ATTACK TREE

Agile threat modeling designed for *modern attack scenarios*.

Scenario-driven threat modeling with built-in control simulations. Map assets, threats and mitigations, then simulate how your controls actually behave against attacker scenarios. Particularly useful for modeling agentic and AI systems, where probabilistic controls (guardrails, classifiers, human-in-the-loop) sit alongside deterministic ones.

attacktree.online · christian-schneider.net/development ↗

EDITION 01

Free SaaS

attacktree.online

Public, browser-based, free to use.

The hosted edition everyone can use instantly: no sign-up, no installation, stateless by design. Ideal for individual practitioners, training sessions, workshops and getting hands-on with a model in minutes.

- → Visual editor in your browser
- → Risk-to-asset mapping
- → What-if analysis of controls
- → Single points of success and failure detection
- → Choke-point and heat-map analysis
- → Dashboards, executive reports, ROI control grids
- → Export to PDF, Excel, JSON, SVG
- → AI features available
- → Threat actor and risk profile customization
- → Fault Tree as Attack Tree alternative
- → Threagile, OTM and OWASP Threat Model Library import
- → Probabilistic simulation of attack paths (Monte Carlo)
- → k-means clustering: quick wins and strategic controls
- → Customizable reports (HTML, PDF)
- → REST API for integration

EDITION 02 BEST OPTION

Custom SaaS

dedicated instance

Your tenant, your branding, your integrations, your customization.

A dedicated, isolated SaaS instance operated for your organization. Customer-specific branding on your domain, your own pattern library, customized templates and wizards, and bring-your-own AI configuration.

Everything in Free SaaS, plus:

- → Isolated tenant on your domain
- → Full customization: templates, attacks, controls, checklists
- → Customizable guided wizard
- → Bring-your-own AI API key, full prompt & review customization
- → Configurable export templates
- → Simple licensing: org-wide, no per-user or per-model limits

EDITION 03

Self-Hosted

on-prem · private cloud · air-gapped

Runs entirely inside your perimeter.

Container-based deployment (Docker or Podman), or a stateless CLI for fully unattended use. Built for regulated industries and air-gapped environments: runs on infrastructure you control, end to end.

Everything in Custom SaaS, plus:

- → Docker, Podman or stateless CLI
- → Air-gap and offline operation
- → Runs entirely on infrastructure you control
- → Minimal hardware footprint (2 GB RAM, 1 CPU)
- → Support and update channel included
- → Source-code review under NDA available for regulated industries

ADD-ONS

Available with any edition. Scoped and billed per engagement.

+ **Custom Feature Development**
On-demand development of customer-specific features inside the platform: bespoke analyses, model extensions, reporting formats or workflow steps.

+ **Custom Backend Integrations**
On-demand development of individual integrations: ticketing, GRC, CI/CD, internal asset systems.

Interested in what can be customized?
Let's arrange a live demo call to walk through the editions, the customization options, and how Attack Tree fits your scenarios.

GET IN TOUCH
mail@christian-schneider.net
christian-schneider.net