

## **AI-Driven Devsecops w Środowiskach Chmurowych**

**Kod przedmiotu: DDSC**

**Rodzaj przedmiotu: obieralny**

**Specjalność: Cyberbezpieczeństwo i AI**

**Wydział: Informatyki**

**Kierunek: Informatyka**

**Poziom studiów: pierwszego stopnia – VI poziom PRK**

**Profil studiów: praktyczny**

**Forma studiów: stacjonarna/niestacjonarna**

**Rok: 3**

**Semestr: 5**

**Formy zajęć i liczba godzin:**

**Forma stacjonarna**

- wykłady – 30
- laboratorium – 45

**Forma niestacjonarna**

- wykłady – 15
- laboratorium – 20

**Zajęcia prowadzone są w języku polskim.**

**Liczba punktów ECTS: 6**

**Osoby prowadzące:**

**wykład:**

**laboratorium/projekt:**

---

### **1. Założenia i cele przedmiotu**

Przedmiot uczy, jak w sposób zautomatyzowany integrować bezpieczeństwo z cyklem życia oprogramowania (CI/CD) w środowiskach chmurowych, wykorzystując do tego nowoczesne narzędzia oparte na sztucznej inteligencji. Studenci poznają w praktyce metodykę DevSecOps, ucząc się budować potoki wdrożeniowe, które potrafią samodzielnie skanować kod, analizować luki w kontenerach oraz blokować niebezpieczne wdrożenia (np. wycieki kluczy API) dzięki modelom AI pracującym w tle. Jest to kurs zorientowany na pracę projektową i symulujący rzeczywiste środowisko pracy inżyniera. Cele:

- Zrozumienie metodyki DevSecOps oraz architektury potoków CI/CD (Continuous Integration / Continuous Deployment) w chmurze.
- Nabycie umiejętności integracji narzędzi testowania bezpieczeństwa (SAST, DAST) wspieranych przez AI w zautomatyzowanych procesach wdrożeniowych.
- Praktyczne zbudowanie i zabezpieczenie środowiska opartego na kontenerach i infrastrukturze jako kodzie (IaC) z uwzględnieniem najlepszych rynkowych praktyk bezpieczeństwa.

## 2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Znajomość podstaw programowania (np. Python, Bash) oraz systemów kontroli wersji (Git).
- Podstawowa wiedza z zakresu sieci komputerowych i systemów operacyjnych z rodziny Linux.
- Zrozumienie podstawowych pojęć związanych z technologiami chmurowymi.

## 3. Opis form zajęć

### a) Wykłady

#### • Treści programowe:

1. Wprowadzenie do DevSecOps: Ewolucja od DevOps do DevSecOps. Cykl życia oprogramowania (SDLC) a bezpieczeństwo. Kultura "Shift-Left".
2. Infrastruktura jako kod (IaC): Koncepcje deklaratywnego zarządzania infrastrukturą. Wprowadzenie do Terraform.
3. Konteneryzacja i jej bezpieczeństwo: Architektura Dockera. Zagrożenia w obrazach kontenerów i metody ich minimalizacji.
4. Narzędzia analityczne i rola AI: Skanery SAST (Static Application Security Testing), DAST (Dynamic Application Security Testing) i SCA (Software Composition Analysis). Wykorzystanie modeli językowych (LLM) do weryfikacji kodu.
5. Zarządzanie sekretami i tożsamością w chmurze: IAM (Identity and Access Management), bezpieczne przechowywanie kluczy API i haseł.

#### • Metody dydaktyczne:

Wykład prowadzony jest w formie prezentacji multimedialnej, uzupełnionej przykładami, analizą przypadków oraz dyskusją nad praktycznymi zastosowaniami prezentowanych treści.

#### • Forma i warunki zaliczenia:

Egzamin pisemny w formie sprawdzianu końcowego, obejmujący najważniejsze zagadnienia z całości wykładów. Warunkiem uzyskania oceny pozytywnej jest udzielenie poprawnej odpowiedzi na co najmniej połowę pytań egzaminacyjnych

#### • Wykaz literatury podstawowej:

1. Zhu, L., et al. (2022). DevSecOps: A Leader's Guide to Producing Secure Software Without Compromising Flow, Feedback and Continuous Improvement.
2. Oficjalna dokumentacja narzędzi: GitLab CI/CD, GitHub Actions, Docker.
3. Wytyczne OWASP (Open Worldwide Application Security Project) dotyczące bezpieczeństwa CI/CD.

#### • Wykaz literatury uzupełniającej:

1. Pytel, M. (2021). Infrastruktura jako kod. Wzorce i antywzorce.
2. Materiały i dokumentacja narzędzi Snyk oraz SonarQube z zakresu integracji AI (AI-assisted coding and scanning).

