



## Cyberbezpieczeństwo + Pentest + AI | Od podstaw | LearnIT

Numer usługi 2026/05/08/182536/3547008

7 100,00 PLN brutto

7 100,00 PLN netto

50,35 PLN brutto/h

50,35 PLN netto/h

157,50 PLN cena rynkowa ⓘ

LEARN IT SPÓŁKA Z  
OGRA NICZONĄ  
ODPOWIEDZIALNOŚĆ  
CIĄ

★★★★★ 4,7 / 5

15 ocen

- 📄 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 📄 Zajęcia grupowe
- 🕒 141:00 h
- 📅 30.07.2026 do 21.01.2027

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Programowanie

### Identyfikatory projektów

Kierunek - Rozwój, Zachodniopomorskie Bony Szkoleniowe, Regionalny Fundusz Szkoleniowy II

### Grupa docelowa usługi

Szkolenie skierowane do osób dorosłych planujących przebranżowienie do sektora IT, bez wymaganego doświadczenia technicznego, prowadzi „od podstaw” do kompetencji na stanowiska: **Analitik SOC, Junior Pentester, AppSec lub Cloud Security Engineer.**

#### Kluczowe zagadnienia i narzędzia:

- **Fundamenty i Offense:** Linux, Kali Linux, Metasploit, Burp Suite (pentesty aplikacji webowych).
- **Defense & Cloud:** Splunk, Wireshark, AWS, Docker, Kubernetes (Blue Team i DevSecOps).
- **Innowacja AI:** Wykorzystanie AI/MCP w cyberbezpieczeństwie – unikalny moduł na polskim rynku.

**Zielone kompetencje:** Optymalizacja retencji logów i architektury chmurowej w celu redukcji śladu węglowego IT.

#### Dlaczego warto?

1. **Certyfikacja:** Dedykowany moduł przygotowujący do międzynarodowego egzaminu **CompTIA Security+ (SY0-701)**.
2. **Elastyczność:** Zajęcia online na żywo, dwa razy w tygodniu w godzinach wieczornych.
3. **Praktyka:** Nauka narzędzi stosowanych w realnych zespołach bezpieczeństwa.

### Minimalna liczba uczestników

2

### Maksymalna liczba uczestników

30

Data zakończenia rekrutacji

29-07-2026

Forma prowadzenia usługi

zdalna w czasie rzeczywistym

Podstawa uzyskania wpisu do BUR

Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

# Cel

## Cel edukacyjny

Celem kursu jest przygotowanie do pracy jako Junior Cybersecurity Specialist (SOC, Pentester, AppSec). Uczestnik zdobędzie umiejętność mitygacji zagrożeń (OWASP Top 10), analizy incydentów w SIEM (Splunk), zabezpieczania chmury (AWS) i kontenerów (Docker, Kubernetes). Pozna techniki optymalizacji infrastruktury (zielone kompetencje) i przygotuje się do egzaminu CompTIA Security+ SY0-701. Kurs obejmuje też wsparcie w wejściu na rynek pracy (CV, LinkedIn, strategie rekrutacyjne).

