



# **CyberArk Privileged Access Management (PAM)**

Detection Strategy Guide

July, 2025

## Product Overview

CyberArk offers a suite of solutions to provide unified identity and access management (IAM). They focus on securing access for all identities (human and machine) to applications, endpoints, and infrastructure. They also offer single sign-on (SSO), multi-factor authentication (MFA), password management, identity lifecycle management, and adaptive access policies to enforce least privilege and reduce risk across all environments.

## Detection Strategy for Identity Integrations

### Detection

Our identity security detection strategy focuses on optimizing user authentication and application access activity monitoring. This is achieved by directly integrating with identity providers and polling for audit and data access logs.

These events are analyzed through a combination of raw log analysis and security alert processing, which are then evaluated by our detection engine for signs of suspicious login activity or post-exploitation behavior. When a threat is identified, our automated response bot, Ruxie, enriches evidence fields with first- and third-party threat intelligence. Additionally, Ruxie queries a wide range of technologies to provide analysts with critical investigative information and related events.

### Response

For alerts that contain source user information, identity technologies can provide rich context such as groups, locations, job title, and other pieces of metadata. Additionally, for cloud and SaaS alerts, identity technologies are queried to provide verbose context around user login behavior. This allows analysts to investigate the underlying session behind the activity they are triaging.

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

## What We Support for CyberArk Privileged Access Management (PAM)

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 CyberArk Privileged Access Management (PAM), you can visit the [Detections page](#) in Workbench or ask your Sales or Support rep for the most recent download.

<b>Supported versions</b>	<ul style="list-style-type: none"> <li>All versions are supported.</li> </ul>
<b>Supported platforms</b>	<ul style="list-style-type: none"> <li>Splunk</li> </ul>
<b>CyberArk Privileged Access Management (PAM) 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 User</li> <li>Query IP Address</li> <li>Query Logs</li> <li>Query Raw Logs</li> <li>SIEM Timeliner Workflow</li> <li>Suspicious Login Workflow</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.