



Szkolenie: Cyberbezpieczeństwo wraz z elementami Green IT.

Numer usługi 2026/03/26/12176/3438872

5 000,00 PLN brutto

5 000,00 PLN netto

208,33 PLN brutto/h

208,33 PLN netto/h

261,33 PLN cena rynkowa ⓘ

ŁĘTOWSKI
CONSULTINGSzkolenia,
Doradztwo, Rozwój
Mateusz Łętowski

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 🕒 24:00 h
- 📅 23.05.2026 do 16.06.2026

★★★★★ 4,8 / 5

1 564 oceny

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Grupą docelową usługi są osoby rozpoczynające swoją przygodę z tematyką cyberbezpieczeństwa i Green IT, a także wszyscy zainteresowani podniesieniem wiedzy w tym obszarze. Program skierowany jest również do pracowników administracji publicznej oraz przedsiębiorstw, którzy chcą rozwijać swoje kompetencje związane z bezpiecznym i odpowiedzialnym korzystaniem z technologii cyfrowych. Szkolenie dedykowane jest osobom dążącym do wdrażania nowoczesnych i ekologicznych rozwiązań w środowisku cyfrowym.

Minimalna liczba uczestników

3

Maksymalna liczba uczestników

10

Data zakończenia rekrutacji

15-05-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Liczba godzin usługi

24

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

Usługa prowadzi do zdobycia wiedzy i praktycznych umiejętności w zakresie cyberbezpieczeństwa oraz Green IT, umożliwiających identyfikację i minimalizację zagrożeń cyfrowych, a także wdrażanie zrównoważonych technologii w organizacjach. Uczestnicy nauczą się stosować nowoczesne narzędzia i strategie wspierające ochronę danych oraz optymalizację zużycia zasobów IT. Szkolenie pozwala na rozwój kompetencji przydatnych zarówno w sektorze prywatnym, jak i publicznym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik stosuje podstawowe zasady i znaczenia cyberbezpieczeństwa oraz Green IT.	Uczestnik wyjaśnia kluczowe pojęcia, wymienia rodzaje zagrożeń i korzyści z wdrożenia Green IT.	Test teoretyczny
Uczestnik identyfikuje i ocenia zagrożenia cyfrowe w organizacji.	Uczestnik analizuje scenariusz ataku i wskazuje odpowiednie środki zapobiegawcze.	Obserwacja w warunkach symulowanych
Uczestnik stosuje narzędzia i metody wspierające cyberbezpieczeństwo.	Uczestnik skutecznie konfiguruje system dwuskładnikowego uwierzytelniania i opisuje proces szyfrowania danych.	Obserwacja w warunkach symulowanych
Uczestnik tworzy plan strategii zasad Green IT w organizacji.	Uczestnik przedstawia plan wdrożenia strategii Green IT w konkretnym środowisku pracy, uwzględniając zarządzanie energią.	Test teoretyczny
Uczestnik tworzy politykę bezpieczeństwa i zrównoważonego rozwoju.	Uczestnik opracowuje dokument polityki bezpieczeństwa lub Green IT zgodnie z wytycznymi.	Test teoretyczny
Uczestnik analizuje przypadki realnych incydentów cyberbezpieczeństwa i Green IT.	Uczestnik omawia przyczyny i skutki incydentów oraz proponuje środki zaradcze.	Obserwacja w warunkach symulowanych
Uczestnik optymalizuje zużycie energii w środowisku IT.	Uczestnik identyfikuje obszary nadmiernego zużycia energii i sugeruje odpowiednie rozwiązania techniczne.	Test teoretyczny
Uczestnik współpracuje w grupie podczas realizacji zadania polegającego na analizie podstawowego zagrożenia cyberbezpieczeństwa z zakresu Green IT.	Uczestnik bierze udział w pracy zespołowej nad wspólnym zadaniem, omawia zaproponowany scenariusz (np. ataku phishingowego lub nadmiernego zużycia energii), dzieli się spostrzeżeniami i współtworzy propozycję działań zapobiegawczych.	Obserwacja w warunkach symulowanych
Uczestnik komunikuje w prosty i zrozumiały sposób zasady cyberbezpieczeństwa w środowisku pracy.	Uczestnik przedstawia dobre praktyki oraz uzasadnia potrzebę ich stosowania, dostosowując komunikację do odbiorców.	Obserwacja w warunkach symulowanych

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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1: Wprowadzenie do Cyberbezpieczeństwa

1. Definicja i znaczenie cyberbezpieczeństwa

- Co to jest cyberbezpieczeństwo?
- Dlaczego jest ważne?

