DATA SHEET

Tanium File Integrity and Unauthorized Change Monitoring for ServiceNow

Real-time identification and event creation for authorized and unauthorized changes to registries and files.

Tanium File Integrity and Unauthorized Change Monitoring for ServiceNow employs the speed, visibility, and control of the Tanium XEM platform to deliver real-time alerts of changes to registries and files, stored as events in ServiceNow.

Greater complexity limits compliance effectiveness

PCI-DSS, GDPR, CIS Critical Security Control 3, HIPAA, SOX, NERC-CIP, and more – most organizations still struggle to consistently manage IT compliance. Increasingly complex networks, multiple operating systems, new regulations, and a hodgepodge of point tools only exacerbate this situation and prevent teams from proactively addressing problems.

The end result is an expensive, inefficient integrity-monitoring process that doesn't lead to better compliance and puts organizations at severe financial and security risk.

After being notified of potential General Data Protection Regulation (GDPR) issues, an IT manager is tasked with determining if all of their organization's systems are GDPR compliant. After some initial investigation, they are struggling to verify the files on all their Windows servers, let alone their devices running Linux, Solaris, and AIX. Fines for violations of GDPR can quickly run into the tens of millions of dollars.

The European Union's GDPR fines for non-compliance range from up to €10-20 million, or 2-4% of an organization's worldwide annual revenue, whichever amount is higher. - https://gdpr.eu/fines/

Tanium File Integrity and Unauthorized Change Monitoring enables event managers to sync, view, investigate, and correlate file and registry change event records with change requests in ServiceNow.

- **Monitor and record registry and file events across operating systems, applications and log files.** Eliminate the need for different monitoring tools and point solutions to cover all of your operating systems. Windows, Linux, Solaris and AIX operating systems are all supported, incorporating them into an integrated workflow and reporting structure.
- **Automate the labeling of events to improve workflow.** Improve the signal-to-noise ratio and reduce false positive events. Automatically label or categorize events using rules, defined criteria, or event information.
- **Help solve file integrity monitoring for regulatory compliance and common standards.** Spend less time researching and investigating new and changing regulatory compliance standards. Create your own configuration or utilize pre-built templates to address regulatory frameworks, including watchlist templates with critical files, directories and registry items for Windows and Linux systems.

Tanium File Integrity and Unauthorized Change Monitoring for ServiceNow enables organizations to sync events from Tanium Integrity Monitor as event records in ServiceNow, where event managers can review each event in detail and automatically correlate with change requests to determine authorization.

- Store events from Tanium Integrity Monitor as event records in ServiceNow.
- Detect authorized changes to files and registries based on existing change requests.
- Automatically flag unauthorized changes and generate alert tickets.

Key capabilities include the ability to:

- Take events from specified watchlists in Tanium Integrity Monitor (IM) and store as event records in ServiceNow, where event managers can review the full details of each event in correlation with the configuration item that generated the event.
- Detect whether there is an existing change request ticket associated with a configuration item that has generated an event.
- Optionally regard events associated with change requests and corresponding change windows as an “authorized change”.
- Optionally create “Tanium IM Alert” records for unauthorized changes.
- Automatically create tickets in a table of your choice from Tanium IM Alert records, with pre-filled dynamic field values.

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.

Schedule a demo

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.