CASE STUDY

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

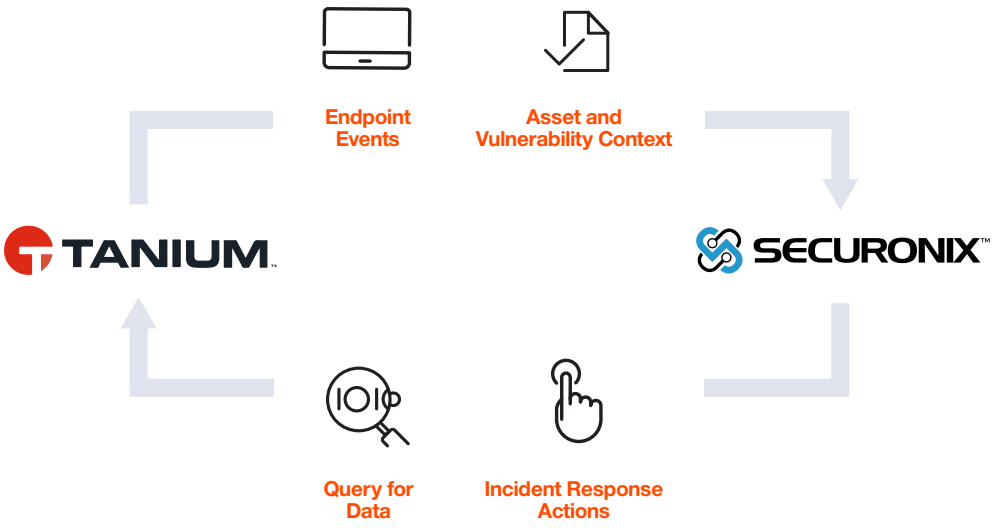
The Challenge: Detecting Advanced Threats Targeting Endpoints

The pharmaceutical industry is seeing a significant uptick in cyber-attacks 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 was receiving low fidelity alerts without adequate context and prioritization. This increased the time and resources needed to investigate threats, putting the organization at a significant risk of a data breach.

The Securonix-Tanium Solution

In order to enhance their threat detection capability, the organization integrated their Tanium and Securonix solutions and implemented the out-of-the-box Tanium use cases Securonix provides to detect and prioritize threats that would otherwise go unnoticed.



Company Profile

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.

How the Securonix-Tanium Integration Works

In order to reduce the risk of insider threats, analysts use Securonix to look for nefarious activities caused by complacent, ignorant, and—most importantly—malicious insiders. For analysts to be able to effectively respond to insider threats, they need as much information as possible up front, so they have the context needed to act on a case. This organization accomplishes that by bringing both technical (email, proxy, DLP, etc.) and non-technical (HR, etc.) data into the Securonix platform so that the data is available for investigations.

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

Integration Use Case in Action: Detect Malicious Command and Control Activity

1. Alert from a phishing tool. An employee has received a phishing email.
2. Alert in Securonix, based on an analysis of Tanium events. There is an anomalous PowerShell process on that employee's endpoint.
3. Alert based on firewall events. The endpoint has attempted to make suspicious connections to an external domain.

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

The Business Impact: Detect and Prioritize Unknown Threats

Reduce Risk and Mean Time To Respond

By integrating Tanium vulnerability and asset context with other data sources, Securonix can accurately determine which assets within the corporate environment are vulnerable, elevating their risk score and reducing the risk of attack success.

Securonix uses Tanium endpoint context data to identify threats and uses built-in queries to proactively collect endpoint telemetry.

Improve Efficiency

Built-in SOAR from Securonix enables faster response to remediate endpoint threats. The Securonix user interface's single pane of glass view means that analysts need to take fewer steps to detect, investigate, and remediate threats.

About Securonix

Securonix is redefining SIEM using the power of big data and machine learning. Globally, customers use Securonix to address their insider threat, cyber threat, cloud security, and application security monitoring requirements. For more information visit **www.securonix.com**.

SECURONIX™

LEARN MORE
www.securonix.com

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