DATA SHEET

Real-time threat hunting with Tanium & Microsoft Sentinel

Identify threats and bad actors in minutes with Tanium's real-time data and Sentinel threat hunting.

Tanium's real-time interaction model with endpoints at scale, combined with Microsoft Sentinel's powerful hunting search and query, empower organizations to proactively look for anomalies, in real time.

Cyber attacks move quickly, and organizations need to see what's happening in real time

Threat hunting plays a critical role in strategic cyber defense, but it is becoming increasingly challenging with teams dealing with evolving threats, both in frequency and sophistication. It's not just threat actors looking for any opening to breach and gain access to the corporate network, ineffective tools and skill gaps and lack of operational resources also play a role.

Traditional threat investigation tools do not have relevant insights for timely response or remediation and lack of automation is forcing SOC staff to spend countless hours trying to make sense of security telemetry.

- A lack of real-time, comprehensive visibility is preventing organizations from managing and securing all endpoints, leaving gaps for attackers to exploit.
- Incidents and investigations can't be efficiently resolved due to the lack of real-time data, and actionable insights.
- After an attack has been successfully stopped, bringing endpoints and the environment back to a healthy state takes too long, leaving them vulnerable to the next attack.

Threat hunting done right means better security with less complexity. Tanium's real-time interaction model with endpoints at scale, combined with Microsoft Sentinel's powerful hunting search and query, provide organizations with the ability to proactively look for anomalies and remediate in real time.

Microsoft

REAL-TIME VISIBILITY

Gather arbitrary endpoint data at scale and combine it with centralized data in Sentinel to reduce time to identification and reduce time to remediation.

FASTER THREAT HUNTING

Proactive action by running threat hunting queries. Early insight into events that may confirm compromise or risk.

LIVE THREAT RESPONSE

Livestream during the compromise and constantly run a specific query. See the compromise and identify location of the next threat action or if the threat is over.

Dynamic, real-time threat investigation and remediation with Tanium & Microsoft Sentinel

Tanium logic app

Tanium pulls live data into Sentinel, which uses advanced KQL to query and visualize the data in log analytics.

- Tanium real-time data enhances Sentinel anomaly queries in minutes.
- All workflows remain within Sentinel (Logic Apps + KQL).

Real-time remediation

Quickly investigate attacks using Tanium-powered Playbooks that are integrated directly into the Sentinel console.

- Execute Tanium remediation actions directly in Sentinel.
- Tanium real-time endpoint data available in the Sentinel console.

Single pane of glass

Tanium & Sentinel integration reduces the load and number of agents required to manage all your endpoints.

- Sentinel is the primary experience for incident response with Tanium's investigation and response capabilities fully integrated.
- Less switching between product consoles lets teams move quickly and accurately to perform incident response.

The Tanium platform

The Tanium 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 the visibility and control needed to help you continuously manage your organization's endpoint risk.

SEE TANIUM IN ACTION

Experience visibility, control, and trust with the industry's only converged endpoint management (XEM) platform.

Schedule a demo

Learn about our Microsoft partnership →

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.