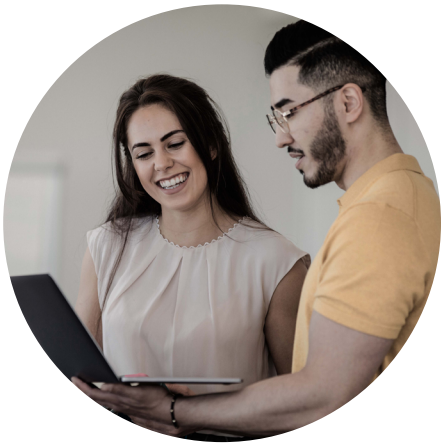
SOLUTION BRIEF

Tanium & Amazon Security Lake

Tanium endpoint data is available in Amazon Security Lake to drive more complete and effective incident investigations.

Tanium logs in Amazon Security Lake create a holistic view of your organization's security risks. With this integration, it's simple and easy to add Tanium's comprehensive visibility to your data lake in an open source format.



Address gaps in security visibility and compliance

Many cyberattacks now go undetected for days, weeks, or even months. The sooner you can spot these attacks, the sooner you can stop them, and the less harm you will suffer. Yet many organizations are struggling to build the holistic view of their environment they need to detect, investigate, and resolve attacks quickly.

Incident response frequently requires the ability to analyze security-relevant telemetry and log data by using multiple tools, technologies, and vendors. Analysts struggle with accessing the logs and having the logs in a format ready for analytics.

Every security tool defines and organizes its security data under its own schema, and often uses different names and conventions for the same things.

Gain a single, unified view of your environment to rapidly detect, investigate, and resolve security incidents

Tanium collects all of the key endpoint data that security and operations teams need to detect, investigate, and resolve incidents. This data is now available in the customer's own data lake in an open source format.

- Combine Tanium's endpoint data with other data sources in your data lake to drive effective incident investigations
- Centralize your security data from Tanium, Amazon Web Services (AWS) environments, SaaS providers, on-premises, and cloud sources into a purpose-built data lake that is stored in your AWS account
- Use an open source schema for the normalization of security telemetry and keep the logs in your own data lake

Operators struggle with a fragmented, inaccurate view of their environment

Tanium Converged Endpoint Management (XEM) platform

Collect endpoint data that your teams need to detect, investigate, and resolve incidents.

- Tanium generates complete, accurate, real-time data for every endpoint – whether managed or unmanaged – across environments of every size and level of complexity

Automatically centralize your security data in a few steps

Amazon Security Lake

Use Amazon Security Lake to unify your security data and improve the protection of your workloads, applications, and data.

- Security teams are spending more time wrangling security data than analyzing it.

Send Tanium Logs to Amazon Security Lake in an open Source format

Tanium logs in the Open Cybersecurity Schema Framework (OCSF) format.

Gain a holistic view of your security risks by using Tanium logs with your other security logs.

- Security operators need logs from multiple tools, technologies to do analytics.

Amazon Security Lake, and Tanium are giving security teams a unified view to stop threats faster

Security operators need logs from multiple tools, technologies to do analytics

Tanium is the only converged endpoint management (XEM) platform that provides visibility, control, and remediation through a single, lightweight, distributed solution.

Tanium generates complete, accurate, real-time data for every endpoint – whether managed or unmanaged – across environments of every size and level of complexity.

- Create a complete and accurate inventory of all endpoints in minutes
- Discover hidden and hard-to-find endpoints that CMDBs and other tools miss
- Identify vulnerabilities, compliance gaps, missing patches and updates, or misconfigurations across every endpoint in the environment in minutes
- Locate changes to sensitive data fields, configurations, access rights, or IoCs
- Monitor sensitive data, and set up alerts that trigger during potential incidents
- Enrich asset catalogs and make security workflows smarter and stronger
- Fill some of the most common gaps in many organizations' security data pools
- Drive a more complete detection, investigation, and remediation of threats

of cybersecurity data across tools and sources

Security Lake centralizes security data from Amazon Web Services (AWS) environments, software as a service (SaaS) providers, on-premises, and cloud sources into a purpose-built data lake that is stored in your AWS account.

Store and analyze multiple years of security data quickly.

- Use your preferred analytics tools to analyze your security data while retaining complete control and ownership over that data
- Centralize data visibility from cloud and on-premises sources across your accounts and AWS Regions
- Optimize and manage your security data for more efficient storage and query

Streamline and accelerate security operations to resolve incidents faster

Amazon Security Lake helps to streamline security investigations by aggregating, normalizing, and optimizing data storage in a single security data lake.

Send your Tanium logs to Amazon Security Lake to simplify incident response and compliance.

- Analyze multiple years of security data quickly
- Simplify your compliance monitoring and reporting
- Facilitate your security investigations with elevated visibility

Create a holistic view

Send your Tanium logs to Amazon Security Lake in an open source format

Amazon Security Lake uses the Open Cybersecurity Schema Framework (OCSF) and the following Tanium logs are available in the OCSF schema:

- Asset metadata from Core platform sensors, Asset module data, or Discover module data to facilitate comprehensive visibility, inventory, and asset enrichment across managed and unmanaged assets
- Tanium Comply vulnerability findings for operational vulnerability reporting and enrichment of security incidents
- Tanium Comply compliance findings for operational configuration compliance and enrichment of security incident

Threat Response recorder data represented as Threat Response Alerts and Stream could fall under several OCSF Category's such as Findings, System Activity, and Network Activity.

LEARN MORE ABOUT TANIUM AND OCSF

Open Cybersecurity Schema Framework (OCSF) is an open standard that can be adopted in any environment, application, or solution provider and fits with existing security standards and processes.

Learn more →