



## Cyberbezpieczeństwo w zrównoważonej transformacji cyfrowej. Kwalifikacje. Szkolenie.

Numer usługi 2026/04/20/163842/3498482

6 081,12 PLN brutto

4 944,00 PLN netto

380,07 PLN brutto/h

309,00 PLN netto/h

175,00 PLN cena rynkowa ⓘ

Digital Marketing  
Krzysztof Szymak

★★★★★ 4,9 / 5

484 oceny

📍 Katowice / stacjonarna

🏠 Usługa szkoleniowa

🕒 16 h

📅 04.07.2026 do 10.07.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Internet

### Grupa docelowa usługi

Szkolenie skierowane jest do osób, które planują z **własnej inicjatywy** podnieść swoje umiejętności w zakresie kwalifikacji cyfrowych, w obszarze cyberbezpieczeństwa. Prowadzi do zdobycia kwalifikacji międzynarodowej **GCCS-DIG-004 Specjalista ds. cyberbezpieczeństwa**.

Usługa szkoleniowa dedykowana jest także dla osób chcących podnieść swoje zielone kompetencje w zakresie bezpiecznego i zrównoważonego wykorzystywania technologii cyfrowych - od ograniczania śladu węglowego infrastruktury IT i zarządzania danymi, po odpowiedzialne, etyczne podejście do ochrony informacji i prywatności.

Usługa skierowana m.in. do:

- właścicieli i pracowników MŚP,
- osób pracujących z danymi (administracja, marketing, sprzedaż, HR),
- osób odpowiedzialnych za bezpieczeństwo informacji w organizacji,
- osób pracujących zdalnie lub hybrydowo
- wszystkich, którzy chcą zwiększyć swoje bezpieczeństwo cyfrowe i jednocześnie działać zgodnie z zasadami zrównoważonego rozwoju.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji

03-07-2026

Forma prowadzenia usługi

stacjonarna

Liczba godzin usługi

16

# Cel

## Cel edukacyjny

Usługa szkoleniowa przygotowuje do samodzielnego, praktycznego zarządzania cyberbezpieczeństwem, z uwzględnieniem zasad zrównoważonego rozwoju. Uczestnicy nauczą się identyfikować i neutralizować zagrożenia, wdrażać zabezpieczenia oraz zarządzać danymi i infrastrukturą IT. Szkolenie rozwija umiejętności w obszarze technologii informacyjno-komunikacyjnych (ICT) oraz zielonych kompetencji, rozumianych jako bezpieczne, odpowiedzialne i efektywne korzystanie z zasobów cyfrowych.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się  | Kryteria weryfikacji   | Metoda walidacji |
|---|--|------------------|
| Rozróżnia rodzaje zagrożeń cyberbezpieczeństwa oraz metody ich identyfikacji w systemach IT.                | Wymienia co najmniej 5 rodzajów zagrożeń cyberbezpieczeństwa i ich charakterystyki.        | Test teoretyczny |
|   | Opisuje metody detekcji zagrożeń w infrastrukturze sieciowej.                              | Test teoretyczny |
| Wyjaśnia zasady energooszczędnego projektowania infrastruktury bezpieczeństwa IT i jej wpływ na środowisko. | Charakteryzuje wpływ serwerów i urządzeń sieciowych na zużycie energii i emisję CO2.       | Test teoretyczny |
|   | Opisuje technologie optymalizacji energetycznej w systemach bezpieczeństwa.                | Test teoretyczny |
| Charakteryzuje przepisy prawne i normalizacyjne dotyczące ochrony danych i bezpieczeństwa informacji.       | Wymienia obowiązujące regulacje prawne w zakresie ochrony danych osobowych.                | Test teoretyczny |
|   | Opisuje standardy i certyfikacje bezpieczeństwa informacyjnego.                            | Test teoretyczny |
| Wyjaśnia zasady zarządzania cyklem życia oprogramowania z uwzględnieniem zrównoważonego rozwoju.            | Opisuje etapy cyklu życia oprogramowania i ich wpływ na produkcję e-odpadów.               | Test teoretyczny |
|   | Charakteryzuje znaczenie open-source i długoterminowego wsparcia dla zmniejszenia odpadów. | Test teoretyczny |

