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).

An insider threat strategy should include a way to easily and efficiently spot unusual data behaviors that are actually risky and require response. Here are just six examples of anomalies that your insider threat solution should be able to spot:

OFF-HOURS ACTIVITY

Even since working from home changed their schedule, Loki never clocks in after 11 P.M.

Yesterday, they sent 30GB to a thumb drive just after midnight.

Hey Loki, can we have a chat?

CLOUD LOOK-ALIKES

Marketing uses the 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:

- Unusual user activity might be inadvertent, but sometimes it's malicious (and even innocent mistakes can cause data loss!).
- A view of all behavior — whether it's files, the vectors by which they move, or the people who move them — can surface that particular activity which represents real risk.
- Insider threats are evolving (but also solvable).