

Cyberbezpieczeństwo i AI w praktyce organizacji

CO ZYSKASZ?

-  Certyfikat
-  Materiały szkoleniowe
-  Sesja QA

PROGRAM SZKOLENIA

1. Cyberbezpieczeństwo w praktyce

- Cyberbezpieczeństwo jako problem ludzki, a nie techniczny
- Realne case study (mail od szefa, pilna faktura, zmiana formatu pliku za pomocą konwertera online etc.)
- Ćwiczenie „Gdzie w tej sytuacji popełniono błąd?”
- Mechanizm: presja czasu, skróty myślowe

2. AI w organizacji – 3 scenariusze w praktyce

- Użycie AI bez zgody kierownictwa
- AI jako zwalidowane narzędzie
- AI jako produkt
- Ryzyka prawne, reputacyjne, cyberbezpieczeństwa dla każdego z tych przypadków
- Granica „pomoc” vs „decyzja”
- Ćwiczenie: klasyfikacja realnych sytuacji do 3 scenariuszy

3. Błędy AI – halucynacje, odpowiedzialność, iluzja obiektywności

- Dlaczego AI się myli
- Dlaczego AI brzmi przekonująco
- Dlaczego człowiek nadal ponosi odpowiedzialność
- Ćwiczenie: analiza wygenerowanego tekstu z błędami



4. AI Impact Assessment – ocena wpływu AI – wprowadzenie warsztatowe

- Czym jest ocena wpływu (a czym nie jest)
- Kiedy jest potrzebna
- Praca w grupach: uproszczona mapa wpływu AI dla przykładowej sytuacji

PROWADZĄCY

Urszula Ciołkowska - Audytor Wiodący ISO/IEC 42001:2023 (Artificial Intelligence Management System) oraz audytor wiodący innych systemów zarządzania z wieloletnim doświadczeniem w obszarze jakości, bezpieczeństwa żywności, bezpieczeństwa informacji i zarządzania ryzykiem. Specjalizuje się w odpowiedzialnym wykorzystaniu sztucznej inteligencji w organizacjach, a zwłaszcza w ocenie wpływu sztucznej inteligencji, zgodności z wymaganiami norm międzynarodowych oraz praktycznym wdrażaniu zasad AI governance.

