



# DIGITALE IN PRATICA

## WORKSHOP

## Intelligenza artificiale e sicurezza: uso consapevole, vantaggi e rischi

Come integrare l'AI in modo sicuro ed efficace nel proprio contesto professionale grazie agli strumenti di Intelligenza Artificiale oggi disponibili comprendendo rischi e vulnerabilità.

## AGENDA

- / Cosa sono gli LLM e come stanno evolvendo
- / Perché la sicurezza dell'IA è una sfida unica
- / Le Vulnerabilità chiave e i rischi secondo OWASP
- / Deep Dive sul Jailbreaking: come gli attaccanti ingannano l'AI
- / I rischi dell'AI autonoma
- / Costruire le Difese: strategie pratiche per la protezione
- / Esercizio Finale: sfida di Jailbreaking!

Riservato ad un massimo di 20 partecipanti.

**ISCRIVITI SUBITO A QUESTO [LINK!](#)**



24 Settembre



SMACT, via  
Tommaseo 59 PD



9:00-13:00