



Fundacja CODE:ME



## Cybersecurity od podstaw - kurs zdalny / dostępny także dla: projekt Wektor/Gdańsk / Pomorskie / Cała Polska

Numer usługi 2025/03/26/32642/2651006

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 105 h

📅 16.09.2025 do 03.02.2026

9 800,00 PLN brutto

9 800,00 PLN netto

93,33 PLN brutto/h

93,33 PLN netto/h

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	<p><i>Kurs jest przeznaczony dla:</i></p> <ul style="list-style-type: none"> <li>• Specjalistów IT, którzy chcą poszerzyć wiedzę o bezpieczeństwie systemów i sieci.</li> <li>• Managerów IT i liderów zespołów, którzy chcą wdrożyć strategię cyberbezpieczeństwa w swoich organizacjach</li> <li>• Pracowników administracji mających dostęp do danych wrażliwych, danych pracowników</li> <li>• Pracowników sektora finansowego, zdrowotnego i innych branż przetwarzających dane wrażliwe</li> <li>• Młodszych specjalistów, administratorów systemów i sieci, odpowiedzialnych za utrzymanie i ochronę infrastruktury IT</li> <li>• Osób bez technicznego doświadczenia, ale chcących zdobyć podstawowe umiejętności cyberbezpieczeństwa (np. kadra zarządzająca, liderzy projektów)</li> </ul> <p><b>Usługa również adresowana dla Uczestników Projektu Małopolski pociąg do kariery i/lub dla Uczestników Projektu Nowy Start w Małopolsce z EURESem</b></p> <p><b>Usługa adresowana również dla Uczestników Projektu "WEKTOR"</b></p>
<b>Minimalna liczba uczestników</b>	1
<b>Maksymalna liczba uczestników</b>	15
<b>Data zakończenia rekrutacji</b>	12-09-2025
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym

# Cel

## Cel edukacyjny

Po ukończeniu kursu uczestnicy będą potrafili:

- samodzielnie analizować ryzyko cyberbezpieczeństwa organizacji
- projektować skuteczną architekturę zabezpieczeń dostosowaną do specyfiki działalności
- planować oraz symulować wdrażanie rozwiązań cyberbezpieczeństwa
- przygotować kompletną dokumentację dotyczącą bezpieczeństwa informacji
- przeprowadzić audyt bezpieczeństwa informacji, analizować jego wyniki oraz wdrażać usprawnienia

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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Analizuje ryzyko cyberbezpieczeństwa organizacji	<ul style="list-style-type: none"> <li>- identyfikuje i klasyfikuje zagrożenia dla bezpieczeństwa organizacji.</li> <li>- ocenia potencjalne skutki zidentyfikowanych zagrożeń</li> <li>- dokonuje analizy prawdopodobieństwa wystąpienia zagrożeń</li> </ul>	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje skuteczną architekturę zabezpieczeń dostosowaną do specyfiki działalności	<ul style="list-style-type: none"> <li>- tworzy projekt zabezpieczeń uwzględniający specyficzne potrzeby organizacji.</li> <li>- uzasadnia wybór zastosowanych technologii i rozwiązań zabezpieczających.</li> <li>- wskazuje potencjalne słabe punkty w projekcie oraz sposoby ich eliminacji.</li> </ul>	Test teoretyczny z wynikiem generowanym automatycznie
Planuje oraz symuluje wdrażanie rozwiązań cyberbezpieczeństwa	<ul style="list-style-type: none"> <li>- opracowuje szczegółowy harmonogram wdrażania rozwiązań.</li> <li>- wskazuje zasoby niezbędne do realizacji planu.</li> <li>- symuluje scenariusze wdrażania oraz ocenia ich skuteczność.</li> </ul>	Test teoretyczny z wynikiem generowanym automatycznie
Przygotowuje kompletną dokumentację dotyczącą bezpieczeństwa informacji	<ul style="list-style-type: none"> <li>- sporządza kompletną dokumentację zgodnie ze standardami bezpieczeństwa.</li> </ul> <p>(Dokumentacja zawiera procedury zarządzania incydentami oraz polityki bezpieczeństwa. Dokumentacja jest logiczna, przejrzysta oraz możliwa do praktycznego zastosowania).</p>	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza audyt bezpieczeństwa informacji, analizować jego wyniki oraz wdrażać usprawnienia	<ul style="list-style-type: none"> <li>- przeprowadza praktyczny audyt bezpieczeństwa,</li> <li>- gromadzi i interpretuje wyniki.</li> <li>- wskazuje kluczowe problemy oraz przedstawia rekomendacje usprawnień.</li> <li>- ocenia skuteczność zaproponowanych usprawnień oraz uzasadnia ich wybór.</li> </ul>	Test teoretyczny z wynikiem generowanym automatycznie

# Kwalifikacje

## Kompetencje

Usługa prowadzi do nabycia kompetencji.

