



Bezpieczeństwo w pracy z technologiami AI w chmurze

Numer usługi 2026/03/23/10671/3429750

1 660,50 PLN brutto
1 350,00 PLN netto
207,56 PLN brutto/h
168,75 PLN netto/h
118,13 PLN cena rynkowa ⓘ

Sages Spółka z ograniczoną odpowiedzialnością

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

★★★★☆ 4,4 / 5

🕒 8 h

310 ocen

📅 22.04.2026 do 22.04.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Programowanie
Identyfikatory projektów	Zachodniopomorskie Bony Szkoleniowe, Małopolski Pociąg do kariery, Kierunek - Rozwój, Akademia HR
Grupa docelowa usługi	Specjaliści IT, DevOps, architekci chmurowi i inżynierowie bezpieczeństwa z doświadczeniem w pracy z chmurą Liderzy zespołów technicznych wdrażający AI oraz osoby odpowiedzialne za bezpieczeństwo i zgodność w organizacjach Osoby zarządzające ryzykiem i ochroną danych w środowiskach wykorzystujących sztuczną inteligencję
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	21-04-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Szkolenie przygotowuje do samodzielnego wdrażania i zabezpieczania rozwiązań AI w środowiskach chmurowych, z uwzględnieniem ochrony danych i zarządzania tożsamością

Szkolenie uczy identyfikowania zagrożeń, monitorowania oraz reagowania na incydenty bezpieczeństwa w aplikacjach wykorzystujących sztuczną inteligencję

Szkolenie pokazuje, jak stosować automatyzację i najlepsze praktyki w zakresie bezpieczeństwa AI oraz jak oceniać ryzyko i zgodność z regulacjami

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik analizuje zagrożenia związane z AI w chmurze	Uczestnik automatyzuje procesy zabezpieczania aplikacji AI	Obserwacja w warunkach rzeczywistych
Uczestnik wdraża mechanizmy ochrony danych i zarządzania tożsamością	Uczestnik ocenia ryzyko i zgodność z regulacjami	
Uczestnik monitoruje i wykrywa incydenty bezpieczeństwa AI	Uczestnik stosuje AI do detekcji oszustw i analizy zachowań	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Każdego dnia zajęcia w godz. 9:00-17:00, z przerwą na lunch około godz. 13:00. Przerwa na lunch jest wliczona w czas usługi rozwojowej. Usługa prowadzona w godzinach zegarowych.

Zajęcia prowadzone są w dwóch blokach: zajęcia teoretyczne, rozmowa na żywo, chat, współdzielenie ekranu oraz zajęcia praktyczne, rozmowa na żywo, chat, współdzielenie ekranu

1. Wprowadzenie do bezpieczeństwa w chmurze
2. Zagrożenia związane z AI w chmurze
3. Podstawy ochrony danych
4. Zarządzanie tożsamością i dostępem (IAM)
5. Bezpieczeństwo aplikacji AI
6. Monitorowanie i wykrywanie zagrożeń
7. Automatyzacja bezpieczeństwa
8. Zarządzanie incydentami bezpieczeństwa
9. Zgodność z regulacjami
10. Ocena ryzyka
11. Praktyczne zastosowania AI w bezpieczeństwie, takie jak detekcja oszustw czy analiza
12. Zachowania użytkowników
13. Zarządzanie cyklem życia modelu AI
14. Etyka i odpowiedzialność w AI
15. Przyszłość bezpieczeństwa AI w chmurze
16. Walidacja - testy, ankiety - ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu

Harmonogram

Liczba przedmiotów/zajęć: 6

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 6 Wprowadzenie do bezpieczeństwa w chmurze Zagrożenia związane z AI w chmurze Podstawy ochrony danych	Przemysław Chmielecki	22-04-2026	09:00	10:30	01:30
2 z 6 Zarządzanie tożsamością i dostępem (IAM) Bezpieczeństwo aplikacji AI Monitorowanie i wykrywanie zagrożeń Automatyzacja bezpieczeństwa	Przemysław Chmielecki	22-04-2026	10:30	13:00	02:30
3 z 6 Przerwa na lunch wliczona w czas trwania usługi rozwojowej	Przemysław Chmielecki	22-04-2026	13:00	13:15	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
4 z 6 Zarządzanie incydentami bezpieczeństwa Zgodność z regulacjami Ocena ryzyka Praktyczne zastosowania AI w bezpieczeństwie, takie jak detekcja oszustw czy analiza	Przemysław Chmielecki	22-04-2026	13:15	15:00	01:45
5 z 6 Zachowania użytkowników Zarządzanie cyklem życia modelu AI Etyka i odpowiedzialność w AI Przyszłość bezpieczeństwa AI w chmurze	Przemysław Chmielecki	22-04-2026	15:00	16:30	01:30
6 z 6 Walidacja - testy, ankiety - ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	-	22-04-2026	16:30	17:00	00:30

Cennik

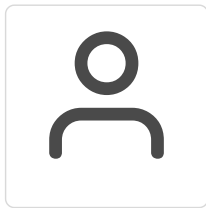
Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 660,50 PLN
Koszt przypadający na 1 uczestnika netto	1 350,00 PLN
Koszt osobogodziny brutto	207,56 PLN
Koszt osobogodziny netto	168,75 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Przemysław Chmielecki

Architekt chmurowy i praktyk podejścia DevSecOps. Od wielu lat poruszam się w obszarze chmury obliczeniowej i sprawia mi to coraz większą radość. W różnych projektach miałem okazję poznać wszystkie chmury głównych dostawców (AWS, Azure, GCP, Alibaba, Oracle) a także poznać sposoby optymalizacji kosztów i dostępnych rozwiązań korzystając z technologii kontenerowych (Kubernetes, Helm, ArgoCD) i automatyzacji na drodze skryptowania (Bash, PowerShell, Python). Mam także doświadczenie w pracy z SDLC (Software Development LifeCycle) w Pythonie, Javie i .NET. Posiadam ponad 35 aktywnych certyfikatów technologicznych z obszaru chmurowego, DevOps, projektowania i programowania. Poza pracą techniczną staram się rozwijać w obszarze naukowym i projektowym co pozwala udoskonalić warsztat trenerski oraz znacznie uporządkować wiedzę.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

część teoretyczna szkolenia, slajdy - zostanie przekazana uczestnikom na szkoleniu w formie pdf.

uczestnik otrzyma certyfikat uczestnictwa z opisem nabytych umiejętności - prowadzone będą listy obecności, frekwencja minimum 80% wymagana do zaliczenia szkolenia

Warunki uczestnictwa

Podstawowe doświadczenie w pracy z chmurą

Podstawowa wiedza o sztucznej inteligencji mile widziana

Podstawowa wiedza z zakresu bezpieczeństwa IT mile widziana

Informacje dodatkowe

Szkolenie będzie prowadzone zdalnie, w czasie rzeczywistym, na żywo, z trenerem, możliwością zadawania pytań.

Szkolenie składa się z wykładu teoretycznego oraz z warsztatów i samodzielnej pracy.

Podczas szkolenia uczestnicy mają dostęp do czatu z trenerem, współdzielą ekran podczas części warsztatowej, żeby zaprezentować postęp swojej pracy.

Walidacja będzie bazowała na ocenie efektów samodzielnej pracy uczestników, będzie sprawdzała nabytą wiedzę teoretyczną i umiejętność jej zastosowania w praktyce.

Warunki techniczne

szkolenie na platformie zoom, wymagane:

stabilne połączenie internetowe (zalecane min. 10Mbit/s download i 1Mbit/s upload)

przeglądarka internetowa Chrome

zainstalowana aplikacja Zoom App

dobrej jakości słuchawki oraz mikrofon (opcjonalnie) kamera internetowa

link do szkolenia zostanie przesłany uczestnikom przed szkoleniem i będzie aktywny do końca szkolenia.

Kontakt



Agata Tuliszka-Kamińska

E-mail a.kaminska@sages.com.pl

Telefon (+48) 530 612 226