kod szkolenia: AI_ARCH_IT / PL DL 3d

Architektura systemów IT w erze AI klasy enterprise

Szkolenie przygotowuje do projektowania, oceny i wdrażania architektur systemów z komponentami AI – od strategii i modelowania domen, przez wybór wzorców integracyjnych i przetwarzania danych, po wdrożenia produkcyjne, monitorowanie i zarządzanie ryzykiem (AI Act, OWASP LLM, MLOps).

Szkolenie realizowane jest z wykorzystaniem narzędzi AI takich jak ChatGPT (GPT), itp., w zależności od tematyki i zakresu szkolenia.

Odbiorcy szkolenia

- Architekci rozwiązań, architekci korporacyjni i architekci oprogramowania
- Tech leaderzy, liderzy zespołów inżynierskich i seniorzy programiści
- Inżynierowie danych, ML/MLOps engineers, specjaliści platform danych
- Product Ownerzy i analitycy biznesowi pracujący z zespołami AI
- Konsultanci i menedżerowie technologii planujący transformację AI

Korzyści

- Zdobędziesz praktyczną wiedzę z projektowania architektury systemów IT wykorzystujących sztuczną inteligencję.
- Nauczysz się projektować rozwiązania oparte na LLM, GenAI oraz architekturze RAG.
- Poznasz uznane standardy architektoniczne, m.in. TOGAF, ArchiMate, C4 i Domain-Driven Design.
- Rozwiniesz umiejętność doboru nowoczesnych wzorców integracyjnych i architektur enterprise.
- Dowiesz się, jak tworzyć bezpieczne i zgodne z AI Act oraz RODO systemy AI.
- Nauczysz się projektować procesy MLOps wspierające wdrażanie i utrzymanie modeli AI.
- Zwiększysz swoją wartość na rynku pracy w obszarach architektury IT, AI i transformacji cyfrowej

Program szkolenia

1 – Wprowadzenie do architektury IT w erze AI
- Platform 4.0 – ewolucja platform technologicznych
- Hype Cycle Gartnera dla AI i technologii enterprise
- Rola architekta w organizacji wykorzystującej AI
- Trendy i kierunki rozwoju systemów klasy enterprise

2 – Standardy i notacje modelowania architektury
- TOGAF – ramy architektury korporacyjnej
- Model C4 – wizualizacja architektury oprogramowania
- Dobre praktyki dokumentowania decyzji architektonicznych (ADR)
- Mapowanie wymagań biznesowych na komponenty techniczne

3 – Domain-Driven Design (DDD)
- Strategiczne DDD – Bounded Context, Context Map
- Taktyczne DDD – Aggregate, Entity, Value Object
- Ubiquitous Language i współpraca z biznesem
- Event Storming jako technika odkrywania domeny

4 – Machine Learning vs Large Language Models
- Klasyczne ML – kiedy stosować, ograniczenia
- LLM – architektura, możliwości i typowe pułapki
- Kryteria wyboru: ML vs LLM vs rozwiązania hybrydowe
- Koszty, latencja i skalowalność modeli

5 – Wzorce integracji AI: RAG i agenci
- Retrieval-Augmented Generation – architektura end-to-end
- Bazy wektorowe i strategie chunkowania
- Wzorce agentowe i orkiestracja narzędzi
- Prompt engineering w kontekście architektury systemu

6 – Architektura sterowana zdarzeniami (Event-Driven)
- Event Sourcing i CQRS
- Brokery zdarzeń: Kafka, RabbitMQ, Pub/Sub
- Saga i wzorce kompensacji w systemach rozproszonych
- Integracja AI w przepływach zdarzeniowych

7 – Bezpieczeństwo i zgodność prawna AI
- AI Act – kategorie ryzyka i obowiązki organizacji
- OWASP Top 10 dla aplikacji LLM
- Prompt injection, data leakage, model poisoning
- Privacy by design oraz zarządzanie danymi treningowymi

8 – MLOps i cykl życia modeli AI

- Pipeline ML/LLMOps – od eksperymentu do produkcji
- Monitoring modeli: drift, halucynacje, jakość odpowiedzi
- Wersjonowanie modeli, danych i promptów
- A/B testing oraz strategie wdrożeń modeli

9 – Architektura serverless i mikroserwisowa dla AI

- Mikroserwisy a monolit – kiedy co wybrać
- Serverless dla obciążeń AI – zalety i ograniczenia
- Konteneryzacja, Kubernetes i orkiestracja workloadów GPU
- Wzorce skalowania i optymalizacja kosztów chmury

10 – Warsztat: projektowanie architektury z AI

- Event Storming dla wybranego case'u biznesowego
- Projekt architektury referencyjnej z komponentem LLM
- Analiza ryzyk bezpieczeństwa i zgodności
- Prezentacja i krytyka rozwiązań w grupach

Oczekiwane przygotowanie uczestnika

• Podstawowa znajomość architektury systemów rozproszonych (HTTP, kolejki, bazy danych)
• Doświadczenie z co najmniej jednym językiem programowania (preferowane Python / Java / TypeScript)
• Świadomość pojęć: chmura publiczna, kontenery, CI/CD
• Mile widziane: pierwsze kontakty z modelami ML lub LLM (np. ChatGPT, scikit-learn)

Czas trwania

3 dni / 24 godzin

Język

Język polski