

AGILE THREAT MODELING

Surface architectural risks early — while they're *still cheap to fix*.

A hands-on workshop package that turns secure-by-design into a working practice your team can repeat as the architecture evolves — not a one-time consulting deliverable aging on the shelf. We look at the architecture together, enumerate what could realistically go wrong, and decide which security controls are actually worth the investment.

christian-schneider.net/consulting/agile-threat-modeling ↗

HOW THE PACKAGE RUNS

• Scoping call

A short upfront session to tailor the workshop — top-down scenario approach or bottom-up dataflow approach, plus focus areas specific to your stack.

• Initial workshop

Targeted interviews cover software architecture, authN/Z & tenant isolation, exposed interfaces, data formats, containerization, cloud connections, crypto & trust, sensitive-data flows, trust boundaries, and GenAI integrations (RAG poisoning, prompt injection, MCP tool abuse, agentic goal hijacking).

• Rework phase

Between sessions I build a preliminary threat model from the gathered insights, using free tooling so your team can keep evolving it afterwards.

• Final workshop

Collaborative session with your team: enrich details, remove inaccuracies, add missing risks, simulate attack paths. The remaining parts of the model are created live — so the team learns the method by doing it.

• Reporting & roadmap

Detailed report with risks, evidence, tailored mitigations and security controls — categorized by business, architecture, development and operations — plus a multistep mitigation roadmap.

A GOOD FIT WHEN

- Planning a new service, major refactor, or cloud migration
- GenAI, agentic or MCP components are being integrated
- You need threat scenarios & attack paths for compliance
- Prior threat modeling stalled as a one-off document

TOP-DOWN · ATTACK TREE

The workshop's primary lens. Using my free **Attack Tree** toolkit (attacktree.online), we map realistic attack scenarios, place security controls on the branches, and simulate how each control changes the residual risk. Intuitive for teams new to threat modeling — no YAML, no ceremony — and perfect for getting started even when architectural details are still fuzzy.



Also available — Threagile (bottom-up). For teams with mature architecture docs who prefer a YAML-modeled dataflow view with auto-generated DFDs and risk rules. We pick the right approach in the scoping call.

WHAT YOU TAKE AWAY

- Living threat model, editable in free tooling
- Detailed risk report with evidence & mitigations
- Multistep mitigation roadmap, role-categorized
- Diagrams, graphs & Excel exports of current vs. reduced risk
- A team that can repeat the method as architecture evolves



Let's scope your team's threat modeling workshop.

Every engagement starts with a free scoping call to choose approach, focus areas and stack examples. Short on time? Ask about the 3-hour intro session.

GET IN TOUCH

mail@christian-schneider.net

christian-schneider.net