Tanium Partnership overview

Joint value proposition

Together, Sumo Logic and Tanium provide organizations the ability to quickly discover, diagnose and remediate both operational and security incidents powered by streamlined endpoint management, real-time security analytics and cloud-native, enterprise SIEM.

IT/Ops

Tanium's Operations Suite and combined with correlated data collected by Sumo Logic's Continuous Intelligence Platform allows IT and Operations teams to discover, classify, monitor and operate on critical assets, infrastructure and services across the entire organization in real-time, reducing time spent diagnosing and troubleshooting issues.

Audit/Compliance & Security Analytics

Manage existing audit and compliance processes in Sumo Logic in a single pane of glass alongside data collected from Tanium's Risk Suite, enabling security teams to quickly react and remediate based off of key security insights and events collected from vulnerability scans, security benchmarks, compliance audits, system integrity monitors and unintended exposure of sensitive data.

SIEM

Collect, normalize, correlate and enrich data from Tanium's Threat Response and Enforce modules with other security alerts via a cloud-to-cloud integration with Sumo Logic's Cloud SIEM to reduce alert fatigue on your SOC and drive more automated, cost effective security investigations.

Technology integration

- Sumo Logic takes advantage of Tanium's existing Connect module.

- Tanium Connect provides out-of-the-box functionality to route the output of various Connect Sources (e.g. Saved Questions and Events) to Sumo Logic as an HTTP or Syslog Destination.

- Tanium Threat Response customers can leverage Stream to send endpoint telemetry directly to Sumo (e.g. launched processes, opened sockets, file changes, etc.).

- Sumo Logic users can then visualize, correlate and act on data in Sumo Logic to address operational alerts, security events and more using Webhook Connections.