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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
obsługuje fundamenty cyberbezpieczeństwa, Linux i sieci komputerowe	<p>Charakteryzuje model ISO/OSI oraz TCP/IP i przypisuje im kluczowe protokoły (HTTP, DNS, SSH, TLS). Analizuje ruch sieciowy w narzędziu Wireshark, identyfikując anomalie i niezasyfrowane dane. Projektuje prostą adresację IP (podsieci) i konfiguruje reguły filtrowania ruchu na zaporze sieciowej (Firewall). Wyjaśnia różnice między szyfrowaniem symetrycznym a asymetrycznym oraz omawia działanie infrastruktury PKI. Zarządza systemem plików z poziomu terminala (nawigacja, edycja plików, uprawnienia chmod/chown). Konfiguruje bezpieczny dostęp zdalny do serwera za pomocą protokołu SSH (klucze RSA/Ed25219, wyłączenie logowania root). Monitoruje procesy systemowe i logi (journalctl, tail, grep) w celu wykrycia podejrzanej aktywności. Tworzy proste skrypty automatyzujące (Bash) do weryfikacji integralności plików lub statusu usług.</p>	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>obsługuje kryptografię, compliance (RODO, NIS2, DORA) oraz Python w automatyzacji security</p>	<p>Dobiera odpowiednie algorytmy szyfrowania (AES, RSA) i funkcje skrótu (SHA-256) do konkretnych scenariuszy ochrony danych.</p> <p>Wskazuje kluczowe obowiązki administratora danych wynikające z RODO oraz wymogi raportowania incydentów w świetle dyrektywy NIS2 i rozporządzenia DORA.</p> <p>Przeprowadza uproszczoną analizę ryzyka dla wybranego procesu biznesowego zgodnie z normą ISO/IEC 27001.</p> <p>Tworzy skrypty automatyzujące powtarzalne zadania bezpieczeństwa (np. skaner portów, parser logów, automatyczny download list IOC).</p> <p>Wykorzystuje biblioteki (np. requests, cryptography) do bezpiecznej komunikacji z API i szyfrowania plików lokalnych.</p> <p>Implementuje prosty mechanizm weryfikacji integralności plików (sprawdzanie sum kontrolnych) za pomocą skryptu.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>
<p>obsługuje pentest aplikacji webowych (OWASP Top 10) oraz infrastruktury i Active Directory</p>	<p>Identyfikuje i eksploatuje podatności z listy OWASP Top 10 (np. SQL Injection, XSS, Broken Access Control) w kontrolowanym środowisku laboratoryjnym.</p> <p>Obsługuje profesjonalny intercepting proxy (Burp Suite) do przechwytywania, analizy i modyfikacji żądań HTTP/S.</p> <p>Wykonuje automatyczny i manualny rekonesans aplikacji w celu wykrycia ukrytych zasobów i błędów konfiguracji.</p> <p>Przeprowadza skanowanie podatności infrastruktury przy użyciu narzędzi takich jak Nmap lub Metasploit Framework.</p> <p>Demonstruje techniki poruszania się wewnątrz domeny AD (np. Password Spraying, LLMNR poisoning) oraz eskalację uprawnień.</p> <p>Wskazuje skuteczne metody mitygacji (poprawki/remediację) dla wykrytych podatności, przygotowując rekomendacje dla działu IT.</p> <p>Dokumentuje przebieg ataku zgodnie z fazami metodyki PTES (od rekonesansu po raportowanie).</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>obsługuje Blue Team, SOC, SIEM (Splunk) oraz incident response zgodnie z NIS2</p>	<p>Konfiguruje reguły detekcji i dashboardy w systemie Splunk, służące do monitorowania podejrzanych logów systemowych i sieciowych.</p> <p>Analizuje korelacje zdarzeń w celu odróżnienia fałszywych alarmów (False Positive) od realnych incydentów bezpieczeństwa.</p> <p>Wyszukuje ślady aktywności intruza (Threat Hunting) przy użyciu języka zapytań (np. SPL) w bazach logów.</p> <p>Przeprowadza pełną procedurę obsługi incydentu (triage, analiza, powstrzymanie, usuwanie skutków) zgodnie z wytycznymi NIST i SANS.</p> <p>Klasyfikuje incydenty pod kątem ich dotkliwości i określa obowiązek ich raportowania zgodnie z wymogami NIS2 (np. incydenty poważne).</p> <p>Przygotowuje raport poincydentalny (Post-Incident Report) zawierający analizę przyczyn źródłowych (Root Cause Analysis) oraz zalecenia naprawcze.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>
<p>obsługuje Cloud Security (AWS, Docker, Kubernetes), DevSecOps i AI/MCP w cyberbezpieczeństwie</p>	<p>Konfiguruje bezpieczne role i polityki dostępu (IAM) w chmurze AWS zgodnie z zasadą najmniejszych uprawnień (Least Privilege).</p> <p>Wykonuje audyt bezpieczeństwa obrazów kontenerowych (Docker) oraz identyfikuje podatności w konfiguracji klastra Kubernetes.</p> <p>Wdraża mechanizmy ochrony danych w chmurze (szyfrowanie at-rest i in-transit) oraz zarządza sekretami.</p> <p>Integruje zautomatyzowane skanery bezpieczeństwa (SAST/DAST) wewnątrz potoku CI/CD, blokując publikację kodu zawierającego krytyczne błędy.</p> <p>Wykorzystuje asystentów AI oraz modele językowe (LLM/MCP) do szybkiej analizy kodu, generowania skryptów obronnych oraz wyjaśniania skomplikowanych logów.</p> <p>Wyjaśnia ryzyka specyficzne dla systemów AI (np. prompt injection) oraz metody zabezpieczania modeli i danych treningowych.</p> <p>Stosuje polityki lifecycle dla danych (zielone kompetencje), optymalizując zużycie zasobów chmurowych i redukując ślad węglowy infrastruktury.</p>	<p>Test teoretyczny z wynikiem generowanym automatycznie</p>

# 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 i fundamenty IT

**Lekcja 1: Wprowadzenie:** Triada CIA, role w branży (SOC, Pentester), analiza incydentów. *Aspekt środowiskowy:* Rola SOC w optymalizacji ruchu sieciowego.

**Lekcja 2: Systemy operacyjne I:** Architektura komputera, proces bootowania, kernel vs user space. *Aspekt środowiskowy:* Dobór energooszczędnych architektur CPU.

**Lekcja 3: Systemy operacyjne II:** Systemy plików, wirtualizacja (VirtualBox). *Aspekt środowiskowy:* Wirtualizacja jako metoda redukcji elektrośmięci.

**Lekcja 4: Internet i komunikacja:** Model klient-serwer, DNS, narzędzia diagnostyczne (ping, curl). *Aspekt środowiskowy:* Cache DNS ograniczający zużycie energii serwerów.

### Moduł 2: Sieci komputerowe i protokoły

**Lekcja 1: Sieci I:** Modele OSI i TCP/IP, hermetyzacja danych. *Aspekt środowiskowy:* Optymalizacja nagłówków w celu zmniejszenia zużycia pasma.

**Lekcja 2: Sieci II:** Protokoły HTTP/HTTPS, SSH, analiza w Wireshark. *Aspekt środowiskowy:* Dobór TCP/UDP a koszty retransmisji danych.

**Lekcja 3: Bezpieczeństwo sieci:** Firewall (NGFW), VPN (WireGuard), IDS/IPS, segmentacja. *Aspekt środowiskowy:* WireGuard jako wydajniejsza i mniej obciążająca CPU alternatywa.

**Lekcja 4: Wireshark i analiza:** Filtrowanie ruchu, wykrywanie ataków w pcap. *Aspekt środowiskowy:* Filtry capture ograniczające zapotrzebowanie na przestrzeń dyskową.

### Moduł 3: Linux dla bezpieczeństwa

**Lekcja 1: Linux I:** Terminal, CLI, potoki (pipes). *Aspekt środowiskowy:* Wykorzystanie pipe'ów zamiast plików tymczasowych (redukcja operacji I/O).

**Lekcja 2: Linux II:** Uprawnienia (chmod, SUID), zarządzanie użytkownikami. *Aspekt środowiskowy:* Zasada najmniejszych uprawnień redukująca koszty remediacji.

**Lekcja 3: Linux III:** Zarządzanie procesami (systemd), logi (journalctl). *Aspekt środowiskowy:* Retencja logów (logrotate) optymalizująca zużycie pamięci.

**Lekcja 4: Bash scripting:** Automatyzacja zadań security, hardening SSH. *Aspekt środowiskowy:* Automatyzacja redukująca czas pracy procesora i zasoby ludzkie.

## Moduł 4: Kryptografia i fundamenty bezpieczeństwa

**Lekcja 1: Modele zagrożeń:** STRIDE, NIST CSF, MITRE ATT&CK. *Aspekt środowiskowy:* Threat modelling redukujący przyszłe koszty energii na naprawę błędów.

