CODE42

USE CASE

INCYDR

CODE42 INCYDR GOV – FEDERAL DATA SPILLAGE AND CUI

Data spillage is when a confidential document is released into an untrusted environment. When a data spillage incident is detected, it's important to quickly asses the scope and impact of the spill, examine user activities around it, and then contain and permanently purge the data from the affected systems. NIST defines Data Spillage as a Security incident that results in the transfer of classified information onto an information system not authorized to store or process that information.

Federal agencies have a responsibility to locate, investigate and then purge the spilled data or files including those that fall into Controlled Unclassified Information (CUI). The Department of Defense (DoD) Defense Counterintelligence and Security Agency (DCSA) defines CUI as follows, 'CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government-wide policies. CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract.' DCSA further states that 'CUI is important because there are fewer controls over CUI as compared to classified information and can often be the path of least resistance for adversaries. Loss of aggregated CUI can be one of the most significant risks to national security, directly affecting lethality of our warfighters.'

The risk of CUI spillage can be exacerbated by the use of government contractors who work with federal agencies and who share sensitive information and files which may contain CUI. Further, it may not be obvious from the file name and metadata that a file contains CUI, which may lead to misclassification by agency employees and contractors. This is further complicated by the fact that while Federal agencies have recognized that they must properly protect and handle government information, there is a lack of national guidance or additional specificity that creates confusion and difficulty within the government on how to classify, handle or share sensitive information.

Incydr Gov and Data Spillage

Our research shows that most agencies are in a reactive mode when it comes to data spills involving CUI. Security teams are often alerted after a data spill has already occurred. This delay to detect and begin investigation poses a significant challenge to contain the spill and significantly increases the odds of additional file versions being created for nefarious use.

Incydr Gov brings powerful monitoring and alerting capabilities on file movement and data exfiltration events across all users, files and vectors as well as forensic capabilities to provide visibility into where else files reside within your environment. Within minutes, if not seconds, security teams are alerted of the event which then launches investigative activities such as:

- To determine whether a data spill has actually occurred
- The sensitivity of the information potentially compromised (CUI)
- The number of users, systems and applications involved

Incydr Gov - Speed, Simplicity and Signal

The table below summarizes how Incydr Gov solves the Data spill issue for federal agencies.

Without Incydr Gov	With Incydr Gov
Do you know where the spill occurred and how?	
When data spills occur, Security teams are usually provided with file information (file names, types, possibly file hashes) by teams that have discovered the spill. Security teams then have to find the files, purge them, and then provide a report of deletion. Finding and investigating the presence of those files, especially on end user devices and removable media, is a huge time-sink. Often, security teams have to simply rely on user responses (interviews) to know if the file was copied somewhere - like SharePoint or a USB drive. They lack independent visibility into this.	With Incydr Gov deployed, security teams can quickly search to determine which users had the spilled files (using file names and hashes and other key metadata, etc.), when they had them, who they were shared with, and where they were sent (eg. thumb drive, sharepoint).
How much time does it take to investigate and search for spilled files?	
It can take agencies hours if not days to assess the scope and impact of spills.	With Incydr Gov, security teams can determine the scope and impact of spills within minutes. The focus on end user activity makes it very easy for security teams to figure out where spilled files ended up. This allows security teams to spend their time in effective remediation. This is a huge time saver for security teams in their remediation efforts.
Do Unknown File names create a blind spot for your security teams?	
A big blind spot for security teams is an unknown file name. These can pose significant time investment in discovering which file or files were exfiltrated and how, extending spill investigations to several days and weeks	In addition to file names, Incydr Gov makes it easy for security teams to find files using partial filenames, or other information such as MD5 file hash or SHA256 hash. This allows security teams to track down specific files even if an end user has changed the file name.
How do you know if files purged as part of previous spill remediation action reappear in the environment?	
Re-emergence of files from previously cleaned-up spills is very hard to detect. Detecting this sort of recontamination often requires end users to re-alert security teams of such an event. There are barely any systematic methods to detect file reemergence.	Incydr Gov makes it easy for security teams to set up saved searches using file names, partial file names, and files hashes (MD5 & SHA256). These search queries can be scripted to run on regular intervals to “hunt” for previously spilled files across the whole environment. Additionally, Incydr Gov allows security admins to be alerted when files with specific file names or partial files names are moved by users to removable media or cloud systems. These capabilities enable security teams to be proactive about detecting recontamination issues.
How do you know the historical context of the spilled files?	
The historical context for file possession is often in question during a data spill investigation. Origin and ownership of Spilled files is often hard to detect because of the agency’s data security blind spots. These include activities that fly under the radar of other security technologies.	Incydr Gov gives you a historical view of file activity making it easy to see which users had a file, when they received it, where they put it (eg. uploaded to Sharepoint), and whom they might have shared it with. This makes spill investigations very easy and speedy.

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."

CROWDSTRIKE

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

snowflake

- **Mario Duarte**, VP of Security at 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."

UserTesting

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

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. (OV2104258)