Panther Cloud SIEM

Detection Strategy Guide

October, 2025

Product Overview

Panther is a cloud-native Security Information and Event Management (SIEM) platform developed by Panther Labs. It is designed to ingest, normalize, and analyze high volumes of security data from diverse sources, including cloud infrastructure, SaaS applications, and endpoints. The platform stores data in a security data lake, enabling long-term retention and investigation. Panther utilizes a "detection-as-code" framework, allowing security teams to write, test, and deploy detection logic using Python and YAML. When a detection rule is triggered, the system generates an alert for investigation and response.

Detection Strategy for Panther Cloud SIEM

Detection

Our Tier 1 SIEM Detection Strategy focuses on actionable, strong leads that fill detection gaps. Expel develops a custom strategy for each customer by evaluating their custom rules against various criteria:

- Fidelity - implied by reasonable volume (<10/week)
- Not Duplicative - not already covered by direct integrations
- Supported Category - detects post-exploitation activity
- Actionable - alert details provide enough context to action

Following the rule evaluation against the above criteria, Expel will provide a report detailing our projected level of support for the custom rules. Rules can be supported by sending to a human SOC analyst, surfacing to the customer as a DUET (did you expect this), or indexing, which subjects them to evaluation by Expel-authored rules and makes them available as evidence for related alerts.

The custom detection strategy is fluid and can change as new rules are developed and evaluated for inclusion, or existing rules no longer meet our criteria. To submit your custom detection rules for evaluation, see How to Submit Your Custom Detection Rule(s) in the Help Center.

Response

SIEM telemetry provides additional information that can be useful for us to disposition alerts. With the exception of investigative-only SIEMs, 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 SIEM logs to search for additional types of data, which we use to enrich our alerts with additional context.

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

What We Support for Panther Cloud SIEM

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 Panther Cloud SIEM, you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Panther Cloud SIEM detection rules support	No.
Detection rules written by Expel	No.
Custom rules support	Yes.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events. ■ Query IP ■ Query User
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.