Możliwość dofinansowania

AI w Cyberbezpieczeństwie - szkolenie

Numer usługi 2026/03/16/7733/3410547

1 722,00 PLN brutto
1 400,00 PLN netto
215,25 PLN brutto/h
175,00 PLN netto/h
183,33 PLN cena rynkowa

Comarch SA

4,5 / 5

1 302 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
08:00 h
05.08.2026 do 05.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Aplikacje biznesowe
Identyfikatory projektów	Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe, Kierunek - Rozwój, Regionalny Fundusz Szkoleniowy II
Grupa docelowa usługi	Szkolenie skierowane jest do: • Specjalistów ds. bezpieczeństwa IT. • Analitków danych i programistów. • Menedżerów IT i kierowników projektów. • Osób odpowiedzialnych za zarządzanie ryzykiem w organizacjach. • Wszystkich zainteresowanych tematyką AI i cyberbezpieczeństwa. **Przygotowanie uczestników** • Podstawowa wiedza z zakresu IT i bezpieczeństwa informatycznego. • Znajomość podstawowych pojęć związanych z sztuczną inteligencją będzie dodatkowym atutem. **Czas trwania kursu wynosi 8 godzin lekcyjnych, godzina lekcyjna to 45 minut.** **Usługa jest dedykowana dla uczestników projektu Małopolski pociąg do kariery.** *Usługa również adresowana dla uczestników projektu Małopolskie Bony rozwojowe Plus" i "Małopolski Pociąg do Kariery"* "Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój"
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	29-07-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	8
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Szkolenie przygotowuje do samodzielnego identyfikowania, analizowania i neutralizowania zagrożeń teleinformatycznych powiązanych z technologiami sztucznej inteligencji, a także do bezpiecznego wdrażania narzędzi AI w strukturach organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe pojęcia związane z cyberbezpieczeństwem i sztuczną inteligencją.	definiuje kluczowe pojęcia z zakresu cyberbezpieczeństwa i AI,	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia podstawowe typy zagrożeń cybernetycznych,	Test teoretyczny z wynikiem generowanym automatycznie
	opisuje rolę sztucznej inteligencji w systemach bezpieczeństwa informatycznego.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i analizuje zagrożenia związane z wykorzystaniem AI w kontekście cyberbezpieczeństwa.	wskazuje przykłady zagrożeń wynikających z wykorzystania AI,	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje scenariusze ataków wykorzystujących technologie AI,	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia wpływ zagrożeń na bezpieczeństwo systemów informatycznych.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykorzystuje narzędzia oparte na AI do identyfikacji i neutralizacji zagrożeń cybernetycznych.	dobiera narzędzia AI wspierające wykrywanie zagrożeń,	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje dane w celu identyfikacji potencjalnych incydentów bezpieczeństwa,	Test teoretyczny z wynikiem generowanym automatycznie
	proponuje działania ograniczające skutki wykrytych zagrożeń.	Test teoretyczny z wynikiem generowanym automatycznie
Ocenia ryzyko cyberbezpieczeństwa oraz proponuje zabezpieczenia na podstawie analizy danych.	identyfikuje potencjalne źródła ryzyka w systemie informatycznym,	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje dane dotyczące incydentów bezpieczeństwa,	Test teoretyczny z wynikiem generowanym automatycznie
	proponuje środki zabezpieczające adekwatne do zidentyfikowanego ryzyka.	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje techniki ataków socjotechnicznych oraz stosuje działania zapobiegawcze.	identyfikuje przykłady ataków socjotechnicznych (np. phishing),	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje scenariusze wykorzystania socjotechniki w cyberatakach,	Test teoretyczny z wynikiem generowanym automatycznie
	wskazuje działania ograniczające skuteczność takich ataków.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady cyberhigieny w pracy z systemami informatycznymi i narzędziami AI.	opisuje zasady bezpiecznego korzystania z systemów informatycznych,	Test teoretyczny z wynikiem generowanym automatycznie
	stosuje dobre praktyki w zakresie ochrony danych i dostępu do systemów,	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia poprawność stosowanych procedur bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1.Usługa jest realizowana w godzinach lekcyjnych, tj. za godzinę usługi szkoleniowej rozumie się 45 minut, łącznie 8 godzin lekcyjnych.

Planowane przerwy w trakcie zajęć: 10:30-10:45, 13:00-13:30, 14:45-15:00. Przerwy nie są wliczone w godziny zajęć usługi. Liczba godzin zajęć praktycznych: 4 godziny lekcyjne , liczba godzin zajęć teoretycznych: 4 godziny lekcyjne, w tym test 10 min.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

2.Grupa docelowa: Szkolenie skierowane jest do: Specjalistów ds. bezpieczeństwa IT, Analitków danych i programistów, Menedżerów IT i kierowników projektów, Osób odpowiedzialnych za zarządzanie ryzykiem w organizacjach, Wszystkich zainteresowanych tematyką AI i cyberbezpieczeństwa.