2. Rodzaje zagrożeń cyberbezpieczeństwa

- Wirusy, malware, ransomware
- Ataki phishingowe, DDoS, man-in-the-middle

3. Podstawowe zasady bezpieczeństwa

- Silne hasła i ich zarządzanie
- Dwuskładnikowe uwierzytelnianie
- Aktualizacje oprogramowania i systemów

4. Praktyczne przykłady i case studies

- Analiza rzeczywistych incydentów

Moduł 2: Wprowadzenie do Green IT

1. Definicja i znaczenie Green IT

- Co to jest Green IT?
- Jakie są korzyści dla środowiska i organizacji?

2. Zrównoważone praktyki w IT

- Eko-projektowanie sprzętu komputerowego
- Zarządzanie energią w centrach danych

3. Zielone technologie i inicjatywy

- Wirtualizacja i chmura obliczeniowa
- Recykling i odpowiedzialne użycie sprzętu

4. Praktyczne przykłady i case studies

- Przykłady firm stosujących Green IT

Moduł 3: Zaawansowane Cyberbezpieczeństwo

1. Bezpieczeństwo sieci

- Firewalle i systemy wykrywania intruzów (IDS/IPS)
- VPN i zabezpieczenia sieci bezprzewodowych

2. Bezpieczeństwo aplikacji i danych

- Testy penetracyjne i audyty bezpieczeństwa
- Szyfrowanie danych i zarządzanie kluczami
- Zabezpieczanie gromadzonych danych
- Przesyłanie danych i informacji w sieciach publicznych

3. Zarządzanie incydentami i reakcja na incydenty

- Planowanie i procedury odpowiedzi na incydenty
- Analiza zagrożeń i informatyka śledcza

4. Prawo i regulacje dotyczące cyberbezpieczeństwa

- RODO, HIPAA, NIS2, DORA i inne regulacje

Moduł 4: Implementacja Green IT w organizacji

1. Strategie wdrażania Green IT

- Analiza i planowanie wdrożeń Green IT
- Edukacja pracowników i zmiana kultury organizacyjnej

2. Monitorowanie i optymalizacja zużycia energii

- Narzędzia do monitorowania zużycia energii
- Optymalizacja pracy serwerów i sprzętu IT

3. Zarządzanie cyklem życia sprzętu IT

- Eko-projektowanie, zakup i recykling sprzętu
- Współpraca z dostawcami ekologicznymi

4. Certyfikacje i standardy Green IT

- ISO 14001, Energy Star, i inne standardy

Moduł 5: Cyberbezpieczeństwo i Green IT w Praktyce

1. Omówienie scenariuszy ataków i obrony

- Przykłady realnych ataków hakerskich
- Praktyczne techniki obrony przed atakami

2. Warsztaty optymalizacji energii

- Praktyczne warsztaty z optymalizacji zużycia energii w organizacji
- Narzędzia do monitorowania i zarządzania energią

3. Opracowanie polityki Green IT

- Praca w grupach nad stworzeniem polityki Green IT dla organizacji
- Prezentacja i omówienie wyników prac

4. Podsumowanie i refleksja

- Dyskusja na temat zdobytej wiedzy i praktyk
- Planowanie dalszych działań w zakresie cyberbezpieczeństwa i Green IT

Walidacja odbywa się w ostatnim dniu szkolenia tj. 06.06.2026 r. godzina 15:00-17:00.

Uczestnicy zdobywają informacje poprzez wykłady i prezentacje, a następnie wykorzystują je w praktyce podczas warsztatów i ćwiczeń w ramach każdego modułu szkolenia, gdzie ten zapis został zastosowany.

ROZDZIELNOŚĆ OSOBOWA WALIDACJI: Rozdzielność szkolenia od walidacji - rozdzielność osobowa. Osoba szkoląca nie ocenia wiedzy i umiejętności swoich kursantów w zakresie, w którym nauczała. Kończącą walidację prowadzi odrębna osoba.

Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.

Podczas szkolenia przeprowadzone zostaną pre-testy oraz post-testy wiedzy, egzamin końcowy.

W ramach szkolenia jest 24 godziny zegarowe na co składa się:

- 10 godzin 15 minut zajęć teoretycznych

- 8 godzin i 45 minut zajęć praktycznych

- 6 przerw po 15 minut i 3 przerwy po 30 minut - 3 godziny

- 2 godziny – Walidacja

Program spełnia zakres technologii PRT z obszaru technologii informacyjnych i telekomunikacyjnych oraz technologii ochrony środowiska, w tym m.in.:

4.2 Technologie informacyjne

4.2.4 Technologie wytwarzania oprogramowania

4.2.5 Technologie data mining

4.6 Bezpieczeństwo informacji

4.6.1 Technologie ochrony prywatności danych

4.7 Technologie telekomunikacyjne i informacyjne wspierające przemysł 4.0

4.7.2 Technologie wspierające internet rzeczy (IoT)

4.7.10 Technologie sztucznej inteligencji i uczenia maszynowego

Wynik walidacji przekazywany jest uczestnikowi w dniu jej przeprowadzenia, tj. w ostatnim dniu realizacji usługi. Certyfikat potwierdzający uzyskanie kompetencji wystawiany i nadawany jest w terminie do 3 dni roboczych od dnia zakończenia szkolenia. Łączny przewidywany czas doręczenia certyfikatu uczestnikowi wynosi od 4 do 7 dni roboczych od dnia zakończenia szkolenia, przy czym termin doręczenia uzależniony jest od czasu realizacji usługi przez operatora pocztowego.

Harmonogram

Liczba pozycji harmonogramu: 21

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 21 Moduł 1: Wprowadzenie do Cyberbezpieczeństwa. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu. + PRE-TEST	Marcin Połacik	23-05-2026	09:00	10:45	01:45
2 z 21 Przerwa.	Marcin Połacik	23-05-2026	10:45	11:00	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 21 Moduł 1: Wprowadzenie do Cyberbezpieczeństwa. Zajęcia praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Marcin Połacik	23-05-2026	11:00	12:30	01:30
4 z 21 Przerwa.	Marcin Połacik	23-05-2026	12:30	13:00	00:30
5 z 21 Moduł 2: Wprowadzenie do Green IT. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Marcin Połacik	23-05-2026	13:00	14:45	01:45
6 z 21 Przerwa.	Marcin Połacik	23-05-2026	14:45	15:00	00:15
7 z 21 Moduł 2: Wprowadzenie do Green IT. Zajęcia praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Marcin Połacik	23-05-2026	15:00	17:00	02:00
8 z 21 Moduł 3: Zaawansowane Cyberbezpieczeństwo. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Marcin Połacik	30-05-2026	09:00	10:45	01:45
9 z 21 Przerwa.	Marcin Połacik	30-05-2026	10:45	11:00	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>10 z 21 Moduł 3: Zaawansowane Cyberbezpieczeństwo. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Marcin Połacik	30-05-2026	11:00	12:30	01:30
<p>11 z 21 Przerwa.</p>	Marcin Połacik	30-05-2026	12:30	13:00	00:30
<p>12 z 21 Moduł 3: Zaawansowane Cyberbezpieczeństwo. Zajęcia praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Marcin Połacik	30-05-2026	13:00	14:45	01:45
<p>13 z 21 Przerwa.</p>	Marcin Połacik	30-05-2026	14:45	15:00	00:15
<p>14 z 21 Moduł 4: Implementacja Green IT w organizacji. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Marcin Połacik	30-05-2026	15:00	17:00	02:00
<p>15 z 21 Moduł 4: Implementacja Green IT w organizacji. Zajęcia praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Marcin Połacik	06-06-2026	09:00	10:45	01:45

