AI-AGENT

Agentic Systems Engineering

An agent allowed to act before passing its gates is not automation, it is an operational risk with API access.

DURATION	GROUP	FORMAT
4 days	**up to 12 people**	In-house · Open · In the lab · German or English

THIS EXISTS AFTERWARDS

- A running agentic workflow on the lab environment: planning, tool calls, result verification, built by your own team
- An explicit state model with defined transitions instead of implicit loops, including persistable state for resumption
- Implemented human-in-the-loop gates: which actions the agent may propose and which execute only after approval
- Abort and escalation logic with budget limits for steps, cost and time, and defined escalation recipients
- An evaluation and sign-off protocol documenting under which conditions the agent may take responsibility and under which it may not

AGENDA

Day 1	Autopsy of an agent failure · Anatomy of a dependable agent · Designing tools a model can operate safely · The first end-to-end run · Day result: running agent with a findings list
Day 2	Making state explicit · Implementing the state model · Context and memory strategy · Failure paths first · Day result: controlled handling of faults
Day 3	Responsibility only after gates · Implementing human-in-the-loop · Abort and escalation logic · Security at the tool boundary · Day result: gates under fire
Day 4	Evaluating agents: trajectories instead of answers · The evaluation run · The sign-off protocol · Transfer to your own process · Day result: sign-off in the stress test

YOUR TRAINER

Dino Bordonaro

Microsoft MVP for eight consecutive years (Microsoft Azure · Cloud and Datacenter Management), Microsoft Certified Trainer, almost 30 years in IT. Builds sovereign AI systems on own hardware (Azure Local, Foundry Local, NVIDIA GPUs) and trains on exactly that. More than 800 professionals trained, every concept proven in his own enterprise lab in a TÜV-audited datacenter.

€31,600 flat, plus VAT

This track builds a training agent and enables your team to design its own. It connects no production systems and replaces neither threat modeling (AI-SEC) nor an implementation project, for those we talk about Sovereign Agents.

AI-AGENT