securitum/szkolenia

hacking_/2/2024

SEKURAK.ACADEMY

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU SEKURAK.ACADEMY 2024

HACKOWANIE VS. AI – EDYCJA 2024

2024 — semestr_02

DLA:

Rafał Szponarski

DATA: 10.07.2024 r. **TRENER:** Tomasz Turba **CZAS TRWANIA:** 3 godziny

AGENDA

- Metody ataków wykorzystujące wątek AI
- Ataki związane z metodami deepfake – pokazy na żywo
- Metody obrony związane z deepfake – pokazy na żywo
- Ataki intencjonalne na modele ChatGPT-4o, Microsoft Copilot i Google Gemini
- Zagrożenia danych służbowych w modelach LLM – wytyczne dla pracowników
- Klasyfikacja zagrożeń AI na podstawie matrycy MITRE ATLAS
- Bezpieczeństwo Agentów AI
- Demonstracja zagrożeń na podstawie listy projektu OWASP TOP 10 LLM
- Narzędzia cyberbezpieczeństwa i OSINT związane z AI
- Zagrożenia i bezpieczeństwo modeli *offline* – pokaz praktyczny
- Prawne aspekty cyberbezpieczeństwa w Polsce i Europie
- Sesja Q&A

ip_scan

5×× Server Error

4×× Client Error

PUNKTY CPE/ECE: 3

SZKOLENIA.SECURITUM.PL

securitum