YOUR WHOLE COMPANY UNSTOPPABLE, IN FLOW WITH AGENTIC ENGINEERING.

Agentic Engineering Security for Development Teams (AE-SEC)

Agents act with your credentials and open new ways into your systems, and they find vulnerabilities for attackers as readily as for your team. In one day your team hardens its agents and uses them for a threat model, a vulnerability hunt and a fix.

WHO IT IS FOR

Engineering teams working with coding agents, and their security owners

FORMAT	GROUP	PRICE
One day, remote or on site	8 to 12 participants	On request

Quoted by volume and part of your offer. Mentoring can be booked afterwards and is billed by the hour.

HANDS-ON
Your agent configuration, your repository once cleared

PREREQUISITE
Daily development work, no security specialisation needed

WHO TRAINS IT
One of our 70+ trainers, with Stefan Munz and Benedikt Stemmildt accountable

LANGUAGE
German or English

TAILORED
In the preparation call, to your team and your stack

CERTIFICATE
Certificate of attendance

PROCUREMENT AND LEGAL
Contract, NDA and DPA

WHAT YOUR TEAM TAKES AWAY

- A map of your agent setups with every input, tool, credential and exit
- Your agent configuration tested against prompt injection, the first gaps closed
- A first draft of a threat model for one of your services
- Where the hunt finds something: the finding with its reproduction and a first fix as a pull request
- Security rules for your agents' instruction file and the next security gate

Your team trains with the coding agent it already uses: Claude Code, Codex, GitHub Copilot, Gemini CLI or Cursor. If it has none yet, we bring one that fits your needs.

AGENDA

Security work with agents, in both directions

- **What attackers do with agents** and what it means for your systems
- **Mapping the attack surface:** inputs, tools, credentials, exits
- **Hardening the agent setup:** plant a prompt injection, bypass guardrails, close the gaps
- **Threat modelling with an agent:** the agent drafts, the team corrects
- **Finding and triaging vulnerabilities:** agents hunt in the code and sort scanner findings
- **Hardening as a loop:** from finding to fix with a test and on to the security gate

HOW THE EXERCISES STAY SAFE

- We practise attacks only on the staging system you name in writing beforehand.
- Every finding comes with a reproduction or a failing test, so your team can check it right away.

GOOD TO KNOW

DAILY HOURS
Usually 9:00 to 17:00, as agreed

LEAD TIME
About four weeks, usually set by your team's calendar

SEVERAL TEAMS
A pilot team first, then team by team in waves of 8 to 12

CANCELLING AND MOVING
Free up to 4 weeks before, then 50%, under 2 weeks 100%. Moving within 8 weeks is free.

YOUR CODE
Stays with you: our trainers never receive, clone or store it.

LICENCES
You provide them, or we bring them and you pay for them.

COMMUNITY
Free for good for every participant

FUNDING
German companies may qualify under the Qualifizierungschancengesetz; we check it with you

> "We went from 2 engineers playing with agentic coding to 20 using it daily. We created 17 skills and 9 agents available to every engineer."
>
> TOM HIBBERT, CHIEF TECHNOLOGY OFFICER, MOONFARE

ABOUT HACKERS&WIZARDS Practitioners with over 20 years of building and running production systems (OTTO, Breuninger, BLUME 2000). Founded in Hamburg by Benedikt Stemmildt and Stefan Munz.

SELECTED CLIENT TEAMS

Tchibo · SIGNAL IDUNA · IONOS · Krombacher · eventim · blaudirekt · PIC NIC · haufe.group · MOIA · VORWERK · Moonfare · LichtBlick · dm · EGYM · statista · EUROGATE · bonprix. · adesso insurance solutions · GLOBAL · OMR · Bünting · unzer · SDK · Suiteify · FRICKE

Want this training for your team?
Tell us about your team and we send you an offer.

summon@hackersandwizards.dev

Book a call: haw.dev/call