Incydr™ + Okta

Leverage user identity to monitor high-risk users and optimize your Insider Risk Management platform

mimecast®

Incydr integrates with Okta to incorporate user attributes within profiles, automate the management of user Watchlists, and respond to Insider Threats.

Integration Overview

Incydr integrates with the Okta Identity Cloud to automate access controls, and speed investigations to Insider Risk incidents involving departing employees or high-risk users. Incydr continually monitors all data movement across computers, cloud collaboration platforms and SaaS applications to surface Incydr Risk Indicators (IRIs). When an IRI triggers a high-fidelity alert in Incydr, the user is automatically added to a specific group in Okta with lower access permissions while a ticket is created in the organization's IT ticketing system (i.e. ServiceNow or Jira). This integrated workflow eliminates gaps and siloed efforts across departments to enable security teams to effectively investigate and mitigate Insider Risk.

Additionally, Incydr has a SAML and SCIM-based integration with Okta to identify behavioral risk indicators such as remote activity, off-hour file events and attempts to conceal exfiltration. This direct integration allows security teams to programmatically monitor users with increased risk factors, such as departing and contract employees.

Features

Watchlist Management

Use Okta information such as department, manager, title, and location to complete a user's profile within Incydr and to automate the employees who should be added and removed from Watchlists

Access Controls

Respond to Insider Threats by quickly removing user access rights within Okta in order to contain risk to data during a security investigation

Single Sign-On

Implement single sign-on (SSO) as the authentication method in your Incydr environment to secure accounts and simplify the user experience
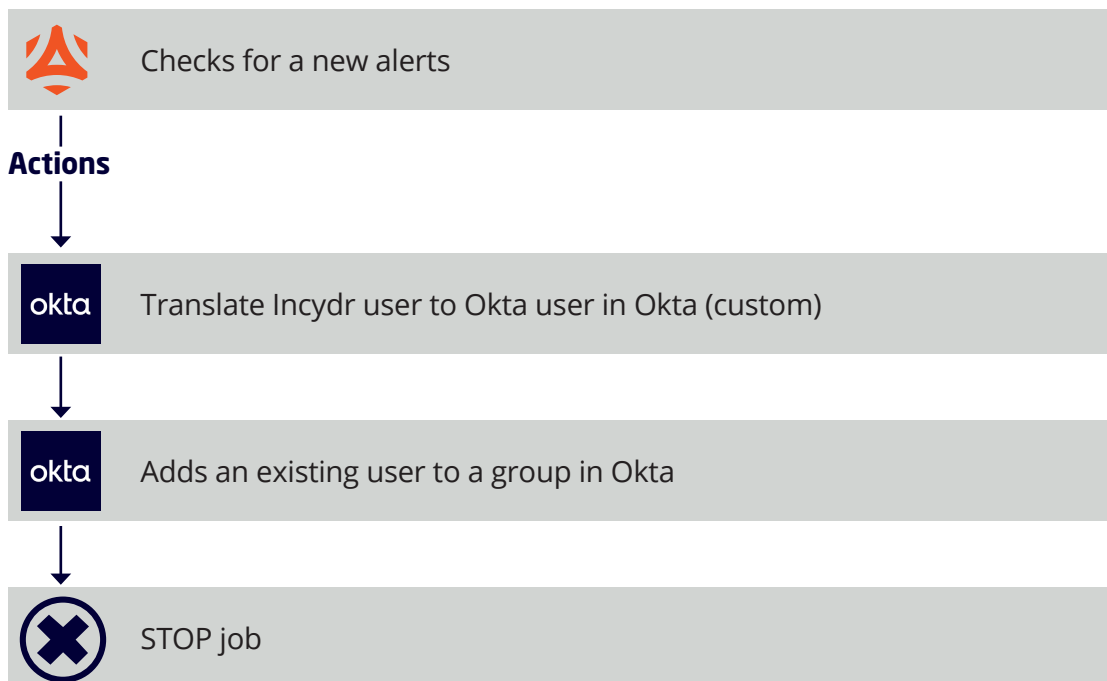
Benefits

Data Protection: Protect data by applying access controls in response to detected threats

Complete Context: Utilize user attributes to provide quick context and speed decision-making during an investigation

Increase Productivity: Effectively monitor and mitigate Insider Threats by automating Watchlist management

Trigger

⚠	Checks for a new alerts

Actions

okta	Translate Incydr user to Okta user in Okta (custom)

okta	Adds an existing user to a group in Okta

✖	STOP job

Together, Incydr and Okta provide organizations with the ability to respond quickly to Insider Risk incidents, while also providing a flexible environment that enables innovation and collaboration.

About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.