



# Cisco Umbrella

Detection Strategy Guide

June, 2025

## Product Overview

Cisco Umbrella uses the Internet's infrastructure to enforce security and block malicious activity before a connection is ever established. It operates in the cloud so there is no hardware to install and no software to manually update.

## Detection Strategy for Network Integrations

### 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).

We pull this information into our detection pipeline as events in the form of both security alerts and raw telemetry (depending on the integration). 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

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.

To learn more about our overall approach to detection strategy, see [About Detection Strategy](#) in the Help Center.

## What We Support for Cisco Umbrella

To see a comprehensive list of the most up-to-date Expel detection rules, vendor detection rules, opt-in detections, and available DUETs (**did you expect this**) that we support for Cisco Umbrella, you can visit the [Detections page](#) in Workbench or ask your Sales or Support rep for the most recent download.

<b>Supported event log sources</b>	<ul style="list-style-type: none"> <li>■ Organization Security Activity Report events</li> </ul>
<b>Cisco Umbrella detection rules support</b>	Yes.
<b>Detection rules written by Expel</b>	Yes.
<b>Investigative support through Workbench</b>	<p>Yes. We are able to take the following investigative actions to gather data for triage and investigation of events.</p> <ul style="list-style-type: none"> <li>■ Query IP</li> <li>■ Query Domain</li> <li>■ Query Host</li> <li>■ Query File</li> <li>■ Recent Network Events</li> <li>■ EDR Correlation Events</li> </ul>
<b>Hunting support</b>	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 (**did you expect this**) 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

Use Case	Description	Reason
Triage of DNS policy categories <i>other than</i> referenced in the detection support above	Monitoring, triage and investigation of other categorized DNS events.	Several of the categories generate high volume, low-fidelity events. This is the first layer of defense for this tech. All known bad domains (known blocked domains and commodity malware) are stopped by the Umbrella DNS service. Additionally, some of the categories are corporate policy-based rather than security-based, such as explicit content categories.
Triage of proxy policy categories other than Malware	Monitoring, triage and investigation of proxy events categorized as anything other than malware.	We haven't had an opportunity to validate any other categorized events from proxy. Currently, out of scope.
Firewall or AMP events	Monitoring, triage and investigation of firewall or AMP events.	We haven't had an opportunity to validate any of these events in a production environment. Currently, out of scope.