CODE42

JOINT SOLUTION BRIEF

CODE42 INCYDR + OKTA IDENTITY CLOUD

Leverage user identity to monitor high-risk users and optimize your insider risk management platform

Remote workforces are changing how data is accessed and shared, hence accelerating businesses' adoption of Zero Trust. Forward-thinking businesses require effective ways to assess data exposure, and mitigate and improve insider risk posture – and traditional data loss prevention solutions have come at the cost of disrupting employees' ability to collaborate and be productive.

Code42 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 insider 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, Code42 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.

Together, Code42 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.

INTEGRATION FEATURES:

- Automatically add users to specific groups within Okta with lower permissions while automating incident documentation and communications tied to your HCM and IT ticketing system.
- Ingest user attributes for all employees and contractors, including name, title, department, manager, and employment type into Incydr from Okta for additional context in identifying signals of insider risk.
- Automate response actions for insider risk workflows including modified access permissions, manager notification or pursuing legal action.
- Easily implement single sign-on (SSO) as the authentication method in your Code42 environment to simplify the user experience while also ensuring data is secure.
- Create and deactivate users and push groups all within the Code42 app for Okta, which automatically syncs information back to Code42 to ensure security changes stay in sync.

BENEFITS

- **Allow conditional access.** Improve insider risk posture by applying the right access controls based on predefined risk tolerance.
- **Identify behavioral risk indicators.** Provision role-based user attributes to identify behavioral risk indicators such as remote activity, off-hour file events and attempts to conceal exfiltration.
- **Streamline and automate response workflows.** Automate insider risk workflows for departing and high-risk employees to speed investigations eliminate gaps in order to to effectively investigate and mitigate insider risk.

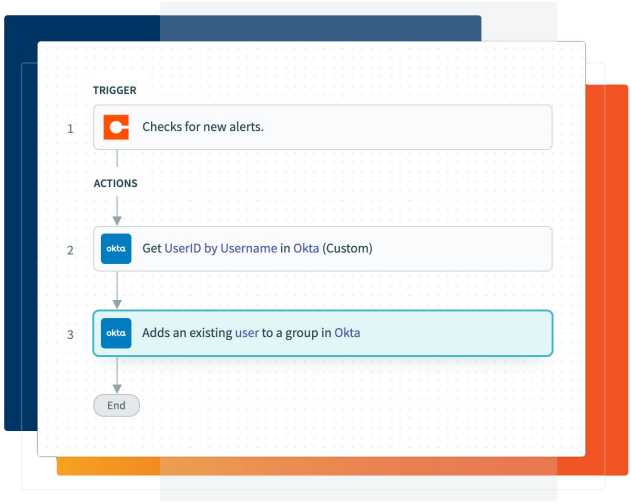
CODE42

USE CASE #1: AUTOMATE USER PERMISSIONS AND ACCESS CONTROLS IN RESPONSE TO INSIDER RISK INDICATORS.

CHALLENGE: Most employees take files with them when they leave – and without access controls, sensitive data could be put at risk of being exfiltrated. When an employee puts in their notice or when there is suspicious file movement or user behavior indicative of insider risk, security teams must be able to quickly take action to protect corporate data from being exposed or exfiltrated.

SOLUTION: 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), documenting the alert details, prompting the security team to investigate the incident.

BENEFIT: Organizations can reduce insider risk exposure and speed response by automating access controls and streamlining an investigation of a departing employee potentially exfiltrating data. Through the automation of manual tasks, data risk can be surfaced quickly, so that security teams can investigate the incident. Using Incydr's risk intelligence, teams have complete context pertaining to file exposure events and can take immediate action, whether that be revoking access, involving an employee's manager, or putting a user on legal hold.



When an alert is triggered from an insider risk indicator (IRI) in Code42 Incydr, the user is added to a group in Okta with lower access permissions while an investigation is automatically prompted.

USE CASE #2: ENHANCE MONITORING OF USERS MORE LIKELY TO PUT DATA AT RISK.

CHALLENGE: Some employees are more likely than others to put data at risk. Users experiencing an employment milestone such as a departure, contractors, or those with access to confidential or sensitive data may require closer monitoring. Furthermore, a remote workforce introduces new risks that make it difficult to ensure data security and compliance.

SOLUTION: Enhance monitoring of users more likely to put data at risk by provisioning role-based user attributes like name, title, department, manager, and employment type. Code42 risk prioritization and signal filter out the noise of harmless activity to only reveal potential file exposure or exfiltration.

BENEFIT: Additional context about the user from Okta allows security teams to mitigate insider risk and monitor certain users more closely using the simplicity, signal and speed of Code42 without slowing down legitimate work.

ABOUT OKTA

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 7,950 organizations, including 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

ABOUT CODE42

Code42 is the Insider Risk Management leader. Native to the cloud, Code42 Incydr 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 threats 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 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.