Incydr Context Flows with IAM, PAM and HRIS

This document gives an overview of what Incydr Context Flows are, and highlights featured use cases and a scenario example.

What are Incydr Context Flows?

Incydr Context Flows enhance Incydr's risk signal by ingesting user attributes, such as employment milestones, departure, or elevated access credentials from corporate IAM, PAM, and HRIS systems. With user context from these systems, Incydr Flows automatically adds users to watchlists and alert rules to improve visibility into your highest risk users and modify prioritization of their file activity.

Context Flows Integration Benefits

- **User context**
  Incydr ingests information like a user's title, department, manager, employment status, departure date and elevated access credentials to prioritize high-risk user types.
- **High-risk user detection**
  Automatically enhances monitoring by adding users to Incydr's watchlists, such as its departing employee watchlist, based on triggers from IAM, PAM or HRIS systems.
- **Alert prioritization**
  Prioritize response to alerts involving high-risk users by automatically adding specific groups or individual users to alerts based on specified attributes.
- **No-code workflows**
  Use API-based integrations to connect Incydr with IAM, PAM and HRIS systems. Your team won't have to develop or manage anything since all custom workflows are built and maintained by members of the Code42 professional services team.

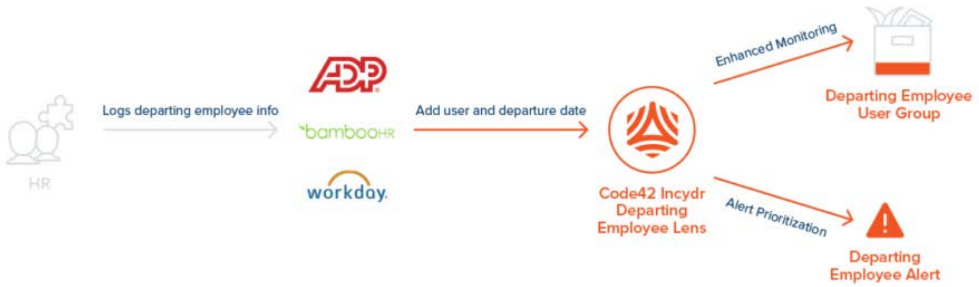
Featured use-cases

Incydr Flows connect to systems such as Workday, ADP, Oracle HCM, BambooHR and Workforce. All Incydr HRIS Flows work by using employment milestones, such as departure date, to add employees to one of Incydr's watchlists and Incydr Risk Detection Lens. This automates the process of enhanced monitoring during high-risk times in the employee lifecycle. Similarly, Incydr Flows connect to IAM and PAM systems such as Okta and CyberArk to add employees to Incydr watchlists based on user attributes or system access.

Recommended Incydr Context Flows to automate monitoring of high-risk users:

- Automatically add departing employees to an Incydr watchlist
- Automatically add new employees to an Incydr watchlist
- Automatically add contractors to an Incydr watchlist
- Automatically add executives and other high impact employees to an Incydr watchlist
- Automatically add privileged users to an Incydr watchlist

Scenario example: Automatically add departing employees to an Incydr watchlist


HR
Logs departing employee info
ADP
bambooHR
workday.
Add user and departure date
Code42 Incydr Departing Employee Lens
Enhanced Monitoring
Departing Employee User Group
Alert Prioritization
Departing Employee Alert

- A member of the business development team quits.
- The departing employee's manager notifies HR of their resignation.
- The HR business partner updates their HRIS system, ADP, with the departing employee's information and departure date.
- ADP notifies Incydr that this employee is departing on July 1.
- Incydr moves the user to the departing employee watchlist for enhanced monitoring during the remainder of their time at the company.
- By being added to this watchlist, the employee will be given an Insider Risk Indicator of “departing employee” which increases the risk score and prioritization of any exfiltration file activity that might take place before departure.

Summary

Managing Insider Risk depends on cross-functional processes and information from disparate systems. The complexity of consistently bringing the right people, processes and technology together to accurately detect and effectively respond to Insider Risk has traditionally been challenging.

By taking this right-sized response to Insider Risk, Incydr allows you to improve Insider Risk posture and create a more risk-aware culture. With Incydr Context Flows, you will:

- Accelerate response times.
- Reduce manual, repetitive, or error-prone tasks.
- Mitigate alert fatigue.
- Simplify processes that rely on disparate systems.