**Lekcja 2: Kryptografia I:** AES, RSA, ECC, hashing. *Aspekt środowiskowy:* Wybór kryptografii krzywych eliptycznych (ECC) – krótsze klucze i mniej cykli CPU.

**Lekcja 3: Kryptografia II:** TLS 1.3, PKI, podpisy cyfrowe. *Aspekt środowiskowy:* Szybszy handshake w TLS 1.3 zmniejszający liczbę pakietów w sieci.

**Lekcja 4: Compliance:** RODO, NIS2, DORA, ISO 27001. *Aspekt środowiskowy:* Minimalizacja danych w RODO przekładająca się na niższy ślad węglowy storage'u.

## Moduł 5: Python dla bezpieczeństwa

**Lekcja 1: Python I:** Składnia, struktury danych, kontrola przepływu. *Aspekt środowiskowy:* Optymalizacja struktur pod kątem zużycia RAM.

**Lekcja 2: Python II:** Programowanie obiektowe, venv, narzędzia CLI. *Aspekt środowiskowy:* venv ograniczający zbędny transfer danych.

**Lekcja 3: Python III:** Praca z plikami (JSON, CSV), Regex. *Aspekt środowiskowy:* Przetwarzanie strumieniowe (generatory) zamiast ładowania dużych zbiorów do RAM.

**Lekcja 4: Python IV:** Biblioteka requests, API REST, BeautifulSoup. *Aspekt środowiskowy:* Reuse połączeń TCP (Session) ograniczający narzut sieciowy.

**Lekcja 5: Python V:** Scapy, sockety, tworzenie skanerów portów. *Aspekt środowiskowy:* Celowane skanowanie zamiast brute-force'u sieciowego.

## Moduł 6: Bezpieczeństwo aplikacji webowych (OWASP Top 10)

**Lekcja 1: Wprowadzenie:** Klasyfikacja podatności (CVSS 4.0), Docker w labach. *Aspekt środowiskowy:* Lekkie konteneryzowane środowiska testowe.

**Lekcja 2: Iniekcje:** SQL Injection, Command Injection, SQLMap. *Aspekt środowiskowy:* Precyzyjne payloady redukujące obciążenie serwerów.

**Lekcja 3: Ataki klienckie:** XSS, CSRF, SSRF, polityka CSP. *Aspekt środowiskowy:* CSP redukujące ładowanie zbędnych skryptów zewnętrznych.

**Lekcja 4: Uwierzytelnianie:** JWT, OAuth 2.0, API Security. *Aspekt środowiskowy:* Rate limiting chroniący infrastrukturę przed przeciążeniem.

**Lekcja 5: Praktyka:** Juice Shop CTF – rozwiązywanie wyzwań. *Aspekt środowiskowy:* Współdzielenie zasobów chmurowych przez grupę szkoleniową.

## Moduł 7: Pentest: Kali Linux, Metasploit, AD

**Lekcja 1: Rekonesans:** OSINT, Shodan, Google Dorking. *Aspekt środowiskowy:* Pasywny rekonesans nieobciążający infrastruktury celu.

**Lekcja 2: Skanowanie:** Nmap, enumeracja usług (SMB, SNMP). *Aspekt środowiskowy:* Optymalizacja timingów skanowania (T3) dla stabilności sieci.

**Lekcja 3: Eksploatacja:** Metasploit, Burp Suite, raportowanie. *Aspekt środowiskowy:* Filtrowanie zakresu skanowania w Burp Suite.

**Lekcja 4: Active Directory:** Kerberos, BloodHound, ataki na AD. *Aspekt środowiskowy:* Optymalizacja zapytań LDAP w celu odciążenia kontrolerów domeny.

**Lekcja 5: Praktyka:** Pełny pentest maszyny i tworzenie raportu. *Aspekt środowiskowy:* Raportowanie jako podstawa do szybkiej i energooszczędnej remediacji.

## Moduł 8: Blue Team, SOC i Incident Response

**Lekcja 1: SOC i SIEM:** Role w SOC, obsługa Splunk. *Aspekt środowiskowy:* Indeksowanie tylko niezbędnych logów (oszczędność energii i miejsca).

**Lekcja 2: Detekcja:** Reguły Sigma, Threat Hunting. *Aspekt środowiskowy:* Efektywne zapytania SPL skracające czas pracy serwerów.

**Lekcja 3: Logi Windows:** Sysmon, Event ID, korelacja zdarzeń. *Aspekt środowiskowy:* Filtrowanie zdarzeń Sysmon u źródła.

**Lekcja 4: Incident Response:** Cykl PICERL, Forensics, NIS2. *Aspekt środowiskowy:* Triage zamiast pełnych obrazów dysków (redukcja danych).

**Lekcja 5: Praktyka:** Symulacja incydentu Blue Team CTF. *Aspekt środowiskowy:* Praca na zoptymalizowanych zasobach platformy TryHackMe.

## Moduł 9: Cloud Security i DevSecOps

**Lekcja 1: AWS Security:** VPC, S3, IAM, Shared Responsibility. *Aspekt środowiskowy:* Wybór regionów AWS zasilanych energią odnawialną.

**Lekcja 2: IAM i ataki Cloud:** Eskalacja uprawnień, audyt w Prowler. *Aspekt środowiskowy:* Minimalizacja wywołań API poprzez poprawne polityki IAM.

**Lekcja 3: Kontenery:** Docker hardening, skanowanie Trivy. *Aspekt środowiskowy:* Obrazy typu "distroless" (mniejsza waga, mniejszy transfer).

**Lekcja 4: Kubernetes:** RBAC, Secrets, limity zasobów. *Aspekt środowiskowy:* Limity CPU/RAM zapobiegające marnotrawieniu prądu.

**Lekcja 5: CI/CD:** Shift-left security, GitHub Actions. *Aspekt środowiskowy:* Cache'owanie buildów w celu skrócenia czasu pracy runnerów.

