

## **Zaawansowane Cyber-Operacje: Zintegrowany Projekt AI (Capstone)**

**Kod przedmiotu: ZCOZ**

**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 ma formę zaawansowanego warsztatu inżynierskiego (tzw. Capstone Project) i stanowi kulminację wiedzy zdobytej podczas całej specjalności. Zadaniem studentów jest praca w zespołach nad zaprojektowaniem i wdrożeniem miniaturowanego środowiska SOC (Security Operations Center). Projekt wymaga zintegrowania usług chmurowych, infrastruktury brzegowej (IoT), systemów monitoringu (SIEM) oraz zautomatyzowanego reagowania z użyciem sztucznej inteligencji (SOAR). Punktem kulminacyjnym kursu jest symulacja ataku na żywo (Red Team vs Blue Team), podczas której systemy obronne studentów wspierane przez AI muszą w czasie rzeczywistym wykryć i zneutralizować zagrożenie. Przedmiot silnie rozwija umiejętności pracy zespołowej i zarządzania projektem informatycznym pod presją.

- Synteza i integracja wiedzy oraz technologii z obszarów DevSecOps, Cloud Security, IoT oraz analizy SIEM/SOAR.

- Zbudowanie działającej, odpornej na ataki architektury sieciowej oraz zautomatyzowanego potoku wykrywania i reagowania na incydenty.
- Nabycie umiejętności pracy w zespole inżynierskim w warunkach symulowanego kryzysu cybernetycznego (odpieranie aktywnych ataków hakerskich).

## 2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Ukończenie wszystkich przedmiotów specjalnościowych z semestrów 5 i 6.
- Praktyczna znajomość środowisk wirtualizacyjnych, kontenerowych oraz podstaw konfiguracji usług chmurowych.

## 3. Opis form zajęć

### a) Wykłady

#### • Treści programowe:

1. Wprowadzenie do głównych zagadnień przedmiotu.
2. Omówienie podstaw teoretycznych oraz standardów i dobrych praktyk.

#### • 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. Whitehouse, A. (2020). Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases.
2. Przeździecki, T. (2021). Praktyczna analiza powłamaniowa. Aplikacja webowa w środowisku Linu

#### • Wykaz literatury uzupełniającej:

1. Clark, R. T., et al. (2014). Red Team Field Manual (RTFM). (w celu zrozumienia technik używanych przez atakujących podczas obrony).
2. Publikacje SANS Institute dotyczące "Incident Handling" oraz "SOC Operations".

### b) Laboratorium

#### • Treści programowe (tematyka zajęć):

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, realizacja projektu końcowego:

- Symulacja obronna na żywo (Live Fire Defense): Ewaluacja zdolności infrastruktury do wykrycia ataku (SIEM) oraz skuteczności i szybkości zadziałania mechanizmów automatycznych (SOAR i AI) (EU\_U01, EU\_U02).
- Raportu z architektury oraz z przebiegu incydentów podczas obrony (Incident Report) (EU\_W01, EU\_K01).
- **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

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

##### 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
--------------	------------------------	---

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

## 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

<b>Efekt przedmiotowy (Symbol)</b>	<b>Efekty uczenia się dla przedmiotu</b>	<b>Odniesienie do kierunkowych efektów uczenia się</b>
ZCOZ_01	... Zna i rozumie zasady integracji złożonych systemów informatycznych oraz cykl życia pełnej operacji cybernetycznej (od projektowania zabezpieczeń po reagowanie i audyt).	K_W02, K_W06
ZCOZ_02	... Potrafi zaprojektować i zaimplementować bezpieczną, rozproszoną architekturę IT (Cloud + IoT), łącząc systemy monitoringu (SIEM) i automatyzacji (SOAR).	K_U02, K_U22
ZCOZ_03	... Umie wykorzystać zaawansowane modele sztucznej inteligencji do obrony infrastruktury krytycznej przed aktywnym, wielowektorowym atakiem.	K_U04, K_U07
ZCOZ_04	... Potrafi zarządzać zadaniami w grupie pod presją czasu, przyjmując odpowiedzialność za powierzoną rolę (np. analityk SOC, inżynier	K_K01, K_K02

	bezpieczeństwa) oraz profesjonalnie raportować przebieg incydentu.	
--	--------------------------------------------------------------------	--

**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	
ZCOZ_01	<i>x</i>		Sprawdzian końcowy,
ZCOZ_02	<i>x</i>	<i>x</i>	Sprawdzian końcowy, dyskusja na zajęciach, sprawozdania z laboratoriów, projekt
ZCOZ_03		<i>x</i>	dyskusja na zajęciach, sprawozdania z laboratoriów, projekt
ZCOZ_04		<i>x</i>	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.