AI-AGENT

Agentic Systems Engineering

Ein Agent, der handeln darf, bevor er Gates bestanden hat, ist keine Automatisierung, sondern ein Betriebsrisiko mit API-Zugriff.

DAUER	GRUPPE	FORMAT
4 Tage	bis 12 Personen	Inhouse · Offen · Im Lab · Deutsch oder Englisch

DAS EXISTIERT DANACH

- Ein lauffähiger agentischer Workflow auf der Lab-Umgebung: Planung, Tool-Aufrufe, Ergebnisprüfung, gebaut vom eigenen Team
- Ein explizites Zustandsmodell mit definierten Übergängen statt impliziter Schleifen, inklusive persistierbarem Zustand für Wiederaufnahme
- Implementierte Human-in-the-Loop-Gates: welche Aktionen der Agent vorschlagen darf und welche erst nach Freigabe ausgeführt werden
- Abbruch- und Eskalationslogik mit Budgetgrenzen für Schritte, Kosten und Zeit sowie definierten Eskalationsempfängern
- Ein Evaluations- und Abnahmeprotokoll, das dokumentiert, unter welchen Bedingungen der Agent Verantwortung übernehmen darf und unter welchen nicht

AGENDA

Tag 1	Autopsie eines Agenten-Fehlschlags · Anatomie eines belastbaren Agenten · Tools entwerfen, die ein Modell sicher bedienen kann · Der erste Durchstich · Tagesergebnis: laufender Agent mit Befundliste
Tag 2	Zustand explizit machen · Das Zustandsmodell implementieren · Kontext- und Speicherstrategie · Fehlerpfade zuerst · Tagesergebnis: kontrollierter Umgang mit Störungen
Tag 3	Verantwortung erst nach Gates · Human-in-the-Loop implementieren · Abbruch- und Eskalationslogik · Sicherheit an der Tool-Grenze · Tagesergebnis: Gates unter Beschuss
Tag 4	Agenten evaluieren: Trajektorien statt Antworten · Der Evaluationslauf · Das Abnahmeprotokoll · Übertrag auf den eigenen Prozess · Tagesergebnis: Abnahme im Härtetest

IHR TRAINER

Dino Bordonaro

8x Microsoft MVP in Folge (Microsoft Azure · Cloud and Datacenter Management), Microsoft Certified Trainer, fast 30 Jahre IT. Baut souveräne KI-Systeme auf eigener Hardware (Azure Local, Foundry Local, NVIDIA-GPUs) und schult genau darauf. Über 800 Professionals ausgebildet, jedes Konzept im eigenen Enterprise-Lab im TÜV-geprüften Rechenzentrum erprobt.

31.600 € pauschal, zzgl. MwSt.

Der Track baut einen Übungsagenten und befähigt Ihr Team zum eigenen Design. Er verbindet keine Produktionssysteme und ersetzt weder Threat Modeling (AI-SEC) noch ein Implementierungsprojekt, dafür sprechen wir über Sovereign Agents.

AI-AGENT