## Moduł 10: AI i MCP w cyberbezpieczeństwie

**Lekcja 1: AI w Cyber:** Detekcja anomalii, phishing LLM. *Aspekt środowiskowy:* Wykorzystanie modeli zoptymalizowanych (Haiku/Flash) dla mniejszego kosztu inferencji.

**Lekcja 2: AI Threats:** Prompt injection, OWASP LLM Top 10. *Aspekt środowiskowy:* Redukcja zbędnych tokenów poprzez skuteczne zabezpieczenia promptów.

**Lekcja 3: MCP:** Model Context Protocol w pracy pentestera. *Aspekt środowiskowy:* MCP jako warstwa ograniczająca redundantne zapytania do modeli.

## Moduł 11: Przygotowanie do CompTIA Security+

**Lekcja 1: Teoria I:** Domeny 1-3 (Architecture, Threats). *Aspekt środowiskowy:* Skupienie na lukach kompetencyjnych zamiast powielania znanych treści.

**Lekcja 2: Teoria II:** Domeny 4-5 (Operations, Management), symulacja egzaminu. *Aspekt środowiskowy:* Skuteczne zdawanie za pierwszym razem (oszczędność zasobów).

## Moduł 12: Przygotowanie do rynku pracy

**Lekcja 1: Rekrutacja:** Budowa CV security i profilu LinkedIn. *Aspekt środowiskowy:* Dokumenty ATS-friendly (optymalizacja procesów cyfrowych).

**Lekcja 2: Projekt dyplomowy:** Prezentacja raportu i obrona. *Aspekt środowiskowy:* Uzasadnienie decyzji projektowych w kontekście zrównoważonego rozwoju.

## Moduł 13: Walidacja końcowa

**Lekcja 1: Egzamin:** Test teoretyczny online z wynikiem generowanym automatycznie. *Aspekt środowiskowy:* Automatyczna ocena i certyfikacja cyfrowa eliminująca zużycie papieru i logistykę.

