INCYDR CONTROLS FOR RIGHT-SIZED RESPONSE

Effective Insider Risk Management response must focus on containment, resolution and education

THE NEED FOR RIGHT-SIZED RESPONSE

Without a purpose-built solution to manage Insider Risk, security practitioners struggle to detect and respond quickly and effectively when employees put corporate data at risk. By nature, protecting data from leaks caused by employees requires a great deal of context. This is because employees have many legitimate reasons to move files to new locations or share them with external parties, such as an approved vendor. Additionally, the tradeoff between security and productivity must continually be weighed. What's the right balance? This depends on your organization's risk tolerance.

Insider Risk tolerance is unique to each organization and each line of business. What is acceptable at one company would be unacceptable at another. What is acceptable by marketing may not be acceptable by engineering. Your highest value files depend on your industry, customers, partners and employees. Your highest risk exfiltration vectors are impacted by your corporate tech stack and your company's culture and demographics. Your highest risk users could be determined by department, role, status, data access, intent, and behavior. And who those high risk users are can change at any time.

A VARIETY OF RESPONSE CONTROLS ARE NEEDED TO MANAGE INSIDER RISK

Because risk tolerance is unique to every organization, there's no one-size-fits-all response to Insider Risk. Risk severity should dictate the type of response or control a security team employs. When it comes to accurately assessing risk severity, context is key. You must know what files are being moved, where, by whom, and when. Incydr provides this through prioritized file, vector and user Insider Risk Indicators (IRIs), and ensures you can quickly act in a way that's appropriate to the level or risk. We call this taking a right-sized response.

Incydr's Approach

Incydr offers three categories of response types: containment, resolution, and education.

Using Incydr to Take a Right-Sized Response

Response Type	Contain	Resolve	Educate
Objective	Stop ongoing data exposure	Remediate detected data exposure	Reduce future data exposure
Controls	• Conditional access controls • Disable USB • Stop local sync apps • Network contain device • Lock device	• Require action from user • Escalate to manager • Escalate to HR • Escalate to Legal	• Assign microtraining • Send policy for acknowledgement

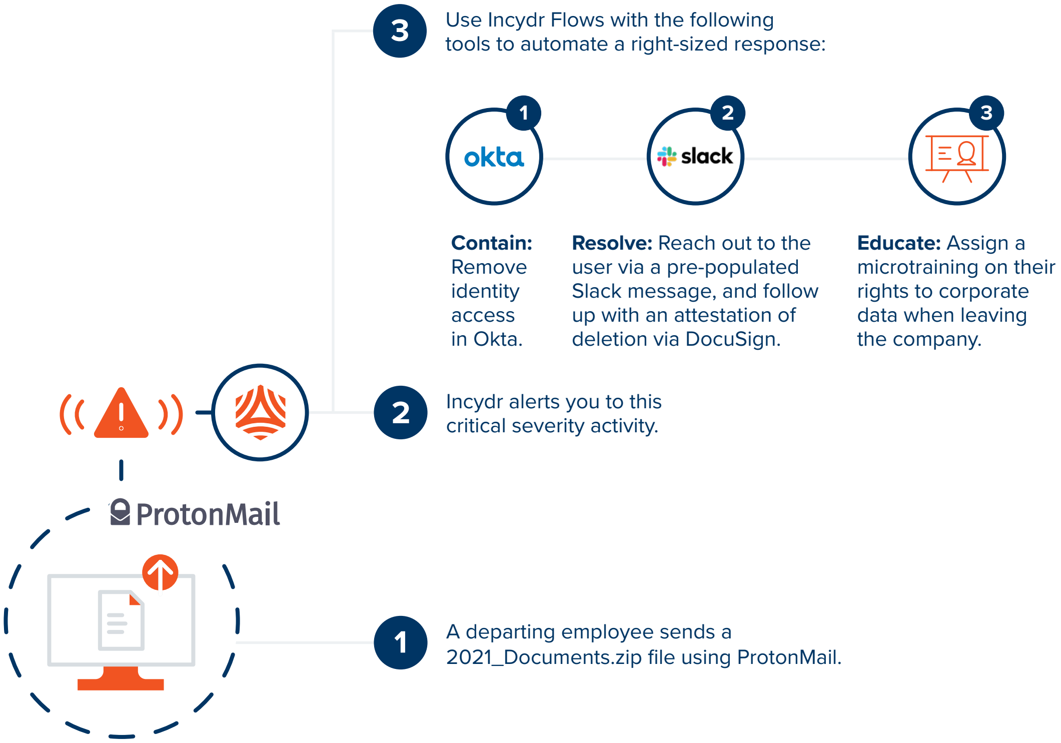
Containment controls take action at the user, network or device level so that no further data exposure takes place while security investigates. Resolution controls address and remediate the data exposure event that was originally detected by Incydr. Education controls are used to reduce future instances of data exposure so that an organization's Insider Risk posture improves over time. It's important to note that you can address the same event with more than one control. You may determine that critical severity events require you to contain, resolve, and educate, while low risk events need education only. Incydr's responses are primarily delivered through Incydr Flows and direct integrations with SOAR products.

WHAT ARE INCYDR FLOWS?

Incydr Flows are no-code automations, powered by Workato. They connect Incydr to other corporate systems like Identity Access Management (IAM), Human Capital Management (HCM), Endpoint Detection and Response (EDR), Privileged Access Management (PAM), IT Service Management (ITSM) and others. They automate and standardize workflows to carry out response controls and accelerate response times. Incydr Flows are set up and maintained by Code42's professional services team.

EXAMPLE INSIDER RISK RESPONSE SCENARIOS

Example 1 | Contain, resolve and educate in response to a critical severity event



3 Use Incydr Flows with the following tools to automate a right-sized response:

1 **Contain:** Remove identity access in Okta.

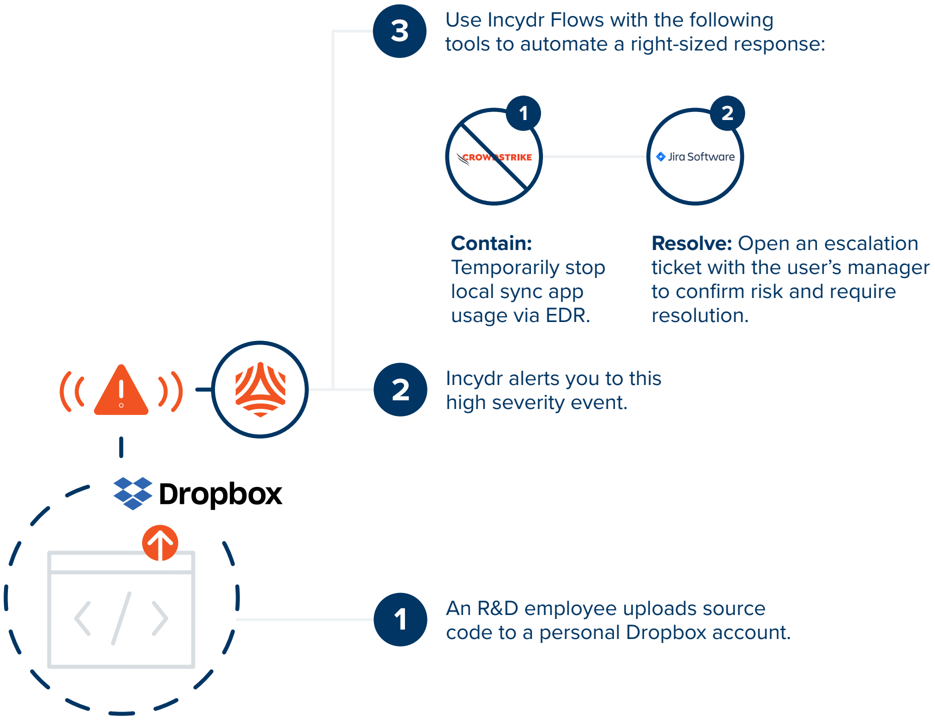
2 **Resolve:** Reach out to the user via a pre-populated Slack message, and follow up with an attestation of deletion via DocuSign.

3 **Educate:** Assign a microtraining on their rights to corporate data when leaving the company.

2 Incydr alerts you to this critical severity activity.

1 A departing employee sends a 2021_Documents.zip file using ProtonMail.

Example 2 | Contain and resolve in response to a high severity event



3 Use Incydr Flows with the following tools to automate a right-sized response:

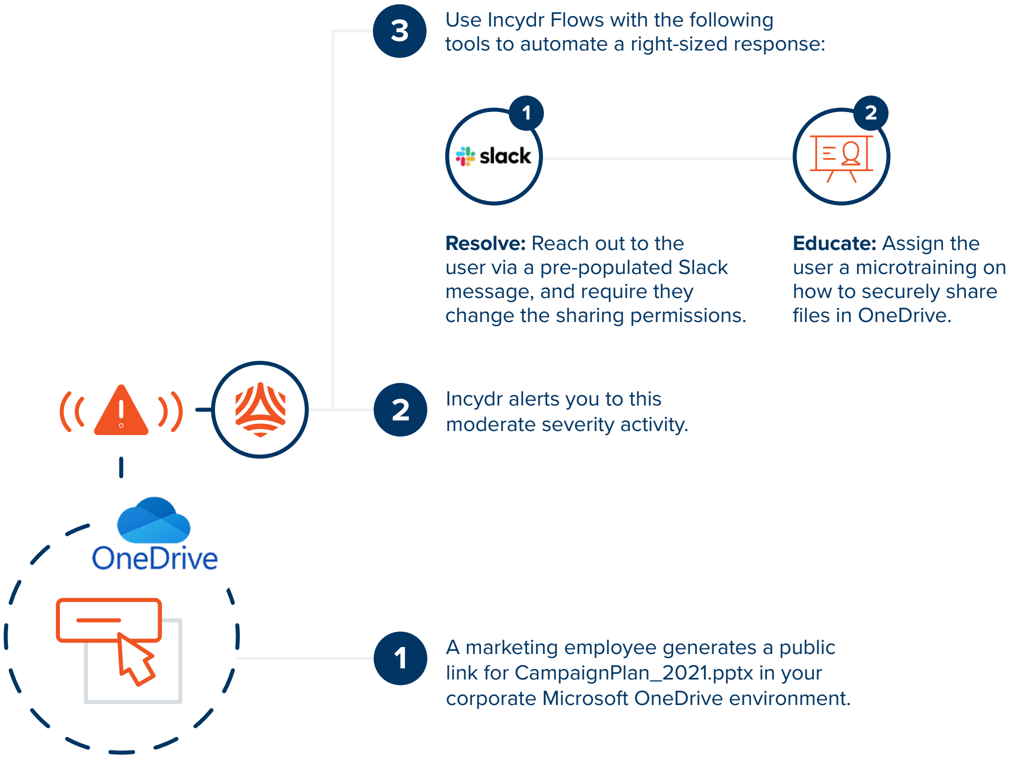
1 **Contain:** Temporarily stop local sync app usage via EDR.

2 **Resolve:** Open an escalation ticket with the user's manager to confirm risk and require resolution.

2 Incydr alerts you to this high severity event.

1 An R&D employee uploads source code to a personal Dropbox account.

Example 3 | Resolve and educate in response to a moderate severity event



3 Use Incydr Flows with the following tools to automate a right-sized response:

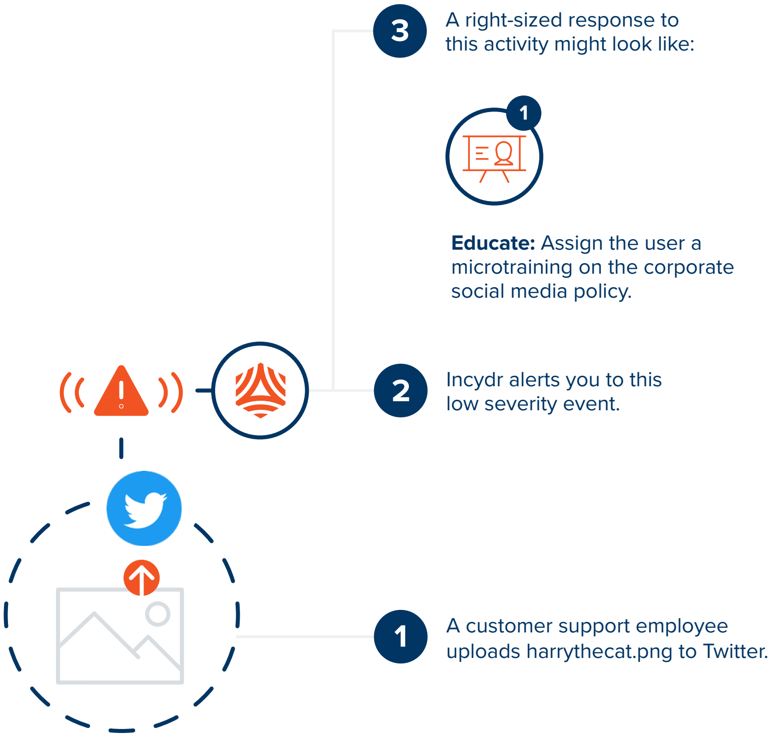
1 **Resolve:** Reach out to the user via a pre-populated Slack message, and require they change the sharing permissions.

2 **Educate:** Assign the user a microtraining on how to securely share files in OneDrive.

2 Incydr alerts you to this moderate severity activity.

1 A marketing employee generates a public link for CampaignPlan_2021.pptx in your corporate Microsoft OneDrive environment.

Example 4 | Educate in response to a low severity event



3 A right-sized response to this activity might look like:

1 **Educate:** Assign the user a microtraining on the corporate social media policy.

2 Incydr alerts you to this low severity event.

1 A customer support employee uploads harrythecat.png to Twitter.

CONTAIN: INCYDR RESPONSE CONTROL BEST PRACTICES

Contain		
	Control	**Description**
User	Conditional access controls	When alerted to a critical exfiltration event, you can automatically add the user to a specific Okta group in order to lower their access permissions. This control is available through an Incydr + Okta Flow.
Device	Stop local sync apps	If a critical exfiltration event to DropBox, iCloud or others is detected, you can avoid further exposure by immediately stopping all local sync applications. This control is available through an Incydr + Crowdstrike Flow.
	Disable USB	You can avoid additional data exposure through removable media by immediately disabling the USB port on a user's device. This control is available through an Incydr + Crowdstrike or Incydr + Jamf Pro Flow.
	Lock device	You can automatically lock a device to prevent a user from having further access. For Mac devices, this control is available through an Incydr + Jamf Pro Flow.
Network	Contain endpoint	You can prevent a user from having further network access following a critical event by taking action to isolate their endpoint. This control is available through an Incydr playbook with Palo Alto XSOAR, or via an Incydr + Crowdstrike Flow.

RESOLVE: INCYDR RESPONSE CONTROL BEST PRACTICES

Resolve

Action	Description	
User inquiry and action	This is the default response for most low risk behavior. The purpose of a user inquiry is to ask the user for more information on why they took or shared files. This allows you to determine intent and ask for resolution. You can do this by sending an email directly from an Incydr alert. Doing so pre-populates the email message with event details such as date, time, method of exfiltration and file names. Or, leverage an Incydr + Slack Flow to manage alerts and automatically generate a direct message template within Slack. An outreach template from Incydr might say: Hello [name], Our security tools picked up the following document(s): *2021-03-08 longfellow-pentest-toolbox.zip, 2021-03-08 CONFIDENTIAL Pentest Runbook V3.1.pdf, 2021-03-08 Pentest Customers Q3 2020-October Update.xlsx,* being moved to a personal cloud service on Monday, 07 June 2021 at 3:00pm. Could you tell me more about this action?	
	Follow up: remote screenshare resolution	If a file has already been moved to a personal location such as Dropbox, iCloud, or Gmail, you may request a video call to watch the user delete the company-owned files from their account. Leverage an Incydr Flow with Zoom, Slack or Google Calendar to quickly initiate these calls and confirm files are safely returned.
	Follow up: attestation of deletion	If you are unable to witness the deletion of exfiltrated files, you may request a user confirm their deletion in writing. Leverage an Incydr + DocuSign Flow to send an attestation of deletion document to a user for their signature.
Manager escalation	In some cases, you may want to escalate an activity to a manager who is better equipped to identify if there is legitimate reason for the file movement. You can escalate to the appropriate people manager using an Incydr Flow with a ticketing system like Jira.	
HR escalation	In the event of a significant incident, you may need to escalate the activity to Human Resources for disciplinary action. You can escalate to the appropriate HR team member using an Incydr Flow with a ticketing system like Jira.	
Legal escalation	In cases of intellectual property (IP) theft that might lead to litigation, your legal team will require information on the detected activities. Incydr's Cases feature allows you to compile and retain the event details to assist this effort. You can escalate to the appropriate legal team member using an Incydr Flow with a ticketing system like Jira.	

EDUCATE: INCYDR RESPONSE CONTROL BEST PRACTICES

Educate

Action	Description
Assign microtraining	One way to increase awareness of risky activity is to assign targeted microtrainings. These easy-to-consume video or infographic trainings are geared toward making employees more risk aware. For example, by explaining the risk associated with creating a public sharing link in Google Drive or moving corporate data to a personal Dropbox account. When security teams automate these types of targeted training, they will never miss a teachable moment. Non-compliance with policy should be seen as an opportunity for employees to learn how to make better security decisions in the future.
Re-acknowledge policy	Every employee should sign an Acceptable Use policy which outlines how files and devices should be handled. It should also explain that monitoring is in place to ensure compliance with this policy. The awareness of this monitoring serves as a deterrent. The Acceptable Use policy should be read and acknowledged by new employees, as well as by all employees at the start of each year. Additionally, if Incydr detects unacceptable activity, security teams can require an employee who breaks policy to read and acknowledge the policy again. Leverage an Incydr + DocuSign Flow to send the Acceptable Use policy to a user for their signature.

CONCLUSION

Incydr was purpose-built to manage this dynamic Insider Risk with simplicity, signal and speed. It offers a context-driven approach to prioritizing risk so you can contain data exposure, accelerate risk resolution, and educate users on appropriate data handling. By taking this right-sized response to Insider Risk, Incydr allows you to improve Insider Risk posture and create a more risk-aware culture.

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (WP2105264)