exabeam

SOLUTION BRIEF

EXABEAM AND CODE42

Quickly detect, investigate and respond to insider threats

Insider threats are now among the most serious security vulnerabilities, and are becoming increasingly difficult to manage using conventional security technologies. The huge shift to remote working in 2020 has increased the use of personal devices and at the same time reduced the effectiveness of existing enterprise security solutions. When devices aren't accessing assets directly through the corporate network or a VPN and instead going straight to the cloud, on-premise network data loss prevention (DLP) techniques and network firewalls have blind spots.

The Exabeam and Code42 integration enables security teams at joint customers to quickly detect and investigate data exfiltration caused by departing and remote employees, as well as compromised, negligent, or malicious insiders. Code42 Incydr's data risk intelligence surfaces insights for subsets of users more likely to put data at risk. This data is ingested into the Exabeam Security Management Platform to provide security teams with actionable insights that can be applied to existing SOC workflows to substantiate insider threat investigations and speed response. Risk scores assigned to individual Incydr events are combined with other abnormal and normal user activities identified using Exabeam's UEBA, to flag notable high-risk users for prioritized investigations. Additionally, these events are presented automatically in Exabeam's Smart Timelines, saving security analysts and insider threat teams hours of investigation time.

CODE42

KEY BENEFITS

- Provide real-time analysis and reporting on security alerts and data exfiltration attempts across their environment.
- Accelerate investigations related to insider threats with detailed incident context across vectors, files and users.
- Close insider risk incident tickets faster by automating response and remediation with prescriptive case management.

USE CASE

Actionable Data Exfiltration Detection Ingest Code42 Incydr data risk intelligence into Exabeam for actionable insights, correlation and triage of insider threats.

CHALLENGE

Security teams have underdeveloped or non-existent processes in place to detect and respond to insider threats or data exfiltration.

SOLUTION

Code42 logs every file event then enriches it with context on the vector, file and user to determine what represents real risk. Risk detection lenses are purpose-built for common insider threat scenarios but can be customized to your environment. When file exposure or exfiltration is detected, high-fidelity alert information is extracted into Exabeam for correlation and triage. Exabeam helps prioritize these alerts by identifying users with the highest risk scores reflecting most suspicious or abnormal activity. This ensures Code42 data can be applied to existing SOC workflows while ensuring complete file context to support investigations and speed response.

BENEFIT

Streamlining alert information and incident triage within Exabeam reduces complexity by correlating event information to deliver actionable insights that speed insider threat response.

> "This technology collaboration between Exabeam and Code42 allows employees to use the tools they need to work in distributed environments, while giving security teams visibility into how files are moving across endpoints and cloud applications."

CHRIS STEWART, SENIOR DIRECTOR,
GLOBAL ALLIANCES, EXABEAM

TOP USE CASES

- Substantiate insider threat investigations with rich behavioral context
- Increase monitoring focus on departing employees
- Protect against theft and accidental data disclosure by trusted insiders
- Reduce mean time to identify data breaches
- Maintain compliance with corporate and governmental data regulations/ Identify non-compliant data migration
- Protect from data loss associated with BYOD and IoT

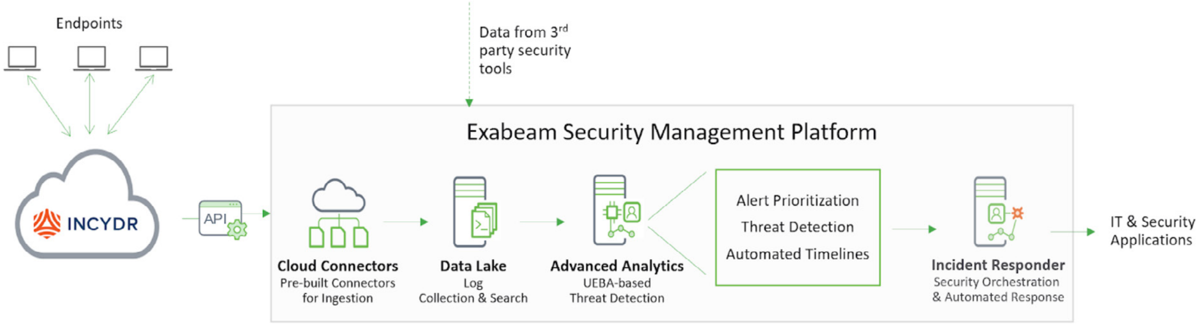
Endpoints
INCYDR
API
Data from 3rd party security tools
Exabeam Security Management Platform
Cloud Connectors
Pre-built Connectors for Ingestion
Data Lake
Log Collection & Search
Advanced Analytics
UEBA-based Threat Detection
Alert Prioritization
Threat Detection
Automated Timelines
Incident Responder
Security Orchestration & Automated Response
IT & Security Applications

FIGURE 1: HIGH-LEVEL INTEGRATION DIAGRAM BETWEEN CODE42 AND EXABEAM

HOW IT WORKS

- Code42 Incydr monitors endpoint activity with a lightweight agent
- Exabeam ingests endpoint telemetry via API or Cloud Connector
- Create custom dashboards within Exabeam using Code42 data -- with the ability to tailor queries based on file, vector or user (i.e. only files that have been uploaded via a browser)
- Using Code42 and other third party security data, Exabeam baselines normal behavior and assigns users risk scores based on anomalous activity
- Exabeam performs alert prioritization based on risk scores to focus analysts on the highest risk incidents
- Exabeam detects additional threats based on anomalous user or machine behavior
- Exabeam's Smart Timelines automatically create incident timelines for rapid investigation
- Out-of-the-box playbooks using pre-built integrations enable semi-automated or fully automated incident response using third party IT & security applications

ABOUT CODE42

Code42 is the leader in insider threat detection, investigation 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 threat 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. For more information, visit code42.com, read Code42's blog or follow the company on Twitter.

ABOUT EXABEAM

Exabeam is the Smarter SIEM™ company. We help security operations and insider threat teams work smarter, allowing them to detect, investigate and respond to cyberattacks in 51 percent less time. Security organizations no longer have to live with excessive logging fees, missed distributed attacks and unknown threats, or manual investigations and remediation. With the modular Exabeam Security Management Platform, analysts can collect unlimited log data, use behavioral analytics to detect attacks, and automate incident response, both on-premises or in the cloud. Exabeam Smart Timelines, sequences of user and device behavior created using machine learning, further reduce the time and specialization required to detect attacker tactics, techniques and procedures.

Exabeam is continuously adding new integrations with best of breed security vendors to its offering. These integrations are included as part of the solution at no additional cost, supporting organizations as they expand their security ecosystem, and providing peace of mind that Exabeam integrations will support your unique environment as it evolves over time. For more information, visit www.exabeam.com.

TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.