Vectra AI (NDR)

Detection Strategy Guide

August, 2025

Product Overview

Vectra AI is a cybersecurity company that uses artificial intelligence to detect and respond to cyber threats, particularly in hybrid and multi-cloud environments. They offer a platform that analyzes network traffic and behavior to identify and prioritize malicious activities, ultimately helping security teams to investigate and remediate threats more effectively.

Detection Strategy for Vectra AI (NDR)

Detection

Network traffic monitoring is a critical element of our detection strategy, offering insight into the activity of data as it moves across an organization's systems. The network traffic data source focuses on network connection creation (the initial construction of a network connection such as socket information, and src and dst IP and Ports), network traffic content (logged network traffic data showing both protocol header and body values like PCAP), and network traffic flow (summarized network packet data, with metrics, such as protocol headers and volume like netflow or http logs).

For Vectra, Expel focuses on ingesting detection events and enriching them with additional entity details. We can then leverage our detection pipeline to surface relevant alerts based on a number of criteria:

- **Severity** - Vectra's AI assigns a 'Severity Score' to every detection. This score is calculated based on threat score, certainty, and potential impact.
- **Certainty** - Vectra's AI assigns a 'Certainty Score' to every detection. This score represents how confident Vectra is that the activity is *not* a false positive.
- **Entity Urgency** - Vectra's AI assigns an 'Urgency Score' to hosts and users in your environment. This score increases and decreases based on observed activity.
- **Redundancy** - We prioritise detections that are not already covered by another integration in order to avoid duplication.

Our strategy for Vectra also aligns with our overall detection strategy, see About Detection Strategy in the Help Center for more information.

Response

Network technologies are utilized for support across many types of Expel Alerts such as endpoint and cloud. The main focus of the response strategy is on source IP, destination IP, and domain tracking to identify related connections, along with user activity summaries to give extra alert context.

What We Support for Vectra AI (NDR)

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 Vectra AI (NDR), you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ API v3.4+ (RUX)
Supported platform	■ Vectra AI (NDR)
Vectra AI (NDR) detection rules support	Yes.
Detection rules written by Expel	No.
Investigative support through Workbench	No. We access the console directly with a "SOC Analyst" role account.
Hunting support	No. Hunting is not currently available for this integration.

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.

Use Cases Not Supported

- We do not support custom or community-provided rules for Vectra.
- We do not support any remediation/auto-remediation actions with our Vectra integration.