

Cyberbezpieczeństwo Zaawansowanych Rozwiązań Chmurowych z AI

Kod przedmiotu: CZRC

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: 4

Semestr: 7

Formy zajęć i liczba godzin:

Forma stacjonarna

- wykłady – 30
- laboratorium – 35

Forma niestacjonarna

- wykłady – 10
- laboratorium – 10

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 5

Osoby prowadzące:

wykład:

laboratorium/projekt:

1. Założenia i cele przedmiotu

Przedmiot przygotowuje studentów do roli inżynierów i audytorów bezpieczeństwa chmurowego (Cloud Security Engineer). W miarę jak organizacje przenoszą swoje zasoby do chmury publicznej (AWS, Azure, GCP), pojawiają się nowe wektory ataków, wynikające najczęściej z błędnych konfiguracji. Studenci dowiedzą się, jak działa Model Współdzielonej Odpowiedzialności i jak stosować architekturę Zero Trust. Główny nacisk położony jest na praktyczne wykorzystanie narzędzi klasy CSPM (Cloud Security Posture Management) wspieranych przez sztuczną inteligencję, które potrafią audytować infrastrukturę 24/7, wykrywając np. publicznie otwarte zasoby (buckets S3) czy wycieki poświadczeń. Przedmiot kończy się przygotowaniem profesjonalnego raportu z audytu.

- Zrozumienie specyfiki zagrożeń w środowiskach chmurowych oraz zasad projektowania bezpiecznej architektury opartej na modelu Zero Trust.

- Nabycie praktycznej umiejętności obsługi zautomatyzowanych narzędzi skanujących infrastrukturę chmurową i kod (IaC) pod kątem błędów konfiguracyjnych i luk bezpieczeństwa.
- Kształtowanie umiejętności miękkich i analitycznych niezbędnych do sporządzania profesjonalnych raportów audytowych (w tym Executive Summary dla kadry zarządzającej).

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Podstawowa znajomość usług przynajmniej jednego wiodącego dostawcy chmury publicznej (AWS, Microsoft Azure lub Google Cloud).
- Zrozumienie koncepcji wirtualizacji, sieci wirtualnych (VPC/VNet) oraz konteneryzacji.
- Znajomość podstawowych koncepcji z zakresu zarządzania tożsamością i dostępem (IAM).

3. Opis form zajęć

a) Wykłady

• Treści programowe:

1. Fundamenty Cloud Security: Model Współdzielonej Odpowiedzialności. Różnice między środowiskiem on-premise a chmurą. Rola Cloud Security Alliance (CSA).
2. Zarządzanie tożsamością jako nowy obwód sieci (Identity is the new perimeter): Zaawansowane mechanizmy IAM (Identity and Access Management), zasada najmniejszych uprawnień (PoLP), polityki warunkowe i MFA.
3. Architektura Zero Trust w Chmurze: Segmentacja sieci wirtualnych, mikrosegmentacja, szyfrowanie danych w spoczynku i w locie (KMS, Key Vault).
4. Automatyzacja Audytu i rola AI: Systemy CSPM (Cloud Security Posture Management) i CWPP (Cloud Workload Protection Platforms). Wykorzystanie AI do ciągłego monitorowania zgodności (Continuous Compliance).
5. Sztuka raportowania incydentów i audytów: Jak pisać raporty bezpieczeństwa, które zarząd chce czytać. Tworzenie Executive Summary i estymacja ryzyka biznesowego.

• Metody dydaktyczne:

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

• Forma i warunki zaliczenia:

Warunkiem zaliczenia wykładu jest uzyskanie pozytywnego wyniku ze sprawdzianu końcowego

• Wykaz literatury podstawowej:

1. Diogenes, Y., Shinder, T., et al. (2021). Microsoft Azure Security Technologies Certification and Beyond. Packt Publishing.
2. Oficjalna dokumentacja bezpieczeństwa: AWS Security Best Practices, Microsoft Defender for Cloud Documentation.
3. Wytyczne Cloud Security Alliance (CSA): Security Guidance for Critical Areas of Focus in Cloud Computing.

