



CORSO AVANZATO {AI}

Building Production AI Agents

Scrivere codice con l'aiuto dell'AI è ormai pratica quotidiana. Il passo successivo, e molto più impegnativo, è costruire prodotti che siano essi stessi agentici: sistemi che ragionano, usano strumenti, mantengono memoria, orchestrano altri agenti e operano in autonomia controllata dentro un ambiente di produzione.

Questo corso intensivo porta sviluppatori esperti dal prototipo al prodotto. Costruiremo insieme agenti reali, partendo dall'anatomia del loop agentico fino all'orchestrazione multi-agente, passando per MCP server custom, RAG robusto, guardrail e gestione dei costi.

Il mondo si è mosso: l'orchestrazione multi-agente non è più un esperimento ma la direzione mainstream, e protocolli come MCP sono diventati lo standard de facto per connettere agenti, strumenti e dati.

Livello

Avanzato

Durata

Corso da 24 ore

Lingua

Italiano

A chi si rivolge

Sviluppatori backend e full-stack con esperienza consolidata e team tecnici che vogliono passare dai prototipi ai prodotti AI in produzione.

Cosa faremo

Costruiremo agenti reali con un approccio hands-on: sessioni teoriche, live coding e pair-programming. Ogni partecipante realizzerà progressivamente un agente in produzione, dal design dell'architettura fino al deploy con guardrail, osservabilità e controllo dei costi.

Lavoreremo con SDK e framework di orchestrazione di riferimento (es. LangGraph, gli agent SDK dei principali provider e simili), confermati a ridosso di ogni edizione.

Takeaway:

- Progettare l'architettura di un agente AI a partire dai requisiti
- Implementare il loop agentico (plan → act → observe) con tool use affidabile
- Costruire MCP server custom per esporre dati e strumenti agli agenti
- Realizzare pipeline RAG robuste ed evitarne gli anti-pattern
- Orchestrare sistemi multi-agente (planner, worker, reviewer)
- Mettere in produzione con guardrail, human-in-the-loop e cost control

Numero massimo di partecipanti: 20

Skill minime necessarie

- Esperienza consolidata con almeno un linguaggio (JavaScript/TypeScript o Python consigliati)
- Familiarità con API REST, Git e workflow di versionamento
- Esperienza, anche minima, con LLM API o tool di AI-assisted coding
- Attitudine alla progettazione software e al pensiero architetturale

Argomenti Trattati

- Modulo 1 — Anatomia di un agente AI
 - Assistant vs agente: cosa cambia davvero
 - Il loop agentico: plan → act → observe → iterate
 - Tool use e function calling: progettazione e affidabilità
 - Scegliere il modello giusto per il compito (e perché conta)
- Modulo 2 — Strumenti, contesto e memoria
 - Model Context Protocol (MCP): perché è lo standard de facto
 - Costruire MCP server custom: database, API, filesystem
 - Context engineering: fornire all'agente il contesto giusto al momento giusto
 - Memoria a breve e lungo termine: pattern e trade-off
- Modulo 3 — RAG fatto bene
 - Quando serve RAG e quando no
 - Ingestion, chunking e strategie di indicizzazione
 - Retrieval ibrido (semantico + keyword) e re-ranking
 - Valutare la qualità del retrieval e anti-pattern comuni
- Modulo 4 — Orchestrazione multi-agente
 - Da singolo agente a team di agenti coordinati
 - Pattern di orchestrazione: planner, worker, reviewer, supervisor
 - Protocolli tra agenti: A2A e Agent Client Protocol (ACP)
 - Parallelizzazione, delega dei task e capability discovery
- Modulo 5 — Affidabilità, sicurezza e guardrail
 - Human-in-the-loop e livelli di autonomia
 - Validazione e structured output: far rispettare i contratti all'agente
 - Gestione di errori, retry e fallback
 - Guardrail di sicurezza: prompt injection e accesso ai dati (cenni)
 - Controllo e ottimizzazione dei costi
- Modulo 6 — Dal design al deploy (caso reale end-to-end)
 - Progettare una codebase agent-friendly
 - Observability: tracing, logging e debugging di un agente
 - Deploy e monitoring in produzione
 - Iterazione e miglioramento continuo basato sui dati

Cosa è necessario

- Il proprio computer portatile
- Tanta buona volontà e voglia di imparare
- Connessione ad Internet
- Account gratuiti su piattaforme di terze parti (verranno indicati prima del corso)
- Una API key per un provider LLM (indicazioni fornite prima del corso)

Cosa è incluso

- Corso pratico con live coding
- Supporto setup environment
- Slide in formato PDF
- Repository del Progetto
- Attestato di Partecipazione
- Follow Up di fine corso
- Canale Slack dedicato ai partecipanti

Dove si svolge

Full-Remote

È possibile svolgere il corso in modalità *full-remote* con gli strumenti messi a disposizione da Devmy suddividendo, se lo si desidera, il tutto in sessioni da 4h.