Tanium XEM Core

Detection Strategy Guide

July, 2025

Product Overview

Tanium XEM Core is a converged endpoint management (XEM) platform that provides real-time visibility, control, and response across distributed endpoints at scale. The platform queries and acts upon every endpoint in seconds, providing a live, accurate picture of the entire IT environment in a single console.

This comprehensive, real-time data allows teams to ask questions about their environment and receive immediate answers, enabling proactive cyber hygiene and rapid incident investigation. It combines deep asset inventory and patch management with endpoint detection and response (EDR), empowering teams to not only identify and remediate system weaknesses but also to hunt for advanced threats and execute immediate, targeted responses.

Detection Strategy for Tanium XEM Core

Detection

Our endpoint detection strategy focuses on two common signal types: process and network events. By integrating directly with EDR vendors, we can process security alerts to extract evidence and normalize event details. These normalized signals are then processed through our detection engine to look for signs of post-exploitation activity.

In addition to categorical handling of vendors' security alerts, Expel maintains a large library of behavioral detections to augment vendor detections. When a threat is detected, our automated response bot, Ruxie, takes action by enriching evidence fields with first- and third-party threat intelligence. Additional Ruxie actions query a wide span of technologies directly to arm analysts with key pieces of investigative information and related events.

Response

Endpoints provide rich context for processes and also support other types of Expel Alerts. For example, we use source device identification across a number of alert types when a source IP or hostname is available, because it provides rich context about the actor behind the activity. Additionally, endpoints provide valuable information for network alerts to help identify what process triggered a connection.

To learn more about our overall approach to detection strategy, see About Detection Strategy in the Help Center.

What We Support for Tanium XEM Core

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Tanium XEM Core, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Tanium XEM Core detection rules support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	Yes. The integration provides multiple capabilities for investigation, including: ■ Query IP ■ Query Files ■ Query Users ■ List Files
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

Additional Details and Common Questions

Console Access

A vendor alert does not typically include all of the contextual timeline activity surrounding the event of interest. Because this integration does not allow us to get all necessary data via the API, we will ask you for a certain level of console access during onboarding.

The level of access that we require is meant to support essential triage and research activities, and to help us determine the vector and extent of attacker activity for an identified threat. At minimum, we will ask for visibility into alert data, timeline events recorded, and live response/real time response shell (if applicable).