Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

22 grudnia 2026 r.
Typ 100
Generatywna AI i cyberbezpieczeństwo
Xopero Software S.A.

10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 10.40	**Wprowadzenie do bezpieczeństwa AI: Nowe narzędzia, nowe zagrożenia** • Jak sztuczna inteligencja wspiera naszą codzienną pracę i gdzie kryją się pułapki (omówienie przystępnym językiem). • Złudzenie kontroli – dlaczego asystenci AI potrafią być podatni na manipulację? • Problem nieświadomego udostępniania danych firmowych w publicznych i firmowych modelach. *Ekspert „Xopero Software”: Łukasz Nowatkowski*
10.40 – 11.20	**Anatomia ataku na AI (Pokaz na żywo)** • Zobrazowanie zagrożenia: Jak wymusić na AI ominięcie narzuconych reguł (Prompt Injection). • Przykłady z życia: kradzież informacji z systemów i manipulacja odpowiedziami modelu. • Dlaczego klasyczne programy antywirusowe nie potrafią wykryć i zatrzymać tego typu zagrożeń. *Ekspert „Xopero Software”: Łukasz Nowatkowski*

11.20 – 12.00	**Autonomiczna obrona w praktyce: Neutralizacja ataków** • Koncepcja niezależnej, autonomicznej warstwy ochrony dla systemów sztucznej inteligencji. • Zablokowanie ataku w czasie rzeczywistym: ponowna demonstracja, tym razem z aktywnym systemem obronnym. • Automatyzacja bezpieczeństwa – jak nowoczesne narzędzia samodzielnie rozpoznają anomalię i interweniują bez ingerencji użytkownika. *Ekspert „Xopero Software”: Łukasz Nowatkowski*
12.00 - 12.10	**Sesja pytań i odpowiedzi do ekspertów**