

Incydr™ + Exabeam

Prioritize the events and users that pose the greatest threat to corporate data

Incydr sends alerts to Exabeam and delivers a prioritized view of top exfiltration destinations, most risky users and types of files exposed so analysts can instantly see a company-wide view of where and who is putting valuable data at risk.

Integration Overview

Exabeam ingests Incydr Risk Indicators (IRIs) and combines it with user and entity behavior analytics (UEBA) based modeling to help you create a baseline for normal behavior so you can better understand if an employee is harmlessly working with a file or is potentially leaking or stealing files. By integrating Incydr with Exabeam Fusion SIEM, you can get all the information you need to investigate, prioritize, manage and respond to Insider Risk incidents.

Features



Alert Triage

Ingest prioritized alerts from Incydr into Exabeam



Custom Dashboards

Analyze and report on data exposure to quickly identify untrusted activity and triage the most critical alerts



Device Health Checks

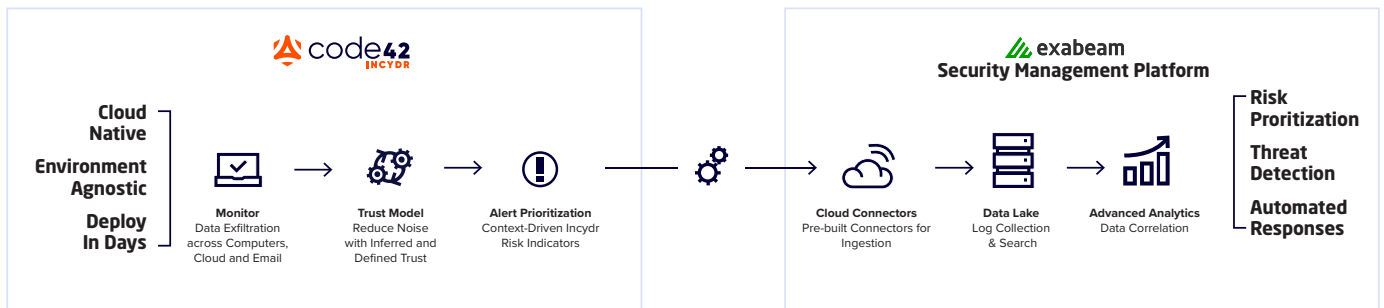
Ensure you're getting accurate, up-to-date information on exfiltration events from all monitored devices

Benefits

Increased Visibility: Leverage Incydr's alert prioritization to manage data risk across all employees and gain a company-wide view of exfiltration activity

Alert Review Efficiency: Streamline workflows by maintaining Exabeam as your preferred system for alert review and triage

Data Protection: Gain complete visibility into data at risk and protect your company's intellectual property and other high-value data



Incydr's endpoint agent monitors all file, exfiltration, vector and user activity across computers, cloud and email systems to prioritize IRIs. Exabeam collects Incydr IRI data and combines it with its behavioral analytics to create combined risk scores.

Once a threat has been identified, the Exabeam Incident Responder automatically orchestrates a response based on your existing SOC procedures, allowing you to react quickly and efficiently. Incydr's forensic search and case management features compile evidence and streamline incident response processes in combination with Exabeam's UEBA so you have all the context and evidence to respond effectively.

About Mimecast

Mimecast is an AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.