

Insider Threats – 2025

What is an Insider Threat?

An insider threat occurs when a current or former employee, contractor, or business partner misuses their access to systems, data, or facilities—intentionally or unintentionally—causing harm to the organization.

2025 Statistics

60–65% of security incidents involve insiders — This range matches the 2025 Ponemon Institute Cost of Insider Threats Global Report (commissioned by Proofpoint), which reported 63% of incidents were caused by negligent or malicious insiders.

Average annual cost of insider threats ≈ \$16.2 million — Same Ponemon 2025 study found a global average cost of \$16.2M per organization, up from \$15.4M in 2023.

Malicious insider incidents take 85+ days to contain — Ponemon 2025 reported the average was 85 days, with some taking over 90 days.

Negligent insiders cause most incidents — The report found 56% of incidents came from negligence, 26% from criminal/malicious insiders, and 18% from credential theft.

Why It Matters?

Insider threats bypass many external defenses since the attacker already has legitimate access.

Incidents often go unnoticed until significant damage occurs.

Regulatory penalties and reputational harm can be long-lasting.

How does Cenegi help?

Security Audits to identify unnecessary access and vulnerabilities.

User Behavior Monitoring to detect suspicious activity early.

Incident Response & Digital Forensics to stop attacks and gather legal-grade evidence.

Security Awareness Training to reduce accidental insider incidents.