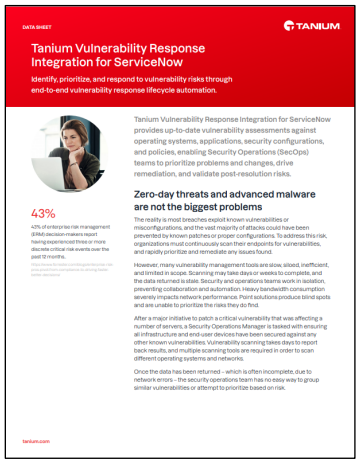

Tanium Vulnerability Response Integration for ServiceNow

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium's solutions, please check out the following resources and information:

For additional resources:
carah.io/taniumresources

For upcoming events:
carah.io/taniumevents

For additional Tanium solutions:
carah.io/taniumsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
tanium@carahsoft.com
703-673-3560

To purchase, check out the contract vehicles available for procurement:
carah.io/taniumcontracts

For more information, contact Carahsoft or our reseller partners:
tanium@carahsoft.com | 703-673-3560

DATA SHEET

Tanium Vulnerability Response Integration for ServiceNow

Identify, prioritize, and respond to vulnerability risks through end-to-end vulnerability response lifecycle automation.

43%

43% of enterprise risk management (ERM) decision-makers report having experienced three or more discrete critical risk events over the past 12 months..

https://www.forrester.com/blogs/enterprise-risk-pros-pivot-from-compliance-to-driving-faster-better-decisions/

Tanium Vulnerability Response Integration for ServiceNow provides up-to-date vulnerability assessments against operating systems, applications, security configurations, and policies, enabling Security Operations (SecOps) teams to prioritize problems and changes, drive remediation, and validate post-resolution risks.

Zero-day threats and advanced malware are not the biggest problems

The reality is most breaches exploit known vulnerabilities or misconfigurations, and the vast majority of attacks could have been prevented by known patches or proper configurations. To address this risk, organizations must continuously scan their endpoints for vulnerabilities, and rapidly prioritize and remediate any issues found.

However, many vulnerability management tools are slow, siloed, inefficient, and limited in scope. Scanning may take days or weeks to complete, and the data returned is stale. Security and operations teams work in isolation, preventing collaboration and automation. Heavy bandwidth consumption severely impacts network performance. Point solutions produce blind spots and are unable to prioritize the risks they do find.

After a major initiative to patch a critical vulnerability that was affecting a number of servers, a Security Operations Manager is tasked with ensuring all infrastructure and end-user devices have been secured against any other known vulnerabilities. Vulnerability scanning takes days to report back results, and multiple scanning tools are required in order to scan different operating systems and networks.

Once the data has been returned – which is often incomplete, due to network errors – the security operations team has no easy way to group similar vulnerabilities or attempt to prioritize based on risk.

Tanium Vulnerability Response Integration for ServiceNow

Provide IT, vulnerability, and security teams with continuous, up-to-date vulnerability assessments of their entire IT estate, enabling them to correlate, prioritize, remediate, and validate in real time.

Automatically correlate vulnerabilities with configuration items in the ServiceNow CMDB

Quickly resolve vulnerabilities across all affected devices with automatic grouping of individual vulnerable items into vulnerability groups.

- Correlate vulnerable items from Tanium-detected vulnerabilities into vulnerability groups for investigation and remediation at scale.

Scan in minutes and report on the most up-to-date vulnerabilities

Reduce time spent hunting vulnerabilities across networks and operating systems, with trusted known vulnerability content and comprehensive scanning across critical endpoints, including offline devices.

- Leverage the Security Content Automation Protocol (SCAP) to use any Open Vulnerability and Assessment Language (OVAL) content in addition to the updated-daily Tanium Comply content library.

Quickly validate vulnerability remediations

Eliminate the time and manual effort of remediation validation with the ability to rescan and confirm change outcomes automatically, and to update change records based on rescanned results.

- Rescan vulnerable items to validate remediation actions and alert on any vulnerabilities that were unsuccessfully closed.

Enable Security Operations (SecOps) teams to identify, prioritize, and remediate vulnerability risks with real-time vulnerability assessments correlated to configuration items in the Configuration Management Database (CMDB).

- Scan and report in minutes on vulnerabilities across all endpoints.
- Automatically correlate vulnerabilities with vulnerable items and vulnerability groups.
- Validate vulnerability remediations with automated rescanning tied to change records.

KEY CAPABILITIES INCLUDE:

- Leverage the Security Content Automation Protocol (SCAP) to use any Open Vulnerability and Assessment Language (OVAL) content in addition to the updated-daily Tanium Comply content library.
- Automatically correlate vulnerabilities with configuration items in the ServiceNow CMDB.
- Prepare for audits with the ability to run vulnerability scans on demand and report back in minutes.
- Eliminate time and effort of manual remediation validation with the ability to automatically rescan to confirm change outcomes.
- Collect real-time vulnerability intelligence anytime with ServiceNow workflow actions.

Combining the Tanium XEM platform capabilities with the ITSM capabilities in ServiceNow provides a better total experience for the IT agent, employee, and customer.

The Tanium Converged Endpoint Management (XEM) platform offers comprehensive IT operations and security management from a single agent. It delivers complete, accurate, and real-time endpoint data, regardless of scale or IT complexity, and uses minimal infrastructure. Tanium XEM provides visibility, control, and remediation needed to help you continuously manage your organization's endpoint risk.

DEMO OUR SOLUTION

Schedule a demonstration to see Tanium XEM live and to visualize exactly how our solution can transform your endpoint management and security.

See Tanium live

Tanium, the industry's only provider of Converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale. More than half of the Fortune 100 and the U.S. armed forces trust Tanium to protect people; defend data; secure systems; and see and control every endpoint, team, and workflow everywhere. That's the power of certainty.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.