Broadcom Carbon Black EDR

Detection Strategy Guide

July 2025

Product Overview

Carbon Black EDR (now part of Broadcom Carbon Black) is a cloud-native endpoint detection and response (EDR) and next-generation antivirus (NGAV) platform that provides comprehensive endpoint security through continuous monitoring and behavioral analysis. The platform combines real-time threat detection, incident response capabilities, and advanced threat hunting tools, utilizing streaming prevention and detection engines to identify malicious activity across Windows, Mac, and Linux endpoints.

Carbon Black's detection engine continuously monitors endpoint behavior and process execution, creating a detailed timeline of system activity that enables security teams to trace attack paths and understand the full scope of security incidents. The platform generates alerts when suspicious behaviors or known malicious activities are detected, with events categorized by severity and threat type in the Carbon Black console.

Carbon Black utilizes a behavioral monitoring approach, which focuses on tracking process relationships and system changes rather than relying solely on signature-based detection. This allows the platform to detect fileless attacks, living-off-the-land techniques, and previously unknown threats through anomalous behavior patterns.

Workbench obtains data from Carbon Black through:

- API polling – retrieves alerts, threats, and security events from the Carbon Black console for evaluation and correlation within Workbench.
- Response Actions – Carbon Black can perform rapid response actions based on Expels SOC workflows.

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 Broadcom Carbon Black EDR

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 Carbon Black EDR, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Carbon Black EDR detection rule support	Yes.
Detection rules written by Expel	Yes.
Investigative support through Workbench	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: ■ 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).