SECURONIX™ | TANIUM™

SOLUTION BRIEF

Securonix + Tanium: Enhanced Endpoint Monitoring Solution

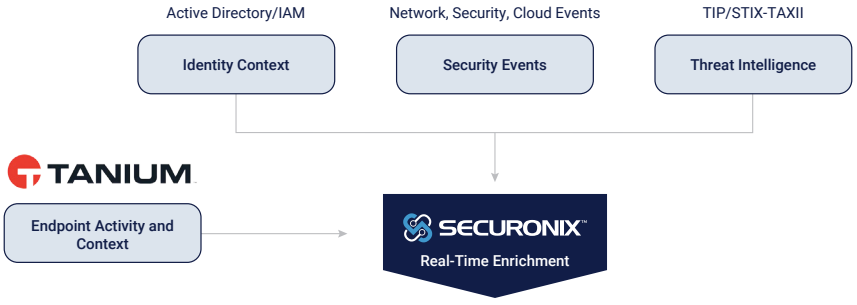
Detecting Advanced Attacks Requires Context and Analytics

Attacks today are much more advanced and harder to detect. The traditional one-dimensional approach of endpoint detection and response (EDR) point solutions, which detect threats based on limited end-point telemetry and basic rule-based techniques, may be sufficient for low-level threats, but does not scale for sophisticated advanced persistent threat (APT) type attacks. This one-dimensional approach leaves your organization vulnerable to attacks that can be significantly damaging, both financially and to your reputation.

The Securonix-Tanium Solution

The partnership between Securonix and Tanium brings together the best of endpoint security and security monitoring to deliver a packaged solution that significantly enhances your ability to detect, investigate, and respond to advanced threats.

Securonix provides out of the box integrations and content needed to collect data from Tanium and analyze it for advanced threat detection and response. With over 50 out of the box queries, Securonix's integration spans across multiple Tanium product modules including Tanium Asset, Tanium Threat Response, and Tanium Comply.



- Context Enriched Events - Search and Investigate
- Analytics Use Cases - MITRE Models
- Incident Response - SOAR Actions via Tanium

Context-Enriched Events

Securonix correlates the telemetry information from Tanium with security event data from other data sources. This contextual data includes identity information, threat intelligence, network context, and more. This enriched data creates a rich correlated event dataset that can be used for advanced analytics, search and investigation, and incident response.

Securonix enrichment happens in real time, so that the point-in-time information is captured. This provides the Securonix analytics engine with a complete picture that allows it to better detect threats, and also allows the SOC analysts to investigate and respond to threats quicker.

Solution Benefits

- **Improved Threat Detection**
  Combine rich endpoint telemetry from Tanium with the advanced behavior analytics of Securonix to detect and prioritize high risk threats.
- **Quick Time to Value**
  Securonix provides out of the box integration and content for Tanium.
- **Faster, More Accurate Searching**
  Securonix enriches Tanium events with additional context, including identity, asset, network, and threat intelligence, significantly reducing the amount of time required to perform root cause analysis.
- **Reduced Mean Time to Respond and Remediate**
  Securonix provides out of the box incident response playbooks for Tanium as part of the SOAR content. Customers can use these playbooks to automate incident response actions and significantly reduce the time to respond to incidents.

Analytics Use Cases

Securonix provides over 80 use cases that can be enabled out of the box without any additional configuration changes. Use cases are mapped to the following broad categories of threats:

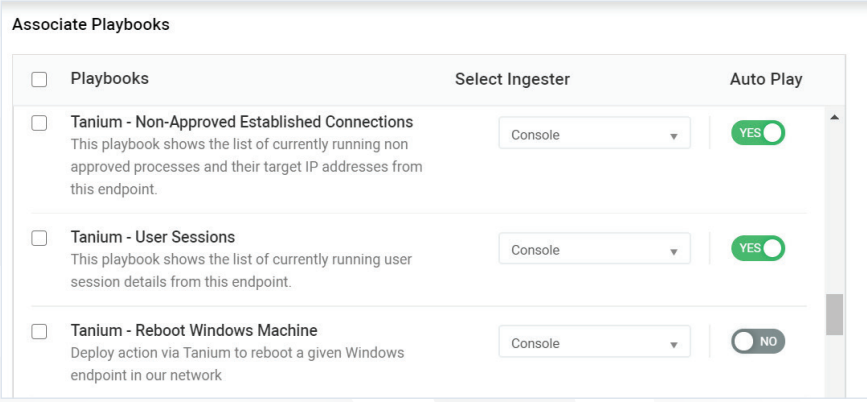
Use Case Category	Sample Tanium Alerts	Sample Threat Chain
Insider Threat: Privilege Misuse	• Anomalous privilege escalation • Suspicious registry changes • Local account usage/ local authentication	Suspicious login (VPN Alert) + Privilege escalation + Anomalous File Operations + Beaconing (Proxy Alert)
Insider Threat: Data Compromise	• Spike in access to critical assets • Changes to file permissions • Access to sensitive shares	Untrusted User (Identity Alert) + Spike in Access to Critical asset + Data Exfil – File Upload, Email to Self (DLP, Email, Proxy Alert)
Cyber Threat	• Vulnerable asset • Rare process or executable • File or registry modifications • Rare port or protocol	Process Anomaly + Unusual Port/Protocol + Beaconing (Firewall Alert) + Malicious Destination IP (Threat Intel Alert)
Insights: Assets/ Patch	Classification of sensitive/ vulnerable assets	Prioritized Asset + Any of the alerts outlined above

MITRE-Based Threat Chains

Securonix analytics do not rely on individual anomalies. Such triggers, in a large and complex organization, can result in a lot of false positives. Securonix uses threat chains, based on the MITRE framework, to stitch together related alerts over a period of time. This enables your organization to prioritize and act on real threats in timely fashion.

Incident Response Automation using Tanium

Securonix has built in playbooks that can automate incident response actions with Tanium. This includes the ability to kill a process, quarantine a file, and more.



About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000