| Efekty uczenia się  | Kryteria weryfikacji   | Metoda walidacji             |
|---|--|------------------------------|
| Wdraża systemy monitorowania ruchu sieciowego z optymalizacją zużycia zasobów i energii.                          | Dobiera rozwiązania monitorujące minimalizujące obciążenie infrastruktury i zużycie energii. | Analiza dowodów i deklaracji |
|   | Konfiguruje kompresję danych i archiwizację logów bezpieczeństwa.                            | Analiza dowodów i deklaracji |
| Obsługuje i zarządza sprzętem sieciowym zgodnie z zasadami gospodarki o obiegu zamkniętym.                        | Organizuje recykling elektroniczny i bezpieczne usuwanie danych ze sprzętu.                  | Analiza dowodów i deklaracji |
|   | Planuje podejście do wycofywania starych urządzeń sieciowych.                                | Analiza dowodów i deklaracji |
| Projektuje i realizuje szkolenia pracowników dotyczące bezpieczeństwa danych z wykorzystaniem platform cyfrowych. | Wybiera platformy e-learningowe minimalizujące emisję CO2 i zużycie papieru.                 | Analiza dowodów i deklaracji |
|   | Opracowuje materiały szkoleniowe w formacie cyfrowym dla efektywnego przekazu.               | Analiza dowodów i deklaracji |
| Analizuje i redukuje ślad węglowy infrastruktury bezpieczeństwa IT poprzez optymalizację zasobów.                 | Identyfikuje sposoby redukcji zużycia energii w systemach monitorowania i ochrony.           | Analiza dowodów i deklaracji |
|   | Planuje migrację do modeli hybrydowych zasilanych energią odnawialną.                        | Analiza dowodów i deklaracji |
| Komunikuje zasady bezpieczeństwa danych pracownikom w sposób jasny, zrozumiały i konstruktywny.                   | Wyjaśnia złożone zagadnienia cyberbezpieczeństwa w prosty i przystępny sposób.               | Test teoretyczny             |
|   | Adaptuje komunikację do różnych poziomów technicznych odbiorców.                             | Test teoretyczny             |
| Odpowiedzialnie zarządza projektami bezpieczeństwa IT z uwzględnieniem wpływu na środowisko naturalne.            | Podejmuje decyzje balansujące bezpieczeństwo danych z ochroną środowiska.                    | Test teoretyczny             |
|   | Dokumentuje i uzasadnia działania zmniejszające negatywny wpływ na ekologię.                 | Test teoretyczny             |

| Efekty uczenia się  | Kryteria weryfikacji   | Metoda walidacji |
|---|--|------------------|
| Współpracuje w zespole wielodyscyplinarnym w celu implementacji rozwiązań cyberbezpieczeństwa.                  | Koordynuje działania z pracownikami IT, menedżerami i specjalistami z innych dziedzin. | Test teoretyczny |
|   | Zgłasza problemy i zagrożenia w sposób konstruktywny, proponując rozwiązania.          | Test teoretyczny |
| Wykazuje zaangażowanie w ciągłe uczenie się i doskonalenie umiejętności w dynamicznym środowisku cyberzagrożeń. | Identyfikuje nowe trendy zagrożeń i metody zrównoważonego bezpieczeństwa.              | Test teoretyczny |
|   | Uczestniczy w szkoleniach podnoszących kompetencje zawodowe i świadomość ekologiczną.  | Test teoretyczny |

## Kwalifikacje

### Kwalifikacje niewłączone do ZSK

#### Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: <https://standardgccs.com/qualifications/>

Strona internetowa Instytucji Walidującej: <https://icvc.eu/kwalifikacje-miedzynarodowe/>

#### Informacje

Nazwa Podmiotu prowadzącego walidację

ICVC CERTYFIKACJA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Nazwa Podmiotu certyfikującego

TALENT ODYSSEY LTD.

