kod szkolenia: GH-600 / PL DL 1d

Developing in Agentic AI Systems

Szkolenie obejmuje kluczowe zagadnienia związane z rozwijaniem, wdrażaniem i zarządzaniem systemami Agentic AI w ramach procesów rozwoju oprogramowania opartych na GitHub.

Odbiorcy szkolenia

Szkolenie przeznaczone jest dla:

- Architektów projektujących i nadzorujących wdrożenia systemów rozwoju oprogramowania opartych na AI, którzy chcą integrować Agentic AI z korporacyjnymi procesami rozwoju oprogramowania.
- Inżynierów platform oraz inżynierów DevOps zarządzających infrastrukturą rozwojową, potokami automatyzacji i procesami CI/CD, którzy chcą wykorzystać agentów AI w swojej pracy operacyjnej.
- Deweloperów aplikacji tworzących i utrzymujących rozwiązania programistyczne, którzy chcą zwiększyć produktywność i jakość kodu dzięki wykorzystaniu agentów AI.
- Menedżerów Produktu (Product Managerów), którzy nadzorują procesy rozwoju oprogramowania i chcą zrozumieć, jak integrować agentów AI z cyklem rozwoju produktu.
- Inżynierów bezpieczeństwa odpowiedzialnych za zapewnienie zgodności, bezpieczeństwa oraz mechanizmów zarządzania w środowiskach rozwojowych wspieranych przez AI.
- Osób przygotowujących się do GitHub Agentic AI Developer Certification.

Korzyści

W trakcie szkolenia zdobędziesz:

- Praktyczne umiejętności w zakresie tworzenia rozwiązań Agentic AI – zdobędziesz praktyczne doświadczenie w integrowaniu agentów AI z rzeczywistymi procesami rozwoju oprogramowania, wykorzystując GitHub jako centralne środowisko zarządzania.
- Zaawansowane projektowanie architektury agentów – nauczysz się rozdzielać planowanie, rozumowanie i wykonanie w systemach agentowych, zwiększając ich niezawodność i kontrolowalność

w środowiskach produkcyjnych.

- Orkiestracja systemów wieloagentowych – opanujesz koordynację wielu agentów AI przy użyciu przepływów pracy GitHub, umożliwiając budowę złożonych i skalowalnych systemów wspieranych przez AI.
- Zarządzanie i bezpieczeństwo gotowe do zastosowań produkcyjnych – wdrożysz solidne mechanizmy zarządzania wykorzystujące natywne funkcje GitHub, zatwierdzenia wykonywane przez człowieka oraz model minimalnych uprawnień, aby zapewnić bezpieczne i zgodne działanie systemów AI.
- Zaawansowane umiejętności zarządzania pamięcią i stanem agentów – nauczysz się utrwalać postęp agentów między środowiskami oraz zarządzać dryfem kontekstu, zapewniając ciągłość działania długotrwałych procesów.
- Integracja narzędzi i implementacja MCP – skonfigurujesz narzędzia agentów, uprawnienia i serwery Model Context Protocol (MCP), umożliwiając agentom efektywną współpracę ze środowiskami programistycznymi.
- Umiejętności ewaluacji i optymalizacji – nauczysz się definiować wskaźniki sukcesu, analizować błędy agentów i systematycznie doskonalić ich działanie w środowiskach produkcyjnych.

Program szkolenia

1. Podstawy Agentic AI w GitHub
   - Wprowadzenie
   - Definiowanie Agentic AI w SDLC
   - Wyjaśnienie cyklu życia agenta: planuj, wykonuj, oceniaj
   - GitHub jako system ewidencji oraz centralne środowisko zarządzania
   - Identyfikacja odpowiedzialności, ryzyk, antywzorców i wymagań związanych z identyfikowalnością
   - Zastosowanie modelu współpracy człowieka i agenta AI do rezultatów generowanych przez agentów
2. Projektowanie architektury agentów i integracja z SDLC
   - Wprowadzenie
   - Mapowanie odpowiedzialności agentów na etapy SDLC
   - Definiowanie danych wejściowych, rezultatów oraz kryteriów sukcesu
   - Rozdzielanie planowania, rozumowania i wykonania
   - Przykłady wdrażania mechanizmów zarządzania pull requestami przy użyciu szablonów, kontroli, CODEOWNERS, reguł i bramek środowiskowych
   - Budowanie niezawodnych przepływów pracy: dane wyjściowe, kontekst, wyzwalacze oraz przekazywanie informacji między zadaniami
   - Kontrola i obsługa agentów: obserwowalność, narzędzia, MCP, sekrety, hooki i niezawodność
3. Narzędzia, MCP i środowiska wykonawcze agentów
   - Wprowadzenie
   - Współpraca agentów z API GitHub i przepływami pracy

- Serwery Model Context Protocol (MCP), rejestry oraz listy dozwolonych zasobów
- Kontekst wykonania i jego granice
- Limity działania agentów i zabezpieczenia

4. Systemy wieloagentowe i orkiestracja
   - Wprowadzenie
   - Definiowanie odpowiedzialności agentów wieloagentowych w SDLC
   - Orkiestracja agentów przy użyciu przepływów pracy GitHub
   - Izolacja wykonania: gałęzie, przepływy pracy, uprawnienia i współbieżność
   - Wykrywanie i rozwiązywanie konfliktów przy użyciu natywnych mechanizmów arbitrażu GitHub
   - Zapewnienie obserwowalności systemu: atrybucja, ślady działania i przekazywanie kontekstu
   - Niezawodna praca na dużą skalę: diagnozowanie awarii i bezpieczne odzyskiwanie działania
5. Pamięć, stan i ewaluacja
   - Wprowadzenie
   - Implementacja strategii pamięci agentów
   - Utrwalanie stanu agentów i zarządzanie dryfem kontekstu
   - Zapewnienie ciągłości pamięci i stanu agentów w różnych narzędziach i środowiskach
   - Definiowanie kryteriów oceny i stosowanie bramek jakości
   - Analiza błędów agentów i doskonalenie ich działania
6. Zarządzanie, zabezpieczenia i operacje
   - Wprowadzenie
   - Definiowanie poziomu autonomii w oparciu o ryzyko oraz granic działania agentów
   - Egzekwowanie zasad zarządzania przy użyciu mechanizmów kontroli GitHub
   - Projektowanie przepływów pracy z udziałem człowieka
   - Kontrola możliwości agentów zgodnie z zasadą najmniejszych uprawnień
   - Zapewnienie, że działania są obserwowalne, identyfikowalne i możliwe do audytowania
   - Utrzymanie ładu organizacyjnego i niezawodności operacyjnej

Oczekiwane przygotowanie uczestnika

- uczestnik musi posiadać założone konto na GitHub
- Podstawowa wiedza z zakresu AI
- Podstawowa znajomość repozytoriów, gałęzi i pull requestów
- Ogólna znajomość koncepcji CI/CD

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć
Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/jak-dzialamy/o-szkoleniach/?distance-learning

Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie: https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii

Czas trwania

1 dni / 7 godzin

Język

- Szkolenie: polski
- Materiały: angielski