Przygotowanie uczestników: Podstawowa wiedza z zakresu IT i bezpieczeństwa informatycznego, Znajomość podstawowych pojęć związanych z sztuczną inteligencją będzie dodatkowym atutem.

Wprowadzenie do cyberbezpieczeństwa i sztucznej inteligencji

- Definicja cyberbezpieczeństwa: Zrozumienie podstawowych terminów i koncepcji związanych z ochroną danych, systemów i sieci przed zagrożeniami, w tym atakami hakerskimi i złośliwym oprogramowaniem.
- OWASP Top 10 dla LLM: Przegląd najważniejszych zagrożeń związanych z modelami językowymi, takich jak manipulacja danymi wejściowymi, generowanie dezinformacji oraz ryzyko związane z przechowywaniem danych.
- Zastosowanie sztucznej inteligencji: Jak AI może wspierać cyberbezpieczeństwo, identyfikując i neutralizując zagrożenia w czasie rzeczywistym.
- Zrozumienie ryzyk: Analiza potencjalnych skutków cyberataków na organizacje w kontekście rosnącej popularności modeli AI.

Wykorzystanie AI w obronie przed cyberzagrożeniami

- Detekcja anomalii: Jak algorytmy AI mogą analizować ruch sieciowy w poszukiwaniu nietypowych wzorców, które mogą wskazywać na atak.
- Automatyzacja odpowiedzi: Wykorzystanie AI do automatyzacji procesów odpowiedzi na incydenty, co pozwala na szybsze reagowanie na zagrożenia.
- Predykcja zagrożeń: Modele AI mogą przewidywać przyszłe ataki na podstawie analizy danych historycznych, co umożliwia wcześniejsze wprowadzenie środków ochronnych.

- Współpraca z zespołami IT: AI jako narzędzie wspierające zespoły bezpieczeństwa w codziennych zadaniach, takich jak analiza logów czy monitorowanie systemów.

Analiza ryzyk i zabezpieczeń z wykorzystaniem AI

- Identyfikacja ryzyk: Jak AI może wspierać proces identyfikacji i oceny ryzyk związanych z infrastrukturą IT.
- Ocena efektywności zabezpieczeń: Wykorzystanie technik AI do oceny, jak skuteczne są obecne zabezpieczenia w organizacji i gdzie można je poprawić.
- Modelowanie scenariuszy ataków: AI może symulować różne scenariusze ataków, co pozwala na lepsze przygotowanie się na potencjalne zagrożenia.
- Dostosowywanie zabezpieczeń: Zastosowanie uczenia maszynowego do ciągłego dostosowywania zabezpieczeń w odpowiedzi na zmieniające się zagrożenia.

Rola AI w zapobieganiu atakom socjotechnicznym

- Wykrywanie phishingu: Jak AI może analizować wiadomości e-mail i inne formy komunikacji, aby identyfikować potencjalnie złośliwe treści.
- Edukacja użytkowników: Użycie AI do tworzenia spersonalizowanych programów szkoleniowych, które zwiększają świadomość pracowników na temat technik socjotechnicznych.
- Analiza zachowań użytkowników: AI może monitorować zachowania pracowników, aby szybko identyfikować nietypowe aktywności, które mogą sugerować próby oszustwa.
- Tworzenie polityk bezpieczeństwa: Wspieranie organizacji w opracowywaniu polityk mających na celu przeciwdziałanie atakom socjotechnicznym przy użyciu analizy danych.

AI w rękach atakujących – Jak się chronić?

- Zrozumienie narzędzi atakujących: Przegląd technik i narzędzi AI, które mogą być wykorzystywane przez cyberprzestępców, takich jak generowanie fałszywych treści.
- Edukacja i świadomość: Szkolenie pracowników w zakresie zagrożeń związanych z użyciem AI przez atakujących oraz wskazówki, jak rozpoznać potencjalne ataki.
- Wdrażanie zaawansowanych zabezpieczeń: Wykorzystanie AI do wzmocnienia zabezpieczeń, np. poprzez analizę ryzyk w czasie rzeczywistym i wprowadzanie dynamicznych środków ochronnych.
- Monitorowanie i analiza: Utworzenie systemów monitorujących, które wykorzystują AI do identyfikacji podejrzanych działań i potencjalnych naruszeń bezpieczeństwa.

Przyszłość cyberbezpieczeństwa z AI

- Ewolucja zagrożeń: Jak rozwój AI może prowadzić do powstawania nowych form cyberzagrożeń oraz jak organizacje powinny się na nie przygotować.
- Kooperacja AI i ludzi: Zrozumienie, jak AI może wspierać ludzkich specjalistów w dziedzinie bezpieczeństwa, a nie ich zastępować.
- Regulacje i etyka: Wyzwania związane z regulacją użycia AI w cyberbezpieczeństwie oraz kwestie etyczne z tym związane.
- Innowacyjne technologie: Zastosowanie nowych technologii, takich jak blockchain czy kwantowe szyfrowanie w połączeniu z AI, w celu wzmocnienia bezpieczeństwa.

