

CompTIA AI Essentials - szkolenie autoryzowane

Szkolenie CompTIA AI Essentials to autoryzowany kurs wprowadzający do świata sztucznej inteligencji – przeznaczony dla osób rozpoczynających karierę w IT lub chcących zrozumieć fundamenty AI bez konieczności posiadania zaawansowanej wiedzy technicznej. Uczestnicy poznają działanie nowoczesnych narzędzi AI, ich praktyczne zastosowania w różnych branżach oraz zagadnienia związane z etyką, bezpieczeństwem i zgodnością z obowiązującymi regulacjami (AI Act, NIS2).

Kurs stanowi kompleksowe wprowadzenie do generatywnej sztucznej inteligencji, inżynierii promptów oraz cyberbezpieczeństwa w kontekście AI. Certyfikat CompTIA stanowi rozpoznawalny dowód kompetencji i solidny fundament do dalszego rozwoju w obszarze nowych technologii.

Dyrektywa NIS2

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Sprawdź swoją wiedzę z zakresu:

- **CompTIA CySA+**
- **CompTIA Security+**
- **CompTIA Network+**
- **OSINT - Biały Wywiad, czyli jak dotrzeć do cennych informacji**
- **CEH - Certified Ethical Hacker**

- [ECIH - Certified Incident Handler](#)
- [Testy penetracyjne \(PenTest+/CPENT\)](#)



Odbiorcy szkolenia

Szkolenie skierowane jest do osób, które chcą rozpocząć przygodę z AI, zdobyć praktyczne podstawy tej technologii i lepiej rozumieć jej wpływ na pracę, biznes i społeczeństwo. W szczególności zapraszamy:

- Początkujących specjalistów IT – osoby wchodzące do branży, które chcą zdobyć pierwszy certyfikat związany z AI.
- Uczestników szkoleń CompTIA – osoby, które wcześniej uczestniczyły w kursach takich jak Security+, Network+, CySA+, i chcą poszerzyć kompetencje o tematykę AI.
- Pracowników firm objętych regulacjami NIS2 lub AI Act – osoby, które muszą rozumieć wpływ AI na bezpieczeństwo, zgodność i procesy w firmie.
- Osoby pracujące w marketingu, HR, analizie danych, edukacji i sprzedaży – zainteresowane wykorzystaniem AI w codziennej pracy.
- Każdego, kto chce świadomie korzystać z generatywnej AI – z poszanowaniem zasad etyki, zgodności i bezpieczeństwa informacji.



Korzyści

- **Praktyczna wiedza o AI** – uczestnicy zdobywają konkretne umiejętności przydatne w pracy z technologiami sztucznej inteligencji.
- **Odpowiedzialne korzystanie z AI** – nauczysz się etycznych i prawnych aspektów generatywnej AI, w tym kwestii prywatności, własności intelektualnej i zgody użytkownika.
- **Bezpieczne wykorzystanie AI w środowisku pracy** – poznasz zagrożenia wynikające z użycia AI oraz dowiesz się, jak AI może wspierać bezpieczeństwo systemów i danych.
- Przygotowanie do dalszego rozwoju zawodowego z zakresu AI, cyberbezpieczeństwa i technologii IT.



Program szkolenia

1 – Oblicze sztucznej inteligencji

- Czym jest AI i jak się rozwijała?
- AI w codziennym życiu i w biznesie
- Różnice między inteligencją ludzką, obliczeniową i sztuczną

- AI wspomagająca człowieka vs. AI zastępująca człowieka
- Pierwsze kroki z AI: mindset, projekt, zarządzanie wdrożeniem
- Wpływ AI na zespoły, kariery i społeczeństwo
- Jak rozmawiać o AI z kolegami z pracy?

2 – Granice generatywnej AI

- Rodzaje generatywnej AI: tekst, obraz, audio, kod
- Przykłady zastosowania: automatyzacja, marketing, edukacja, analiza danych
- Jak odróżnić treści generowane przez człowieka i przez AI?
- Dobór odpowiedniego narzędzia AI do konkretnego zadania
- Narzędzia: ChatGPT, Gemini, DALL·E, Synthesia, ElevenLabs
- Generatywna AI w tłumaczeniach i matematyce

3 – Projektowanie skutecznych promptów

- Czym jest prompt engineering i dlaczego ma znaczenie?
- Rodzaje promptów: instrukcja, pytanie, rola (persona), format, styl
- Praktyka pisania promptów do tekstu, obrazu, dźwięku
- Jak uniknąć błędów: niejednoznaczność, nieetyczność, stronniczość
- Zasady inkluzywności i różnorodności w tworzeniu promptów

4 – Równowaga między innowacją a prywatnością

- Jak AI wspiera cyberbezpieczeństwo (detekcja phishingu, analiza logów, SIEM)?
- Jak AI wspiera cyberprzestępców (deepfake, scam, automatyzacja ataków)?
- Kwestie prawne i etyczne: prywatność, dane osobowe, własność intelektualna
- Rola transparentności i zgody użytkownika
- Wpływ AI na podejmowanie decyzji – ryzyko błędów i uprzedzeń
- Walidacja wyników i ograniczanie biasu

5 – Przyszłość AI i nowe trendy

- Nadchodzące przełomy: Digital Twins, AI w motoryzacji, opiece zdrowotnej, edukacji
- Jak AI wpłynie na rynek pracy – nowe role, automatyzacja, reskilling
- Narzędzia, które warto znać i śledzić
- Dlaczego warto znać techniczne podstawy AI
- Jak implementować AI w swojej branży
- Tworzenie własnej "AI Time Capsule"

6 – Cyberbezpieczeństwo i zagrożenia związane z AI

- AI w rekonesansie i skanowaniu oraz automatyzacji ataków
- Prompt injection, jailbreakingi, zagrożenia w modelach LLM
- Bezpieczeństwo haseł a AI
- OSINT z AI
- AI w socjotechnikach
- AI w atakach aplikacji webowych

7 – Cyberbezpieczeństwo a kwestie zgodności i regulacji AI

- Przegląd regulacji: AI Act (UE), NIST AI RMF, zasady ISO/IEC
- Wyzwania w ochronie danych osobowych i metadanych

- Dokumentacja modeli i Explainable AI (XAI)



Oczekiwane przygotowanie uczestnika

- **Podstawową znajomość technologii informacyjnych** – ogólna orientacja w pracy z komputerem, aplikacjami i internetem.
- **Zainteresowanie nowymi technologiami** – chęć uczenia się o sztucznej inteligencji i jej zastosowaniach w różnych dziedzinach.
- **Podstawowe umiejętności logicznego myślenia** – przydatne w zrozumieniu działania algorytmów i procesów AI.



Szkolenie obejmuje

- 2 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Podręcznik w wersji elektronicznej
- Środowisko laboratoryjne

Metoda szkolenia

- wykład
- warsztaty



Czas trwania

2 dni / 14 godzin

Język

Szkolenie: polski

Materiały: angielski