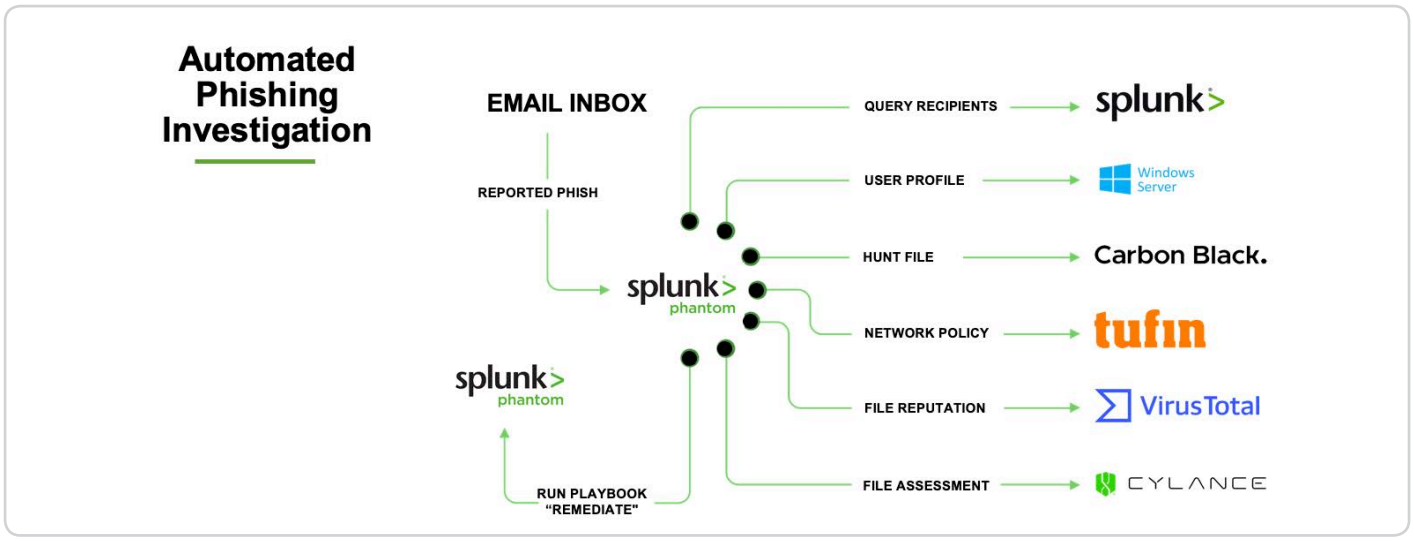
While organizations deploy a broad range of security tools to defend against advanced attacks, the sheer volume of alarms they generate overwhelm SecOps teams with a constant barrage of potential threats. Compounding this risk is a growing shortage of trained security personnel required to keep up with the volume of threats targeting your network.

Splunk Phantom helps organizations get the most out of existing resources by automating time- intensive, manual processes and operational workflows in real-time. The Phantom Visual Playbook Editor (VPE) allows both developers and non-developers to construct and customize complex Phantom Playbooks with drag-and-drop ease.

Tufin designs new access changes that align with policy and minimize introduced risk, and provisions changes across network devices within minutes. During incident response, time is critical. Pre-built automated tasks such as Server Decommissioning allow users to modify their policy enterprise wide quickly.

Working an investigation with Tufin and Splunk Phantom

Together with Splunk Phantom analysts can integrate Tufin's security policy management into their security incident response.



The Tufin-Splunk Phantom integration fulfils many use cases for expediting the incident response process. By delivering accurate and up-to-date policy information via integration, Tufin helps companies accelerate the Observe phase by automatically supplying relevant policy information for an incident. With this information the Splunk Phantom platform creates a complete picture of an incident, moving through Orient and Decide with crafted playbooks.

When it comes time to Act on an event, users of the joint solution instigate Tufin's award-winning change management and automation capabilities directly from inside a playbook. Utilizing Tufin's provisioning capabilities, users ensure that policy changes have a complete audit trail and business approval along with intelligent provisioning in-line with the vendor and customer's best practices.

Benefits

The combined Tufin Orchestration Suite and Phantom Splunk:

- Enrich investigations withTufin-supplied policy data to security analysts directly inside Phantom Cyber
- Execute automated playbooks based on accurate and up-to-date network policy data
- Automatically update policies within Tufin in response to specific threats
- Respond to network threats faster and within best practices through automated incident response playbooks

About

Splunk was founded to pursue a disruptive new vision: make machine data accessible, usable and valuable to everyone. Machine data is one of the fastest growing and most pervasive segments of "big data"--generated by websites, applications, servers, networks, mobile devices and the like that organizations rely on every day. By monitoring and analyzing everything from customer clickstreams and transactions to network activity and call records and more, Splunk turns machine data into valuable insights no matter what business you're in. It's what we call operational intelligence.

To learn more, please visit: Splunk Platform 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.

SB-04-19