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 21 Przerwa.	Marcin Połacik	06-06-2026	10:45	11:00	00:15
17 z 21 Moduł 5: Cyberbezpieczeństwo i Green IT w Praktyce. Zajęcia teoretyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Marcin Połacik	06-06-2026	11:00	12:30	01:30
18 z 21 Przerwa.	Marcin Połacik	06-06-2026	12:30	13:00	00:30
19 z 21 Moduł 5: Cyberbezpieczeństwo i Green IT w Praktyce. Zajęcia praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu. + POST TEST	Marcin Połacik	06-06-2026	13:00	14:45	01:45
20 z 21 Przerwa.	Marcin Połacik	06-06-2026	14:45	15:00	00:15
21 z 21 Walidacja (15:00-16:30 Obserwacja w warunkach symulowanych, 16:30-17:00 Test teoretyczny z wynikiem generowanym automatycznie)	-	06-06-2026	15:00	17:00	02:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	

Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	208,33 PLN
Koszt osobogodziny netto	208,33 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Marcin Połacik

Ukończył studia podyplomowe z filologii polskiej oraz studia podyplomowe z informatyki. Posiada uprawnienia MEN oraz kilkunastoletnie praktyczne doświadczenie nauczyciela i wykładowcy. Doświadczenie zdobywał jako lektor i spiker radiowy. Od 2014 roku właściciel i pomysłodawca agencji kreatywnej. Członek zarządu w agencji marketingowej. Realizował szkolenia dla instytucji edukacyjnych i samorządowych, przedstawicieli różnych grup społecznych i zawodów, a także osób zagrożonych wykluczeniem. Zajęcia prowadził w formie zamkniętych i otwartych szkoleń w firmach prywatnych i państwowych, urzędach, szkołach i na uczelniach. Od wielu lat współpracuje z Centrum Szkoleniowo-Doradczym w Zabrze oraz Niepublicznym Centrum Kształcenia Ustawicznego w Mysłowicach. Specjalizuje się w szkoleniach informatycznych na poziomie podstawowym i zaawansowanym, w tym w szkoleniach specjalistycznych, w szkoleniach z działalności biznesowej w świecie cyfrowym oraz z nowoczesnych technologii, a także w szkoleniach z występów publicznych i emisji głosu. W ciągu ostatnich 5 lat przeprowadził 11 szkoleń z zakresu tematyki szkolenia, w których uczestniczyło ponad 100 osób. W ciągu ostatnich 5 lat uczestniczył również w kursach związanych z cyberbezpieczeństwem podnosząc swoją wiedzę i umiejętności - 3 kursy.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Opracowania własne trenera, prezentacja, skrypty szkoleniowe.

Informacje dodatkowe

Dla uczestników z dofinansowaniem min. 70% kwoty szkolenia (minimum dofinansowania 3500,00 zł = 70% kwoty 5000,00 zł netto) - stawka „zw” – „§ 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. - cena 5000,00 netto.

W przypadku uczestników z dofinansowaniem poniżej 70% kwoty szkolenia (poniżej dofinansowania 3500,00 zł = 70% kwoty 5000,00 zł netto) stawka VAT 23% - cena 6150,00 zł brutto

Potwierdzeniem deklaracji zawartych w fiskach złożonych w naborach przeprowadzonych przez Operatorów w okresie do 30.03.2026 r., że usługa będzie prowadzić do uzyskania kwalifikacji, będzie obowiązywała archiwalna wersja karty - wersja 1.

Warunki techniczne

iOS: iOS 11

Windows: Windows 10 kompilacja 14393

Android: Android OS 5.0

Funkcje sieci Web. Najnowsza wersja przeglądarki Safari, Internet Explorer 11, Chrome, Edge lub Firefox

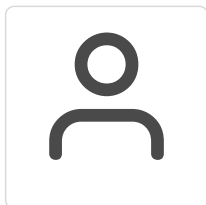
Komputer Mac: MacOS 10.13

Połączenie internetowe: wymagane jest połączenie internetowe przewodowe lub bezprzewodowe (3G, 4G, LTE) o następujących parametrach:

- dla transmisji wideo w jakości HD 720p minimalna przepustowość łącza internetowego wynosi: 1.5Mbps/1.5Mbps (wysyłanie/odbieranie).
- dla transmisji wideo w jakości FullHD 1080p minimalna przepustowość łącza internetowego wynosi: 3Mbps/3Mbps (wysyłanie/odbieranie).

Okres ważności linku: Link będzie ważny w dniach i godzinach wskazanych w harmonogramie usługi.

Kontakt



Oliwia Duch

E-mail oliwiaduch@letowskiconsulting.pl

Telefon (+48) 798 893 087