## Program

**Efekty uczenia się, kryteria weryfikacji i metody walidacji są zależne od specyfikacji kwalifikacji międzynarodowej i nie podlegają ingerencji ze strony Dostawcy Usługi.**

Usługa prowadzi do nabycia kwalifikacji: międzynarodowej **Specjalista ds. cyberbezpieczeństwa (GCCS-DIG-004)**. W ramach szkolenia zapewniono **walidację efektów uczenia się**, mającą na celu ocenę poziomu osiągnięcia efektów kształcenia. Uczestnik, który pozytywnie ukończy proces walidacji i zda formalny egzamin, uzyskuje **kwalifikację międzynarodową: GCCS-DIG-004 Specjalista ds. cyberbezpieczeństwa**.

Szkolenie wpisuje się w cele **Regionalnej Strategii Innowacji Województwa Śląskiego 2030 (RIS WSL 2030)**, w szczególności w obszarach:

- **Technologie informacyjno-komunikacyjne (ICT),**
- **Zielona gospodarka.**

Program wspiera rozwój kompetencji w zakresie cyberbezpieczeństwa, ochrony danych oraz zrównoważonego zarządzania infrastrukturą IT, uwzględniając aspekty **efektywności energetycznej i ograniczania wpływu technologii cyfrowych na środowisko.**

Szkolenie odpowiada również na potrzeby transformacji regionu w kierunku gospodarki niskoemisyjnej i opartej na wiedzy, przygotowując uczestników do pracy w środowisku, w którym rośnie znaczenie bezpieczeństwa cyfrowego oraz odpowiedzialnego wykorzystania zasobów technologicznych.

Program odnosi się do **Programu Rozwoju Technologii Województwa Śląskiego** poprzez:

- rozwój kompetencji w zakresie cyberbezpieczeństwa i ochrony danych,
- praktyczne zastosowanie narzędzi i procedur bezpieczeństwa IT,
- kształtowanie umiejętności optymalizacji infrastruktury cyfrowej pod kątem energooszczędności.

Ukończenie szkolenia zwiększa konkurencyjność uczestników na rynku pracy oraz ich gotowość do pracy w sektorach związanych z cyberbezpieczeństwem, IT oraz zieloną transformacją.

#### **Przykładowe perspektywy zawodowe:**

- specjalista ds. cyberbezpieczeństwa w MŚP,
- koordynator bezpieczeństwa informacji,
- specjalista ds. ochrony danych i RODO,
- specjalista ds. green IT,
- konsultant ds. bezpieczeństwa cyfrowego.

**Szkolenie będzie miało formę głównie warsztatową.** Każdy uczestnik będzie pracował przy komputerze. **Forma warsztatowa zapewni realizację celu edukacyjnego usługi.**

**Usługa realizowana jest w godzinach zegarowych, tj. 1 godzina lekcyjna = 60 minut.**

**Uwaga do harmonogramu:** przerwy na lunch są wliczone w czas trwania usługi i zostały ustalone na godzinę 12:00-12:45 - uwzględniono w harmonogramie.

**!!! WAŻNE: Szkolenie realizowane jest w terminie 04-05.07.2026 r.** Po zakończeniu szkolenia uczestnicy przystępują do egzaminu certyfikującego, który jest organizowany i oceniany przez międzynarodowy podmiot zewnętrzny. Czas oczekiwania na wynik walidacji wynosi średnio ok. 5 dni roboczych od dnia przeprowadzenia egzaminu. W związku z tym - według Zał. 2 (2.4) do Regulaminu BUR **termin realizacji usługi został określony w karcie na 04-10.07.2026, ponieważ obejmuje:**

- **okres prowadzenia szkolenia (4-5 lipca)**
- **oraz okres oczekiwania na wynik walidacji (do 10 lipca).**

**Część teoretyczna obejmuje 3,5 godziny zegarowe zajęć, natomiast część praktyczna - 9,5 godziny.** Pozostały czas trwania usługi to: 2 przerwy (w pierwszym oraz drugim dniu zajęć) po 45 minut oraz 1,5 godziny przeznaczone na kwestie organizacyjne (m.in. przywitanie, pre-testy, post-testy, pytania, podsumowanie zajęć) i walidację usługi oraz egzamin.

