Will this

CrowdStrike Falcon Insight XDR

Detection Strategy Guide

June 2025

Product Overview

CrowdStrike Falcon Insight XDR is a cloud-native platform that provides comprehensive endpoint security by combining next-generation antivirus (NGAV), endpoint detection and response (EDR), and managed hunting services through a single lightweight agent. This platform leverages AI and machine learning to detect and prevent threats, including malware, fileless attacks, and zero-day threats, while also offering visibility into endpoint activity and the ability to quickly investigate and respond to security incidents.

Detection logic curated by CrowdStrike is applied to events on the endpoint, with an evaluation of executables loaded into memory, or is applied to events received by the cloud server. Events that match the CrowdStrike detection logic generate alerts (known as detections) in the CrowdStrike console.

CrowdStrike has an add-on called Overwatch that provides the expertise of CrowdStrike human analysts for alert review and threat hunting. Workbench obtains data from CrowdStrike in two ways:

- Alert polling – done through CrowdStrike APIs so Workbench can evaluate CrowdStrike detections and incidents.
- Falcon Data Replicator (FDR) – forwards a copy of CrowdStrike Falcon Insight XDR's endpoint data stream to Splunk or Sumo Logic to support the Expel Hunting service.

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

See more about our overall approach to Detection Strategy here in our overview guide. 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 CrowdStrike Falcon Insight XDR

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 CrowdStrike Falcon Insight XDR, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ Falcon Enterprise ■ Falcon Premium ■ Falcon Complete
Supported platform	■ Windows ■ Linux ■ Falcon Complete
CrowdStrike Falcon Insight XDR detection rules support	Yes.
Detection rules written by Expel	Yes.
Remediation support	Yes. We offer a full suite of remediation actions for this integration, and use our expertise to determine which ones are most appropriate for your specific incident. For a detailed list of *all possible* remediation actions, contact your Sales or Support rep.

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: ■ Block Bad Hashes ■ Contain Hosts ■ Delete Malicious FIles ■ Delete Registry Key ■ Kill Processes To enable auto remediations for your environment, see Enable an Auto Remediation in Workbench in the Help Center.
Investigative support through Workbench	No. We access the console directly with an "Investigator" role account.
Hunting support	Yes, if CrowdStrike Data Replicator is enabled and sending all events to supported SIEMs (Sumo Logic or Splunk). If you plan to enroll in the Expel Hunting service, your organization needs a Falcon Data Replicator subscription and provide access for Expel to extract logs via supported SIEMs.

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.

Machine Learning and Cloud-Based ML Alerts

The Expel alert poller consumes all Falcon alerts except Machine Learning and Cloud-based ML with a vendor severity of Information or Low.

IOA/IOC Detections

Custom IOA/IOC detections are supported on a case-by-case basis by request. In general, Expel ingests CrowdStrike custom IOCs/IOAs and processes them against our general detection rules, but does not map them as lead alerts. We cannot surface them wholesale due to concerns with fidelity and volume.

Generally, they will only surface as an Expel Alert directly if there are indicators or patterns detected by broad detections. If you have questions about specific IOA/IOC alerts, please file a support ticket with as much detail as possible about the fidelity and use case.

CrowdStrike Console Alert Resolution

When onboarding CrowdStrike in Workbench, if “Mark in console” is enabled then Workbench updates alerts as “in-progress” in the CrowdStrike console after the SOC analysts starts investigating a CrowdStrike alert through Workbench. Workbench doesn't currently have the capability to update an alert in the CrowdStrike console upon investigation completion. SOC analysts don't manually update the status of alerts in the CrowdStrike console.