Tvorba AI agentů s praktickým zaměřením na Microsoft AI Red Teaming Agent

Kód kurzu: WAIA

AI Red Teaming spoléhá na kreativitu a odborné znalosti vysoce kvalifikovaných specialistů na bezpečnost, kteří simulují útoky na AI systémy. Tento proces je časově i kapacitně náročný, což může představovat překážku pro organizace usilující o rychlejší adopci umělé inteligence. Díky nástroji AI Red Teaming Agent mohou nyní firmy využít hluboké know-how společnosti Microsoft a škálovat svůj vývoj AI s důrazem na důvěryhodnost a bezpečnost. Workshop bude probíhat v anglickém jazyce.

Osnova:

- Definice a typy AI agentů
- Reálné aplikace a příklady použití
- Diskuze: Role AI agentů v?moderních technologiích
- Co je AI Red Teaming a proč je důležitý
- Představení nástroje Microsoft AI Red Teaming Agent
- Klíčové funkce: automatizované skenování, útokové strategie a generování reportů
- Podporované kategorie rizik a techniky útoků
- Instalace potřebných nástrojů a závislostí
- Konfigurace prostředí Azure AI Foundry a AI Red Teaming Agent
- Spouštění skenů na vzorovém AI modelu
- Závěrečný projekt: Vytvoření AI agenta pro úlohy síťové exploatace

Vstupní požadavky:

- Základní znalost pojmů z oblasti AI a strojového učení
- Aktivní účet Microsoft Azure
- Znalost AJ

Pro koho je workshop určen?

Pro AI inženýry, odborníky na strojové učení, bezpečnostní výzkumníky a technické lídry, kteří chtějí začlenit Trustworthy AI a proaktivní testování do svého vývojového procesu.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved