AI-AGENT

# Agentic Systems Engineering

**Un agente autorizzato ad agire prima di aver superato i gate non è automazione, è un rischio operativo con accesso alle API.**

| DURATA | GRUPPO | FORMATO |
|---|---|---|
| **4 giorni** | **fino a 12 persone** | In-house · Aperto · Nel lab · Tedesco o inglese |

## QUESTO ESISTE DOPO

- Un workflow agentico funzionante sull'ambiente Lab: pianificazione, chiamate ai tool, verifica dei risultati, costruito dal proprio team
- Un modello a stati esplicito con transizioni definite invece di loop impliciti, incluso stato persistibile per la ripresa
- Gate human-in-the-loop implementati: quali azioni l'agente può proporre e quali vengono eseguite solo dopo approvazione
- Logica di interruzione ed escalation con limiti di budget per passi, costi e tempo e destinatari di escalation definiti
- Un protocollo di evaluation e collaudo che documenta a quali condizioni l'agente può assumersi responsabilità e a quali no

## AGENDA

| | |
|---|---|
| **Giorno 1** | Autopsia di un fallimento di agente · Anatomia di un agente affidabile · Progettare tool che un modello può usare in sicurezza · Il primo passaggio completo · Risultato della giornata: agente funzionante con lista dei rilievi |
| **Giorno 2** | Rendere esplicito lo stato · Implementare il modello a stati · Strategia di contesto e memoria · Prima i percorsi di errore · Risultato della giornata: gestione controllata dei disturbi |
| **Giorno 3** | Responsabilità solo dopo i gate · Implementare lo human-in-the-loop · Logica di interruzione ed escalation · Sicurezza al confine dei tool · Risultato della giornata: gate sotto attacco |
| **Giorno 4** | Valutare gli agenti: traiettorie invece di risposte · Il run di valutazione · Il protocollo di collaudo · Trasferimento sul proprio processo · Risultato della giornata: collaudo nello stress test |

IL SUO TRAINER

### Dino Bordonaro

Microsoft MVP per otto anni consecutivi (Microsoft Azure · Cloud and Datacenter Management), Microsoft Certified Trainer, quasi 30 anni di IT. Costruisce sistemi AI sovrani su hardware proprio (Azure Local, Foundry Local, GPU NVIDIA) e forma esattamente su questo. Oltre 800 professionisti formati, ogni concetto collaudato nel proprio enterprise lab in un datacenter certificato TÜV.

## 31.600 € forfettario, IVA esclusa

Il track costruisce un agente di esercitazione e mette il Suo team in condizione di progettare in proprio. Non collega sistemi di produzione e non sostituisce né il threat modeling (AI-SEC) né un progetto di implementazione, per questo parliamo di Sovereign Agents.

AI-AGENT