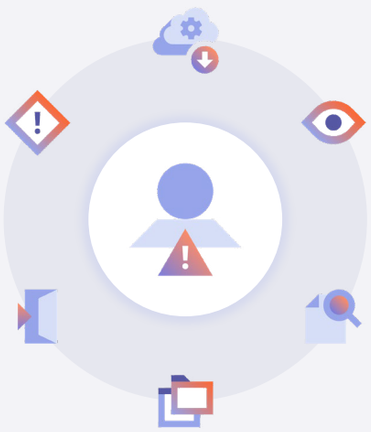
code42

code42.com/resources

6 Unusual Data Behaviors That Indicate Insider Threat

Most data security breaches are inside jobs — either mistakes (oops) or malicious theft of important company files (ouch).

Insider threat strategies designed to stop exfiltration need to easily and effectively spot the riskiest activity to the data you care about most.



HERE ARE JUST SIX EXAMPLES OF ANOMALIES THAT YOUR INSIDER THREAT SOLUTION SHOULD BE ABLE TO SPOT:

DOWNLOADS TO UNMANAGED DEVICES

Loki works remotely, which means no one can tell if a few **Salesforce reports are downloaded to a personal device**, right?

CLOUD LOOK-ALIKES

Marketing uses corporate Google instance for email and file sharing.

What's this big upload to a marketer's **personal Google Drive account** all about?

FILE MIME TYPE MISMATCH

Thanos just renamed a file "Cute Cat Pix" and gave it a .jpeg extension. Just one problem: the actual content of the file is **source code**, not an image.

PERMISSIONS ALERT

Ultron just changed the permission on a Google Doc to "Anyone can edit."

And guess what — it's your "top secret product roadmap."

Time to check in with Ultron.

SMART PEOPLE PLAN THEIR EXIT

Hela just quit.

Anyone can watch whether Hela downloads huge files in the next two weeks.

But can you see what was moved over the **past 90 days?**

STARTING TO SEE A PATTERN?

Sometimes it's not one action, it's a set.

Like that time Hydra encrypted 50 files containing customer lists, zipped them up and sent them to an unrecognized email.

Unusual, right?

Remember:

- Risky data activity requires context so that you can respond confidently.
- A view of all activity with the context to understand what's riskiest — can surface data moving to places you don't trust.
- Insider threats are evolving (but also solvable).