#### **PROGRAM:**

**I DZIEŃ SZKOLENIA [część teoretyczna: 2 godziny, część praktyczna: 5 godzin, przerwa: 45 min, kwestie organizacyjne: 15 min] - 04.07.2026:**

**08:30 - 08:45 Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego poziomu wiedzy uczestników.**

**08:45 - 10:15 MODUŁ I: Anatomia współczesnego ataku i jego wpływ na zasoby organizacji.**

1. Dlaczego sektor MŚP jest celem numer jeden - aktualne statystyki i konsekwencje biznesowe.
2. Łańcuch ataku (rekonesans → dostęp → eskalacja → exfiltracja danych).
3. Rodzaje zagrożeń: phishing, ransomware, malware, ataki socjotechniczne, wycieki danych.
4. Wartość danych i wpływ incydentów na środowisko (np. utrata danych = konieczność ich odtwarzania = dodatkowe zużycie energii i zasobów IT).
5. Wprowadzenie do metod detekcji zagrożeń (monitoring, analiza logów, systemy SIEM)

**10:15 - 12:00 MODUŁ II: Psychologia oszustwa i zagrożenia komunikacyjne (Phishing, Smishing, Vishing).**

1. Mechanizmy manipulacji: presja czasu, autorytet, strach, emocje.

2. Analiza rzeczywistych przypadków phishingu - identyfikacja zagrożeń w praktyce.
3. Scenariusze ataków telefonicznych i SMS.
4. Warsztat: rozpoznawanie zagrożeń i podejmowanie decyzji.
5. Jak ograniczenie liczby incydentów wpływa na zmniejszenie strat zasobów i energii w organizacji.

**12:00 - 12:45 Przerwa.**

**12:45 - 14:30 MODUŁ III: Zarządzanie tożsamością i bezpieczeństwo dostępu (warsztat).**

1. Hasła: frazy zamiast schematów - jak zwiększyć bezpieczeństwo i ograniczyć potrzebę resetów (redukcja obciążenia systemów).
2. Menedżery haseł (Bitwarden, 1Password) - konfiguracja i praktyczne użycie.
3. Weryfikacja wycieków danych (Have I Been Pwned).
4. Wpływ bezpiecznego zarządzania dostępem na ograniczenie incydentów i zużycia zasobów IT.

**14:30 - 16:30 MODUŁ IV: AI w cyberbezpieczeństwie i efektywność energetyczna systemów.**

1. Deepfake i klonowanie głosu - rozpoznawanie zagrożeń.
2. AI w atakach (automatyzacja phishingu).
3. AI w ochronie - jak nowoczesne programy antywirusowe wykorzystują uczenie maszynowe do wykrywania nieznanych wcześniej wirusów.
4. Wpływ systemów AI na zużycie energii - jak wybierać rozwiązania efektywne energetycznie.
5. Warsztat: analiza przypadków + wykorzystanie narzędzi AI w cyberbezpieczeństwie.

**II DZIEŃ SZKOLENIA [część teoretyczna: 1,5 godziny, część praktyczna: 4,5 godziny, przerwa: 45 min, kwestie organizacyjne: 30 min, walidacja oraz egzamin: 45 min] - 05.07.2026:**

**08:30 - 08:45 Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązywanie ewentualnych trudności na aktualnym etapie szkolenia.**

**08:45 - 10:15 MODUŁ V: Bezpieczeństwo sieci i energooszczędna infrastruktura IT.**

1. Konfiguracja sieci Wi-Fi - bezpieczeństwo i optymalizacja zużycia energii.
2. Publiczne sieci i zagrożenia.
3. VPN - zastosowanie, wybór dostawcy (rozwiązania przyjazne środowisku i efektywne energetycznie).
4. Monitoring sieci - jak ograniczyć obciążenie infrastruktury.
5. Warsztat: konfiguracja bezpiecznego i odpowiedzialnego środowiska pracy.

