Proofpoint Insider Threat Management (via SIEM)

Detection Strategy Guide

July, 2025

Product Overview

Proofpoint Insider Threat Management (ITM) is a people-centric SaaS solution designed to detect, prevent, and respond to insider threats and data loss at the endpoint. It achieves this by providing deep visibility into user activities, correlating user behavior with sensitive data movement across various channels (endpoint, email, cloud), and offering real-time alerts with rich context. This allows it to accelerate investigations and provide irrefutable evidence of wrongdoing by identifying malicious, negligent, or compromised insiders.

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 Proofpoint Insider Threat Management (via 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 Proofpoint Insider Threat Management (via SIEM), you can visit the Detections page in Workbench or ask your Sales or Support rep for the most recent download.

Supported versions	■ All versions supported.
Supported platforms	■ Sumo Logic
Proofpoint Insider Threat Management (via SIEM) detection rules support	Yes.
Detection rules written by Expel	No.
Remediation support	Yes. We offer a full suite of remediation actions for this integration, and use our expertise to determine which ones are most appropriate for your specific incident. For a detailed list of *all possible* remediation actions, contact your Sales or Support rep.
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
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.