What is an insider threat?

An insider threat is a current or former employee, contractor, or partner who misuses legitimate access, whether maliciously (theft, sabotage) or negligently (falling for phishing, mishandling data). Negligent insiders cause far more incidents than malicious ones. Because the access is authorised, the defenses are least privilege, access reviews, prompt offboarding, monitoring of sensitive actions, and a blameless reporting culture.

HOW IT WORKS

01 Why insiders are hard to catch

External attacks trip alarms because the access is abnormal. Insider actions do not, because the access is expected. A finance manager reading finance data, or an engineer touching production, is exactly what should happen, until it is not.

That means insider detection is behavioural rather than technical: it is about noticing when someone touches data they do not usually touch, downloads far more than normal, or acts right before or after leaving the company. Trust is the vulnerability, so the controls have to assume access will sometimes be misused.

02 What insider incidents look like

In practice, insider incidents tend to look like this:

- A departing employee downloading customer lists or source code before their last day.
- Sensitive files emailed or uploaded to a personal account.
- Data copied to a USB drive.
- A careless misconfiguration that exposes data to the internet.
- A privileged administrator quietly abusing their access, or a compromised admin account doing it for them.

HOW TO DEFEND

- Least privilege and regular access reviews, so people can only reach what their role needs, and access does not accumulate.
- Prompt, complete offboarding, disabling accounts and reclaiming devices the same day someone leaves.
- Logging and monitoring of sensitive actions, so unusual access to important data is visible.
- Separation of duties for high-impact actions, so no one person can act alone.
- A blameless reporting culture, so honest mistakes surface early instead of being hidden.

SOURCES

[1] Insider Threat Mitigation

[2] Computer Security Resource Center Glossary

[3] Data Breach Investigations Report

See what a single account could reach if it turned against you.

securelayer7.net/learn/threats/insider-threats

Open online