OpenClaw Masterclass

Autonome KI-Agenten aufsetzen, absichern und produktiv einsetzen

Artikelnummer: ITSM-10156

Seminarinhalt: OpenClaw ist der aktuell am schnellsten wachsende Open-Source-KI-Agent weltweit. Im Gegensatz zu klassischen Chatbots handelt OpenClaw autonom: Es verarbeitet E-Mails, steuert Kalender, automatisiert Browser und führt komplexe Workflows eigenständig aus. Dieses Intensivseminar vermittelt praxisnah, wie OpenClaw im Unternehmenseinsatz sicher installiert, konfiguriert, gehärtet und produktiv betrieben wird. Dabei werden sowohl die technischen Grundlagen als auch die erheblichen Sicherheitsrisiken (Prompt Injection, Skill-Malware, Credential-Exfiltration) behandelt und in Hands-on-Übungen auf der eigenen Maschine direkt umgesetzt.

Seminardauer: 3 Tag(e)

Seminarpreis: Online Seminar: 1970,00 € / Vor-Ort Seminar: 2240,00 €

Alle Preise netto zzgl. MwSt. inkl. Arbeitsmaterial, Teilnahmebestätigung, Mittagessen und Getränke (Mittagessen und Getränke bei Online-Seminaren ausgenommen)

Seminarort(e):

Online-Veranstaltungen finden in einem virtuellen Seminarraum per Microsoft Teams-Konferenz statt. Alle unsere Standorte für Präsenzveranstaltungen sind zentral gelegen. Die endgültige Adresse erhalten Sie mit Ihrer offiziellen Einladung - vier Wochen vor dem Beginn der Veranstaltung.

AGENDA:

TAG 1 - GRUNDLAGEN & SICHERHEIT

EINFÜHRUNG IN OPENCLAW UND AGENTIC AI

- Was ist ein automomer KI-Agent und was unterscheidet OpenClaw von Chatbots und Copiloten?
- Geschichte und Ökosystem: Von Clawdbot über Moltbot zu OpenClaw (Peter Steinberger, MIT-Lizenz, 145.000+ GitHub-Stars)
- Architektur im Überblick: Gateway, Sessions, Channels, Skills, ClawHub
- Unterstützte LLM-Provider. Anthropic Claude, OpenAI GPT, DeepSeek - Auswahl und Kriterien
- Abgrenzung zu SaaS-Lösungen (ChatGPT Enterprise, Microsoft CoPilot) - Vorteile und Risiken des Self-Hostings

SICHERHEITSRISIKEN VERSTEHEN UND BEHERRSCHEN

- Warum Cisco, Microsoft Defender und die OpenClaw-Community selbst warnen
- Die zwei Angriffsoberfächen: Untrusted Code (Skills/ Extensions) und Untrusted Instructions (externe Inhalte/ Prompt Injection)
- Konkrete Angriffsszenarien: Skill-Malware aus ClawHub, Indirect Prompt Injection über Moltbook/ Deeds, Credential-Exfiltration, State-/ Memory-Manipulation
- DM-Pairing, Sandbox-Modi, Tools-Policies und Isolation (Docker, dedizierte VM)
- DSGVO-Relevanz: Welche Daten fließen wohin und wird das kontrolliert?

TAG 2 - INSTALLATION, KONFIGURATION & ANBINDUNG

OPENCLAW AUF DEM EIGENEN SERVER AUFSETZEN (HANDS-ON)

- Systemvoraussetzungen: Node 22, Docker, ESL2 (Windows)
- Installation und Onboarding-Wizard (openclaw onboard --install-daemon)
- Gateway-Konfiguration: Bind, Port, Auth-Mode, Tailscale Serve/ Funnel
- LLM Provider abindinden: API-Keys, OAuth, Model-Failover-Konfiguration
- Erster Funktionstest und Diagnostik mit openclaw doctor

CHANNELS VERBINDEN UND ABSICHERN

- Channel-Anbindung live: Telegram, Slack, Discord, Microsoft Teams oder WebChat
- DM-Policies konfigurieren: Pairing vs. Open und warum die Standardeinstellung entscheidend ist
- Allowlists, Gruppen-Routing und Aktivierungsmodi
- Remote-Zugang sicher einrichten: Tailscale, SSH-Tunnel, Token-/ Passwort-Auth

TAG 3 - WORKFLOWS, AUTOMATION & DAUERBERTRIEB

PRODUKTIVE WORKFLOWS UND AUTOMATION BAUEN (HANDS-ON)

- Skills aus ClawHub evaluieren, installieren und absichern - worauf man achten muss
- Cron-Jobs und Webhooks einrichten für zeit- und eventgesteuerte Automatisierung
- Browser-Automation: Dedicated Chrome/ Chromium mit CDP-Steuerung
- Multi-Agent-Routing: Sessions isolieren udn Agent-to-Agent-Kommunikation (sessions_send) nutzen
- Praxisbeispiel: Einen vollständigen Workflow von der E-Mail-Triage bis zur automatisierten Antwort live aufbauen

BETRIEB, MONITORING & HARDENING FÜR DEN DAUEREINSATZ

- Update-Strategie: Stable, Beta, Dev - Channels und Versionierung
- State-Backups (.openclaw/workspace/) und Credential-Management
- Regelmäßige Rebuilds als Sicherheitskontrolle - warum und wie
- Logging, Anomalie-Erkennung und Notfall-Playbook
- Sandbox-Konfiguration für Gruppen-/ Channel-Sessions im Teameinsatz
- Vom Einzelplatz-Setup zur teamfähigen Infrastruktur: Skalierung und Rollenkonzept

EXKURS: MODELL- & PROVIDER-STRATEGIE

- Welches LLM für welchen Use-Case) (Code, Text, Analyse, Agenten-Steuerung)
- Prompt-Injection-Resistenz: Warum Steinberger selbst Claude Opus empfiehlt
- Lokale Modelle vs. API-Provider: Kosten-Nutzen-Abwägung für den Unternehmenseinsatz

ABSCHLUSS & AUSBLICK

- Zusammenfassung der wichtigsten Learnings und Sicherheitscheckliste
- Ressourcen: Offizielle Docs, Community (Discord), DeepWiKi, ClawCon-Talks
- Offene Fragenrunde und individuelle Setup-Beratung

Inhouse-/ Firmen-Seminar:

Individuell für Ihre Bedürfnisse bieten wir dieses Seminar auch als Inhouse-Seminar bzw. Einzelcoaching für Ihr Unternehmen an. Sie bestimmen die Inhalte, den Zeitpunkt und die Dauer des Seminars. Wir freuen uns auf Ihre Anfrage!

Service-Hotline:

Telefonische Unterstützung und Beratung unter:
0251 / 9811566428
Montag bis Freitag | 08:00 – 20:00 Uhr

E-Mail: **seminar@itsm-cologne.de**