mimecast®

Incydr Flows, Powered by Tines

Simplify manual, error-prone and cross-functional workflows

Incydr Flows, powered by Tines, allow security teams to automate actions between Incydr and other corporate systems like IAM, PAM, EDR, HCM, ITSM, and email security in order to save time and increase effectiveness. It does this by utilizing no-code automation. Incydr Flows can be added to the Incydr product for a nominal fee.

About Incydr Flows

There are two types of Incydr Flows available:

Context flows

Ingest user attributes, such as employment milestones, departure or elevated access credentials from corporate IAM, PAM, HCM, and email security systems. With user context from these systems, Incydr Flows automatically add users to alert rules or watchlists for heightened monitoring.

Response flows

Orchestrate response controls to mitigate corporate data leak when data exfiltration events are detected. These controls are intended to contain active insider threats and can be automated based on the severity of an event. They are delivered through integrations with systems like IAM, PAM, EDR and ITSM.
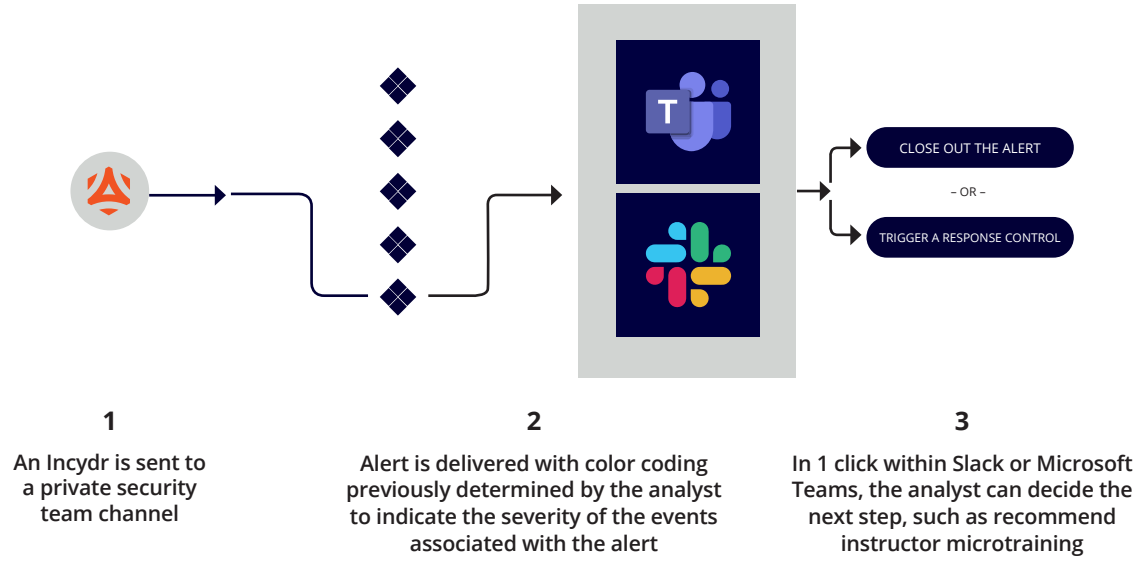
Incydr Flows Benefits

- Accelerate response times
- Reduce manual, repetitive, or error-prone tasks
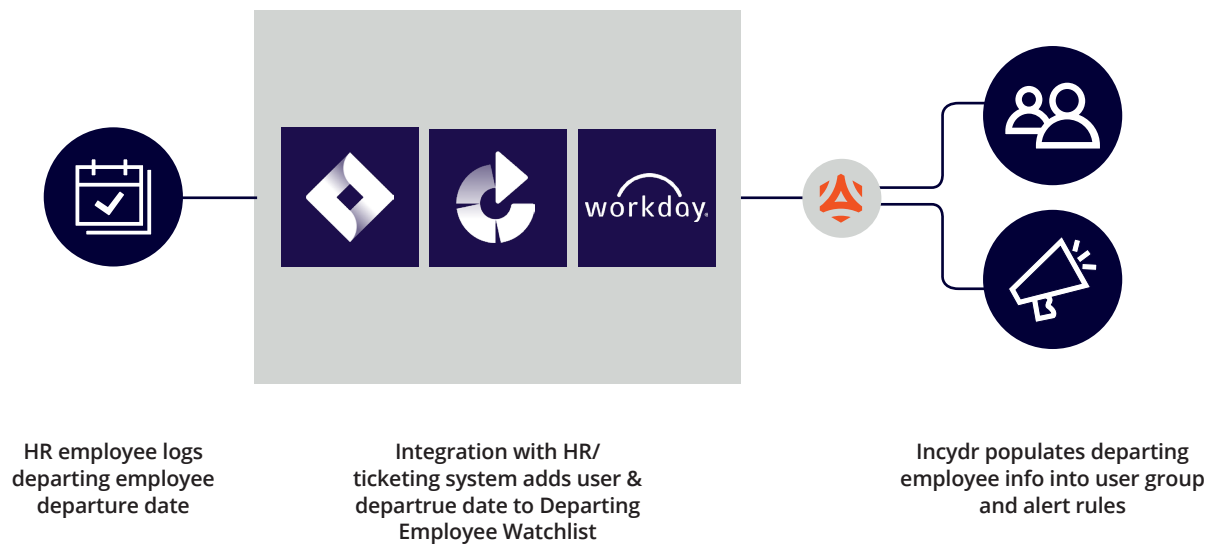- Simplify processes that rely on multiple teams

Use Cases

Triage alerts

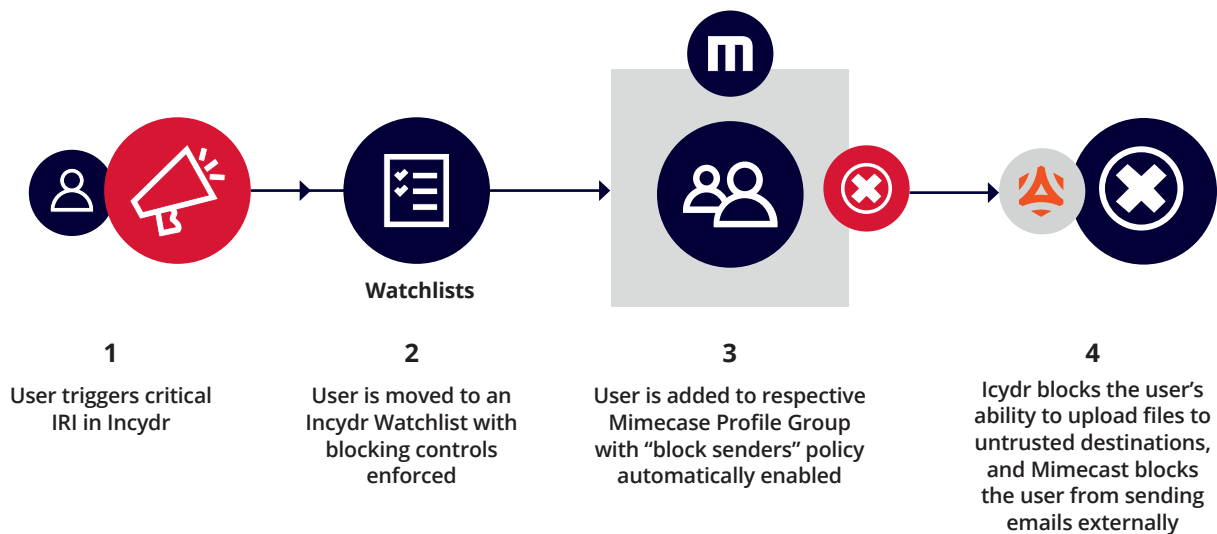Triage alerts using ticketing and messaging systems, such as Microsoft Teams, ServiceNow, and Slack

CLOSE OUT THE ALERT

– OR –

TRIGGER A RESPONSE CONTROL

1

An Incydr is sent to a private security team channel

2

Alert is delivered with color coding previously determined by the analyst to indicate the severity of the events associated with the alert

3

In 1 click within Slack or Microsoft Teams, the analyst can decide the next step, such as recommend instructor microtraining

Manage departing employee watchlist

Automate monitoring for new and departing employees with Bamboo, Workday, and Jira

HR employee logs departing employee departure date

Integration with HR/ ticketing system adds user & departrue date to Departing Employee Watchlist