# Harmonogram

Liczba pozycji harmonogramu: 141

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 141</b> Wprowadzenie do cyberbezpieczeństwa   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	30-07-2026	18:00	19:20	01:20
<b>2 z 141</b> -	Przerwa	-	30-07-2026	19:20	19:35	00:15
<b>3 z 141</b> Wprowadzenie do cyberbezpieczeństwa   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	30-07-2026	19:35	21:00	01:25
<b>4 z 141</b> Systemy operacyjne. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	03-08-2026	18:00	19:20	01:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 141 -	Przerwa	-	03-08-2026	19:20	19:35	00:15
6 z 141 Systemy operacyjne. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	03-08-2026	19:35	21:00	01:25
7 z 141 Systemy operacyjne. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	06-08-2026	18:00	19:20	01:20
8 z 141 -	Przerwa	-	06-08-2026	19:20	19:35	00:15
9 z 141 Systemy operacyjne. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	06-08-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>10 z 141</p> <p>Internet i komunikacja sieciowa   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	10-08-2026	18:00	19:20	01:20
<p>11 z 141 -</p>	Przerwa	-	10-08-2026	19:20	19:35	00:15
<p>12 z 141</p> <p>Internet i komunikacja sieciowa   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	10-08-2026	19:35	21:00	01:25
<p>13 z 141</p> <p>Sieci komputerowe. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	13-08-2026	18:00	19:20	01:20
<p>14 z 141 -</p>	Przerwa	-	13-08-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>15 z 141</b> Sieci komputerowe. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	13-08-2026	19:35	21:00	01:25
<p><b>16 z 141</b> Sieci komputerowe. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	17-08-2026	18:00	19:20	01:20
<p><b>17 z 141</b> -</p>	Przerwa	-	17-08-2026	19:20	19:35	00:15
<p><b>18 z 141</b> Sieci komputerowe. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	17-08-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>19 z 141 Linux. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	20-08-2026	18:00	19:20	01:20
<p>20 z 141 -</p>	Przerwa	-	20-08-2026	19:20	19:35	00:15
<p>21 z 141 Linux. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	20-08-2026	19:35	21:00	01:25
<p>22 z 141 Linux. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	24-08-2026	18:00	19:20	01:20
<p>23 z 141 -</p>	Przerwa	-	24-08-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>24 z 141</b> Linux. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	24-08-2026	19:35	21:00	01:25
<p><b>25 z 141</b> Linux. Część 3   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	27-08-2026	18:00	19:20	01:20
<p><b>26 z 141</b> -</p>	Przerwa	-	27-08-2026	19:20	19:35	00:15
<p><b>27 z 141</b> Linux. Część 3   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	27-08-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 141 Bash scripting   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	31-08-2026	18:00	19:20	01:20
29 z 141 -	Przerwa	-	31-08-2026	19:20	19:35	00:15
30 z 141 Bash scripting   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	31-08-2026	19:35	21:00	01:25
31 z 141 Modele zagrożeń i zarządzanie ryzykiem   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	03-09-2026	18:00	19:20	01:20
32 z 141 -	Przerwa	-	03-09-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>33 z 141</b></p> <p>Modele zagrożeń i zarządzanie ryzykiem   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	03-09-2026	19:35	21:00	01:25
<p><b>34 z 141</b></p> <p>Kryptografia. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	07-09-2026	18:00	19:20	01:20
<p><b>35 z 141</b> -</p>	Przerwa	-	07-09-2026	19:20	19:35	00:15
<p><b>36 z 141</b></p> <p>Kryptografia. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	07-09-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>37 z 141</p> <p>Kryptografia. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	10-09-2026	18:00	19:20	01:20
<p>38 z 141 -</p>	Przerwa	-	10-09-2026	19:20	19:35	00:15
<p>39 z 141</p> <p>Kryptografia. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	10-09-2026	19:35	21:00	01:25
<p>40 z 141</p> <p>Compliance i regulacje   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	14-09-2026	18:00	19:20	01:20
<p>41 z 141 -</p>	Przerwa	-	14-09-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>42 z 141</p> <p>Compliance i regulacje   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	14-09-2026	19:35	21:00	01:25
<p>43 z 141</p> <p>Python. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	17-09-2026	18:00	19:20	01:20
<p>44 z 141</p> <p>-</p>	Przerwa	-	17-09-2026	19:20	19:35	00:15
<p>45 z 141</p> <p>Python. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	17-09-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>46 z 141</p> <p>Python. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	21-09-2026	18:00	19:20	01:20
<p>47 z 141 -</p>	Przerwa	-	21-09-2026	19:20	19:35	00:15
<p>48 z 141</p> <p>Python. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	21-09-2026	19:35	21:00	01:25
<p>49 z 141</p> <p>Python. Część 3   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	24-09-2026	18:00	19:20	01:20
<p>50 z 141 -</p>	Przerwa	-	24-09-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>51 z 141</p> <p>Python. Część 3   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	24-09-2026	19:35	21:00	01:25
<p>52 z 141</p> <p>Python. Część 4   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	28-09-2026	18:00	19:20	01:20
<p>53 z 141</p> <p>-</p>	Przerwa	-	28-09-2026	19:20	19:35	00:15
<p>54 z 141</p> <p>Python. Część 4   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	28-09-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>55 z 141</p> <p>Python. Część 5   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	01-10-2026	18:00	19:20	01:20
<p>56 z 141 -</p>	Przerwa	-	01-10-2026	19:20	19:35	00:15
<p>57 z 141</p> <p>Python. Część 5   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	01-10-2026	19:35	21:00	01:25
<p>58 z 141</p> <p>OWASP Top 10. Wprowadzenie i DVWA   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	05-10-2026	18:00	19:20	01:20
<p>59 z 141 -</p>	Przerwa	-	05-10-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>60 z 141</p> <p>OWASP Top 10. Wprowadzenie i DVWA   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	05-10-2026	19:35	21:00	01:25
<p>61 z 141</p> <p>SQL Injection i Command Injection   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	08-10-2026	18:00	19:20	01:20
<p>62 z 141</p> <p>-</p>	Przerwa	-	08-10-2026	19:20	19:35	00:15
<p>63 z 141</p> <p>SQL Injection i Command Injection   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	08-10-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>64 z 141</b> XSS, CSRF, SSRF   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	12-10-2026	18:00	19:20	01:20
<b>65 z 141</b> -	Przerwa	-	12-10-2026	19:20	19:35	00:15
<p><b>66 z 141</b> XSS, CSRF, SSRF   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	12-10-2026	19:35	21:00	01:25
<p><b>67 z 141</b> Broken authentication, JWT, API security   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	15-10-2026	18:00	19:20	01:20
<b>68 z 141</b> -	Przerwa	-	15-10-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>69 z 141</b> Broken authentication, JWT, API security   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	15-10-2026	19:35	21:00	01:25
<p><b>70 z 141</b> Dzień praktyki – Juice Shop CTF   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	19-10-2026	18:00	19:20	01:20
<p><b>71 z 141</b> -</p>	Przerwa	-	19-10-2026	19:20	19:35	00:15
<p><b>72 z 141</b> Dzień praktyki – Juice Shop CTF   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	19-10-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>73 z 141</b></p> Rekonesans i OSINT   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	26-10-2026	18:00	19:20	01:20
<p><b>74 z 141</b> -</p>	Przerwa	-	26-10-2026	19:20	19:35	00:15
<p><b>75 z 141</b></p> Rekonesans i OSINT   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	26-10-2026	19:35	21:00	01:25
<p><b>76 z 141</b></p> Skanowanie i enumeracja   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	29-10-2026	18:00	19:20	01:20
<p><b>77 z 141</b> -</p>	Przerwa	-	29-10-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>78 z 141</b></p> <p>Skanowanie i enumeracja   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	29-10-2026	19:35	21:00	01:25
<p><b>79 z 141</b></p> <p>Eksploracja. Metasploit. Burp Suite   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	02-11-2026	18:00	19:20	01:20
<p><b>80 z 141</b> -</p>	Przerwa	-	02-11-2026	19:20	19:35	00:15
<p><b>81 z 141</b></p> <p>Eksploracja. Metasploit. Burp Suite   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	02-11-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
82 z 141 Active Directory i Windows enterprise security   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	05-11-2026	18:00	19:20	01:20
83 z 141 -	Przerwa	-	05-11-2026	19:20	19:35	00:15
84 z 141 Active Directory i Windows enterprise security   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	05-11-2026	19:35	21:00	01:25
85 z 141 Dzień praktyki – pentest Vulnerable VM   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	09-11-2026	18:00	19:20	01:20
86 z 141 -	Przerwa	-	09-11-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>87 z 141</b> Dzień praktyki – pentest Vulnerable VM   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	09-11-2026	19:35	21:00	01:25
<p><b>88 z 141</b> SOC i SIEM   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	12-11-2026	18:00	19:20	01:20
<p><b>89 z 141</b> -</p>	Przerwa	-	12-11-2026	19:20	19:35	00:15
<p><b>90 z 141</b> SOC i SIEM   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	12-11-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>91 z 141</p> <p>Detection rules i threat hunting   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	16-11-2026	18:00	19:20	01:20
<p>92 z 141 -</p>	Przerwa	-	16-11-2026	19:20	19:35	00:15
<p>93 z 141</p> <p>Detection rules i threat hunting   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	16-11-2026	19:35	21:00	01:25
<p>94 z 141</p> <p>Logi Windows i AD detection   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	19-11-2026	18:00	19:20	01:20
<p>95 z 141 -</p>	Przerwa	-	19-11-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>96 z 141</b> Logi Windows i AD detection   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	19-11-2026	19:35	21:00	01:25
<p><b>97 z 141</b> Incident Response. Digital Forensics   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	23-11-2026	18:00	19:20	01:20
<p><b>98 z 141</b> -</p>	Przerwa	-	23-11-2026	19:20	19:35	00:15
<p><b>99 z 141</b> Incident Response. Digital Forensics   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	23-11-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>100 z 141</b> Dzień praktyki – Blue Team CTF (TryHackMe)  Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	26-11-2026	18:00	19:20	01:20
<b>101 z 141</b> -	Przerwa	-	26-11-2026	19:20	19:35	00:15
<b>102 z 141</b> Dzień praktyki – Blue Team CTF (TryHackMe)   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	26-11-2026	19:35	21:00	01:25
<b>103 z 141</b> AWS Security – fundamenty   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	30-11-2026	18:00	19:20	01:20
<b>104 z 141</b> -	Przerwa	-	30-11-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>105 z 141</b> AWS Security – fundamenty   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	30-11-2026	19:35	21:00	01:25
<p><b>106 z 141</b> IAM i ataki cloud-native   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	03-12-2026	18:00	19:20	01:20
<p><b>107 z 141</b> -</p>	Przerwa	-	03-12-2026	19:20	19:35	00:15
<p><b>108 z 141</b> IAM i ataki cloud-native   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	03-12-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>109 z 141</b> Bezpieczeństwo kontenerów. Docker   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	07-12-2026	18:00	19:20	01:20
<b>110 z 141</b> -	Przerwa	-	07-12-2026	19:20	19:35	00:15
<b>111 z 141</b> Bezpieczeństwo kontenerów. Docker   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	07-12-2026	19:35	21:00	01:25
<b>112 z 141</b> Kubernetes security – podstawy   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	10-12-2026	18:00	19:20	01:20
<b>113 z 141</b> -	Przerwa	-	10-12-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>114 z 141</b>  Kubernetes security – podstawy   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	10-12-2026	19:35	21:00	01:25
<p><b>115 z 141</b>  DevSecOps w CI/CD   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	14-12-2026	18:00	19:20	01:20
<p><b>116 z 141</b> -</p>	Przerwa	-	14-12-2026	19:20	19:35	00:15
<p><b>117 z 141</b>  DevSecOps w CI/CD   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	14-12-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
118 z 141 AI w cyberbezpieczeństwie   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	17-12-2026	18:00	19:20	01:20
119 z 141 -	Przerwa	-	17-12-2026	19:20	19:35	00:15
120 z 141 AI w cyberbezpieczeństwie   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	17-12-2026	19:35	21:00	01:25
121 z 141 AI threats – prompt injection i pentest aplikacji AI   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	21-12-2026	18:00	19:20	01:20
122 z 141 -	Przerwa	-	21-12-2026	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p><b>123 z 141</b> AI threats – prompt injection i pentest aplikacji AI   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	21-12-2026	19:35	21:00	01:25
<p><b>124 z 141</b> MCP – AI-asystent pentestera   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	28-12-2026	18:00	19:20	01:20
<p><b>125 z 141</b> -</p>	Przerwa	-	28-12-2026	19:20	19:35	00:15
<p><b>126 z 141</b> MCP – AI-asystent pentestera   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	28-12-2026	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>127 z 141</p> <p>CompTIA Security+. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	04-01-2027	18:00	19:20	01:20
<p>128 z 141 -</p>	Przerwa	-	04-01-2027	19:20	19:35	00:15
<p>129 z 141</p> <p>CompTIA Security+. Część 1   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	04-01-2027	19:35	21:00	01:25
<p>130 z 141</p> <p>CompTIA Security+. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	07-01-2027	18:00	19:20	01:20
<p>131 z 141 -</p>	Przerwa	-	07-01-2027	19:20	19:35	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<p>132 z 141</p> <p>CompTIA Security+. Część 2   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	07-01-2027	19:35	21:00	01:25
<p>133 z 141</p> <p>Pierwszy krok do zatrudnienia   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	11-01-2027	18:00	19:20	01:20
<p>134 z 141</p> <p>-</p>	Przerwa	-	11-01-2027	19:20	19:35	00:15
<p>135 z 141</p> <p>Pierwszy krok do zatrudnienia   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.</p>	Zajęcia	ANDRZEJ SZESZKO	11-01-2027	19:35	21:00	01:25

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
136 z 141 Obrona projektu dyplomowego   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	14-01-2027	18:00	19:20	01:20
137 z 141 -	Przerwa	-	14-01-2027	19:20	19:35	00:15
138 z 141 Obrona projektu dyplomowego   Zajęcia teoretyczno-praktyczne. Zajęcia w formie wykładu, rozmowy na żywo, chatu oraz współdzielenie ekranu.	Zajęcia	ANDRZEJ SZESZKO	14-01-2027	19:35	21:00	01:25
139 z 141 -	Walidacja	-	21-01-2027	18:00	19:20	01:20
140 z 141 -	Przerwa	-	21-01-2027	19:20	19:35	00:15
141 z 141 -	Walidacja	-	21-01-2027	19:35	21:00	01:25

## Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	81:00
w tym suma godzin zajęć	66:30
w tym suma godzin walidacji	02:45
w tym suma przerw	11:45

Rodzaj godzin

Liczba godzin

Suma godzin dydaktycznych bez przerw

92:15

# Cennik

## Cennik

Rodzaj ceny	Cena
<b>Koszt przypadający na 1 uczestnika brutto</b>	7 100,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
<b>Koszt przypadający na 1 uczestnika netto</b>	7 100,00 PLN
<b>Koszt osobogodziny brutto</b>	50,35 PLN
<b>Koszt osobogodziny netto</b>	50,35 PLN

## Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	141:00

# Prowadzący

Liczba prowadzących: 4



1 z 4

## ANDRZEJ SZESZKO

Jestem profesjonalnym programistą i modelarzem danych z wykształceniem w zakresie danych przestrzennych, UML oraz GIS (tytuł magistra inżyniera). W ciągu ostatnich kilku lat zdobyłem doświadczenie zawodowe jako programista oraz praktyczną wiedzę z zakresu tworzenia aplikacji webowych z wykorzystaniem różnorodnych narzędzi, ze szczególnym uwzględnieniem języka Python i frameworka Django, a także narzędzi z obszaru cyberbezpieczeństwa. Moje doświadczenie akademickie pozwoliło mi pogłębić znajomość fundamentów IT oraz rozwinąć umiejętności efektywnego przekazywania wiedzy. Uczestniczyłem w projektach o znaczeniu krajowym i międzynarodowym, takich jak Geospatial Foundation Theme Governance dla Królestwa Arabii Saudyjskiej oraz Greek Local Spatial Plans Data Model, co umożliwiło mi współpracę z zespołami międzynarodowymi, w których kluczowa była skuteczna komunikacja. W swojej pracy programistycznej i security aktywnie stosuję zasady zielonych kompetencji cyfrowych: projektuję rozwiązania o niskim zużyciu zasobów obliczeniowych, optymalizuję zapytania, retencję logów i

struktury danych pod kątem efektywności energetycznej, a także wdrażam dobre praktyki zmniejszające ślad węglowy aplikacji – takie jak świadomy dobór algorytmów, minimalizacja zbędnych operacji I/O oraz odpowiedzialne zarządzanie infrastrukturą. Ma doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.



2 z 4

## PAWEŁ PIETRASZKO

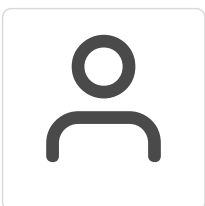
Ekspert w dziedzinie inżynierii oprogramowania i automatyzacji z wieloletnim doświadczeniem zdobytym zarówno w sektorze komercyjnym, jak i projektach badawczo-rozwojowych. Specjalizuje się w tworzeniu rozwiązań na styku software i hardware, kładąc szczególny nacisk na jakość kodu, wydajność przetwarzania danych oraz niezawodność systemów – kompetencje istotne także w obszarze cyberbezpieczeństwa. Biegłość w językach wysokiego poziomu (Python, Java, C#, JavaScript/PHP) oraz systemowych (C++), co pozwala na elastyczne dopasowanie technologii do wymagań projektu, w tym do narzędzi security. Quality Assurance & Test Automation: Doświadczenie jako SDET (Software Development Engineer in Test) w projektowaniu zaawansowanych frameworków do testów automatycznych, w tym testów bezpieczeństwa. Integracja Sprzętowa: Tworzenie aplikacji pracujących blisko fizycznych komponentów i systemów pomiarowych. Optymalizacja Procesów: Projektowanie i wdrażanie autorskich narzędzi automatyzujących powtarzalne operacje, co realnie przekłada się na oszczędność czasu i redukcję błędów ludzkich. W pracy dydaktycznej i projektowej stawia na praktyczne zastosowanie technologii. Dzięki doświadczeniu w testowaniu, promuje podejście "Quality First", ucząc nie tylko jak pisać kod, ale jak tworzyć systemy odporne na błędy i łatwe w utrzymaniu – co bezpośrednio przekłada się na bezpieczeństwo aplikacji. Ma doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.



3 z 4

## Paweł Wyżykowski

Programista. Technologie: Python, JavaScript, SQL. Programista back-end z ponad 5-letnim doświadczeniem w branży IT, specjalizujący się w komercyjnym tworzeniu aplikacji serwerowych w języku Python, ze szczególnym uwzględnieniem aspektów bezpieczeństwa. Posiada praktyczne doświadczenie w projektowaniu, implementacji i utrzymaniu backendów opartych o Python, w tym pracy z frameworkami webowymi, przetwarzaniem danych, integracjami API oraz logiką biznesową aplikacji. W swojej pracy wykorzystuje nowoczesne podejście do wytwarzania oprogramowania, obejmujące m.in. konteneryzację (Docker), pracę z bazami danych, tworzenie skalowalnych usług backendowych oraz współpracę z zespołami frontendowymi. W codziennej praktyce programistycznej stosuje zasady zielonych kompetencji cyfrowych – projektuje energooszczędny kod, optymalizuje zapytania i struktury danych oraz minimalizuje zbędne operacje obliczeniowe, ograniczając ślad środowiskowy tworzonych aplikacji. Doświadczenie dydaktyczne oraz praca projektowa pozwalają mu skutecznie przekazywać wiedzę i tłumaczyć zagadnienia programistyczne i security w sposób praktyczny i zrozumiały dla uczestników szkoleń. Ma doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.



4 z 4

## Leszek Bartmiński

Jestem Python Developerem oraz certyfikowanym inżynierem DevOps z ponad 5-letnim doświadczeniem w branży IT. Komercyjnie pracuję niemal wyłącznie w Pythonie, realizując projekty programistyczne i automatyzacyjne, w tym z obszaru cyberbezpieczeństwa. Moje kompetencje obejmują m.in. Docker, Kubernetes, Terraform, Jenkins oraz narzędzia monitorujące (ELK, Grafana), co pozwala mi łączyć wiedzę programistyczną z praktyką inżynierii chmurowej, automatyzacji i security, w tym projektowania energooszczędnych rozwiązań infrastrukturalnych zgodnych z zasadami zielonych kompetencji cyfrowych. Pełniłem rolę trenera i mentora – m.in. prowadziłem pierwszą edycję Akademii DevOps w Onwelo SA, w ramach której szkoliłem pracowników i

uczestników w zakresie nowoczesnych narzędzi DevOps, programowania w Pythonie i dobrych praktyk w pracy zespołowej. Mam doświadczenie w prowadzeniu zarówno szkoleń technicznych, jak i techniczno-językowych (filologia angielska), co ułatwia mi skuteczne przekazywanie wiedzy, dostosowane do poziomu uczestników. Jako inżynier informatyki oraz magister filologii angielskiej łączę kompetencje techniczne z umiejętnościami dydaktycznymi i komunikacyjnymi. W pracy trenerskiej stawiam na praktykę, przykłady z realnych projektów oraz aktywizację uczestników, aby zdobyte umiejętności mogli od razu wykorzystać w środowisku zawodowym. Ma doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą publikacji usługi w BUR.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

Uczestnicy kursu otrzymują dostęp do kompletnego zestawu materiałów edukacyjnych, w tym autorskich podręczników, prezentacji, przykładów kodu oraz nagrań wszystkich zajęć, co umożliwia naukę w indywidualnym tempie i powrót do omawianych treści w dowolnym momencie.

