SEKURAK.ACADEMY

CERTIFICATE

OF PARTICIPATION IN THE SEKURAK.ACADEMY 2025 TRAINING

HACKING VS AI (PART III)

GRANTED TO:

Marcin Basiura

DATE: 19.05.2025 | **TRAINER:** Tomasz Turba | **DURATION:** 2 hours

AGENDA

1. Introduction to AI security – the biology of a model
2. Attack methods using the AI thread
3. Threats to business data in LLM models – guidelines for employees and employers
4. AI threat classification based on the MITRE ATLAS matrix
5. AI threat modeling based on the CRISP-ML(Q) methodology
6. Threat demonstration based on the OWASP TOP 10 LLM project list
7. New and unusual attacks
8. Cybersecurity and OSINT tools related to AI
9. Threats and security of offline models – practical demonstration
10. Legal aspects of cybersecurity in Poland and Europe
11. Q&A session

CPE/ECE POINTS: 2

SZKOLENIA.SECURITUM.PL

securitum