CASE STUDY

Leading Pharmaceutical Company Uses Securonix With Tanium To Identify Threats To Vulnerable Endpoints

CASE STUDY

Leading Pharmaceutical Company Uses Securonix With Tanium To Identify Threats To Vulnerable Endpoints

Large Pharmaceutical Distribution Company

Based in the United States, this company is one of the world's largest pharmaceutical distributors with over 150 global offices in more than 50 countries worldwide. It provides drug distribution and related services designed to reduce costs and improve patient outcomes. As of 2019 they are ranked in the top 10 of the Fortune 500.

The Challenge: Detecting Advanced Threats to Vulnerable Endpoints

The pharmaceutical industry is seeing a significant uptick in cyberattacks targeting research patents and trade secrets. Targeted attacks are becoming more advanced and require an approach that can detect malicious zero-day type attacks.

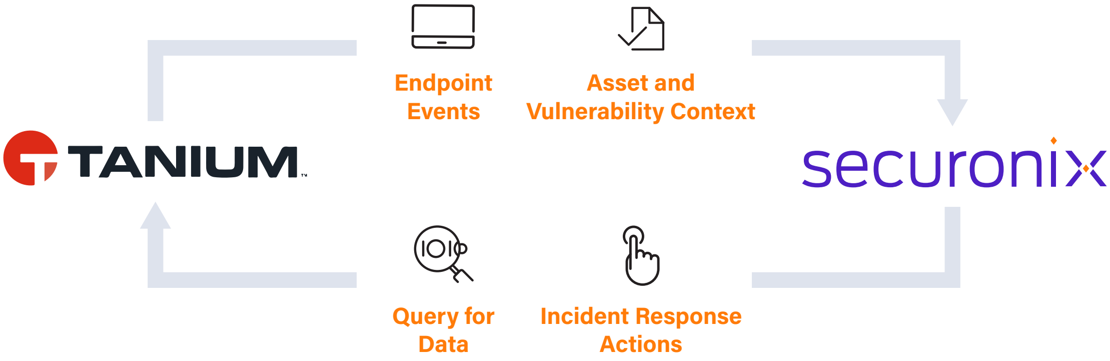
With siloed endpoint and security monitoring tools, the organization received low fidelity alerts without the adequate context to prioritize alerts. This made investigation a highly manual process, putting the organization at a significant risk of a data breach.

Key Challenges

- Inability to differentiate between true threats and false alarms
- Long detection and investigation times increase the risk of a data breach
- Inability to quickly detect and respond to phishing attacks
- Lack of behavioral analytics to contextualize insider behaviors

The Solution: Securonix and Tanium Integration

In order to enhance threat detection, the organization integrated Tanium and Securonix Next-Gen SIEM implementations to unlock out-of-the-box use cases to detect and prioritize threats.



How the Securonix-Tanium Integration Works

Securonix uses Tanium endpoint context data to identify threats and uses built-in queries to proactively collect endpoint telemetry. Analysts need as much information as possible up front to respond successfully to insider threats, so they have the context they need to respond. The organization did so by integrating both technical (email, proxy, DLP, etc.) and non-technical (HR, etc.) data into the Securonix platform, making it available for investigations.

Here's how it works:

1. Securonix provides out-of-the-box queries to collect endpoint telemetry and events from Tanium.
2. Securonix analyzes and correlates Tanium data with other network, cloud, and application anomalies to detect malicious threat patterns.
3. Securonix uses Tanium asset and vulnerability context to determine risk scores for vulnerable and high priority assets.
4. Securonix initiates remediation actions on endpoints using Tanium response integration.

Integration Use Case in Action: Detect Malicious Command and Control

- The security team recieves an alert from a phishing attack, such as an employee receiving a phishing email.
- The alert was triggered based on an analysis of Tanium events, such as an anomalous PowerShell process on that employee's endpoint.
- Another alert is based on firewall events, such as an endpoint attempting to make suspicious connections to an external domain.

Securonix threat chains combine these alerts into a single event and prioritizes the threat for investigation and remediation.

The Business Impact: Detect and Prioritize Unknown Threats

Reduced Risk and Mean Time To Respond

By integrating Tanium vulnerability and asset context with other data sources, Securonix accurately determines which assets within the corporate environment are vulnerable, and elevates their risk score in order to reduce the risk of attack success.

Improved Efficiency

Built-in Securonix SOAR enabled the organization to respond faster and remediate endpoint threats. A single pane of glass view gave the analysts the visibility they needed to take fewer steps to detect, investigate, and remediate threats.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, SOAR, Security Data Lake, NDR and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information visit www.securonix.com.