EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 13 · Part 1 of 2 · 6 November 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Jessy Lang

Free-Range Fear

Eight threats and eight rules for AI inside your company

Fear without an address is a mood. A threat has a place: a system, a piece of data, a permission. Before you act on any claim about AI, ask the three questions below. The sum of the answers is the reach somebody granted to the system.

GRANTED REACH
An AI system has only the reach somebody gave it.

1. What can it read?

2. What can it do?

3. Where does the output go?

THREATS AND WHAT TO DO ABOUT THEM

1	**Shadow AI** Data leaves through tools nobody approved.	Offer an approved tool that people like to use. Write one page of rules: what may go in, what never goes in (credentials, personal data without a contract, unreleased financials, third-party secrets), where to ask. Find out what is already in use, and look without blaming.
2	**Oversharing** The assistant finds what permissions never really protected.	Clean up access rights before you connect it. Make it answer with the rights of the person asking, not with one master key. Ask: whose permissions does it use to fetch a document?
3	**Words that give orders** Instructions hidden in mails, documents and web pages.	Treat everything it reads from outside as untrusted. Limit what it may do after reading untrusted content. Let a human confirm anything with consequences. Never chain a summary step and a send step without supervision.
4	**Hands on the controls** Agents with more rights than the job needs.	Give the agent its own identity, not a person's login. Least privilege, read access unless writing is the point, limits on amounts and recipients. Approval for irreversible actions, and an off switch that works within a minute.
5	**Confident and wrong** Fluent output that nobody checked.	A named person owns every document that leaves the company or that it relies on. Match the review depth to the stakes. Ask for the source of each statement and check two or three.
6	**No trail** Nobody can reconstruct what happened.	Log requests, data sources and actions, keep the log long enough to be useful, and secure it, because the prompts contain sensitive things.
7	**Silent changes** The vendor changes the model, the behaviour or the terms.	Keep an inventory of AI services: use, data, contract, owner, exit. Rerun a small set of test questions whenever something changes. Know how you would leave.
8	**Attackers with AI** More convincing pretexts, same old goals.	Verify payment changes and urgent requests through a second channel you chose yourself, for example a call-back on a number from your own directory. Never rely on recognising a voice. Use multi-factor authentication. Train with realistic examples.

YOUR ONE-PAGE REGISTER

One row per AI tool in the company. If you cannot fill in what it can read, you have found your first problem. If no name goes into the owner column, you have found your second. Check each row against the eight threats. A small company needs an afternoon; a large one starts with its two or three most used tools.

System	What it can read	What it can do	What could go wrong	Owner

Listen to the episode
Free-Range Fear and the rest of the series.
eacg.de
/en/podcast/s13-free-range-fear

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH