



Enhances Privileged Monitoring Integration

Name of Company: Code42

Website: <https://www.code42.com/>

Name of Product: Code42 Incydr™

Version: SaaS

Date: August 23, 2021

PARTNER SOLUTION OVERVIEW

Partner Product Overview: Code42 Incydr™

Code42 Incydr™ is a SaaS product used for Insider Risk Management. It allows security teams to mitigate file exposure and exfiltration risks without disrupting employee productivity and collaboration. It correlates and enriches signals from files, vectors and users to accurately detect Insider Risk Indicators (IRIs) and expedite response. It uses an agent and direct cloud system integrations to provide both a company-wide and per-user understanding of data risk.

What makes Incydr unique is its simplicity, signal and speed. It monitors all file activity, regardless of what is considered acceptable or unacceptable by an organization. From this complete view of all file activity, it looks for IRIs to determine and prioritize what represents real risk. This allows Incydr to not only reduce time spent reviewing and investigating alerts, but also surface risk that goes unnoticed by traditional DLP.

Once risks are detected, Incydr expedites a variety of human and technical remediation actions so organizations can take an informed and right-sized response.

Feature Overview: Incydr Flows

Incydr Flows are no-code automated integrations, powered by Workato, that add context and accelerate response to Insider Risk workflows. Together, response and context flows make it easy to automate response controls that are in alignment with your risk tolerance. Incydr Flows streamline workflows between Incydr and corporate systems like IAM, PAM, EDR, HCM, ITSM and others.

Integration Overview: Incydr + CyberArk Flow

The Incydr + CyberArk Flow automatically adds users who have access to high-value safes in CyberArk to Incydr's high-risk detection lens. Now these users in an elevated access user group for enhanced monitoring by Incydr. When a user in this group takes an action that puts data at critical risk, Incydr detects this and signals that a critical severity Insider Risk Indicator (IRI) has occurred. When this happens, Incydr automatically triggers CyberArk to remove this user's access to specific safes with high-value data. This workflow automates controls to contain detected data leaks while security investigates further.

Integration components:

- **High-risk user group monitoring:** Enhanced monitoring for groups of users who have privileged access to CyberArk safes with high-value data.
- **Risk detection lens automation:** Add user context from CyberArk to Incydr's High Risk detection lens automatically, in near real time
- **Privileged access controls:** Revoke privileged access to CyberArk safes to contain data leaks and reduce additional risk exposure.

- **No-code automation:** Code42 professional services sets up and maintains the Incydr + CyberArk Flow

KEY BENEFITS

Benefits of Code42 Incydr (™)

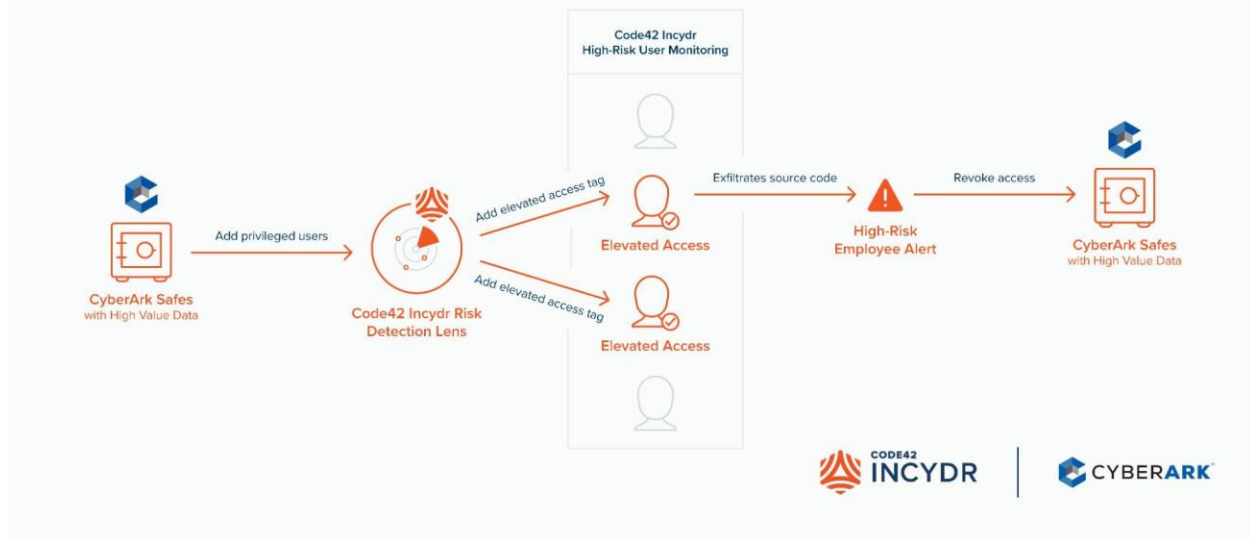
- Continuously monitors file activity on computers as well as via corporate cloud and email services, without inhibiting employee productivity
- Detects file exfiltration activities including uploading files to web browsers and apps, syncing files to personal cloud apps, transferring files to removable media devices, printing files and sharing or emailing files from corporate accounts.
- Detects Insider Risk Indicators and prioritizes the activities that require investigation
- Provides you with an efficient way to compile, document and disseminate pertinent investigation details so you can make a fast and informed decision about how to respond
- Informs and expedites both human and technical controls to contain, resolve, and educate on data exfiltration events.

