CODE42

JOINT SOLUTION BRIEF

CODE42 INCYDR + LOGRHYTHM

Integrate Code42 Incydr with the LogRhythm NextGen SIEM Platform to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence

More than half (53%) of security teams are blind to users moving files to untrusted domains – and nearly two-thirds (63%) of security leaders don't know which insider risks to prioritize. On top of that, alert fatigue is real, so having the ability to prioritize the specific events that bring the greatest risk to your organization today has become more crucial than ever.

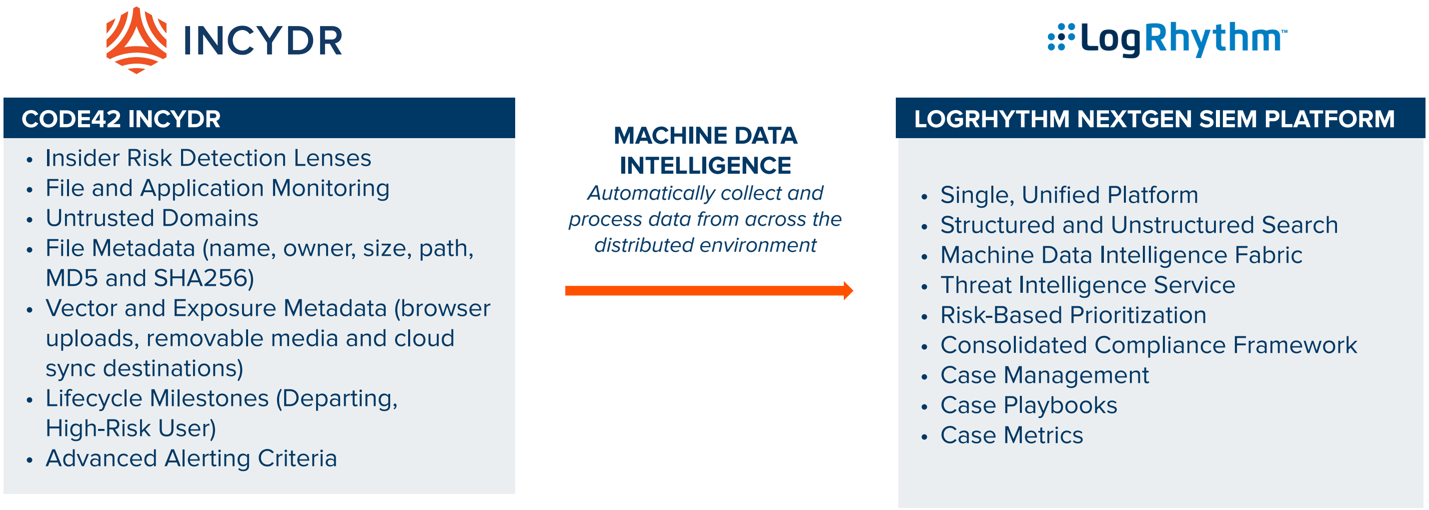
Code42 Incydr integrates with LogRhythm to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence. Security teams can configure rules to alert on Incydr-specific file exposure and exfiltration events, create customized dashboards using Incydr data, and run saved searches against Incydr data to detect exposure events – all from within LogRhythm.

INTEGRATION FEATURES:

- Ingest file telemetry information from Incydr into LogRhythm to visualize top files exposed; top users with exposure events; exposure types by source, file, and file type; removable media activity; and cloud file shares and desktop sync activity
- Create and run saved searches against Incydr data to detect exposure events tied to insider risk use cases, including departing employees or high risk users and contractors
- Deliver file and exposure data into LogRhythm using Common Event Format (CEF)
- Collect and retain Incydr exposure data and audit logs for an extended period of time to meet compliance and audit requirements

BENEFITS

- Manage insider risk throughout the employee lifecycle and across users more likely to put data at risk
- Reduce complexity by applying Incydr file telemetry information into LogRhythm dashboards or AI Engine correlation alerts
- Speed response to insider risk incidents with actionable insights to substantiate investigations