Cyber higiena, a AI

- Podstawy cyber higieny: Definicja i znaczenie cyber higieny w kontekście ochrony danych i systemów.
- Zastosowanie AI w monitorowaniu: Jak narzędzia AI mogą wspierać organizacje w utrzymaniu odpowiednich standardów cyber higieny poprzez automatyczne skanowanie i analizę systemów.
- Personalizacja praktyk bezpieczeństwa: Użycie AI do dostosowywania praktyk cyber higieny do specyficznych potrzeb i ryzyk danej organizacji.
- Wzmacnianie kultury bezpieczeństwa: Jak AI może pomóc w tworzeniu kultury bezpieczeństwa w organizacjach, w tym poprzez analizę danych dotyczących zachowań użytkowników i identyfikację obszarów do poprawy.

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 722,00 PLN
Koszt przypadający na 1 uczestnika netto	1 400,00 PLN
Koszt osobogodziny brutto	215,25 PLN
Koszt osobogodziny netto	175,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Marek Jeleśniański

Ekspert i trener i doradca z zakresu AI, wykształcenie wyższe, od 20 lat związany z branżą IT, wspiera zarówno międzynarodowe korporacje, jak i małe firmy. W swojej karierze pełnił różne role – od programisty po dyrektora. Jako pasjonat sztucznej inteligencji i jej wpływu na przyszłość rynku pracy, dzieli się swoją wiedzą i przewidywaniami na blogu: https://jelesnianski.pl/.
Autor programów szkoleniowych i publikacji. Bardzo dobrze oceniany przez uczestników swoich szkoleń.
Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują podręcznik w wersji elektronicznej.

W czasie zajęć wykorzystywane są autorskie materiały dydaktyczne przygotowane przez wykładowcę oraz inne materiały dydaktyczne przygotowane przez organizatora szkolenia.

Warunki uczestnictwa

Warunkiem skorzystania ze szkolenia jest dokonanie równolegle rejestracji na kurs na stronie www.comarch.pl/szkolenia w formie:

- elektronicznego zamówienia szkolenia (przycisk "Zamów" przy wybranym temacie i terminie). Opcja ta dotyczy osób fizycznych oraz firm/instytucji

albo

- poprzez uzupełnienie i odesłanie na adres szkolenia@comarch.pl tradycyjnego formularza zgłoszeniowego który jest dostępny na stronie www.comarch.pl/szkolenia (przycisk "Pobierz formularz zgłoszeniowy"). Opcja ta dotyczy wyłącznie firm/Instytucji.

W obu przypadkach przy dokonaniu zgłoszenia prosimy o informacje dotyczącą projektu z którego dofinansowania korzysta Uczestnik.

Planowana przerwa: –obiadowa 30 min plus 2 kawowe po 15 minut.

Wykładowca ma prawo zmienić godziny przerw, jeśli wymaga tego proces dydaktyczny (np. rozpoczęte ćwiczenie) lub na życzenie większości uczestników kursu (zmęczenie, większa trudność treści kształcenia).

Informacje dodatkowe

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być zwolnienione z VAT-u w zależności od rodzaju dofinasowania

Zawarto umowę z WUP Kraków na rozliczanie Usług z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu „Małopolski Pociąg do Kariery” i "Małopolskie Bony Rozwojowe Plus"

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój.

Warunki techniczne

Wymagania techniczne:

- Komputer / laptop ze stałym dostępem do Internetu (Szybkość pobierania/przesyłania: minimalna 2 Mb/s / 128 kb/s; zalecana 4 Mb/s / 512 kb/s
- przeglądarka internetowa – zalecane: Google Chrome, Mozilla Firefox, Microsoft Edge
- słuchawki lub dobrej jakości głośniki
- mikrofon

Zalecane

- dodatkowy monitor
- kamera (w przypadku komputerów stacjonarnych)
- spokojne miejsce, odizolowane od zewnętrznych czynników rozpraszających
- podstawowa znajomość języka angielskiego (do sprawnego poruszania się po platformie zdalnej)

Informacje dodatkowe

Szkolenie Zdalne prowadzone jest w czasie rzeczywistymi i transmitowane za pomocą kanału internetowego z wykorzystaniem systemu ZOOM, który umożliwia komunikację głosową oraz wideo z Uczestnikami przebywających w dowolnym miejscu ze sprawnie działającym stałym łączem internetowym. Każdy z uczestników szkolenia otrzymuje przed szkoleniem link dostarczony w wiadomości mailowej z informacjami dotyczącymi szkolenia zdalnego. Link umożliwiający uczestnictwo w spotkaniu jest ważny do momentu zakończenia szkolenia.

Szkolenie zakończone jest testem wiedzy z zakresu tematycznego omawianego na szkoleniu.

Szkolenie może być nagrywane /rejestrowane w celu kontroli/audytu zgodnie z Regulaminem Świadczenia Usług Szkoleniowych Organizatora.

Uczestnicy szkolenia otrzymają materiały szkoleniowe w wersji elektronicznej.

Kontakt

Aneta Lewkowska

E-mail aneta.lewkowska@comarch.pl
Telefon (+48) 126 877 811