SEKURAK.ACADEMY

CERTYFIKAT

UCZESTNICTWA W SZKOLENIU SEKURAK.ACADEMY 2025

HACKOWANIE VS AI (CZĘŚĆ III)

DLA:

Sebastian Ciborowski

DATA: 19.05.2025 r.	**TRENER:** Tomasz Turba	**CZAS TRWANIA:** 2 godziny

AGENDA

1. Wprowadzenie do tematyki bezpieczeństwa AI – biologia modelu
2. Metody ataków wykorzystujące wątek AI
3. Zagrożenia danych służbowych w modelach LLM – wytyczne dla pracowników i pracodawców
4. Klasyfikacja zagrożeń AI w oparciu o matrycę MITRE ATLAS
5. Modelowanie zagrożeń AI w oparciu o metodologię CRISP-ML(Q)
6. Demonstracja zagrożeń w oparciu o listę projektu OWASP TOP 10 LLM
7. Ataki nowe i nietypowe
8. Narzędzia cyberbezpieczeństwa i OSINT związane z AI
9. Zagrożenia i bezpieczeństwo modeli offline – pokaz praktyczny
10. Prawne aspekty cyberbezpieczeństwa w Polsce i Europie
11. Sesja Q&A

PUNKTY CPE/ECE: 2