FLA ACADEMY

marika.petrillo@federlegnoarredo.it • 02 8060 4302

FLA Eventi

CYBER SECURITY & A.I.

CORSO ONLINE

DATE
20,27 maggio 2026

ORARIO
09.30-12.30

DURATA
6 ore complessive

COSTO
Associato
300€ +iva prima iscrizione
30% di sconto
dalla seconda

Non associato
360€+iva prima iscrizione
15% di sconto
dalla seconda

DESTINATARI
Tutti

ISCRIVITI QUI

OBIETTIVI

Attraverso esercitazioni hands-on, i partecipanti sperimentano tecniche di adversarial prompting e imparano a proteggere workflow e agenti AI. Il corso fornisce checklist operative e best practice per implementare sistemi AI sicuri in azienda.

ARGOMENTI

Data Security e Privacy

- Introduzione alla Cybersecurity
- Le vulnerabilità AI Specific
- Adversarial Prompting
- Sicurezza nel Deployment
- Dati e AI Governance
- Focus: AI Act e Data Act

Architettura Framework di sicurezza

- Architettura di un sistema AI
- RAG e Agenti
- Framework di sicurezza: NIST AI RMF, OWASP Top 10 for LLM
- Framework di monitoraggio / Evaluation (es. SAGE by Arkage)
- Workshop: Red Teaming

DOCENTE: **Team Arkage** Linkedin