EUER GANZES UNTERNEHMEN UNAUFHALTSAM, IM FLOW MIT AGENTIC ENGINEERING.

Agentic Engineering Security for Development Teams (AE-SEC)

Agenten handeln mit euren Zugangsdaten und öffnen neue Wege in eure Systeme, und sie finden Schwachstellen für Angreifer:innen genauso wie für euer Team. An einem Tag härtet euer Team seine Agenten und macht mit ihnen Bedrohungsmodell, Schwachstellensuche und Fix.

FÜR WEN

Entwicklungsteams mit Coding-Agenten und ihre Security-Verantwortlichen

FORMAT	GRUPPE	PREIS
Ein Tag, remote oder vor Ort	**8 bis 12 Teilnehmende**	**Auf Anfrage**

Nach Umfang kalkuliert und Teil eures Angebots. Mentoring ist im Anschluss buchbar und wird nach Stunden abgerechnet.

HANDS-ON
Eure Agenten-Konfiguration, euer Repository nach Freigabe

VORAUSSETZUNG
Tägliche Entwicklungsarbeit, keine Security-Spezialisierung nötig

WER SIE GIBT
Eine:r unserer 70+ Trainer:innen, verantwortet von Stefan Munz und Benedikt Stemmildt

SPRACHE
Deutsch oder Englisch

ZUSCHNITT
Im Vorbereitungsgespräch auf euer Team und euren Stack

ABSCHLUSS
Teilnahmezertifikat

EINKAUF UND RECHT
Vertrag, NDA und AVV

WAS EUER TEAM MITNIMMT

- Eine Karte eurer Agenten-Setups mit allen Inputs, Tools, Zugangsdaten und Ausgängen
- Eure Agenten-Konfiguration, gegen Prompt Injection getestet, die ersten Lücken geschlossen
- Einen ersten Entwurf eines Bedrohungsmodells für einen eurer Services
- Wo die Suche etwas findet: den Befund mit Reproduktion und einen ersten Fix als Pull Request
- Security-Regeln für die Instruktionsdatei eurer Agenten und das nächste Security-Gate

Euer Team trainiert mit dem Coding-Agenten, den es schon nutzt: Claude Code, Codex, GitHub Copilot, Gemini CLI oder Cursor. Hat es noch keinen, bringen wir einen mit, der zu euch passt.

ABLAUF

Security-Arbeit mit Agenten, in beide Richtungen

- **Was Angreifer:innen mit Agenten tun** und was das für eure Systeme bedeutet
- **Die Angriffsfläche kartieren:** Inputs, Tools, Zugangsdaten, Ausgänge
- **Das Agenten-Setup härten:** Prompt Injection platzieren, Guardrails umgehen, Lücken schließen
- **Threat Modeling mit einem Agenten:** Der Agent entwirft, das Team korrigiert
- **Schwachstellen finden und einordnen:** Agenten suchen im Code und sortieren Scanner-Befunde
- **Härten als Kreislauf:** vom Befund zum Fix mit Test und zum Security-Gate

SO BLEIBEN DIE ÜBUNGEN SICHER

- Angriffe üben wir nur auf dem Staging-System, das ihr vorher schriftlich benennt.
- Jeder Befund kommt mit Reproduktion oder fehlschlagendem Test, euer Team kann ihn sofort prüfen.

GUT ZU WISSEN

TAGESZEITEN
Meist 9 bis 17 Uhr, nach Absprache

VORLAUF
Etwa vier Wochen, meist bestimmt euer Kalender den Termin

MEHRERE TEAMS
Erst ein Pilotteam, dann Team für Team in Wellen zu 8 bis 12

ABSAGE UND VERSCHIEBUNG
Bis 4 Wochen vorher kostenfrei, dann 50 %, unter 2 Wochen 100 %. Verschieben binnen 8 Wochen kostenfrei.

EUER CODE
Bleibt bei euch: Trainer:innen bekommen, klonen und speichern ihn nie.

LIZENZEN
Stellt ihr, oder wir bringen sie mit und ihr zahlt sie.

COMMUNITY
Dauerhaft kostenlos für alle Teilnehmenden

FÖRDERUNG
Über das Qualifizierungschancengesetz möglich, wir prüfen das mit euch

> „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

ÜBER HACKERS&WIZARDS Praktiker mit über 20 Jahren Erfahrung im Aufbau und Betrieb von Produktionssystemen (OTTO, Breuninger, BLUME 2000). Gegründet in Hamburg von Benedikt Stemmildt und Stefan Munz.

AUSGEWÄHLTE KUNDENTEAMS

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

Diese Schulung für euer Team?
Erzählt uns von eurem Team, und wir schicken euch ein Angebot.

summon@hackersandwizards.dev
Gespräch buchen: haw.dev/call