Benefits of the Incydr + CyberArk Flow

- Simplify security operation processes that rely on data and actions taken in Incydr and CyberArk
- Accelerate response times when privileged users put data at risk
- Mitigate analyst burnout by reducing manual, repetitive or error prone tasks

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

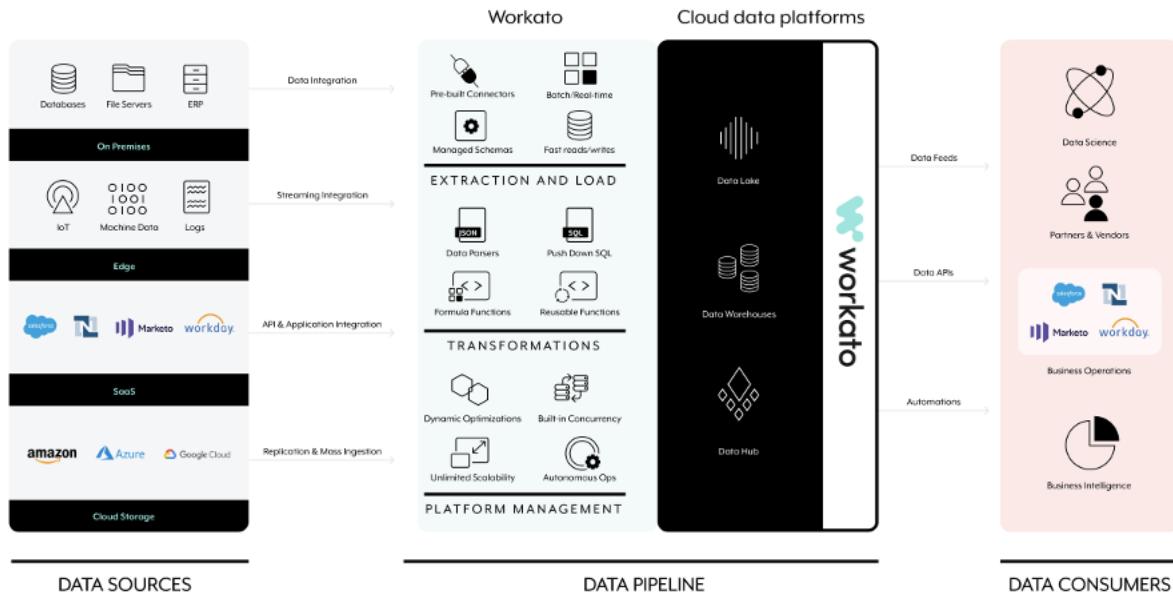
The Incydr + CyberArk Flow is a no-code automated integration that enables the removal of privileged access credentials in response to a critical Insider Risk Indicator (IRI). This containment response ensures that no further data exposure takes place while security investigates.



INTEGRATION

Incydr and CyberArk are connected via an automated integration built through Workato. Workato is a Next-Gen iPaaS with a fully-cloud native architecture. This enables Code42 Professional Services to build low to no-code integrations between Incydr and third parties, like CyberArk, through cloud connectors.

This diagram shows how Workato's data pipeline connects data sources with data consumers. Incydr consumes data sourced from CyberArk in order to trigger users to be added to Incydr's risk detection lens and alerts. CyberArk consumes data sourced from Incydr, so that Insider Risk Indicators (IRIs) trigger CyberArk to revoke user's access to specific vaults.



PROFILE RETRIEVAL

The Incydr + CyberArk Flow automatically retrieves user profiles from CyberArk every 5 minutes. The profiles retrieved include the list of users who have access to CyberArk safes that contain high-value data, as specified by the customer. CyberArk identifies these safe members, their user information and email address, and triggers Incydr to add them to its High-Risk Detection Lens. When the users are on Incydr's high-risk detection lens, they will be tagged as a user with elevated access. Incydr enhances monitoring for the group of users who have elevated access.

