SOLUTION BRIEF

Tanium for SOAR

The Tanium Platform integrates with security orchestration, automation, response (SOAR), and other IT platforms to automate tasks. It helps manage and secure endpoints at scale, increasing IT efficiency and strengthening digital defenses.

Companies Need Faster Threat Detection and Remediation

Endpoint device are more distributed and varied than ever before. This is creating all new management and security challenges for businesses.

More employees are working remotely, outside the protection of a corporate firewall and beyond the reach of internal security tools or VPNs. And many employees are using "bring-your-own" devices (BYOD) that the IT department hasn't provisioned or tested.

At the same time, cybercriminals are taking advantage of this increased exposure to create subtle phishing attacks, drive-by malware installation scripts, and other forms of cybercrime to catch vulnerable employees off-guard and infiltrate company networks.

IT organizations need a way to automatically detect and remediate threats faster than ever before.

Companies Need Faster Threat Detection and Remediation

Fast, flexible, and extensible, the Tanium Platform brings automation to the "last mile" of corporate networks — to endpoint devices themselves.

The Tanium Platform API integrations, in concert with other leading security automation and orchestration response (SOAR) platforms, provides the connectivity and feature-rich functionality enterprises need to control and protect endpoints at scale in automated workflows.

Tanium offers the vital real-time connection to endpoints that IT teams need for taking action, quickly and effectively.

Use Tanium to respond to a SOAR platform's request for data artifacts from endpoints that may be under attack. It can also help quarantine or clean a compromised device.

Key Benefits

With its real-time visibility into endpoints and granular configuration controls, Tanium makes it far easier to automate endpoint tasks for IT operations, ticketing and threat response.

Accelerated IT Operations: By integrating with "SOAR" platforms, the Tanium Platform helps security operations center (SOC) teams to quickly make changes on endpoints — at scale, anywhere, anytime.

Accelerated Collection of Threat Artifacts: When SIEM systems or SOAR platforms raise alerts, Tanium can automatically collect endpoint data, including Indicators of Compromise (IoC).

Accelerated Threat Mitigation: When SOAR platforms initiate a playbook workflow, Tanium can perform workflows steps that involve endpoints, including working with security agents on endpoints themselves.

Improved Coordination With Ticketing Platforms: When integrated with ticketing platforms, Tanium can open tickets, append endpoint data to tickets, and close tickets as part of IT workflows.

How It Works

The Tanium Platform offers integrations with leading service management platforms, SOAR platforms, ticketing platforms, and other IT security and operations platforms. Tanium's open APIs help customers integrate Tanium products with other IT tools and services to accelerate and streamline IT operations.

Features

If a SOAR platform raises an alert about a malware hash detected on an endpoint, the Tanium Platform can receive that alert, quarantine the endpoint, collect forensic artifacts related to the malware infection, and open a ticket in Jira or ServiceNow — all automatically.

The Tanium Platform can also undertake other actions useful for SOAR playbooks, such as reporting real-time data about endpoint status, including details about active processes, memory usage, software and hardware configurations, and patch status.

Tanium can initiate endpoint scans, send data to VirusTotal for threat analysis, launch other programs installed on endpoints, and more.

Critically, it provides SOAR platforms with detailed, up-to-date information about endpoint hardware and software that helps SOC teams determine which endpoints are vulnerable to which types of threats.

By providing SOAR platforms with more detailed information about endpoints, Tanium helps SOAR platforms improve the speed and accuracy of their threat detection and threat response workflows.

Through its integration with SOAR platforms, Tanium helps IT organizations automate common endpoint management and endpoint security tasks. At the same time, it helps reduce IT workloads, shortens mean time to remediation (MTTR), and improves employees' IT experience.

The Tanium Platform integrates with leading SOAR platforms, including:

- Cyware
- Palo Alto Networks Cortex XSOAR
- Splunk Phantom

Tanium also integrates with SIEM platforms, identity ad access management platforms, ticketing platforms, endpoint telemetry management platforms, and other IT tools that SOAR platforms commonly interoperate with.