Palo Alto Networks Cortex XDR Pro

Detection Strategy Guide

July, 2025

Product Overview

Cortex XDR is an extended detection and response (XDR) platform that integrates data from endpoint, network, cloud, and identity sources to provide comprehensive visibility and stop sophisticated attacks. The platform is designed to move beyond traditional, siloed security tools by correlating disparate data points to reveal the root cause and sequence of an attack, significantly reducing alert volume and simplifying investigations for security analysts. By applying machine learning and behavioral analytics, Cortex XDR profiles user and device activity to detect anomalous behaviors indicative of a compromise. It combines next-generation antivirus capabilities with endpoint detection and response (EDR), enabling security teams to not only prevent known and unknown malware but also to hunt for threats and orchestrate a rapid response directly from the console, such as isolating endpoints or blocking malicious indicators.

Detection Strategy for Endpoint Integrations

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 Palo Alto Networks Cortex XDR Pro

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 Palo Alto Networks Cortex XDR Pro, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported event log sources	■ Alert ■ Incident
Palo Alto Networks Cortex XDR Pro detection rules support	Yes.
Detection rules written by Expel	Yes.
Auto remediations	Yes. Expel supports automatic execution of some remediation actions for this integration when you follow our setup guide to update the permissions in your vendor device, and then enable the auto remediation in Workbench. The available auto remediations for this integration include: ■ Palo Alto Cortex XDR: Block Bad Hashes ■ Cortex XDR: Contain Hosts To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
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).

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain events as needing an immediate verification or notification, and bypasses the normal internal event triage process. The events subject to DUET rules contain behaviors that are not typically indicative of true security incidents, as they are related to policy violations or *potential* risk.

There are a number of workflows that a DUET may follow. When enabled, the activity will be flagged for investigation and will be routed to you (rather than to us) to take a specified first action. To see the specific DUET rules currently supported for this integration, visit the Detections page in Workbench.