Bezpieczeństwo danych w projektach sztucznej inteligencji

Kategoria	Czas trwania	Termin	Cena
AI	16h / 2 dni	ustalamy indywidualnie	ustalamy indywidualnie

Program szkolenia:

Poniżej przedstawiamy przykładowy program szkolenia, który może zostać zmodyfikowany zgodnie z oczekiwaniami oraz poziomem grupy szkoleniowej. Przed przygotowaniem docelowego programu szkolenia, przeprowadzamy rozmowę techniczną, w której bierze udział trener oraz osoba techniczna lub cały zespół developerów reprezentujący klienta, w celu ustalenia szczegółów szkolenia.

Dzień 1 Fundamenty bezpieczeństwa danych w AI

Moduł 1: Wprowadzenie do bezpieczeństwa danych w AI

- Analiza kluczowych zagrożeń bezpieczeństwa w projektach AI
- Przegląd najczęstszych wektorów ataków na systemy sztucznej inteligencji
- Omówienie ram prawnych i regulacyjnych (RODO, GDPR)

Moduł 2: Ochrona zbiorów danych

- Metody szyfrowania w procesach przechowywania i transferu danych
- Techniki anonimizacji i pseudonimizacji danych
- Techniki differential privacy
- Techniki federated learning dla zwiększenia prywatności
- Praktyczne warsztaty: Implementacja bezpiecznego preprocessingu danych

Moduł 3: Warsztat praktyczny – Analiza podatności modeli AI

- Identyfikacja luk bezpieczeństwa w modelach machine learning
- Narzędzia do automatycznej detekcji ataków
- Praktyczne próby manipulacji modelami (adversarial examples)
- Techniki obrony przed atakami na modele AI

Dzień 2: Zaawansowane techniki ochrony danych

Moduł 4: Bezpieczeństwo modeli i algorytmów

- Metody ochrony własności intelektualnej modeli AI
- Techniki zabezpieczania algorytmów przed nieuprawnionym dostępem
- Case studies: Rzeczywiste scenariusze naruszeń bezpieczeństwa
- Procedury reagowania na incydenty

Moduł 5: Prywatność i etyka w AI

- Zasady projektowania systemów z zachowaniem prywatności (Privacy by Design)
- Etyczne aspekty przetwarzania danych osobowych
- Mechanizmy kontroli zgody i dostępu do danych

Moduł 6: Warsztat końcowy – Kompleksowy projekt bezpieczeństwa

- Budowa całościowej strategii bezpieczeństwa dla projektu AI
- Symulacja scenariuszy naruszenia bezpieczeństwa
- Opracowanie planu mitygacji ryzyka

KONTAKT

Jesteś zainteresowany dedykowanym szkoleniem dla Twojej firmy?

Skontaktuj się z Przemkiem!

PRZEMYSŁAW WOŁOSZ

Key Account Manager

(+48) 730 830 801

przemyslaw.wolosz@infoShareAcademy.com