Security and risk leaders are shifting their notion of “prevention” – recognizing that real-time blocking isn’t practical in remote or hybrid work environments. But as the workforce becomes more distributed, relying on traditional data loss prevention (DLP) tools to detect insider threats and other data risks in your environment will leave you with blindspots – from sensitive files being modified in an attempt to circumvent policies, to valuable data being classified inaccurately, or users adopting unsanctioned technologies that introduce new vectors for exfiltration. When security can’t keep pace with the business, it can take months, if not years, to discover there has been a data breach.

Code42 Incydr integrates with Rapid7 InsightIDR to allow security teams to visualize Incydr data within custom dashboards in InsightIDR. The integration helps SOC teams identify, prioritize and triage the most critical Insider Risk Indicators (IRIs), such as those that signal theft of corporate data. IRIs, which are surfaced within Incydr, are activities or characteristics that indicate data is at a high likelihood of exposure or exfiltration. With Incydr configured as a data collection source in InsightIDR, the highest severity events can be monitored in the same control plane as other threat types to ensure swift action.

Common examples of Code42 IRIs that can be visualized in InsightIDR include:

- File extension mismatch activity
- Removable media activity
- AirDrop syncs & printed files
- Source code repository activity
- Unsanctioned Dropbox activity by user
- Zip file exposures by user
- Outside active hours activity

When further investigation is required, SOC analysts can access Incydr directly from InsightIDR with one click to gather file, user and vector activity including how files were modified to the vectors in which they were exfiltrated, to the contents of the files themselves.

In addition, security teams leveraging InsightIDR as their single plane of control can create dashboards to visualize and triage non-malicious events that pose insider risk to corporate data – such as open file shares in the cloud and Shadow IT usage.

INTEGRATION BENEFITS

- Centralize the initial triage of IRIs that matter most to your organization – including user activity or file events indicative of data theft or an attempt to conceal exfiltration
- Access Incydr directly from InsightIDR to execute fast, contextualized insider risk investigations to inform the right human and automated response actions
- Strengthen compliance and file integrity monitoring (FIM) by validating critical file modification events and directly attributing users to suspicious activity in real-time
CODE42 INCYDR RISK EXPOSURE DASHBOARD:

- **Alert centralization** – Ingest the most critical Incydr IRIs into InsightIDR to centralize monitoring and initial triage of certain events within a single control plane.
- **One-click investigations** – Access Incydr from Rapid7 in one click to run saved searches against Incydr data using the filename or file hash (MD5 or SHA256) to detect exposure events tried to insider risk use cases, to see how a specific file moved, or how many users may have access to a certain file.
- **File integrity monitoring** – See and validate all file modification events, such as a file extension change, then directly attribute users to suspicious activity in real-time.
- **Compliance and audits** – Create and schedule reports of aggregated Incydr data for targeted metrics gathering, then retain Incydr exposure data and audit logs for an extended period of time to meet audit and compliance requirements.

EXAMPLE PANEL VISUALIZATIONS:

- **File extension mismatch activity within the last 30 days, grouped by Device Username, filename, and md5Checksum.**
- **Exposure events where users have moved files to removable media that are grouped by username and filename.**
- **Email exposure events in the last 30 days, grouped by username and filename.**

INTEGRATION FEATURES:

The example Code42 Incydr dashboard shown to the left displays visualizations based on specific use cases. Panels can be customized to align to an organization’s risk tolerance – and analysts can visualize Incydr data based on vectors, activities or scenarios deemed to put data at a higher risk.
USE CASE #1: VISUALIZE AND TRIAGE DATA RISK AS A RESULT OF INSIDER THREAT.

**CHALLENGE:** In 2020, more than three-quarters of organizations suffered a data breach despite having a DLP solution in place. Traditional data loss prevention (DLP) technologies built to address regulatory compliance don’t account for unstructured intellectual property – such as product roadmaps or source code – or have policies in place that can be easily circumvented by a malicious insider who changes the file extension type to disguise a spreadsheet with customer data disguised as a low-value file type, such as a JPEG.

**SOLUTION:** Incydr data visualizations in InsightIDR enable security teams to prioritize data risk detected by Incydr. For events requiring further investigation, teams can access Incydr from InsightIDR with one click and build their case. Teams can also download files in question within Incydr for additional context.

**BENEFIT:** Teams leveraging InsightIDR as a single control plane to view and triage threats in their environment can centralize how high-severity IRIs are monitored and initially triaged. For events requiring additional investigation, SOC teams can leverage the full extent of Incydr’s purpose-built insider risk management platform, while also being able to seamlessly toggle between Incydr and InsightIDR in order to align to organizational processes around incident documentation and response.

USE CASE #2: DETECT INSIDER THREAT VULNERABILITIES WITHIN YOUR MODERN COMPLIANCE PROGRAM.

**CHALLENGE:** Organizations must meet certain data protection compliance mandates such as PCI DSS, HIPAA and GDPR, but motivated insiders can circumvent policies or modify file extensions as a means to conceal exfiltration or intentionally leak data to a competitor.

**SOLUTION:** InsightIDR’s file integrity monitoring (FIM) feature allows teams to audit changes to critical files and folders for compliance reasons. Leveraging InsightIDR’s integration with Incydr, teams can now detect file extension mismatches, and attribute these changes to users in order to quickly assess if activity is benign or if its an attempt to conceal malicious exfiltration.

**BENEFIT:** Enrich file integrity monitoring (FIM) and strengthen mandated compliance by leveraging Incydr’s ability to look at granular file-level details, including the contents of a file and a complete history of how it was modified.

ABOUT RAPID7
Rapid7’s IT security data and analytics software and services help organizations reduce the risk of a breach, detect and respond to attacks, and build effective IT security programs. With comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques, Rapid7 strengthens an enterprise’s ability to defend against everything from opportunistic drive-by attacks to advanced threats. Unlike traditional vulnerability management and incident detection technologies, Rapid7 provides visibility, monitoring, and insight across assets and users from the endpoint to the cloud. To learn more about Rapid7, visit www.rapid7.com.

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.