code42

What You Get from An

Incydr Proof of Value

Run Incydr in your organization for free. After only 4 weeks, with an average of 4 hours of engagement total, you'll get a detailed view of your organization's data risk exposure and our recommendations on how to mitigate and reduce that risk.

Here's an example of the executive summary from a recent Proof of Value which demonstrates that organization's top 3 risks, and personalized recommendations:

According to our model, here are the top risks in your environment over the last 30 days:

TOP SOURCE OF DATA THAT HAS RESULTED IN CRITICAL EVENTS:

ADP

16

events including Compensation data and PII.

Code42 Recommendation

Create critical alert for movement of data that comes from ADP. Use Incydr Flows to automate response to these events using Code42 ecosystem integrations.

TOP EXFILTRATION VECTOR BY VOLUME OF CRITICAL EVENTS:

File attachments to personal Gmail

1,312

events

Code42 Recommendation

Cut down on the volume of low severity events by sending automated training on your email policy via Code42 Instructor video lessons. Alert users that you are monitoring uploads to personal email with an updated log on banner. Continue monitoring data movement to any non-corporate Google domain. Use Incydr Flows with your EDR to lock endpoint access for critical severity events.

RISKIEST WATCHLIST OR USER BEHAVIOR:

iCloud App syncing (specific to engineering department)

471

files synced

Code42 Recommendation

The security and IT teams were unaware that engineering users preferred to share data and work via Airdrop and their iCloud accounts. Consider making these sanctioned applications and creating alerts for the detection of Corporate IP moving beyond the sanctioned environments.

The process is easy. For more on what to expect, **check out our guide** or **sign up for a POV**.

code42