Dodatkowo kursanci korzystają ze wskazówek przygotowanych przez Doradcę Kariery, które obejmują m.in. tworzenie skutecznego CV oraz budowanie profesjonalnego profilu na LinkedIn – z uwzględnieniem wymagań branży IT i specyfiki rekrutacji na stanowisko Junior Python Developera.

Nasza usługa została przygotowana w zgodzie z założeniami programu **Zielone Kompetencje**, co oznacza, że w trakcie kursu uczestnicy rozwijają również umiejętności wspierające zrównoważony rozwój, efektywne wykorzystanie zasobów i technologii przyjaznych środowisku – zgodnie z aktualnymi trendami i oczekiwaniami rynku pracy.

#### Weryfikacja obecności i frekwencji

Obecność uczestników będzie weryfikowana poprzez:

- system LMS, w którym generowane są listy obecności z każdego spotkania online,
- raporty z platformy (czas logowania, czas aktywności),
- potwierdzenie obecności przez trenera prowadzącego.

Wymagana minimalna frekwencja do zaliczenia kursu wynosi **80%**.

#### Dodatkowe elementy monitorowania postępów

- Uczestnicy zobowiązani są do systematycznego wykonywania zadań domowych, które są weryfikowane w systemie LMS.
- Każda sesja jest nagrywana, a nagrania są udostępniane w LMS, co umożliwia weryfikację przebiegu zajęć oraz ewentualne uzupełnienie wiedzy przez uczestników.
- Brak realizacji wymaganych zadań oraz niewystarczająca obecność (poniżej 80%) skutkuje niezaliczeniem szkolenia i brakiem możliwości otrzymania dokumentu potwierdzającego kompetencje.

*Z przyczyn niezależnych od Wykonawcy (np. losowych) harmonogram szkolenia może zostać nieznacznie zmieniony. Wszystkie informacje dostępne w jednostce szkolejcej zostaną przekazane Operatorowi*

Walidacja efektów uczenia się jest wliczona w czas trwania usługi i zostanie przeprowadzona na zakończenie szkolenia w formie testu teoretycznego z wynikiem generowanym automatycznie

#### Warunki organizacyjne szkolenia

Szkolenie online w czasie rzeczywistym w małych grupach, z samodzielnym stanowiskiem komputerowym i testem końcowym online.

Nasz kurs to intensywna, praktyczna ścieżka do zawodu Junior Python Developera. Uczymy w czasie rzeczywistym – Godzina szkoleniowa trwa 45 minut, przerwy w usłudze są wliczone w czas usługi rozwojowej. Łącznie 188 godziny dydaktyczne, w tym 20% (37,6 g) zajęć teoretycznych i 80% (150,4 g) praktycznych.

#### Informacje dodatkowe

Szkolenie realizowane w obszarze technologii informacyjnych (4.2 PRT), obejmujące programowanie w języku Python z zastosowaniem w modelowaniu i symulacji procesów (4.4 PRT) oraz automatyzacji wspierającej transformację cyfrową przedsiębiorstw w kierunku przemysłu 4.0 (4.7 PRT). Usługa powiązana z Programem Rozwoju Technologii Województwa Śląskiego 2019-2030 (PRT) w zakresie:

technologii informacyjnych (4.2), modelowania i symulacji procesów (4.4) oraz technologii wspierających przemysł 4.0 (4.7).

**Certyfikat potwierdzający ukończenie szkolenia zostanie wydany uczestnikowi w ciągu 5 dni roboczych od daty zakończenia usługi.**

## Informacje dodatkowe

Zapewniamy:

- ✔ praktyczną wiedzę i umiejętności zgodne z wymaganiami rynku IT
- ✔ wsparcie mentorów i trenerów z doświadczeniem komercyjnym
- ✔ doradztwo kariery – pomoc w stworzeniu profesjonalnego CV, profilu na LinkedIn i GitHub
- ✔ zajęcia na żywo online, prowadzone w małych grupach poprzez platformę Zoom.

Szkolenie prowadzone jest przez zespół ekspertów – każdy temat omawiany jest przez dedykowanego trenera, co gwarantuje najwyższą jakość nauki.

Po ukończeniu kursu uczestnik otrzymuje oficjalne zaświadczenie potwierdzające zdobyte kompetencje.

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

Kolejna edycja usługi przewidziana jest w przeciągu najbliższych **1,5 – 2 miesięcy**.

**Usługa zwolniona z podatku VAT na podstawie art. 43 ust. 1 pkt 29 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. 2004 nr 54 poz. 535 z późn. zm.), jeśli jest finansowana w co najmniej 70% ze środków publicznych.**

## Warunki techniczne

**Minimalne wymagania** sprzętowe obejmują komputer z systemem operacyjnym Windows 10, macOS lub Linux. **Rekomendowana konfiguracja** to procesor klasy i5 lub wyższy, co najmniej 16 GB pamięci RAM oraz dysk SSD dla płynnej pracy z maszynami wirtualnymi (VirtualBox, Kali Linux, Vulnerable VM, Docker).

Niezbędne jest również **posiadanie kamery internetowej, słuchawek oraz stabilnego łącza internetowego** o prędkości min. 5 Mb/s (zarówno dla pobierania, jak i wysyłania danych) – zwiększone wymagania w stosunku do standardowych szkoleń, ze względu na pracę z chmurą AWS, platformami CTF (TryHackMe, Hack The Box) i przesyłanie obrazów dyskowych w ćwiczeniach forensicznych.

**Wszystkie zajęcia – zarówno część teoretyczna, jak i praktyczna (warsztaty i projekty) – realizowane są w formie zdalnej, na żywo, za pośrednictwem platformy Zoom.**

## Kontakt



**SIARHEI HLEBKA**

**E-mail** s.glebko@learnit.com.pl

**Telefon** (+48) 571 500 809