### b) Laboratorium

#### • Treści programowe :

1. Realizacja ćwiczeń praktycznych zgodnych z zakresem przedmiotu.
2. Analiza przypadków i rozwiązywanie problemów praktycznych.
3. Opracowanie projektu końcowego związanego z tematyką przedmiotu.

• **Metody dydaktyczne:**

W trakcie zajęć prowadzący omawia zagadnienia związane z realizacją poszczególnych laboratoriów, a następnie studenci samodzielnie lub zespołowo realizują zadania określone przez prowadzącego. Metoda laboratoryjna – ćwiczenia laboratoryjne z wykorzystaniem komputerów

• **Forma i warunki zaliczenia:**

Warunkiem zaliczenia jest aktywne uczestnictwo w zajęciach, wykonanie ćwiczeń laboratoryjnych, oraz realizacja projektu końcowego.

• **Wykaz literatury podstawowej:**

- Jak w przypadku wykładu.

• **Wykaz literatury uzupełniającej:**

- Jak w przypadku wykładu.

**4. Opis sposobu wyznaczania punktów ECTS**

**a. forma stacjonarna**

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	30
	Czytanie wskazanej literatury	10
	Przygotowanie do egzaminu	10
Laboratorium	Kontakt z nauczycielem	45
	Czytanie wskazanej literatury	10
	Wykonanie zadań laboratoryjnych	19
	Przygotowanie projektu	20
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
<b>Całkowita ilość godzin aktywności studenta</b>		<b>150</b>
<b>Liczba punktów ECTS dla modułu/przedmiotu</b>		<b>6</b>

**a. forma niestacjonarna**

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	15
	Czytanie wskazanej literatury	15
	Przygotowanie do egzaminu	20
Laboratorium	Kontakt z nauczycielem	20

	Czytanie wskazanej literatury	24
	Wykonanie zadań laboratoryjnych	20
	Przygotowanie projektu	30
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
<b>Całkowita ilość godzin aktywności studenta</b>		<b>150</b>
<b>Liczba punktów ECTS dla modułu/przedmiotu</b>		<b>6</b>

## 5. Wskaźniki sumaryczne

### a. forma stacjonarna

- liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
  - Liczba godzin kontaktowych – 81
  - Liczba punktów ECTS – 3,2
- liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
  - Liczba godzin kontaktowych – 45
  - Liczba punktów ECTS – 3,8

### b. forma niestacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
  - Liczba godzin kontaktowych – 41
  - Liczba punktów ECTS – 1,6
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
  - Liczba godzin kontaktowych – 20
  - Liczba punktów ECTS – 3,8

## 6. Zakładane efekty uczenia się

<b>Efekt przedmiotowy (Symbol)</b>	<b>Efekty uczenia się dla przedmiotu</b>	<b>Odniesienie do kierunkowych efektów uczenia się</b>
DDSC_01	... Zna i rozumie zasady bezpiecznego wytwarzania oprogramowania, cykl CI/CD oraz mechanizmy integracji zabezpieczeń opartych na AI w środowiskach chmurowych.	K_W13, K_W04
DDSC_02	... Potrafi zaprojektować i zaimplementować bezpieczny potok CI/CD, wykorzystując konteneryzację (Docker) i narzędzia do automatycznego skanowania kodu.	K_U10, K_U11
DDSC_03	... Umie wykorzystać asystentów AI i zaawansowane skanery do identyfikacji i naprawy podatności w kodzie oraz konfiguracji infrastruktury (IaC).	K_U12, K_U22

DDSC_04	... Rozumie wagę automatyzacji w zapewnieniu bezpieczeństwa i potrafi efektywnie współpracować w zespole inżynierskim przy rozwiązywaniu problemów wdrożeniowych.	K_K01, K_K02
---------	---	-----------------

**7. Odniesienie efektów uczenia się do form zajęć i sposób oceny osiągnięcia przez studenta efektów uczenia się**

Efekt przedmiotowy (Symbol)	Forma zajęć		Sposób sprawdzenia osiągnięcia efektu
	Wykład	Laboratorium	
DDSC_01	x		Egzamin końcowy
DDSC_02	x	x	Egzamin końcowy, dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne
DDSC_03		x	dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne
DDSC_04		x	dyskusja na zajęciach, sprawozdanie z projektu, zadania praktyczne

**8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się**

Efekt przedmiotowy (Symbol)	Efekt jest uznawany za osiągnięty, gdy student:
DDSC_01	Odpowiedział na ponad 50% pytań egzaminacyjnych
DDSC_02	Odpowiedział na ponad 50% pytań egzaminacyjnych Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu
DDSC_03	Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu
DDSC_04	Poprawnie wykonuje zadania w czasie zajęć. Potrafi objaśnić elementy projektu