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

Opis i cel szkolenia

Praktyczne, dwudniowe warsztaty na temat wykorzystania technik i narzędzi AI w cybersecurity.

Zajmiemy się automatyzacją detekcji zagrożeń i wzmacnianiem systemów obronnych (analiza od strony defensywnej - rola "Blue Team"), jak również testowaniem ich odporności na ataki, m.in. wykorzystując modele generatywne - od strony ofensywnej ("Red Team") .

Będziemy pracować na scenariuszach odpowiadających realnym sytuacjom. Skupimy się na narzędziach open source.

Warsztaty obejmują również techniki zabezpieczania samych modeli uczenia maszynowego przed manipulacją, analizę kodu i danych wejściowych do modeli. A także, wykorzystanie AI w procesach threat intelligence i incident response.

Jako, że zajęcia prezentują zarówno metody defensywnego wykorzystania AI (Blue Team), jak testowania bezpieczeństwa systemów z jej użyciem (Red Team) - szkolenie przeznaczone jest dla szerokiego grona specjalistów IT. Zapraszamy wszystkich, którzy chcieliby rozumieć zarówno potencjał, jak i ograniczenia sztucznej inteligencji w cyberbezpieczeństwie.

Oprócz prezentacji i podstaw teorii, zapewniamy pracę w środowiskach testowych, konkretne ćwiczenia i propozycje gotowych do wdrożenia rozwiązań.

Czego się nauczysz? Po ukończeniu szkolenia będziesz potrafił/a: Budować i trenować modele uczenia maszynowego w Pythonie do identyfikacji anomalii sieciowych, czy złośliwego oprogramowania. Wykorzystywać narzędzia open-source (Scikit-learn, TensorFlow, Pandas) do analizy danych bezpieczeństwa. Rozumieć i symulować ataki na modele językowe (LLM), takie jak Prompt Injection i Data Leakage. Stosować ramy postępowania (frameworki) takie jak NIST AI RMF i OWASP Top 10 for LLM do zabezpieczania systemów AI. Automatyzować procesy reagowania na incydenty z wykorzystaniem AI w systemach SIEM/SOAR. Identyfikować i przeciwdziałać zagrożeniom związanym z deepfake, generatywnym malware i zaawansowanym phishingiem.

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.

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

Najbliższe terminy
2026-06-18 (Zdalnie)
2026-06-18 (Warszawa)
2026-09-24 (Zdalnie)
2026-09-24 (Warszawa)

2. **Moduł 2: Uczenie maszynowe w służbie analityka - od detekcji anomalii po threat intelligence**
   — Przegląd kluczowych defensywnych zastosowań modeli ML w pracy analityka.
   — Wykrywanie anomalii w ruchu sieciowym i logach systemowych (clustering, autoenkodery).
   — Klasyfikacja złośliwego oprogramowania i analiza sentymentu w danych OSINT.
   — Wykorzystanie AI do predykcji zagrożeń, oceny ryzyka i priorytetyzacji alertów w SOC.
3. **Moduł 3: Warsztat praktyczny - budowa modelu do identyfikacji złośliwego ruchu sieciowego**
   — Praktyczne ćwiczenia w przygotowanym środowisku (Python, Jupyter Notebook, Pandas, Scikit-learn).
   — Wczytywanie, przygotowanie i analiza danych z publicznie dostępnych zbiorów (np. NSL-KDD, CICIDS2017).
   — Inżynieria cech (feature engineering) w danych dotyczących bezpieczeństwa.
   — Trening i ewaluacja modeli klasyfikacyjnych (np. Las Losowy, Regresja Logistyczna) pod kątem skuteczności.
4. **Moduł 4: Inteligentna automatyzacja reagowania - AI w platformach SIEM i SOAR**
   — Integracja wytrenowanych modeli ML z ekosystemem narzędzi SOC.
   — 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.
   — Przegląd narzędzi komercyjnych i open-source (np. Snyk, CAI Framework).

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

1. **Moduł 5: AI w arsenale atakującego - generowanie phishingu, malware i techniki omijania zabezpieczeń**
   — Wykorzystanie dużych modeli językowych (LLM) do generowania wysoce wiarygodnych, kontekstowych wiadomości phishingowych.
   — Tworzenie polimorficznego malware i 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 6: Ataki na modele AI/LLM. Warsztat praktyczny/symulacja.**
   — Interaktywne ćwiczenia polegające na "łamaniu" zabezpieczeń modelu LLM w dedykowanym środowisku.
   — Wykorzystanie otwartych frameworków do testowania bezpieczeństwa AI (np. TextAttack, Counterfit).
   — Praktyczne ataki typu Prompt Injection w celu ominięcia filtrów bezpieczeństwa.
   — Ataki typu Data Leakage w celu odtworzenia wrażliwych danych treningowych.
   — Analiza podatności w oparciu o ramy OWASP Top 10 for LLM.
3. **Moduł 7: Zabezpieczanie ekosystemów AI - wprowadzenie do adversarial machine learning**
   — Taksonomia ataków na modele ML: Evasion, Poisoning, Model Inversion i Model Stealing.
   — Defensywne techniki ochrony systemów AI: Adversarial Training, walidacja danych wejściowych i wzmacnianie modelu.

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

Najbliższe terminy
2026-06-18 (Zdalnie)
2026-06-18 (Warszawa)
2026-09-24 (Zdalnie)
2026-09-24 (Warszawa)

- — Praktyczne wykorzystanie frameworków do testowania odporności modeli (np. Adversarial Robustness Toolbox od IBM).
- — Osadzenie technik obronnych w kontekście ram zarządzania ryzykiem (np. NIST AI Risk Management Framework).

4. **Moduł 8: 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.

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

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
- — Podstawowa umiejętność czytania skryptów w dowolnym języku (doświadczenie z Pythonem będzie dodatkowym atutem, ale nie jest bezwzględnie wymagane).

Najbliższe terminy
2026-06-18 (Zdalnie)
2026-06-18 (Warszawa)
2026-09-24 (Zdalnie)
2026-09-24 (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)

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.

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

Najbliższe terminy
2026-06-18 (Zdalnie)
2026-06-18 (Warszawa)
2026-09-24 (Zdalnie)
2026-09-24 (Warszawa)