Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

10 kwietnia 2025 r.
Typ 200
Wykrywanie zagrożeń z wykorzystaniem sztucznej inteligencji
Google Cloud Poland sp. z o.o.

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 10.40	**Sztuczna inteligencja w wykrywaniu cyberzagrożeń - przegląd** • Omówienie kluczowych technologii (ML, deep learning, NLP) • Aktualne trendy oraz innowacje • Wyzwania oraz ograniczenia • Przykłady zastosowań *Ekspert „Google Cloud": Krzysztof Gabrych*
10.40 – 11.45	**Zabezpieczenia LLM-ów jako produktu - wykorzystanie w pracy SOC (DEMO)** • Infekowanie LLM i obrona przeciwko atakom - demo online • Rankingi bezpieczeństwa / mowa nienawiści - demo online • Budowanie reguł SECOPS za pomocą NLP - demo online • Wykorzystanie Gemini do wyszukiwania cyberzagrożeń, sumaryzacji oraz propozycji remediacji - demo online *Ekspert „Google Cloud": Krzysztof Gabrych*
11.45 – 12.10	**Sesja pytań i odpowiedzi do ekspertów**