When a user who belongs to the elevated access user group triggers a high-risk user alert, Incydr triggers CyberArk to remove that user's access to the specific safes that contain high-value data. This containment response is triggered within 5 minutes of the detected IRI.

REQUIREMENTS

- **Incydr agent deployed:** This integration requires that the organization has CyberArk and Incydr deployed within their environment. Incydr detects file exposure and exfiltration across computers, cloud and email through an endpoint agent, direct and automated integrations.
- **Prepare a Code42 user account:** to configure Code42 automated integrations, create a Code42 user service account. [Find details in this support article.](#)
- **Enable third-party cookies:** Third-party cookies must be enabled in your web browser settings. [Find details in this support article.](#)

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

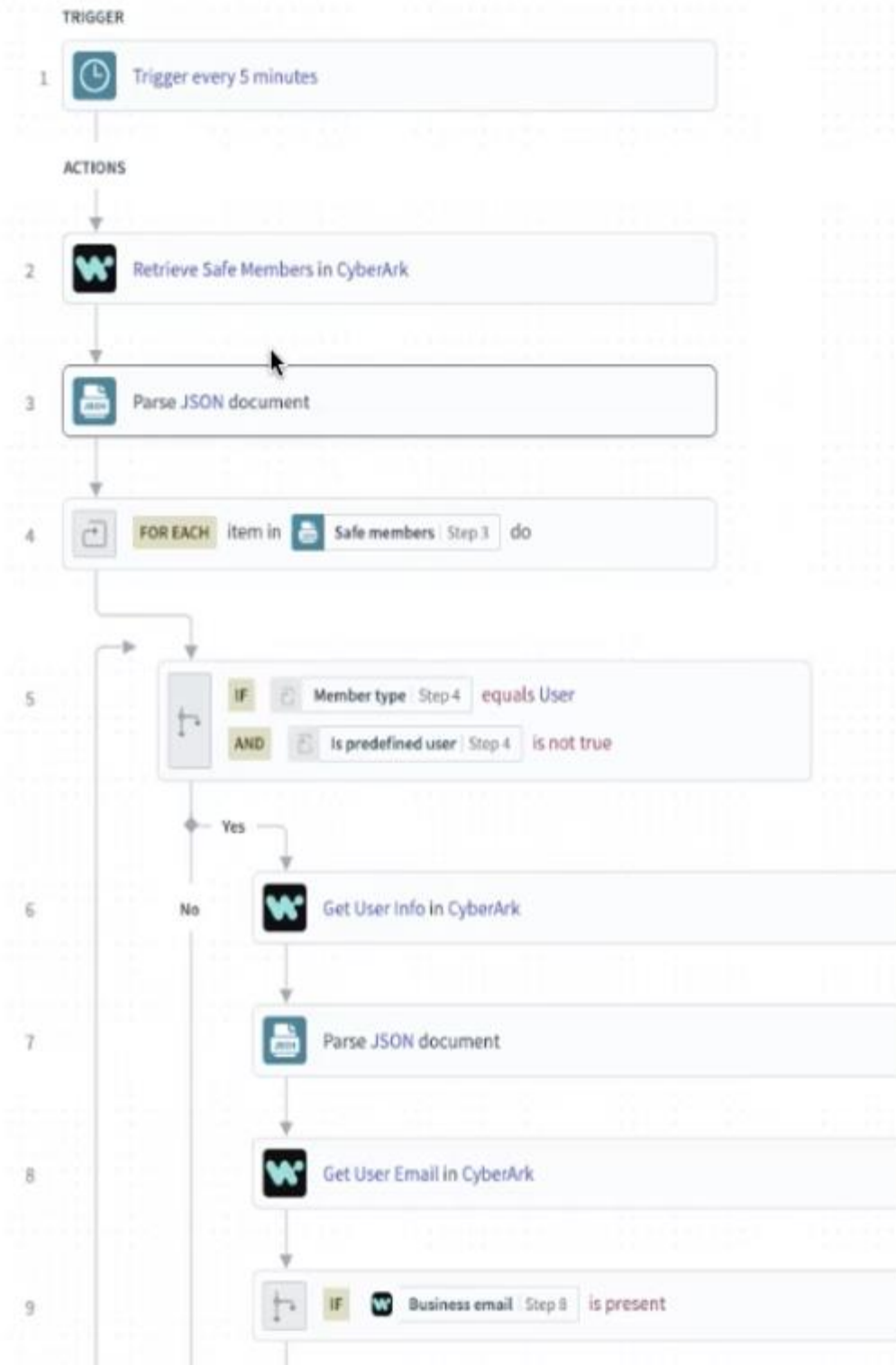
The integration between Code42 Incydr and CyberArk is an automated integration called Incydr Flows. All Incydr Flows are set up, managed and monitored by Code42. The Incydr + CyberArk Flow is a paid integration that will be implemented by the Code42 team. To get started, contact Code42 sales at www.code42.com/contact/sales/ or reach out to the business contact listed below.

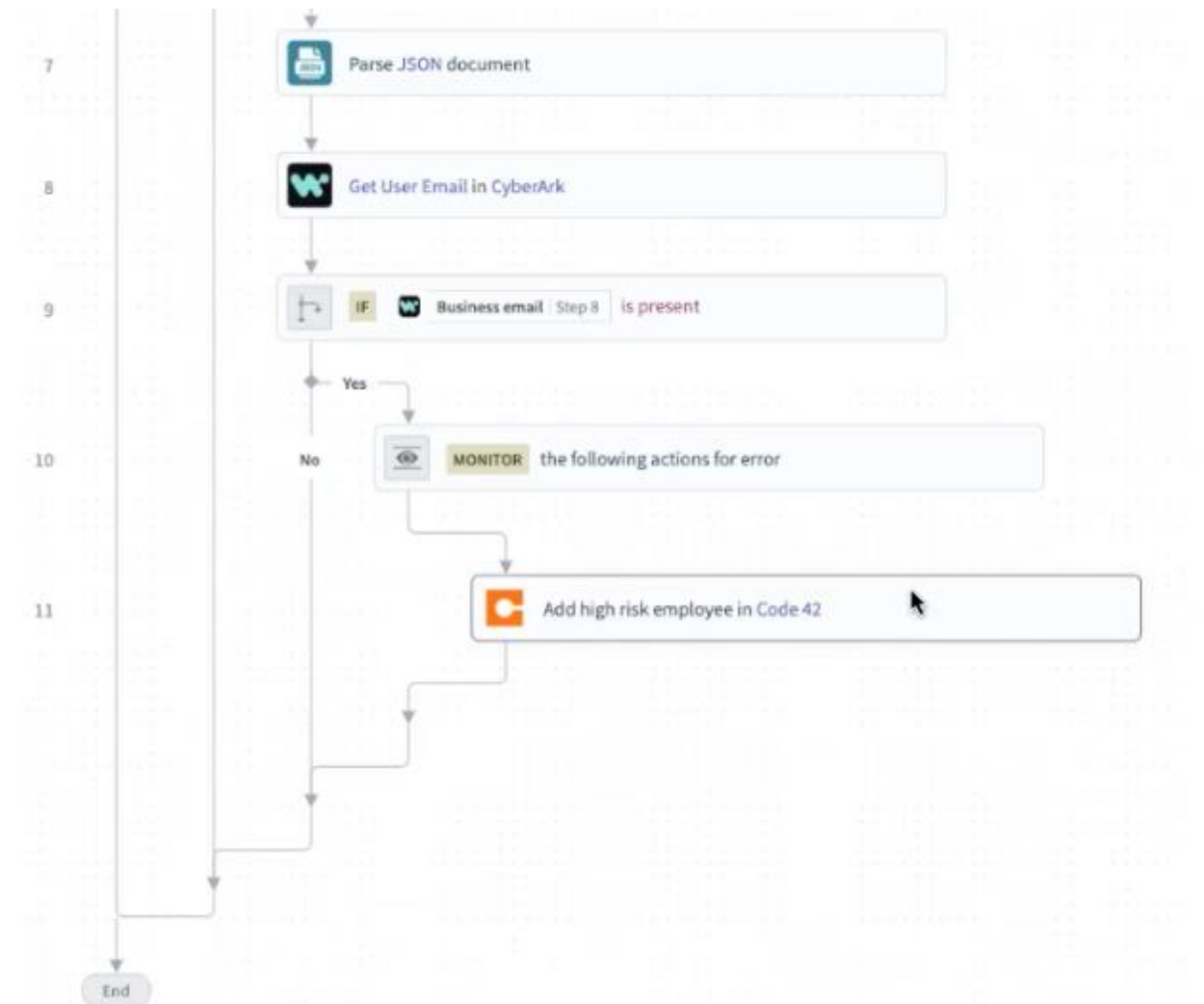
During implementation, Code42 professional services will custom build the integration using Workato's recipe builder. Here is an example of a Workato recipe that Code42 Professional Services would customize in order to automatically populate Incydr's high-risk detection lens with the list of users who have access to high-value safes in CyberArk workflows between Incydr and CyberArk looks like.

Test job #6615968079 ▾ Repeated job #2 ▾

Started at 11:11:53 am (CDT) on 16 Aug, 2021 using recipe [version 102](#) 

 **Successful**



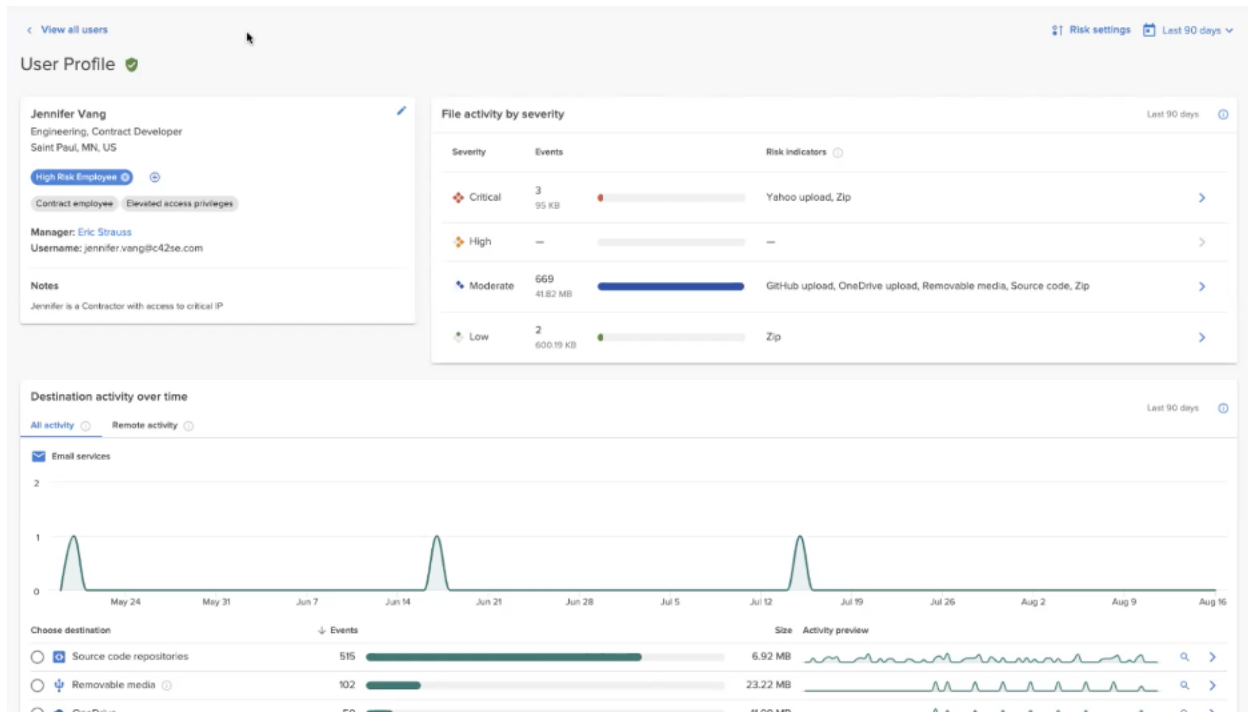


This screen shot provides an example of a recipe that Code42 Professional Services would customize to trigger CyberArk to revoke privileged access in response to an Incydr alert.



This [Code42 support article](#) provides technical documentation necessary to explain the configurations of Incydr Flows (formerly known as Code42 automated integrations).

Code42 Incydr UI:



Featured use case:

1. Contain detected data leak events
 1. Admin identifies the safe names that contain high value data
 2. CyberArk populates Incydr's High Risk Detection Lens with the list of users who have access the safe names identified
 3. Incydr tags these users with the elevated access risk factor.
 4. All users with this tag are automatically added to the high-risk employee alert rule.
 5. When an alert triggers for the high-risk employee alert rule, Incydr triggers the user's access to be removed from the CyberArk safe.

PARTNER CONTACT INFO

Business Contact	Name	John Schimelpfenig
	Email	john.schimelpfenig@code42.com

	Tel	201.240.6566
Technical Contact	Name	Tony Schwandt
	Email	tony.schwandt@code42.com
	Tel	952.204.9188
Support Contact	Name	Tony Schwandt
	Email	tony.schwandt@code42.com
	Tel	952.204.9188