• Wykaz literatury uzupełniającej:

1. Bisson, J. (2022). AWS Security Cookbook. Packt Publishing.
2. Raporty branżowe (np. Palo Alto Networks Unit 42 Cloud Threat Report) dotyczące wektorów ataków w chmurze i roli AI w cyber-obronie.

b) Laboratorium

• Treści programowe:

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

• Metody dydaktyczne:

W trakcie zajęć prowadzący omawia zagadnienia związane z realizacją poszczególnych ćwiczeń, a następnie studenci samodzielnie lub zespołowo realizują zadania określone przez prowadzącego.

• Forma i warunki zaliczenia:

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

- Raport z audytu chmury (Case Study): Ocena kompletności wykrytych podatności, prawidłowości oceny ryzyka oraz jakości propozycji naprawczych
- Weryfikacja umiejętności obsługi skanerów bezpieczeństwa.

• 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 zaliczenia	10
Laboratorium	Kontakt z nauczycielem	35
	Opracowanie zadań laboratoryjnych	9
	Realizacja projektu	15
	Przygotowanie dokumentacji	10
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3

Całkowita ilość godzin aktywności studenta	125
Liczba punktów ECTS dla modułu/przedmiotu	5

b. forma niestacjonarna

Forma zajęć	Formy aktywności studenta	Średnia liczba godzin na zrealizowanie aktywności
Wykład	Kontakt z nauczycielem	10
	Czytanie wskazanej literatury	20
	Przygotowanie do zaliczenia	20
Laboratorium	Kontakt z nauczycielem	10
	Opracowanie zadań laboratoryjnych	14
	Realizacja projektu	20
	Przygotowanie dokumentacji	25
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3

Całkowita ilość godzin aktywności studenta	125
Liczba punktów ECTS dla modułu/przedmiotu	5

1. Wskaźniki sumaryczne

a. forma stacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
 - Liczba godzin kontaktowych – 71
 - Liczba punktów ECTS – 2,8
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
 - Liczba godzin kontaktowych – 20
 - Liczba punktów ECTS – 2,8

b. forma niestacjonarna

- a) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach wymagających bezpośredniego udziału nauczycieli akademickich
 - Liczba godzin kontaktowych – 26
 - Liczba punktów ECTS – 1,0
- b) liczba godzin dydaktycznych (tzw. kontaktowych) i liczba punktów ECTS na zajęciach o charakterze praktycznym.
 - Liczba godzin kontaktowych – 10
 - Liczba punktów ECTS – 2,8

6. Zakładane efekty uczenia się

Efekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się

CZRC_01	... Zna i rozumie Model Współdzielonej Odpowiedzialności (Shared Responsibility Model) oraz rynkowe standardy i frameworki bezpieczeństwa chmurowego (np. zaleceń Cloud Security Alliance).	K_W02, K_W06
CZRC_02	... Potrafi zastosować narzędzia klasy CSPM oraz wbudowane mechanizmy dostawców chmury (np. AWS Security Hub, Microsoft Defender for Cloud) do przeprowadzenia technicznego audytu środowiska.	K_U02, K_U22
CZRC_03	... Umie syntetyzować wyniki ze skanerów bezpieczeństwa (wspieranych przez AI) i opracować ustrukturyzowany raport poaudytowy zawierający plan mitygacji (Remediation Plan).	K_U04, K_U07
CZRC_04	... Rozumie biznesowe konsekwencje wycieku danych z chmury (wymiar finansowy, wizerunkowy, prawny) i potrafi efektywnie komunikować ryzyko techniczne osobom nietechnicznym	K_K03, K_K04

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		Sprawdzian końcowy,
DDSC_02	x	x	Sprawdzian końcowy, dyskusja na zajęciach, sprawozdania z laboratoriów, projekt
DDSC_03		x	dyskusja na zajęciach, sprawozdania z laboratoriów, projekt
DDSC_04		x	dyskusja na zajęciach, sprawozdania z laboratoriów, projekt

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się

Efekt	Efekt jest uznawany za osiągnięty gdy:
CZRC_01	poprawnie wykonał sprawdzian końcowy uzyskując wymaganą liczbę punktów;
CZRC_02	poprawnie wykonał sprawdzian końcowy uzyskując wymaganą liczbę punktów; wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe
CZRC_03	wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe
CZRC_04	wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe.