CODE42

USE CASE

INCYDR

CODE42 INCYDR GOV – DEPARTING FEDERAL EMPLOYEE CONTRACTOR MONITORING

While government agencies and private sector companies continue to toughen their computer networks against the risk of a cyber attack, the biggest threat may be an employee who walks through the front door. Edward Joseph Snowden, the American former CIA employee and subcontractor who copied and leaked highly classified information from the NSA in 2013, remains a prime example that the weakest link is often an employee. According to The National Insider Threat Task Force, “an insider can do just as much damage in the 30 to 90 days after leaving as in the time prior to departure.”

When the Office of Management and Budget, OMB rolled out its far-reaching blueprint for federal agencies to improve their cybersecurity posture, it also highlighted the need for agencies to take steps to mitigate one of the more pervasive -- and overlooked -- security risks: insider threats. The OMB’s plan called for agency CISO’s to embrace stronger identity and access management, including the use of Personal Identity Verification (PIV) cards, and to bolster employee training on security issues, among other initiatives.

That framework follows a stark reminder of the vulnerabilities agencies face from insiders -- federal employees or contractors -- who routinely break agency protocols and gain access to information that they are not authorized to view.

Code42’s Incydr Gov Solution for the Federal Government

Incydr Gov is a FedRAMP Moderate Authorized SaaS data risk detection and response solution for Insider Risk in the federal government. It correlates three dimensions of risk on files, vectors and users to quickly and accurately detect and respond if federal employees or contractors attempt to move or exfiltrate federal data when they leave.

- Incydr Gov detects file sharing and exfiltration across computers, cloud and email through an silent agent and direct cloud and email integrations. Say a member of the scientific research team has given their notice and the HR system has been updated with their departure date.

- Within Incydr Gov, the employee will be programmatically added to the risk detection lens for departing employees. This allows the agency security team to receive alerts when files are moved from their endpoint or computer or corporate cloud and email services to an untrusted destination.
- Code42's Incydr Gov product preserves agency endpoint data to allow for recovery and restore of data for investigations. It also identifies files that are shared externally via corporate OneDrive, Google Drive and Box accounts.
- Agency security teams will get a 90-day view of the employee's historical activity as well as alerts on any high-risk movement. The Incydr Gov product will also surface file events with additional risk indicators, such as the employee moving files during times they don't typically work or while off the agency network. This allows security to quickly prioritize what activity to review first.
- If something needs to be investigated, security will get detailed context on the files, vector and user involved and can even review the file contents in question.
- Incydr Gov allows agency CISO's and their security teams to quickly detect, investigate and take action when employees try to take data with them when they leave, whether that be through the SOAR platform, personal outreach to the user, legal escalation or more.

CODE42 QUICK FACTS

Founded in 2001

Locations:

Minneapolis (HQ) | Denver
Washington DC | London

Trusted by:

Customers include leading security brands such as CrowdStrike, Splunk, Ping Identity, and Okta

6 of **10** of the largest tech companies

13 of the world's most valuable brands

Gartner Peer Insights

35+ Verified Security Reviews

★★★★★

4.9 out of 5 stars

Code42.com/federal

FAST AND EASY DEPLOYMENT

- FedRAMP Moderate Cloud-based
- Mac, Windows and Linux
- 2-week average deployment time
- 230% ROI in 3 years
- Agent on endpoint can be deployed silently

WHAT OUR CUSTOMERS SAY

"Once deployed, this is an immediate data loss detection solution. I would not need someone to keep the rules up to data. The dashboard is simple and anyone can identify where to review without much training."

- **Tim Briggs**, Director of incident Response and eDiscovery at CrowdStrike

CROWDSTRIKE

"When we looked at solutions like the more traditional DLP or the CASBs, it seemed like they work under very limited conditions. But, the minute you put them out in the real world, they just break down. Without hesitation, Incydr... is central to our security program."

- **Mario Duarte**, VP of Security at Snowflake

snowflake®

"Code42 is the only solution we have found that gives us the visibility we need to understand where data is moving, while still letting our team work how — and where — they need to."

- **Dustin Fritiz**, Sr. Security Architect at UserTesting

UserTesting®

CODE42

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.