HOW INCYDR PRIORITIZES RISK TO DATA:

AN OVERVIEW OF INCYDR'S RISK PRIORITIZATION MODEL

INCYDR

Without a purpose-built solution designed to manage Insider Risk, security practitioners struggle to differentiate between harmless file movement and meaningful data leak or theft. In fact, nearly two-thirds of IT security leaders say they don't know which Insider Risks to prioritize.[1] Much of this is because security professionals say they lack the context needed to quickly identify if an activity represents risk 72% of the time.[2] Incydr addresses this challenge head-on with an approach to Insider Risk that's rooted in simplicity, signal and speed. Its methodology for prioritizing Insider Risk is:

1 | Context-driven: Designed to manage dynamic Insider Risk using file, vector and user Insider Risk Indicators (IRIs)

2 | Pragmatic: Rooted in real-world Insider Risk expertise to deliver a use-case centric approach to Insider Risk Management

3 | Adaptable: Easily tuned to an organization's unique Insider Risk tolerance through adjustable prioritization settings

PRIORITIZATION METHODOLOGY

IRIs prioritize the users and events that matter most

When monitoring file activity, Incydr watches for Insider Risk Indicators (IRIs). IRIs are activities or characteristics that suggest corporate data is at a higher risk of exposure or exfiltration. They are used to prioritize the users and events that represent the greatest risk to the organization, and support a use-case centric approach to Insider Risk Management.

Cumulative risk scores determine event severity

Incydr's extensive library of IRIs is categorized by file, vector and user risk indicators. Incydr assigns a numerical risk score to every IRI. These scores are totaled to determine the overall risk of a detected event. The risk score of an event determines the event's severity: critical, high, moderate or low. Events are prioritized by severity, and users are prioritized by the number of critical events they trigger. Code42 determines these scores by combining its own product telemetry data on the highest risk IRIs with qualitative research on security practitioner experiences.

Prioritization settings are easily adapted based on risk tolerance

If needed, administrators can adjust the prioritization model to fit their own risk tolerance. Risk settings adjust the risk scores and modify how users and events are prioritized. Trust settings tell Incydr what activity it should de-prioritize. This includes trusted domain information that allows Incydr to distinguish between sanctioned and personal or unsanctioned activity, and prevents approved file activity from triggering alerts or cluttering dashboard views. The result is an accurate, prioritized list of the highest risk users and events.

[1-2]Code42 Data Exposure Report 2021

INSIDER RISK INDICATOR (IRI) EXAMPLES

File
- Zip file exfiltration
- Source code exfiltration
- SalesForce report exfiltration
- Earnings report exfiltration

Vector
- Public link in Google Drive
- Dropbox sync app
- Attachment to ProtonMail
- Airdrop transfer

User
- Departing employee
- Contract employee
- Off hours activity
- File mismatch (concealed exfiltration)

PRIORITIZATION SCENARIOS:

Below are examples of how Incydr prioritizes Insider Risk events. Remember, all defaults can be tuned to your risk tolerance. For example, Incydr does not assign a risk score to video files by default. However, if you run a production studio where video files comprise much of your intellectual property, you can increase their risk score.

Example Events

= **16, Critical Severity**

A **departing employee** sends a **zip file** using **ProtonMail**.

= **12, Critical Severity**

A **contract employee** sends a **zip file** to **Airdrop** during **off hours**.

= **8, High Severity**

An **employee** uploads **source code** to **Dropbox**.

= **4, Moderate Severity**

An employee with **poor security practices shares a video file** in **OneDrive to an untrusted domain**.

