TANIUM

Chronicle for Tanium

Unleash Endpoint Security Telemetry for Threat Investigation, Hunting and Detection

Tanium Endpoint Protection Platform

Tanium is a market leader in endpoint security management. The combination of Tanium's Core EDR capabilities coupled with its response and compliance modules provide unparalleled speed, visibility and scale in managing endpoints including laptops, servers, virtual machines, and cloud infrastructure. The Tanium platform provides rich security telemetry about actions and events on endpoints that are critical to modern security operations - across detective, investigative and response workflows. This data is ideally meant to enrich systems such as SIEMs, log analytics tools, help desk ticketing systems etc. by feeding them with up-to-the-second data from every endpoint in the environment.

Benefits

- Endpoint Management: built to scale to support any organization
- Lower TCO: single solution for security and operations
- Visibility: spanning threat detection, system configuration, and compliance

Benefits

- Infinite elasticity: with a backend built on core Google infrastructure
- Disruptive pricing: that removes disincentives to ingest and analyze all security telemetry
- Instant search: across a full year of security telemetry to uncover latent threats
- Cloud-native: solution built to auto-scale and eliminate data management overhead

chronicle

Addressing EDR Telemetry Analysis Challenges with Chronicle

Organizations struggle to harness the value of endpoint security telemetry due to scale, cost and deployment challenges that arise when sending complete endpoint data to legacy security analytics solutions. Chronicle is a security analytics platform built on core Google infrastructure that transforms security operations outcomes by addressing those very problems. Specifically Chronicle provides the only security analytics platform designed for:

Chronicle for Tanium

Many Tanium customers already send endpoint data to Chronicle and combine it with other data types to extract the full analytical value of their security telemetry. The augmented integration now enables an additional advantages and capabilities that are only available with Tanium EDR deployments:

Time to Value

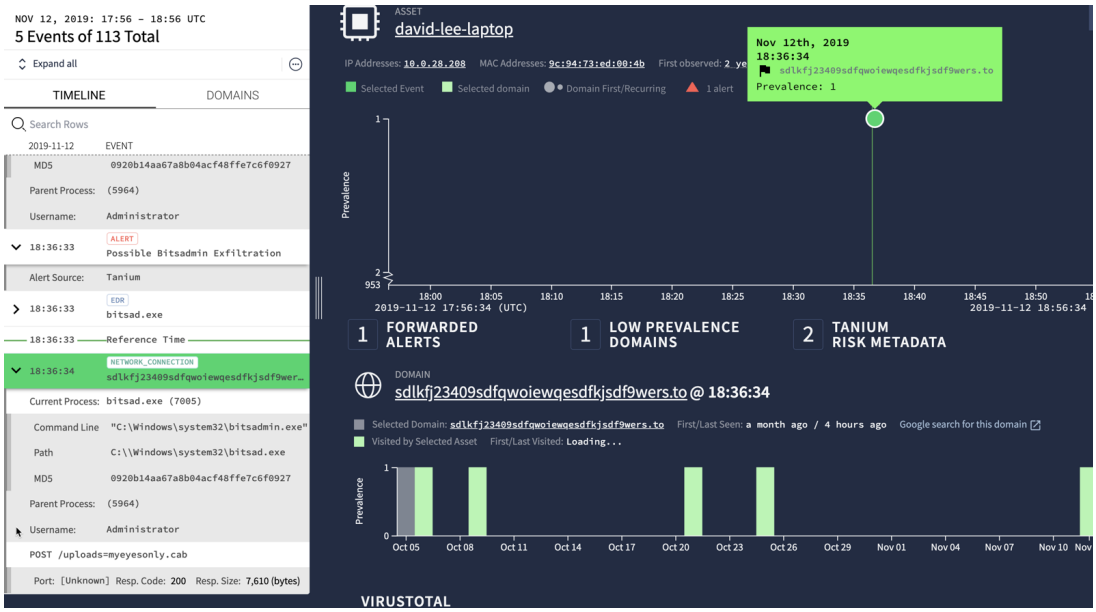
The Tanium platform now supports direct integration with Chronicle's ingestion APIs and its Unified Data Model (UDM). The API integration enables Tanium agents to stream data directly to Chronicle's cloud pipeline and into a private tenant with a zero-footprint deployment. By streaming data to Chronicle's ingest APIs directly in UDM format, Tanium is also pre-integrated with future capabilities such as the Chronicle Rules Engine.

Full Visibility

Chronicle is the only solution that can be instantly provisioned as a pre-integrated backend for all Tanium endpoint events. Other security analytics solutions are limited to ingesting endpoint alerts with deployment overhead of parsers and forwarding components. The full set of telemetry includes all process, registry, file and other endpoint event and sub-event types. Additionally, the entire set of telemetry is retained for a full year by default in hot state with guaranteed sub-second search latency.

Security Operations Efficiency:

A common challenge with threat investigations in traditional log search driven tools is the complexity of searches needed to uncover connections between data elements. For example, making connections between parent process IDs and child processes requires executing advanced queries and combining results. Chronicle provides highly curated views that enable any security analyst to seamlessly pivot across domain, IP, URL, hash/process centric views with the connections pre-aliased and stitched together. This automated and continuous aliasing and correlation across Tanium endpoint events and other data sources (DNS, DHCP, web proxy, security alerts and more) enables security teams to investigate and hunt 100x faster.



chronicle