AI w cyberbezpieczeństwie (kod: AI-IN-CYBERSEC)

Opis i cel szkolenia

Praktyczne, dwudniowe warsztaty na temat wykorzystania technik i narzędzi sztucznej inteligencji w cyberbezpieczeństwie.

Zajmiemy się automatyzacją detekcji zagrożeń i wzmacnianiem systemów obronnych (analiza od strony defensywnej – rola „Blue Team"), jak również testowaniem ich odporności na ataki z wykorzystaniem modeli generatywnych (perspektywa „Red & Purple Team"). Będziemy pracować na scenariuszach odpowiadających realnym sytuacjom w organizacjach.

Szkolenie prezentuje metody defensywnego wykorzystania AI, inteligentną automatyzację z użyciem systemów klasy SIEM/SOAR, a także warsztat z zakresu łamania zabezpieczeń modeli językowych (LLM). Kurs przeznaczony jest dla szerokiego grona specjalistów IT i managerów, którzy chcą zrozumieć zarówno potencjał, jak i ograniczenia oraz ryzyka prawne (EU AI Act) związane ze sztuczną inteligencją w bezpieczeństwie. Oprócz teorii zapewniamy interaktywne ćwiczenia w dedykowanych środowiskach testowych.

Czego się nauczysz? Po ukończeniu szkolenia będziesz potrafił/a: Rozumieć architekturę, taksonomię zagrożeń oraz krajobraz AI w cyberbezpieczeństwie w oparciu o uznane standardy (np. NIST). Wykorzystywać uczenie maszynowe w pracy analityka SOC do detekcji anomalii w ruchu sieciowym i logach systemowych. Wdrażać i konfigurować lokalne modele AI na potrzeby bezpieczeństwa organizacji. Automatyzować procesy reagowania na incydenty w nowoczesnych platformach SIEM i SOAR (np. Microsoft Sentinel). Identyfikować zagrożenia oraz techniki stosowane przez napastników (zaawansowany phishing oparty na LLM, deepfake audio/wideo, automatyzacja ataków przez AutoGPT). Przeprowadzać symulacje ataków na modele językowe (LLM) – w tym praktyczne testy technik typu Prompt Injection w celu ominięcia filtrów bezpieczeństwa. Budować skuteczną strategię wdrożenia AI w dziale bezpieczeństwa (od etapu PoC do produkcji), uwzględniając aspekty etyczne, prywatność danych oraz wymogi unijnego aktu o sztucznej inteligencji (EU AI Act).

Czas trwania

2 dni

Program

Dzień 1: Fundamenty i defensywne zastosowania AI (perspektywa Blue Team)

1. **Moduł 1: Krajobraz AI w cyberbezpieczeństwie - taksonomia, ryzyka i możliwości**
   - — Wprowadzenie do kluczowych koncepcji uczenia maszynowego (nadzorowane, nienadzorowane, ze wzmocnieniem) w kontekście cyberbezpieczeństwa.
   - — Taksonomia zagrożeń i zastosowań AI w oparciu o uznane frameworki (np. NIST).
   - — Dwojaka natura AI: jako "wzmacniacz siły" dla obrońców i "ułatwiacz/wyrównywacz umiejętności" dla atakujących.
   - — Analiza realnych studiów przypadków wykorzystania AI do wykrywania ataków na dużą skalę.
2. **Moduł 2: Uczenie maszynowe w służbie analityka - od detekcji anomalii po threat intelligence**

Zapytaj o szczegóły

tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy

2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)

- Przegląd kluczowych defensywnych zastosowań modeli ML w pracy analityka.
- Wykrywanie anomalii w ruchu sieciowym i logach systemowych (clustering, autoenkodery).
- Implementacja lokalnych modeli AI.
- Wykorzystanie AI do predykcji zagrożeń, oceny ryzyka i priorytetyzacji alertów w SOC.

3. **Moduł 3: Inteligentna automatyzacja reagowania - AI w platformach SIEM i SOAR**
   - Rola AI w nowoczesnych platformach SIEM (np. Microsoft Sentinel) i jej zastosowanie w automatyzacji reagowania (SOAR).
   - Analiza przykładów playbooków SOAR, w których decyzje są wspierane przez modele ML.

Dzień 2: Ofensywne AI. Ochrona systemów uczących się (perspektywa Red & Purple Team)

1. **Moduł 4: AI w arsenale atakującego - generowanie phishingu, malware, techniki omijania zabezpieczeń**
   - Wykorzystanie dużych modeli językowych (LLM) do generowania wysoce wiarygodnych, kontekstowych wiadomości phishingowych.
   - Wykorzystanie AI do generowania deepfake'ów (audio i wideo) w atakach socjotechnicznych.
   - Automatyzacja rekonesansu i planowania ataków przy użyciu narzędzi takich jak AutoGPT.
2. **Moduł 5: Ataki na modele AI/LLM. Warsztat praktyczny/symulacja**
   - Interaktywne ćwiczenia polegające na "łamaniu" zabezpieczeń modelu LLM w dedykowanym środowisku.
   - Praktyczne ataki typu Prompt Injection w celu ominięcia filtrów bezpieczeństwa.
3. **Moduł 6: Aspekty etyczne, regulacyjne i strategiczne. Wdrażanie AI w organizacji**
   - Omówienie kluczowych założeń unijnego aktu o sztucznej inteligencji (EU AI Act) i jego wpływu na cyberbezpieczeństwo.
   - Dylematy etyczne: stronniczość (bias) algorytmów i ochrona prywatności.
   - Jak zbudować strategię wdrożenia AI w dziale bezpieczeństwa - od etapu PoC do pełnej produkcji.
   - Sesja pytań i odpowiedzi, podsumowanie szkolenia.

Przeznaczenie i wymagania

Dla kogo:

- Analitycy Bezpieczeństwa (SOC, Threat Intelligence) chcący zautomatyzować analizę i priorytetyzację zagrożeń.
- Inżynierowie Bezpieczeństwa i Architekci pragnący integrować rozwiązania AI z istniejącą infrastrukturą (SIEM, SOAR).
- Pentesterzy i członkowie Red Teamów, którzy chcą poszerzyć swój arsenał o techniki ofensywnego wykorzystania AI.
- Menedżerowie IT i Security, którzy potrzebują głębszego technicznego zrozumienia możliwości i ryzyk związanych z AI, aby podejmować świadome decyzje strategiczne.
- oraz dla Specjalistów IT i specjalistów ds. bezpieczeństwa.

Co musisz wiedzieć przed:

- Podstawowa znajomość zagadnień z zakresu cyberbezpieczeństwa (terminologia, podstawowe typy ataków).
- Ogólna wiedza informatyczna z zakresu systemów operacyjnych i sieci

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Najbliższe terminy
2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Cena szkolenia

2490 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Najbliższe terminy
2026-12-21 (Zdalnie)
2026-12-21 (Warszawa)