### Warunki uznania kompetencji

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

Tak, uczestnik otrzymuje dokument, w którym zawarte są efekty uczenia się zrealizowanego kursu.

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

Tak, dokument potwierdza, że walidacja została przeprowadzona zgodnie z ustalonymi kryteriami weryfikacji zawartymi w efektach uczenia się.

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

Tak

# Program

Nie jest wymagane wcześniejsze doświadczenie w cyberbezpieczeństwie, wystarczy podstawowa znajomość obsługi systemów komputerowych i Internetu.

### Zakres tematyczny kursu:

#### 1. Wprowadzenie do Cyberbezpieczeństwa

- Podstawowe zagrożenia i pojęcia
- Wprowadzenie do rozpoznania w cyberprzestrzeni

#### 2. Systemy operacyjne – podstawy

- Podstawy systemów operacyjnych
- Instalacja i konfiguracja zabezpieczeń
- Zarządzanie uprawnieniami użytkowników

#### 3. Zarządzanie ryzykiem i politykami

- Analiza ryzyka w cyberbezpieczeństwie
- Tworzenie polityk bezpieczeństwa

- Zarządzanie incydentami i audyty bezpieczeństwa

#### 4. Bezpieczeństwo danych i urządzeń

- Klasyfikacja danych, szyfrowanie, zarządzanie urządzeniami
- Zabezpieczanie danych z użyciem np. BitLocker, VeraCrypt, EFS
- Procedury backupu oraz zarządzanie urządzeniami mobilnymi

#### 5. Architektura bezpieczeństwa sieci

- Zasady projektowania bezpiecznej sieci
- Konfiguracja firewall i segmentacja sieci

#### 6. Bezpieczeństwo komunikacji i ruchu sieciowego

- Protokoły komunikacyjne i zabezpieczenia
- Konfiguracja VPN i zabezpieczeń sieciowych
- Konfiguracja IDS/IPS oraz analiza logów

#### 7. Zarządzanie Tożsamością i Dostępem (IAM)

- Zarządzanie dostępem, SSO, MFA
- Implementacja Single Sign-On, federacja tożsamości oraz Multi-Factor Authentication
- Audyt i analiza aktywności użytkowników

#### 8. Analiza i Weryfikacja bezpieczeństwa systemów

- Metody testowania, testy penetracyjne
- OSINT
- Praktyczne testy penetracyjne
- Zastosowanie technik OSINT w praktyce

#### 9. Cyberbezpieczeństwo – kluczowe regulacje i standardy

- Różnice między **standardami**, **dyrektywami**, **rozporządzeniami** i **strategiami** w zakresie cyberbezpieczeństwa. Kluczowe regulacje wpływające na organizacje w Polsce i Europie
- zgłaszanie incydentów, testowanie systemów, zarządzanie ryzykiem IT. Wskazanie, które przepisy mają charakter **dobrowolny (np. ISO)**, a które są **obowiązkowe (np. NIS2, DORA)**

#### 10. Bezpieczeństwo w Tworzeniu Oprogramowania

- Secure coding, secure scripting, DevSecOps
- Analiza bezpieczeństwa kodu aplikacji

#### 11. Techniki Obrony w Cyberprzestrzeni

- Zarządzanie incydentami
- Ćwiczenia praktyczne w zakresie obrony/ataku przed zaawansowanymi atakami
- Skanowanie podatności oraz raportowanie
- Implementacja SIEM oraz analiza incydentów bezpieczeństwa

Usługa jest realizowana zdalnie w czasie rzeczywistym, co oznacza, że każdy uczestnik w trakcie zajęć pracuje indywidualnie na swoim komputerze.

Wszystkie szczegóły dotyczące wymagań technicznych zostały opisane poniżej, w sekcji Warunki techniczne.

Usługa prowadzona jest w trybie godzin zegarowych.

Na koniec kursu przeprowadzona jest walidacja w formie testu teoretycznego z wynikiem generowanym automatycznie.

## Harmonogram

Liczba przedmiotów/zajęć: 70

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>1 z 70</b></p> <p>Wprowadzenie do Cyberbezpieczeństwa - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	16-09-2025	17:00	19:00	02:00
<p><b>2 z 70</b></p> <p>Wprowadzenie do Cyberbezpieczeństwa - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	16-09-2025	19:05	20:05	01:00
<p><b>3 z 70</b></p> <p>Wprowadzenie do Cyberbezpieczeństwa - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	18-09-2025	17:00	19:00	02:00
<p><b>4 z 70</b></p> <p>Wprowadzenie do Cyberbezpieczeństwa - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	18-09-2025	19:05	20:05	01:00
<p><b>5 z 70</b> Systemy operacyjne - Podstawy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	23-09-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>6 z 70</b> Systemy operacyjne - Podstawy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	23-09-2025	19:05	20:05	01:00
<b>7 z 70</b> Systemy operacyjne - Podstawy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	25-09-2025	17:00	19:00	02:00
<b>8 z 70</b> Systemy operacyjne - Podstawy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	25-09-2025	19:05	20:05	01:00
<b>9 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	30-09-2025	17:00	19:00	02:00
<b>10 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	30-09-2025	19:05	20:05	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>11 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	02-10-2025	17:00	19:00	02:00
<b>12 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	02-10-2025	19:05	20:05	01:00
<b>13 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	07-10-2025	17:00	19:00	02:00
<b>14 z 70</b> Zarządzanie ryzykiem i politykami - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	07-10-2025	19:05	20:05	01:00
<b>15 z 70</b> Bezpieczeństwo danych i urządzeń - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	09-10-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>16 z 70</b> Bezpieczeństwo danych i urzędzeń - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	09-10-2025	19:05	20:05	01:00
<b>17 z 70</b> Bezpieczeństwo danych i urzędzeń - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	14-10-2025	17:00	19:00	02:00
<b>18 z 70</b> Architektura bezpieczeństwa sieci - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	14-10-2025	19:05	20:05	01:00
<b>19 z 70</b> Architektura bezpieczeństwa sieci - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	16-10-2025	17:00	19:00	02:00
<b>20 z 70</b> Architektura bezpieczeństwa sieci - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	16-10-2025	19:05	20:05	01:00



Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>21 z 70</b> Architektura bezpieczeństwa sieci - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	21-10-2025	17:00	19:00	02:00
<b>22 z 70</b> Architektura bezpieczeństwa sieci - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	21-10-2025	19:05	20:05	01:00
<b>23 z 70</b> Bezpieczeństwo komunikacji i ruchu sieciowego - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	23-10-2025	17:00	19:00	02:00
<b>24 z 70</b> Bezpieczeństwo komunikacji i ruchu sieciowego - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	23-10-2025	19:05	20:05	01:00
<b>25 z 70</b> Bezpieczeństwo komunikacji i ruchu sieciowego - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	28-10-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>26 z 70</b></p> Bezpieczeństwo komunikacji i ruchu sieciowego - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	28-10-2025	19:05	20:05	01:00
<p><b>27 z 70</b></p> Bezpieczeństwo komunikacji i ruchu sieciowego - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	30-10-2025	17:00	19:00	02:00
<p><b>28 z 70</b></p> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	30-10-2025	19:05	20:05	01:00
<p><b>29 z 70</b></p> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	04-11-2025	17:00	19:00	02:00
<p><b>30 z 70</b></p> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	04-11-2025	19:05	20:05	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>31 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	06-11-2025	17:00	19:00	02:00
<b>32 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	06-11-2025	19:05	20:05	01:00
<b>33 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	13-11-2025	17:00	19:00	02:00
<b>34 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	13-11-2025	19:05	20:05	01:00
<b>35 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	18-11-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>36 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłós	18-11-2025	19:05	20:05	01:00
<b>37 z 70</b> Zarządzanie Tożsamością i Dostępem (IAM) - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłós	20-11-2025	17:00	19:00	02:00
<b>38 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłós	20-11-2025	19:05	20:05	01:00
<b>39 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłós	25-11-2025	17:00	19:00	02:00
<b>40 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłós	25-11-2025	19:05	20:05	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>41 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	27-11-2025	17:00	19:00	02:00
<b>42 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	27-11-2025	19:05	20:05	01:00
<b>43 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	02-12-2025	17:00	19:00	02:00
<b>44 z 70</b> Analiza i Weryfikacja bezpieczeństwa systemów - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	02-12-2025	19:05	20:05	01:00
<b>45 z 70</b> Cyberbezpieczeństwo – kluczowe regulacje i standardy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	04-12-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>46 z 70</b></p> <p>Cyberbezpieczeństwo – kluczowe regulacje i standardy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	04-12-2025	19:05	20:05	01:00
<p><b>47 z 70</b></p> <p>Cyberbezpieczeństwo – kluczowe regulacje i standardy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	09-12-2025	17:00	19:00	02:00
<p><b>48 z 70</b></p> <p>Cyberbezpieczeństwo – kluczowe regulacje i standardy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	09-12-2025	19:05	20:05	01:00
<p><b>49 z 70</b></p> <p>Cyberbezpieczeństwo – kluczowe regulacje i standardy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa</p>	Dariusz Kłos	11-12-2025	17:00	19:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>50 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	11-12-2025	19:05	20:05	01:00
<b>51 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	16-12-2025	17:00	19:00	02:00
<b>52 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	16-12-2025	19:05	20:05	01:00
<b>53 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	18-12-2025	17:00	19:00	02:00
<b>54 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	18-12-2025	19:05	20:05	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>55 z 70</b> Bezpieczeństwo w Tworzeniu Oprogramowania ,Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	08-01-2026	17:00	19:00	02:00
<b>56 z 70</b> Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	08-01-2026	19:05	20:05	01:00
<b>57 z 70</b> Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	13-01-2026	17:00	19:00	02:00
<b>58 z 70</b> Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	13-01-2026	19:05	20:05	01:00
<b>59 z 70</b> Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	15-01-2026	17:00	19:00	02:00



Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
60 z 70 Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	15-01-2026	19:05	20:05	01:00
61 z 70 Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	20-01-2026	17:00	19:00	02:00
62 z 70 Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	20-01-2026	19:05	20:05	01:00
63 z 70 Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	22-01-2026	17:00	19:00	02:00
64 z 70 Techniki Obrony w Cyberprzestrzeni - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	22-01-2026	19:05	20:05	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>65 z 70</b> Techniki Obrony w Cyberprzestrzeni, Projekt końcowy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	27-01-2026	17:00	19:00	02:00
<b>66 z 70</b> Projekt końcowy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	27-01-2026	19:05	20:05	01:00
<b>67 z 70</b> Projekt końcowy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	29-01-2026	17:00	19:00	02:00
<b>68 z 70</b> Projekt końcowy - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	29-01-2026	19:05	20:05	01:00
<b>69 z 70</b> Projekt końcowy, Podsumowanie - Sposób realizacji zajęć: współdzielenie ekranu, ćwiczenia, chat, rozmowa	Dariusz Kłos	03-02-2026	17:00	19:00	02:00
<b>70 z 70</b> Walidacja w formie testu teoretycznego z wynikiem generowanym automatycznie	Dariusz Kłos	03-02-2026	19:05	20:05	01:00

# Cennik

## Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 800,00 PLN
Koszt przypadający na 1 uczestnika netto	9 800,00 PLN
Koszt osobogodziny brutto	93,33 PLN
Koszt osobogodziny netto	93,33 PLN

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Dariusz Kłos

Project Manager, Architect IT, współzałożyciel firmy teleinformatycznej. Konsultant z zakresu rozwiązań, architektury i bezpieczeństwa rozwiązań IT od ponad 20 lat. Posiada kompetencje oparte na projektowaniu, wdrażaniu nowych technologii, nadzorowaniu zespołów oraz doświadczenie konsultingowe w zakresie bezpieczeństwa i wdrażania nowych technologii w środowisku biznesowym. Posiada wiele certyfikacji technologicznych i bezpieczeństwa. Na co dzień zajmuje się projektowaniem i integracją mechanizmów zwiększających bezpieczeństwo oraz dynamikę hybrydowej infrastruktury informatycznej. Szkoli z tematyki związanej z bezpieczeństwem infrastruktur sieciowych oraz służących podnoszeniu świadomości cyberzagrożeń. Zajmuje się również przekazywaniem wiedzy związanej z cyberbezpieczeństwem.

W wolnym czasie aktywnie pogłębia swoją wiedzę z zakresu socjotechniki oraz białego wywiadu, bezpieczeństwa działań w sieci oraz z przeciwdziałania dezinformacji tworząc także rozwiązania usprawniające analizę informacji z otwartych źródeł.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Każdy uczestnik przed rozpoczęciem szkolenia otrzyma informacje organizacyjne jak przygotować się do szkolenia.

W trakcie kursu uczestnik otrzyma materiały szkoleniowe w postaci prezentacji (pliki pdf).

### Informacje dodatkowe

Uczestnicy po zakończeniu kursu otrzymają Certyfikat ukończenia kursu.

Organizator kursu, zastrzega sobie, że harmonogram kursu może ulec zmianie w przypadkach niezależnych od organizatora.

Usługa realizowana jest w godzinach zegarowych - za godzinę usługi szkoleniowej rozumie się 60 minut, łącznie 102 godziny.

Przerwy nie są wliczane do czasu trwania usługi.

## Warunki techniczne

- rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa - **zoom**
- minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji - **laptop/komputer z dostępem do Internetu oraz mikrofonem i kamerką** - Zalecamy korzystanie z dwóch monitorów podczas kursu,
- minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik - **stałe połączenie WI-FI/ Internet, minimalna przepustowość 10mb/s**
- niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów - przeglądarka internetowa, przed rozpoczęciem kursu uczestnik otrzyma informacje i instrukcje dotyczące instalacji programu wykorzystywanego podczas szkolenia.
- okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line - **link dostępny jedynie w czasie trwania zajęć (czas rzeczywisty)**

## Kontakt



**Paulina Radwańska - Zubrzycka**

**E-mail** [kontakt@codeme.pl](mailto:kontakt@codeme.pl)

**Telefon** (+48) 732 023 206