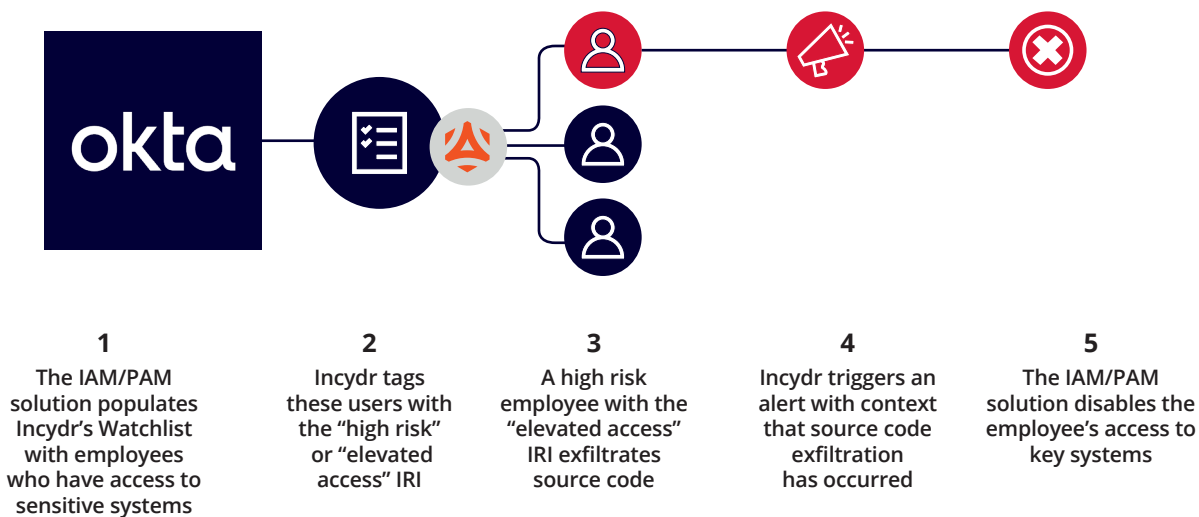**Incydr populates departing employee info into user group and alert rules**

Sync Incydr's watchlists with Mimecast's profile groups

Automate monitoring and managing high risk user groups with Mimecast

Watchlists

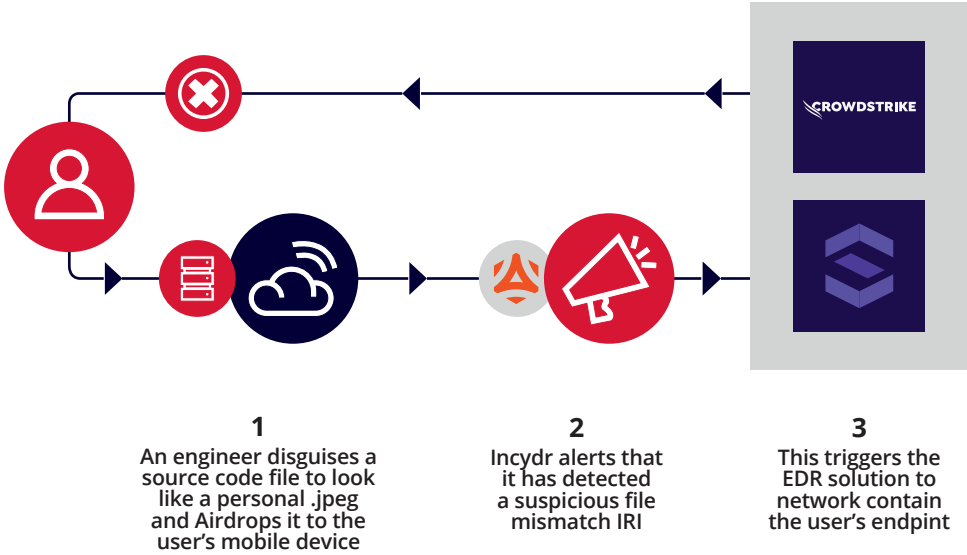**1**
User triggers critical IRI in Incydr

2
User is moved to an Incydr Watchlist with blocking controls enforced

3
User is added to respective Mimecase Profile Group with "block senders" policy automatically enabled

4
Icydr blocks the user's ability to upload files to untrusted destinations, and Mimecast blocks the user from sending emails externally

Contain threats by removing user access

Remove employee access to systems using Okta

1
The IAM/PAM solution populates Incydr's Watchlist with employees who have access to sensitive systems

2
Incydr tags these users with the "high risk" or "elevated access" IRI

3
A high risk employee with the "elevated access" IRI exfiltrates source code

4
Incydr triggers an alert with context that source code exfiltration has occurred

5
The IAM/PAM solution disables the employee's access to key systems

Contain threats by quarantining endpoint

Quarantine endpoints during active insider threat investigations with Crowdstrike and SentinelOne

1
An engineer disguises a source code file to look like a personal .jpeg and Airdrops it to the user's mobile device

2
Incydr alerts that it has detected a suspicious file mismatch IRI

3
This triggers the EDR solution to network contain the user's endpint

Contact sales to learn more about automating workflows between Incydr and your tech stack.

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.