DATA SHEET

Tanium Security Operations Integration for ServiceNow

Improve security incident response times and mitigate the cost of breaches through proactive data enrichment.

< 15%

Fewer than 15% of organizations have yet to achieve continuous visibility of their attack surface.

https://noeticcyber.com/resources/esg-security-hygiene-report-2023/

Tanium Security Operations Integration for ServiceNow automatically enriches data with real-time intelligence for endpoints associated with security incidents – as well as quickly search for other affected endpoints – eliminating the time-consuming steps that IT, security, and risk teams need to perform during critical investigations.

Time is of the essence for security incident response

With ever-greater reliance on the digital estate, security incident response teams are constantly under siege from evolving threats. In order to minimize business disruption and proactively reduce risk, security operations need to understand what is happening in real time, and what is the true scope of security incidents.

However, many teams rely on poorly integrated and fragmented point tools providing incomplete data, which could be hours, days, or even weeks old. Manual investigations and efforts to coordinate between IT, security, and risk teams lead to costly, time-consuming inefficiencies and increased risk exposure.

After advanced malware was found on a production server, an organization's security operations team immediately opened a high-level security incident. Due to stale CMDB data, the security incident response team was delayed in attempting to establish a remote connection to the affected server to begin the initial investigation – which was further delayed because of issues in coordination between IT, security, and risk teams.

Once the malware was remediated on the production server, the security operations team needed to understand what other endpoints were also affected and currently exposing the organization to significant risk. Attackers could be infiltrating other devices, while the team awaited scanning results from different integrated tools.

Tanium Security Operations Integration for ServiceNow

Enable security operations teams to bridge the gap between IT, security, and risk teams and accelerate the investigation and remediation of security incidents at scale through real-time intelligence.

Enhance the data for configuration items associated with security incidents

Expedite the investigation, response, and remediation of security incidents to minimize impact, data loss, and exposure, and drive maturity of security operations teams.

- Automatically provide relevant real-time data to security operations teams – including logged-in users, network statistics, running processes, and running services.

Bridge the gap between IT, security, and risk teams

Eliminate the need for costly integrations and time-consuming coordination between teams, so you can focus on resolving security incidents – not chasing people and data.

- Get real-time configuration item data enrichment directly inside of the security incident record in ServiceNow, without needing to switch context between tools.

Quickly determine the true scope of security incidents across the entirety of your IT infrastructure

Uncover the actual scope of security incidents as they occur, enabling security operations teams to analyze, prioritize, and remediate at scale – when time is of the essence.

- Run Sightings Searches to uncover the prevalence of threats by leveraging Tanium Threat Response to find occurrences of MD5 hashes or IP addresses across all endpoints.

Provide security operations teams with the real-time intelligence they need to investigate, respond to, and remediate security incidents – at scale – when every second matters.

- Enhance the data for configuration items associated with security incidents.
- Bridge the gap between IT, security, and risk teams and eliminate the need for costly integrations and time-consuming coordination.
- Quickly determine the true scope of security incidents by searching for threat prevalence across the entirety of your IT infrastructure.

KEY CAPABILITIES INCLUDE:

- Provide relevant real-time data about configuration items associated with security incidents, including logged-in users, network statistics, running processes, and running services.
- Spend less time chasing people and data with the ability for IT, security, and risk teams to access the same high fidelity, real-time data.
- Leverage Tanium Trace for Sighting Searches in ServiceNow, ensuring that threat occurrences are discovered and remediated across all endpoints.

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.