CyberArk Identity

Detection Strategy Guide

July 2025

Product Overview

CyberArk Identity is an Identity and Access Management (IAM) solution that delivers secure access to applications and resources for any user, from any device, anywhere. It provides a comprehensive set of capabilities including Single Sign-On (SSO), adaptive Multi-Factor Authentication (MFA), and user lifecycle management to enforce intelligent, context-aware access policies and protect against identity-based threats. The platform is built on the principles of Zero Trust, verifying every access request to ensure that only authorized users can access sensitive data. By integrating with a wide range of applications, both in the cloud and on-premises, CyberArk Identity helps organizations reduce password-related risks, streamline compliance and auditing, and provide a seamless and secure user experience.

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.

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 Identity

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 CyberArk Identity,

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

Supported versions	■ 21.11.133+
Supported event log sources	■ Expel collects all CyberArk Identity event types from the Events (RedRock) API. Detection coverage prioritizes authentication, MFA, credential-change, and administrative or privilege event types, while all event types remain available for both detection and investigation.
CyberArk Identity detection rules support	No.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	Yes. We are able to take the following investigative actions to gather data for triage and investigation of events: ■ Query User ■ Query IP Address ■ Query Logs ■ Query Raw Logs
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.