= **3, Low Severity**

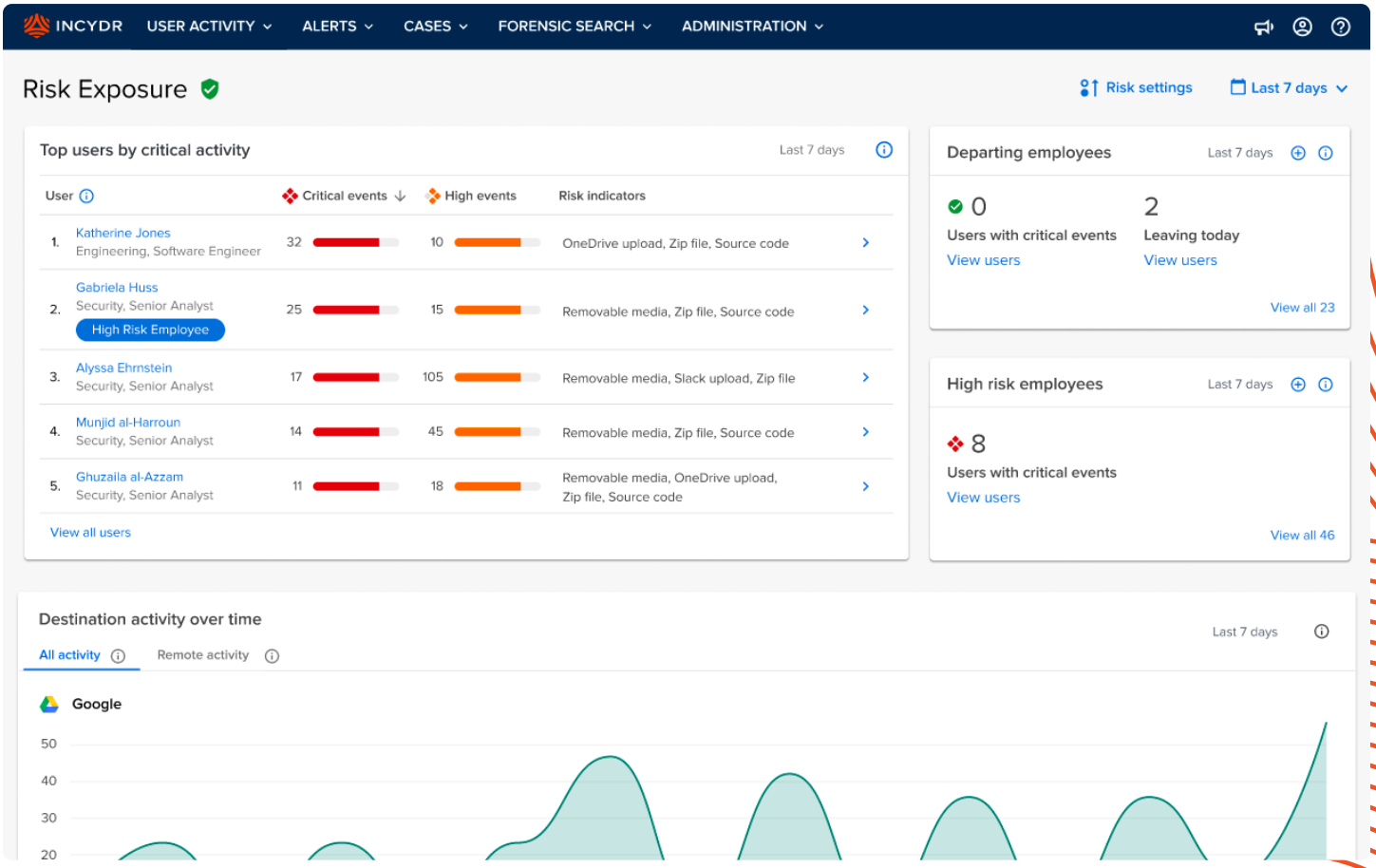
An **employee sends a video** to a **personal Gmail address**.

Severity Thresholds

No risk indicated: 0 | **Low:** 1-3 | **Moderate:** 4-6 | **High:** 7-8 | **Critical:** 9+

If all events are critical, no events are critical

The goal of prioritization is to focus security teams on the risks that matter most. It's important that severity thresholds actually result in clear prioritization. If all events are critical, no events are critical. Incydr's prioritization model ensures security teams will not be bombarded by loads of "critical" alerts that ultimately create noise. On average, customers using model defaults might expect about 1-3% of their users to have one or more critical-severity events each week, and about 1-4% to have one or more high-severity events.



Security teams get a prioritized list of the users whose activity needs review. Users are prioritized by the number of critical events they trigger.

Conclusion

Incydr offers a context-driven approach to prioritize risk, contain data exposure, accelerate resolution, and educate users on appropriate data handling. Ultimately, security teams who utilize Incydr are able to avoid corporate data leak and drive the behavioral change needed to improve their Insider Risk posture.

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com