



INFOSHARE  
ACADEMY SPÓŁKA  
Z OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ  
★★★★★ 4,6 / 5  
220 ocen

## Kurs CyberSecurity Engineer | forma zdalna w czasie rzeczywistym

Numer usługi 2025/10/24/11051/3103995

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 66 h

📅 19.01.2026 do 13.05.2026

5 500,00 PLN brutto

4 471,54 PLN netto

83,33 PLN brutto/h

67,75 PLN netto/h

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Identyfikatory projektów

Małopolski Pociąg do kariery, Kierunek - Rozwój, Zachodniopomorskie  
Bony Szkoleniowe

### Grupa docelowa usługi

**Kurs CyberSecurity Engineer jest dla osób związanych z IT.**

Dla kogo jest ten kurs?

- znają podstawy systemów operacyjnych (Windows/Linux)
- mają ogólne pojęcie o sieciach komputerowych

Zapisz się, jeśli:

- Interesuje Cię cyberbezpieczeństwo i chcesz rozpocząć w nim karierę
- Lubisz rozwiązywać zagadki i analizować, jak systemy można złamać lub zabezpieczyć
- Chcesz poznać narzędzia i metody pracy pentestera
- Pracujesz w IT i chcesz rozwinąć swoje kompetencje o bezpieczeństwo

**Usługa również adresowana dla Uczestników Projektu MP i/lub dla Uczestników Projektu NSE.**

Usługa rozwojowa adresowana również dla Uczestników projektu Zachodniopomorskie Bony Szkoleniowe.

### Minimalna liczba uczestników

12

### Maksymalna liczba uczestników

14

### Data zakończenia rekrutacji

12-01-2026

|                                 |                                    |
|---------------------------------|------------------------------------|
| Forma prowadzenia usługi        | zdalna w czasie rzeczywistym       |
| Liczba godzin usługi            | 66                                 |
| Podstawa uzyskania wpisu do BUR | Znak Jakości TGLS Quality Alliance |

# Cel

## Cel edukacyjny

Celem kursu jest wprowadzenie uczestnika krok po kroku w kluczowe obszary: od podstaw cyberbezpieczeństwa, przez testy penetracyjne i bezpieczeństwo aplikacji webowych, aż po nowoczesne tematy chmurowe i DevSecOps.

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

| Efekty uczenia się                                        | Kryteria weryfikacji                                                                                                                                                                                 | Metoda walidacji                                      |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Charakteryzuje zasady bezpieczeństwa                      | Opisuje typowe zagrożenia bezpieczeństwa, podstawy modelowania zagrożeń. Charakteryzuje kluczowe pojęcia: exploit, payload, wektory ataku.                                                           | Test teoretyczny z wynikiem generowanym automatycznie |
| Definiuje podstawy sieci i systemów                       | Charakteryzuje model OSI i stos TCP/IP. Opisuje podstawy subnettingu. Charakteryzuje zasady przeprowadzania ataków ARP spoofing, DHCP starvation, MITM.                                              | Test teoretyczny z wynikiem generowanym automatycznie |
| Charakteryzuje narzędzia i metodykę testów penetracyjnych | Stosuje metodykę pentestów (Recon, Scanning, Exploitation, Reporting). Opisuje mechanizmy unikania detekcji (AV/IDS/EDR bypass) i narzędzia do łamania haseł (John the Ripper, Hashcat).             | Test teoretyczny z wynikiem generowanym automatycznie |
| Charakteryzuje bezpieczeństwo aplikacji webowych          | Opisuje najczęstsze podatności webowe (SQLi, XSS, CSRF, SSRF, XXE, RCE). Opisuje testowanie ataków brute force i credential stuffing. Przedstawia sposoby obchodzenia zabezpieczeń przez pentestera. | Test teoretyczny z wynikiem generowanym automatycznie |
| Definiuje bezpieczeństwo chmurowe i DevSecOps             | Charakteryzuje modele chmurowe i typowe ataki w chmurze (misconfigured S3, klucze dostępu).                                                                                                          | Test teoretyczny z wynikiem generowanym automatycznie |
| Definiuje Cyber Threat Intelligence i nowoczesną obronę   | Opisuje podstawy Cyber Threat Intelligence (CTI). Definiuje narzędzia do analizy logów (Sysmon, Graylog, ELK).                                                                                       | Test teoretyczny z wynikiem generowanym automatycznie |

| Efekty uczenia się                          | Kryteria weryfikacji                                                                                            | Metoda walidacji                                      |
|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Charakteryzuje proces projektu pentestowego | Opisuje zasady pełnego projektu pentestowego (Recon → Scanning → Exploitation → Post-Exploitation → Reporting). | 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

**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

Uczestnik po pomyślnym ukończeniu kursu otrzyma Zaświadczenie Instytucji Szkoleniowej oraz certyfikat. Będą to dokumenty świadczące o ukończeniu szkolenia.

Materiały przekazywane kursantom podczas zajęć są udostępniane w formie linków do źródeł, nie udostępniamy ich przed rozpoczęciem szkolenia, a w trakcie zajęć. Przed pierwszymi zajęciami uczestnicy otrzymują prework, są to materiały do samodzielnej nauki przygotowujące do kursu.

Zajęcia będą miały w przeważającej części charakter praktyczny - warsztat i ćwiczenia. Na każdym zajęciach będzie część teoretyczna i ćwiczeniowa.

Zajęcia są realizowane w godzinach zegarowych. W czasie zajęć mogą wystąpić krótkie przerwy, po uzgodnieniu z grupą i trenerem prowadzącym zajęcia. Przerwy wliczone są do czasu trwania kursu.

W ramach tego kursu przygotujesz się do certyfikacji CPTe, która zwiększa Twoją wiarygodność jako specjalisty, podnosi atrakcyjność na rynku pracy i otwiera drogę do dalszych certyfikacji takich, jak OSCP czy CEH. Jeśli uczestnik zdecyduje się podejść do certyfikacji, opłaca ją samodzielnie.

Program Kursu CyberSecurity Engineer:

Moduł 0: Prework.

Moduł 1: Wprowadzenie do bezpieczeństwa:

- Model CIA (Confidentiality, Integrity, Availability) – fundament cyberbezpieczeństwa
- Kluczowe pojęcia: exploit, payload, wektory ataku

- Różne rodzaje testowania: black box, white box, grey box
- Znaczenie prawa i etyki w pracy specjalisty security
- Typowe zagrożenia i realne case studies
- Podstawy modelowania zagrożeń (STRIDE, DFD)

#### Moduł 2: Podstawy sieci i systemów:

- Model OSI i stos TCP/IP
- Protokoły: TCP, UDP, ICMP, DNS
- Podstawy subnettingu
- Narzędzia tcpdump i Wireshark
- Zasady przeprowadzania ataków ARP spoofing, DHCP starvation, MITM
- Różnice między Linux a Windows w kontekście bezpieczeństwa
- Techniki eskalacji uprawnień i poznasz narzędzia LinPEAS, WinPEAS, BloodHound

#### Moduł 3: Narzędzia i metodyka testów penetracyjnych:

- Metodyka pentestów (Recon, Scanning, Exploitation, Reporting)
- Sposób działania narzędzia Metasploit i modułów exploitów/payloadów?
- Praktyczne exploity (np. EternalBlue)
- Mechanizmy unikania detekcji (AV/IDS/EDR bypass)
- Narzędzia do łamania haseł (John the Ripper, Hashcat)
- Rola Social Engineering (phishing, trojany, SET)
- Ataki wspierane przez AI (AI phishing, deepfake)

#### Moduł 4: Bezpieczeństwo aplikacji webowych:

- Najczęstsze podatności webowe (SQLi, XSS, CSRF, SSRF, XXE, RCE)
- Wykorzystanie Burp Suite (proxy, fuzzing, automatyczne skany)
- Enumerowanie katalogów i plików ukrytych (Gobuster, Dirbuster)
- Podstawy bezpieczeństwa API (REST, GraphQL, OpenAPI)
- Testowanie ataków brute force i credential stuffing
- Typowe błędy implementacyjne w JWT i BOLA
- Działanie WAF (Web Application Firewall), walidacja danych, szyfrowanie, security headers
- Sposoby obchodzenia zabezpieczeń przez pentestera

#### Moduł 5: Bezpieczeństwo chmurowe i DevSecOps:

- Modele chmurowe (IaaS, PaaS, SaaS)
- Model odpowiedzialności dzielonej (AWS, Azure, GCP)
- Typowe ataki w chmurze (misconfigured S3, klucze dostępu)
- Użycie ScoutSuite i kube-bench przy audycie
- Idea DevSecOps i shift-left security
- Różnice między SAST i DAST oraz narzędzia (SonarQube, OWASP ZAP)
- SBOM i supply chain attacks

