Microsoft Defender XDR

Detection Strategy Guide

September, 2025

Product Overview

Microsoft Defender XDR is a unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks. Microsoft Defender XDR helps security teams protect their organizations and detect threats by using information from other Microsoft security products.

Detection Strategy for XDR Integrations

Detection

XDR technology combines the capabilities of a standalone detection engine to generate alerts, with the ability to leverage raw vendor telemetry for custom detections. The custom detections are not authored by Expel, so how we ingest and action on the XDR alerts depends on the XDR category.

This XDR integration is categorized as supporting both **native detections** and **custom detection rules**. This means we may leverage either native alerts or custom rules to map the XDR alerts to our own ingestion criteria.

For native detections, we consume these events through a mix of raw log analysis and security alert processing, which are then run through our detection engine to look for signs of post-exploitation activity. 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 in order to directly arm analysts with key pieces of investigative information and related events

Custom rules are subject to Expel's evaluation and will be accepted based on:

1. **Fidelity** - the detection rule should have an alert volume that suggests high fidelity (for example, an average weekly alert volume less than 10 generally suggests the rule has high fidelity)
2. **Redundancy** - the detection rule name, description, and query should not duplicate (or suggest a duplication of) alerts that would surface through a direct API integration with a non-XDR technology
3. **Evidence** - the detection rule must provide Expel with an adequate number of artifacts to action upon (two or fewer artifacts suggests insufficient information for our SOC analysts)
4. **Scope** - the detection rule name, description, and query must align with your service and should not be written for a different category of service

If we are unable to support a custom rule because it does not meet the criteria above, we will let you know so that you can make modifications and resubmit.

For accepted custom rules, Expel will provide you with a report that details our projected level of support. Contact your Sales or Support rep for more details.

Response

XDR telemetry provides additional information that can be useful for Expel to disposition alerts. With the exception of investigative-only XDRs, we will follow our normal event triage process and create an Expel Alert that is sent to our SOC analysts for analysis. We may also run queries against your XDR logs to search for additional types of data, which we use to enrich our alerts with additional context.

What We Support for Microsoft Defender XDR

To see a comprehensive list of the most up-to-date XDR rules and available DUETs (**d**id yo**u** **e**xpect **t**his) that we support for Microsoft Defender XDR, ask your Sales or Support rep for the most recent download (not all XDR rules are visible on the Detections page in Workbench).

Supported event log sources	Microsoft 365 Defender and associated detection sources
Microsoft Defender XDR detection rules support	Yes.
Detection rules written by Expel	Yes.
Custom rules support	Yes.
Investigative support through Workbench	Yes. Expel analysts are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query Host ■ Query IP ■ Query Logs ■ Query User
Hunting support	No. Hunting is not currently available for this integration.

Additional Details and Common Questions

Console Access

An XDR 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. Granting it is optional, but is strongly recommended.

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).

Historic Volume

We use historic volume to determine projected XDR alert volume, which helps us decide whether or not a particular detection is appropriate to send to our SOC. We target 30 days as the ideal period of time to check on volume, and two weeks as the minimum. This gives us the confidence we need to properly evaluate incoming XDR alerts in a way that does not flood the SOC with benign activity.

DUET

A DUET (**d**id yo**u** **e**xpect **t**his) rule flags certain XDR alerts as needing an immediate verification or notification, and bypasses the normal internal event triage process. The alerts 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

Use Case	Description	Reason
Defender for O365 and Defender for Cloud - Investigative Only Support	Microsoft Defender XDR ingests Defender for O365 and Defender for Cloud alerts and signals.	Expel currently does not support Defender for O365 and Defender for Cloud. We will provide investigative-only support for the interim; Expel will be able to provide full support once these integrations and detection strategies are developed and released.