AI threat modeling agents

Threat model acceptance record

[ ] System or change modeled, and the design artifacts the agent read (versions and dates)
[ ] Agent, version and model used
[ ] For each threat: source rule or standard, or "agent-drafted, no source"
[ ] Threats the reviewer added, removed or changed
[ ] Reviewer name, role and date
[ ] Open items accepted without mitigation, and who owns them
[ ] Date the model must be re-checked, or the design change that triggers it

Agentic AI in Cybersecurity, AI threat modeling agents, edition 19 Nov 2026, https://agenticaiincybersecurity.com/use-cases/threat-modeling/. License CC BY 4.0.