#### Moduł 6: Cyber Threat Intelligence i nowoczesna obrona:

- Podstawy Cyber Threat Intelligence (CTI)
- Korzystanie z VirusTotal, AbuseIPDB, Shodan
- Ramy MITRE ATT&CK
- Sposób działania Blue Team i jego zadania
- Narzędzia do analizy logów (Sysmon, Graylog, ELK)
- Podstawy pracy z EDR (np. CrowdStrike, Defender)

#### Moduł 7: Projekty praktyczne i przygotowanie do egzaminu:

- Realizacja pełnego projektu pentestowego (Recon → Scanning → Exploitation → Post-Exploitation → Reporting)
- Tworzenie raportów zgodne ze standardami CPTe/CEPH
- Realne scenariusze ataków (AD, API)
- Struktura pytań egzaminacyjnych i sposoby podejścia do testów
- Quizy i analiza pytań egzaminacyjnych
- Wskazówki dotyczące zarządzania czasem i przygotowania do egzaminu
- Dalsze ścieżki rozwoju (OSCP, CISSP, inne certyfikacje)

# Harmonogram

Liczba przedmiotów/zajęć: 23

| Przedmiot / temat zajęć                                                | Prowadzący       | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|------------------------------------------------------------------------|------------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 23</div> Podstawy cyberbezpieczeństwa, prawo i etyka          | Mateusz Wiatrzyk | 19-01-2026            | 17:30               | 20:30               | 03:00         |
| <div>2 z 23</div> Krajobraz zagrożeń                                   | Mateusz Wiatrzyk | 21-01-2026            | 17:30               | 20:30               | 03:00         |
| <div>3 z 23</div> Threat Modeling                                      | Mateusz Wiatrzyk | 02-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>4 z 23</div> Podstawy sieci – model OSI i TCP/IP   Ataki sieciowe | Mateusz Wiatrzyk | 04-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>5 z 23</div> Wprowadzenie do systemów operacyjnych                | Mateusz Wiatrzyk | 09-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>6 z 23</div> Privilege escalation                                 | Mateusz Wiatrzyk | 11-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>7 z 23</div> Metodyka pentestów i Recon                           | Mateusz Wiatrzyk | 23-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>8 z 23</div> Scanning i Enumeration                               | Mateusz Wiatrzyk | 25-02-2026            | 17:30               | 20:30               | 03:00         |
| <div>9 z 23</div> Exploitation i narzędzia                             | Mateusz Wiatrzyk | 02-03-2026            | 17:30               | 20:30               | 03:00         |
| <div>10 z 23</div> Post-Exploitation i pivoting                        | Mateusz Wiatrzyk | 04-03-2026            | 17:30               | 20:30               | 03:00         |
| <div>11 z 23</div> Social Engineering                                  | Mateusz Wiatrzyk | 16-03-2026            | 17:30               | 20:30               | 03:00         |
| <div>12 z 23</div> OWASP Top 10 1/2                                    | Mateusz Wiatrzyk | 18-03-2026            | 17:30               | 20:30               | 03:00         |

| Przedmiot / temat zajęć                                                       | Prowadzący       | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|-------------------------------------------------------------------------------|------------------|-----------------------|---------------------|---------------------|---------------|
| <b>13 z 23</b> OWASP Top 10 2/2                                               | Mateusz Wiatrzyk | 23-03-2026            | 17:30               | 20:30               | 03:00         |
| <b>14 z 23</b> Narzędzia do testów webowych                                   | Mateusz Wiatrzyk | 25-03-2026            | 17:30               | 20:30               | 03:00         |
| <b>15 z 23</b> Bezpieczeństwo API                                             | Mateusz Wiatrzyk | 13-04-2026            | 17:30               | 20:30               | 03:00         |
| <b>16 z 23</b> Hardening web                                                  | Mateusz Wiatrzyk | 15-04-2026            | 17:30               | 20:30               | 03:00         |
| <b>17 z 23</b> Podstawy bezpieczeństwa w chmurze                              | Mateusz Wiatrzyk | 20-04-2026            | 17:30               | 20:30               | 03:00         |
| <b>18 z 23</b> DevSecOps                                                      | Mateusz Wiatrzyk | 22-04-2026            | 17:30               | 20:30               | 03:00         |
| <b>19 z 23</b> Threat Intelligence i działania Blue Team                      | Mateusz Wiatrzyk | 04-05-2026            | 17:30               | 20:30               | 03:00         |
| <b>20 z 23</b> Całościowy projekt pentestowy 1/2                              | Mateusz Wiatrzyk | 06-05-2026            | 17:30               | 20:30               | 03:00         |
| <b>21 z 23</b> Całościowy projekt pentestowy 2/2                              | Mateusz Wiatrzyk | 11-05-2026            | 17:30               | 20:30               | 03:00         |
| <b>22 z 23</b> Walidacja za pomocą testu z wynikiem generowanym automatycznie | Mateusz Wiatrzyk | 13-05-2026            | 17:30               | 18:00               | 00:30         |
| <b>23 z 23</b> Przygotowanie do egzaminu                                      | Mateusz Wiatrzyk | 13-05-2026            | 18:00               | 20:30               | 02:30         |

## Cennik

### Cennik

| Rodzaj ceny                               | Cena         |
|-------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika brutto | 5 500,00 PLN |
| Koszt przypadający na 1 uczestnika netto  | 4 471,54 PLN |
| Koszt osobogodziny brutto                 | 83,33 PLN    |
| Koszt osobogodziny netto                  | 67,75 PLN    |

## Prowadzący

Liczba prowadzących: 1



1 z 1

**Mateusz Wiatryk**

Specjalista C#, trener infoShare Academy

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Kursanci otrzymują materiały po każdym bloku tematycznym. Trenerzy udostępniają autorskie materiały.

Materiały będą udostępniane głównie w formie pdf lub power point - prezentacje z zajęć, a także kody źródłowe tworzone na zajęciach.

**Szkolenie będzie prowadzone przez wielu trenerów w zależności od technologii, jak będzie wykładana. Mogą się oni powtarzać. Na koniec kursu mogą podesłać dokładną rozpiskę z imieniem i nazwiskiem trenera, który prowadził w konkretnym dniu szkolenie.**

**Kurs również dedykowany jest dla osób chcących skorzystać z projektu "Małopolski pociąg do kariery"**

**Na zakończenie kursu jest przeprowadzany egzamin końcowy, który jest wymagany do zaliczenia kursu.**

### Warunki uczestnictwa

- konieczność posiadania wbudowanej kamerki, słuchawek, Internetu 3Mb/s download i 3Mb/s upload.
- Laptop/PC z min. 8 GB RAM (preferowane 16 GB), 50+ GB wolnego miejsca
- System: Windows 10/11 (zalecane: WSL2 + Ubuntu), macOS, lub Linux (Ubuntu/Debian)

**Przed zapisaniem się na kursu Kandydat musi przejść proces rekrutacji. W tym celu skontaktuj się z infoShare Academy.**

Uczestnik powinien posiadać umiejętnościami analitycznego myślenia oraz znajomością języka angielskiego umożliwiającą czytanie oraz rozumienie dokumentacji.

### Informacje dodatkowe

Uczestnikowi oferujemy:

- Materiały szkoleniowe i nagrania zajęć – dostępne przez 6 miesięcy po zakończeniu kursu.

- Praca w środowisku labowum – maszyny i narzędzia do ćwiczeń w realistycznych scenariuszach ataków i obrony.
- Zadania praktyczne – ćwiczysz na realnych atakach i obronach systemów
- Ponad 60 godzin nauki – intensywny program krok po kroku, od podstaw po egzaminacyjne przygotowanie.
- Certyfikat ukończenia – potwierdzenie zdobytych kompetencji oraz przygotowanie do międzynarodowego egzaminu CPTE (Mile2).

Zapewniamy:

|   |                                                                        |
|---|------------------------------------------------------------------------|
| + | Slack-a jako narzędzie do komunikacji                                  |
| + | wszystkie niezbędne licencje na oprogramowanie w trakcie trwania kursu |
| + | wsparcie techniczne                                                    |
| + | dostęp do materiałów                                                   |

Zajęcia są nagrywane i udostępniane dla uczestników kursu po każdych zajęciach. Nagrywanie usługi odbywa się za zgodą prowadzących oraz uczestników, co znajduje swoje odzwierciedlenie w umowach zawartych przez wszystkie strony.

Do poszczególnych spotkań będą generowane kolejne linki do platformy zoom, które uczest

## Warunki techniczne

- konieczność posiadania wbudowanej kamerki, słuchawek, Internetu 3Mb/s download i 3Mb/s upload.
- Laptop/PC z min. 8 GB RAM (preferowane 16 GB), 50+ GB wolnego miejsca
- System: Windows 10/11 (zalecane: WSL2 + Ubuntu), macOS, lub Linux (Ubuntu/Debian)

## Kontakt



**Anna Mikulska**

**E-mail** [anna.mikulska@infoshareacademy.com](mailto:anna.mikulska@infoshareacademy.com)

**Telefon** (+48) 730 822 802