CODE42 INCYDR

- Insider Risk Detection Lenses
- File and Application Monitoring
- Untrusted Domains
- File Metadata (name, owner, size, path, MD5 and SHA256)
- Vector and Exposure Metadata (browser uploads, removable media and cloud sync destinations)
- Lifecycle Milestones (Departing, High-Risk User)
- Advanced Alerting Criteria

MACHINE DATA INTELLIGENCE

Automatically collect and process data from across the distributed environment

LOGRHYTHM NEXTGEN SIEM PLATFORM

- Single, Unified Platform
- Structured and Unstructured Search
- Machine Data Intelligence Fabric
- Threat Intelligence Service
- Risk-Based Prioritization
- Consolidated Compliance Framework
- Case Management
- Case Playbooks
- Case Metrics

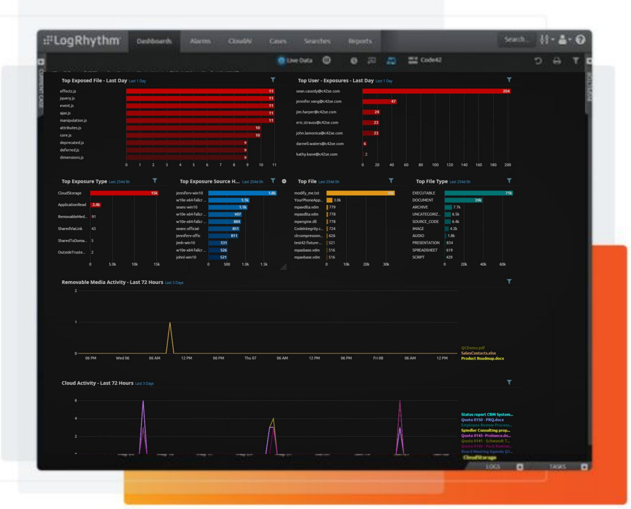
CODE42

USE CASE: INGEST FILE TELEMETRY INFORMATION FROM CODE42 INCYDR INTO LOGRHYTHM TO CORRELATE AND ANALYZE INSIDER RISK INDICATORS WITH ADDITIONAL DATA SOURCES FOR ENHANCED RISK INTELLIGENCE.

CHALLENGE: In 2020, data exfiltration was the most common insider risk in the U.S, more than tripling privilege misuse. While most organizations have mechanisms in place to prevent regulated data from leaving corporate systems, proprietary business documents should be protected differently and this is often overlooked.

SOLUTION: LogRhythm's Machine Data Intelligence (MDI) fabric seamlessly ingests Code42 Incydr data to correlate and analyze insider risk indicators with additional data sources for enhanced risk intelligence. Incydr records all employee file activity, and makes it searchable for investigation, but only alerts you to the events that indicate insider risk. Incydr enriches detected activities with context on the vector, file and user, including the type of files involved, whether the activity took place remotely, was performed during hours when the user is not typically active on their device, and even the ability to review full file contents. Within LogRhythm, security teams can configure rules to alert on Incydr-specific file exposure and exfiltration events, create customized dashboards using Incydr data, and run saved searches against Incydr data to detect exposure events to support investigations and speed response.

BENEFIT: Streamlining alert information and incident triage within LogRhythm reduces complexity by correlating event information to deliver actionable insights that speed insider risk response.



Code42 Incydr data showing top files exposed; top users with file exposure events; top exposure types by source, file and file type; removable media activity; and cloud file shares and sync activity visualized within LogRhythm.

ABOUT LOGRHYTHM

LogRhythm empowers more than 4,000 customers across the globe to measurably mature their security operations program. LogRhythm's award-winning NextGen SIEM Platform delivers comprehensive security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) within a single, integrated platform for rapid detection, response, and neutralization of threats. Built by security professionals for security professionals, LogRhythm enables security professionals at leading organizations like NASA, XcelEnergy, and Temple University to promote visibility for their cybersecurity program and reduce risk to their organization each and every day. LogRhythm is the only provider to earn the Gartner Peer Insights' Customer Choice for SIEM designation four years in a row. To learn more, please visit logrhythm.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.