



## Kurs CyberSecurity Engineer | forma zdalna w czasie rzeczywistym

Numer usługi 2025/12/19/11051/3222547

6 900,00 PLN brutto  
5 609,76 PLN netto  
104,55 PLN brutto/h  
85,00 PLN netto/h

INFOSHARE  
ACADEMY SPÓŁKA  
Z OGRANICZONĄ  
ODPOWIEDZIALNOŚ  
CIĄ

★★★★★ 4,6 / 5

253 oceny

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 66 h

📅 24.03.2026 do 23.07.2026

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Identyfikatory projektów

Małopolski Pociąg do kariery, Kierunek - Rozwój, Zachodniopomorskie Bony Szkoleniowe, FELB.06.03-IZ.00-0003/24 ZIPH

### 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

17-03-2026

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
Współpracuje z innymi członkami zespołu w organizacji, korzystając z narzędzi do pracy grupowej w celu realizacji wyznaczonego celu lub projektu. Identyfikuje wyzwania związane z wyznaczonym celem, planuje etapy ich realizacji, monitoruje ich wykonanie oraz ocenia ich efektywność.	Współdzieli informacje ze współpracownikami i wykorzystuje narzędzia do pracy nad danymi w ramach zespołów.	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 każdych 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/CPEH
- 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
<b>1 z 23</b> Wprowadzenie do bezpieczeństwa: Podstawy cyberbezpieczeństwa, prawo i etyka - rozmowa na żywo	Paweł Reclaw	24-03-2026	17:30	20:30	03:00
<b>2 z 23</b> Wprowadzenie do bezpieczeństwa: Krajobraz zagrożeń - rozmowa na żywo	Paweł Reclaw	26-03-2026	17:30	20:30	03:00
<b>3 z 23</b> Wprowadzenie do bezpieczeństwa: Threat Intelligence i działania Blue Team - rozmowa na żywo	Paweł Reclaw	14-04-2026	17:30	20:30	03:00
<b>4 z 23</b> Podstawy sieci i systemów: Podstawy sieci – model OSI i TCP/IP   Ataki sieciowe - rozmowa na żywo	Paweł Rączkowski	16-04-2026	17:30	20:30	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>5 z 23</b> Podstawy sieci i systemów: Wprowadzenie do systemów operacyjnych - rozmowa na żywo	Paweł Reclaw	21-04-2026	17:30	20:30	03:00
<b>6 z 23</b> Podstawy sieci i systemów: Privilege escalation - rozmowa na żywo	Patryk Kowalik	23-04-2026	17:30	20:30	03:00
<b>7 z 23</b> Narzędzia i metodyka testów penetracyjnych: Metodyka pentestów i Recon - rozmowa na żywo	Paweł Reclaw	05-05-2026	17:30	20:30	03:00
<b>8 z 23</b> Narzędzia i metodyka testów penetracyjnych: Scanning i Enumeration - rozmowa na żywo	Paweł Reclaw	07-05-2026	17:30	20:30	03:00
<b>9 z 23</b> Narzędzia i metodyka testów penetracyjnych: Exploitation i narzędzia - rozmowa na żywo	Paweł Reclaw	12-05-2026	17:30	20:30	03:00
<b>10 z 23</b> Narzędzia i metodyka testów penetracyjnych: Post-Exploitation i pivoting - rozmowa na żywo	Paweł Reclaw	14-05-2026	17:30	20:30	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>11 z 23</b> Narzędzia i metodyka testów penetracyjnych: Social Engineering - rozmowa na żywo	Paweł Reclaw	26-05-2026	17:30	20:30	03:00
<b>12 z 23</b> Bezpieczeństwo aplikacji webowych: OWASP Top 10 1/2 - rozmowa na żywo	Mateusz Wiatrzyk	28-05-2026	17:30	20:30	03:00
<b>13 z 23</b> Bezpieczeństwo aplikacji webowych: OWASP Top 10 2/2 - rozmowa na żywo	Mateusz Wiatrzyk	09-06-2026	17:30	20:30	03:00
<b>14 z 23</b> Bezpieczeństwo aplikacji webowych: Narzędzia do testów webowych - rozmowa na żywo	Paweł Reclaw	11-06-2026	17:30	20:30	03:00
<b>15 z 23</b> Bezpieczeństwo aplikacji webowych: Bezpieczeństwo API - rozmowa na żywo	Paweł Reclaw	16-06-2026	17:30	20:30	03:00
<b>16 z 23</b> Bezpieczeństwo aplikacji webowych: Hardening web - rozmowa na żywo	Mateusz Wiatrzyk	18-06-2026	17:30	20:30	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>17 z 23</b> Bezpieczeństwo chmurowe i DevSecOps: Podstawy bezpieczeństwa w chmurze - rozmowa na żywo	Mateusz Wiatrzyk	30-06-2026	17:30	20:30	03:00
<b>18 z 23</b> Bezpieczeństwo chmurowe i DevSecOps: DevSecOps - rozmowa na żywo	Mateusz Wiatrzyk	02-07-2026	17:30	20:30	03:00
<b>19 z 23</b> Cyber Threat Intelligence i nowoczesna obrona: Threat Modeling - rozmowa na żywo	Mateusz Wiatrzyk	07-07-2026	17:30	20:30	03:00
<b>20 z 23</b> Projekty praktyczne i przygotowanie do egzaminu: Całościowy projekt pentestowy 1/2 - rozmowa na żywo	Mateusz Wiatrzyk	09-07-2026	17:30	20:30	03:00
<b>21 z 23</b> Projekty praktyczne i przygotowanie do egzaminu: Całościowy projekt pentestowy 2/2 - rozmowa na żywo	Mateusz Wiatrzyk	21-07-2026	17:30	20:30	03:00
<b>22 z 23</b> Walidacja za pomocą testu z wynikiem generowanym automatycznie	Mateusz Wiatrzyk	23-07-2026	17:30	18:00	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>23 z 23</b> Projekty praktyczne i przygotowanie do egzaminu: Przygotowanie do egzaminu - rozmowa na żywo	Mateusz Wiatrzyk	23-07-2026	18:00	20:30	02:30