**10:15 - 12:00 MODUŁ VI: Ochrona danych i zarządzanie sprzętem w duchu gospodarki obiegu zamkniętego.**

1. Szyfrowanie danych (BitLocker, FileVault).
2. Backup (zasada 3-2-1) - efektywne zarządzanie kopiami. Ograniczanie duplikacji plików i archiwizacja jako element redukcji zużycia energii i zasobów cyfrowych.
3. Chmura kontra dysk - porównanie bezpieczeństwa dokumentów trzymanyh lokalnie i w profesjonalnej chmurze.
4. Cykl życia sprzętu IT - kiedy modernizować, a kiedy wymieniać urządzenia w kontekście ograniczania e-odpadów.
5. Wydłużanie życia sprzętu - dobre praktyki użytkowania i konserwacji urządzeń jako element strategii zrównoważonego rozwoju.
6. Recykling sprzętu i bezpieczne usuwanie danych.
7. Warsztat: plan zabezpieczenia danych i sprzętu w organizacji.

**12:00 - 12:45 Przerwa.**

**12:45 - 14:15 MODUŁ VII: Prywatność, komunikacja i bezpieczeństwo w organizacji.**

1. Cyfrowy ślad i over-sharing. Jak informacje publikowane w social mediach (LinkedIn, FB) ułatwiają hakerom precyzyjne ataki?
2. Narzędzia ochrony prywatności (przełęczarki, blokery).
3. Bezpieczne komunikatory (Signal, WhatsApp) - efektywna i odpowiedzialna komunikacja cyfrowa w organizacji.
4. Ochrona kont firmowych - minimalizacja ryzyka przejęć i strat danych.
5. Tryb incognito - co naprawdę ukrywa, a czego nie?
6. Warsztat: analiza ryzyk i wdrożenie dobrych praktyk z uwzględnieniem ograniczania nadmiarowych danych i optymalizacji ich przechowywania.
7. Jak komunikować zasady cyberbezpieczeństwa w organizacji - budowanie świadomości pracowników w zakresie bezpieczeństwa i odpowiedzialnego korzystania z zasobów cyfrowych.
8. Wprowadzenie do polityki „data minimalism” - ograniczanie przechowywania danych jako element strategii bezpieczeństwa i zrównoważonego rozwoju.

**14:15 - 15:30 MODUŁ VIII: Prawo, procedury i green IT w cyberbezpieczeństwie.**

1. RODO i obowiązki przedsiębiorcy.
2. Zgłaszanie incydentów (CERT Polska).
3. Standardy i dobre praktyki bezpieczeństwa.
4. Green IT:

- cyfrowy minimalizm (redukcja danych, maili, plików),
- wpływ infrastruktury IT na emisję CO2,
- optymalizacja systemów bezpieczeństwa pod kątem zużycia energii.

1. Warsztat: opracowanie procedury reagowania na incydent.

**15:30 - 15:45 Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.**

**15:45 - 16:30 Walidacja (analiza dowodów i deklaracji) i egzamin - test teoretyczny online.**

**\*UWAGI DOTYCZĄCE WALIDACJI:**

Walidacja **przeprowadzana jest w formie ZDALNEJ** [forma zdalna dotyczy tylko i wyłącznie instytucji walidującej i certyfikującej - uczestnicy wypełniają test i realizują ćwiczenia, będąc na sali szkoleniowej] - i podzielona jest na 2 etapy:

- walidację **części praktycznej**: uczestnicy podczas szkolenia wykonują ćwiczenia, gromadząc tym samym dowody pracy własnej i nabycia efektów uczenia się prowadzących do zdobycia umiejętności, pod koniec szkolenia zostają one przesłane do weryfikacji przez instytucję zewnętrzną (analiza dowodów i deklaracji).
- walidację **części teoretycznej**: uczestnicy pod koniec szkolenia wypełniają elektroniczny test teoretyczny, który zostaje przygotowany i przesłany przez instytucję zewnętrzną, na podstawie efektów uczenia się określonych w zakresie kwalifikacji (test teoretyczny online - wynik NIE generuje się automatycznie; egzamin jest weryfikowany przez instytucję zewnętrzną).

