Ochrona modeli uczenia maszynowego przed atakami

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 modeli ML

Moduł 1: Wprowadzenie do zagrożeń w ekosystemie ML

- Charakterystyka współczesnych ataków na modele AI
- Konsekwencje udanych ataków
- Analiza przypadków włamań i manipulacji modelami w rzeczywistych projektach

Moduł 2: Rodzaje ataków na modele ML

- Ataki adversarial: metody generowania przeciwpróbek
- Ataki na prywatność danych treningowych
- Techniki wycieku informacji z wytrenowanych modeli
- Analiza podatności różnych architektur ML na manipulacje
- Ataki na infrastrukturę ML

Moduł 3: Warsztat – Identyfikacja zagrożeń

- Symulacja ataków na przykładowe modele klasyfikacyjne i regresyjne
- Analiza śladów oraz mechanizmów penetracji modeli

Dzień 2: Zaawansowane techniki ochrony

Moduł 4: Metody zabezpieczeń modeli ML

- Techniki adversarial training
- Techniki federated learning dla zwiększenia prywatności
- Implementacja mechanizmów obfuskacji i prywatności danych
- Strategie redukcji ryzyka w procesach machine learning

Moduł 5: Warsztat – Praktyczna ochrona modeli

- Budowa odpornych architektur ML
- Implementacja zaawansowanych technik obronnych
- Testowanie modeli pod kątem bezpieczeństwa
- Tworzenie polityk bezpieczeństwa dla zespołów ML

Moduł 6: Narzędzia i frameworki bezpieczeństwa

- Przegląd narzędzi open-source do ochrony modeli
- Analiza bibliotek specjalizowanych w cyberbezpieczeństwie ML
- Automatyzacja procesów weryfikacji bezpieczeństwa
- Integracja narzędzi bezpieczeństwa z pipeline'ami ML

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