OneLogin

Detection Strategy Guide

July 2025

Product Overview

OneLogin provides a cloud-based Identity and Access Management (IAM) platform that unifies access for an organization's users, devices, and applications. The platform helps secure and centralize user authentication through services like Single Sign-On (SSO) and Multi-Factor Authentication (MFA), simplifying access for end-users while strengthening security for IT administrators. The solution is designed to manage identities across cloud and on-premises applications, allowing for streamlined user provisioning and de-provisioning. By creating a single, secure identity for each user, OneLogin helps organizations enforce consistent access policies, reduce password fatigue, and gain visibility into application usage and user activity, thereby mitigating risks associated with unauthorized access.

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.

What We Support for OneLogin

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

Supported versions	■ V1 ■ V2
Supported event log sources	■ Event
OneLogin detection rules support	No.
Detection rules written by Expel	Yes.
Auto remediations	No.
Investigative support through Workbench	No. We access the console directly with an "Investigator" role account.
Hunting support	Yes. Hunting is available for this integration to customers who purchase this option. Contact your Sales or Support rep for help understanding the hypotheses and objectives for each hunting technique. For a full list of techniques by integration, see Hunting Techniques in the Help Center.

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.