Wszystkie narzędzia używane podczas szkolenia działają w przeglądarce (rekomendujemy Google Chrome) - nie jest wymagana instalacja dodatkowego oprogramowania. Specyfikacja sprzętowa: dowolny laptop z minimum 4 GB RAM, procesorem klasy np. Intel Core i3 (lub nowszym) oraz sprawną kartą Wi-Fi.

## Harmonogram

Liczba przedmiotów/zajęć: 14

| Przedmiot / temat zajęć   | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|--------------|-----------------------|---------------------|---------------------|---------------|
| <b>1 z 14</b><br>Przywitanie uczestników, omówienie szkolenia, przeprowadzenie pre-testów w celu oceny początkowego poziomu wiedzy uczestników. | Kamil Urbacz | 04-07-2026            | 08:30               | 08:45               | 00:15         |
| <b>2 z 14</b> MODUŁ I:<br>Anatomia współczesnego ataku i jego wpływ na zasoby organizacji.  | Kamil Urbacz | 04-07-2026            | 08:45               | 10:15               | 01:30         |

| Przedmiot / temat zajęć  | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|--|--------------|-----------------------|---------------------|---------------------|---------------|
| <b>3 z 14</b> MODUŁ II:<br>Psychologia oszustwa i zagrożenia komunikacyjne (Phishing, Smishing, Vishing).  | Kamil Urbacz | 04-07-2026            | 10:15               | 12:00               | 01:45         |
| <b>4 z 14</b> Przerwa.   | Kamil Urbacz | 04-07-2026            | 12:00               | 12:45               | 00:45         |
| <b>5 z 14</b> MODUŁ III:<br>Zarządzanie tożsamością i bezpieczeństwo dostępu.  | Kamil Urbacz | 04-07-2026            | 12:45               | 14:30               | 01:45         |
| <b>6 z 14</b> MODUŁ IV:<br>AI w cyberbezpieczeństwie i efektywność energetyczna systemów.  | Kamil Urbacz | 04-07-2026            | 14:30               | 16:30               | 02:00         |
| <b>7 z 14</b><br>Przywitanie uczestników, krótkie przypomnienie materiału z poprzedniego dnia, sprawdzenie i rozwiązanie ewentualnych trudności na aktualnym etapie szkolenia. | Kamil Urbacz | 05-07-2026            | 08:30               | 08:45               | 00:15         |
| <b>8 z 14</b> MODUŁ V:<br>Bezpieczeństwo sieci i energooszczędna infrastruktura IT.  | Kamil Urbacz | 05-07-2026            | 08:45               | 10:15               | 01:30         |

| Przedmiot / temat zajęć  | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|--|--------------|-----------------------|---------------------|---------------------|---------------|
| <b>9 z 14</b> MODUŁ VI: Ochrona danych i zarządzanie sprzętem w duchu gospodarki obiegu zamkniętego. | Kamil Urbacz | 05-07-2026            | 10:15               | 12:00               | 01:45         |
| <b>10 z 14</b> Przerwa.  | Kamil Urbacz | 05-07-2026            | 12:00               | 12:45               | 00:45         |
| <b>11 z 14</b> MODUŁ VII: Prywatność, komunikacja i bezpieczeństwo w organizacji.                    | Kamil Urbacz | 05-07-2026            | 12:45               | 14:15               | 01:30         |
| <b>12 z 14</b> MODUŁ VIII: Prawo, procedury i green IT w cyberbezpieczeństwie.                       | Kamil Urbacz | 05-07-2026            | 14:15               | 15:30               | 01:15         |
| <b>13 z 14</b> Podsumowanie szkolenia, sesja pytań, przeprowadzenie post-testów.                     | Kamil Urbacz | 05-07-2026            | 15:30               | 15:45               | 00:15         |
| <b>14 z 14</b> Walidacja (analiza dowodów i deklaracji) i egzamin - test teoretyczny online.         | -            | 05-07-2026            | 15:45               | 16:30               | 00:45         |

