

Certified Offensive AI Security Professional

CODICE	DT0324
DURATA	3 gg
PREZZO	2.100,00 €
EXAM	

DESCRIZIONE

C|OASP è una certificazione pratica a livello professionale che attesta la tua capacità di attaccare in modo etico i sistemi di IA, in modo da poterli difendere con controlli di livello ingegneristico.

C|OASP non riguarda la creazione di modelli di IA o l'esecuzione di programmi di IA. Si tratta di dimostrare che sei in grado di:

- Pensare come un aggressore all'interno dei sistemi di IA
- Scoprire i punti deboli dei modelli e delle pipeline
- Convalidare i controlli di sicurezza
- Ridurre il rischio operativo prima dell'implementazione

TARGET

COASP è progettato per i professionisti della sicurezza che desiderano padroneggiare tecniche di sicurezza AI offensive e difensive.

CONTENUTI

- Modulo 1: Offensive AI and AI System Hacking Methodology
- Modulo 2: AI Reconnaissance and Attack Surface Mapping
- Modulo 3: AI Vulnerability Scanning and Fuzzing
- Modulo 4: Prompt Injection and LLM Application Attacks
- Modulo 5: Adversarial Machine Learning and Model Privacy Attacks
- Modulo 6: Data and Training Pipeline Attacks
- Modulo 7: Agentic AI and Model-to-Model Attacks
- Modulo 8: AI Infrastructure and Supply Chain Attacks
- Modulo 9: AI Security Testing, Evaluation, and Hardening
- Modulo 10: AI Incident Response and Forensics