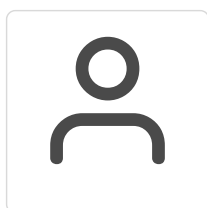
## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 900,00 PLN
Koszt przypadający na 1 uczestnika netto	5 609,76 PLN
Koszt osobogodziny brutto	104,55 PLN
Koszt osobogodziny netto	85,00 PLN

## Prowadzący

Liczba prowadzących: 4



**1 z 4**

### Mateusz Wiatrzyk

Doświadczony trener i lider techniczny, absolwent Politechniki Lubelskiej na kierunku Informatyka (magister inżynier). Ukończył również studia podyplomowe Lider Innowacji w Akademii Leona Koźmińskiego. Z branżą IT związany jest od ponad 13 lat, a od 2017 roku pełni rolę Team Leadera, łącząc kompetencje techniczne z zarządzaniem zespołami i projektami. Specjalizuje się w technologiach .NET, architekturze oprogramowania, tworzeniu aplikacji webowych oraz rozwiązaniach chmurowych i bezpieczeństwie aplikacji. Z infoShare Academy współpracuje od 2023 roku jako trener, projektując i prowadząc szkolenia oraz bootcampy dla programistów i zespołów biznesowych, skoncentrowane na praktycznym wykorzystaniu technologii, realnych problemach projektowych oraz efektywnym zastosowaniu AI w procesie wytwarzania oprogramowania. Posiada wieloletnie doświadczenie komercyjne zdobywane m.in. jako .NET Developer i Team Leader, a także jako lider społeczności developerskiej dotnetomaniak. Pasjonuje się dzieleniem wiedzy, pracą z ludźmi i podnoszeniem kompetencji technicznych zespołów poprzez praktyczne, warsztatowe podejście do nauki.

**2 z 4**



## Paweł Reclaw

Ukończył projekty i budował doświadczenie jako inżynier oraz lider techniczny w obszarze systemów czasu rzeczywistego i rozwiązań krytycznych. W latach 2016–2020 Lead of Software Engineering i Project Managerem w Advanced Protection Systems, gdzie prowadził zespół rozwijający technologie radarowe counter-UAV. Odpowiadał za rozwój software'u i firmware'u radarów, metodyki testów oraz integrację rozwiązań zewnętrznych (m.in. głowice PTZ, kamery dzienne i termalne, detektory oraz jammers RF). Modernizował platformę C2, migrując ją do w pełni skalowalnej, rozproszonej architektury mikroserwisowej o wymaganiach real-time. Od 2020 roku pracował na poziomie Principal/Tech Lead w Pure Storage (FlashBlade Engineering EMEA), realizując inicjatywy związane z konteneryzacją, zarządzaniem kluczami szyfrowania, log management oraz rozwojem control plane, we współpracy z zespołami security i simulation. Prowadził zespół odpowiedzialny za bezpieczeństwo danych. W latach 2021–2024 kontynuował także consulting i utrzymanie produktów APS. Obecnie pracuje jako freelancer, rozwijając projekty dla klientów oraz własne inicjatywy w ramach Smart Software House (ssh). W SDA jest trenerem, a jego pasją pozostają elektronika, telekomunikacja i budowanie niezawodnych i bezpiecznych systemów „end-to-end”.



3 z 4

## Paweł Rączkowski

Specjalista Cyber Security, trener infoShare Academy



4 z 4

## Patryk Kowalik

Specjalista Cyber Security, 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.**

Obecność uczestników potwierdzona będzie za pomocą rejestru logowań. Wymagana obecność to minimum 80% czasu zajęć.

W przypadku kiedy kurs zostanie opłacony środkami publicznymi przez operatora do Dostawcy Usługi i dofinansowanie wynosi co najmniej 70%, cena kursu może zostać zwolniona z podatku VAT, na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień.

## 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

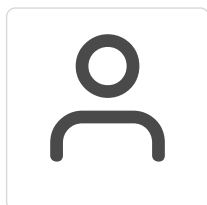
Zajęcia są nagrywane i udostępniane dla uczestników kursu po każdym zajęciach. Nagrywanie usługi odbywa się za zgodą prowadzących oraz uczestników, co znajduje swoje odzwierciedlenie w umowach zawartych przez wszystkie strony.

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