## 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 | 6 081,12 PLN |

|  |              |
|--|--------------|
| Koszt przypadający na 1 uczestnika netto | 4 944,00 PLN |
| Koszt osobogodziny brutto                | 380,07 PLN   |
| Koszt osobogodziny netto                 | 309,00 PLN   |
| W tym koszt walidacji brutto             | 150,00 PLN   |
| W tym koszt walidacji netto              | 121,95 PLN   |
| W tym koszt certyfikowania brutto        | 200,00 PLN   |
| W tym koszt certyfikowania netto         | 162,60 PLN   |

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Kamil Urbacz

Informatyk, projektant energooszczędnych stron internetowych, ekspert w dziedzinie green marketingu oraz doświadczony trener z wieloletnią praktyką w dziedzinie technologii cyfrowych. Od 2017 roku nieustannie zdobywa doświadczenie w programowaniu i projektowaniu stron i aplikacji webowych (m.in. HTML, Python, WordPress, CSS, Java).

Jako ekspert specjalizuje się w obszarach: generatywnej sztucznej inteligencji i projektowaniu stron internetowych zgodnych z zasadami no-code. Kładzie nacisk na przekazywanie praktycznych umiejętności, dzięki czemu uczestnicy zdobywają wiedzę gotową do natychmiastowego wdrożenia, co stanowi realne wsparcie w ich rozwoju zawodowym.

Doświadczenie zawodowe lub kwalifikacje zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia usługi: m.in.: PARP - Komunikacja marketingowa (2021), PARP - Cyberbezpieczeństwo w MŚP (2021), Google - Podstawy marketingu internetowego (2021), IT & Desktop Computer Support (2021), Google - Foundations of User Experience (UX) Design (2021), Google - Crash Course of Python (2022), Google - Technical Support Fundamentals (2022), Poznaj AI - Praktyka, narzędzia, ciekawostki (2025), Oracle Certified Associate Java Programmer (2025), Climate Change: From Learning to Action (UN-CC Learn, 2025), How to prevent e-waste? (UN-CC Learn, 2025), Gemini Certified Educator (2025), Google & SGH: Wykorzystanie AI w rozwoju firmy (2025).

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Każdy Uczestnik otrzyma **konspekt z materiałami w wersji drukowanej**, który zdecydowanie ułatwia pracę podczas szkolenia, a także posłuży utrwaleniu wiadomości po odbytych szkoleniu. Zapewniamy także notesy i długopisy. Dla chętnych udostępniamy również konspekt w wersji cyfrowej.

## Informacje dodatkowe

**Kontakt do osoby prowadzącej usługę:** [kamil.urbacz@simply.edu.pl](mailto:kamil.urbacz@simply.edu.pl)

Uprzejmie prosimy uczestników **o zabranie ze sobą laptopa**. W przypadku braku dostępu do wymienionego sprzętu lub niemożności jego zabrania na szkolenie, **prosimy o wcześniejsze poinformowanie Dostawcy Usługi**. Dostawca ma możliwość zapewnienia sprzętu **dla każdego Uczestnika**.

**Możliwość zwolnienia z VAT na podstawie:** Dz.U. 2013 poz. 1722 (Rozporządzenie Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień) §3, ust. 1, pkt 14.

## Adres

ul. Henryka Jordana 18

40-043 Katowice

woj. śląskie

Centrum Konferencyjne "Jordana18", budynek Instytutu/Wydziału Nauk Teologicznych Uniwersytetu Śląskiego

## Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

## Kontakt



**Maria Szymak**

**E-mail** [maria.szymak@simply.edu.pl](mailto:maria.szymak@simply.edu.pl)

**Telefon** (+48) 721 324 130