

LEZIONE 05: BEST PRACTICES E SICUREZZA

LEZIONE 05: BEST PRACTICES E SICUREZZA

COSA SERVE E PERCHÉ

Obiettivi - Evitare i pericoli reali - Scaling e troubleshooting - Guardare al futuro post-OpenAI

Contenuti principali - Sicurezza: Docker sandbox, permission minime, spending limits, no root access -

Problemi noti: prompt injection, agenti “ribelli”

(articoli NYT/Wired feb 2026) - Casi studio: automazione business, coding 24/7, home assistant -

Futuro: fondazione open-source + supporto OpenAI, multi-agente avanzato

Risorse - SECURITY.md su GitHub - Guida Microsoft sicurezza: cerca “Running OpenAI safely Microsoft”

COME ESEGUIRE CORRETTAMENTE

[Descrizione passo passo]

ERRORI COMUNI

- []

NOTE

[Extra]