# KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Zarządzanie incydentami i bezpieczeństwo instytucji [S1Cybez1>ZIiBI]

## Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

## Liczba godzin

Wykład
16

Laboratorium
0

Inne
0

Ćwiczenia
0

Projekty/seminaria
16

## Liczba punktów ECTS

2,00

## Koordynatorzy

dr inż. Anna Grocholewska-Czuryło
anna.grocholewska-czurylo@put.poznan.pl

## Wykładowcy

## Wymagania wstępne

Znajomość sieci IP i systemów IoT, znajomość zagrożeń i ataków w sieciach teleinformatycznych

## Cel przedmiotu

• Zapoznanie studentów z procesami i narzędziami zarządzania incydentami bezpieczeństwa. • Rozwinięcie umiejętności korzystania z platform CTI w celu analizy zagrożeń i podejmowania decyzji operacyjnych. • Przygotowanie studentów do pracy w zespołach SOC oraz reagowania na rzeczywiste incydenty bezpieczeństwa.

## Przedmiotowe efekty uczenia się

Wiedza:
• Student zna standardy i procedury zarządzania incydentami bezpieczeństwa. [K1_W17]
• Rozumie podstawy działania platform CTI i ich znaczenie w analizie zagrożeń. [K1_W20]
• Posiada wiedzę na temat cyklu życia incydentu oraz metod reagowania na zagrożenia. [K1_W09]

Umiejętności:
• Potrafi zarządzać procesem reagowania na incydenty w oparciu o wytyczne NIST lub SANS. [K1_U09]

• Umie integrować dane z platform CTI z systemami SIEM oraz analizować zagrożenia. [K1_U04]
• Efektywnie współpracuje w zespole przy realizacji projektów związanych z zarządzaniem incydentami. [K1_U15]

Kompetencje społeczne:
• Rozumie znaczenie szybkiego i precyzyjnego reagowania na incydenty w organizacji. [K1_K02]
• Jest świadomy odpowiedzialności za proponowane działania w kontekście bezpieczeństwa IT. [K1_K05]

## Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

1. Wiedza: test podsumowujący na zakończenie wykładów.
2. Umiejętności: bieżąca ocena realizacji zadań projektowych oraz ocena raportu końcowego.
W każdej formie zaliczenia przedmiotu ocena zależy od liczby zdobytych przez studenta punktów w stosunku do maksymalnej liczby punktów obowiązkowych. Warunkiem pozytywnego zaliczenia jest otrzymanie co najmniej 50% punktów możliwych do zdobycia. Zależność oceny od liczby punktów definiuje Regulamin Studiów. Dodatkowo zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

## Treści programowe

Przedmiot „Zarządzanie incydentami i platformy CTI” wprowadza studentów w zaawansowane zagadnienia związane z reagowaniem na incydenty bezpieczeństwa oraz wykorzystaniem platform wywiadu o zagrożeniach cybernetycznych (Cyber Threat Intelligence - CTI). Kurs rozwija praktyczne umiejętności zarządzania incydentami w oparciu o istniejące procedury, narzędzia oraz standardy międzynarodowe, a także uczy integrowania danych z platform CTI w celu analizy zagrożeń i podejmowania skutecznych decyzji operacyjnych. Studenci realizują praktyczny projekt zespołowy, odzwierciedlający rzeczywiste wyzwania w obszarze SOC (Security Operations Center).

## Tematyka zajęć

I. Zarządzanie incydentami bezpieczeństwa
1. Podstawowe pojęcia i definicje
o Definicja incydentu bezpieczeństwa i jego klasyfikacja.
o Cykl życia incydentu: identyfikacja, eskalacja, reakcja, analiza, raportowanie.
2. Standardy i procedury
o Wytyczne NIST (cykl reagowania na incydenty).
o Modele i frameworki: SANS, ISO/IEC 27035.
o Rola zespołów CSIRT i SOC w zarządzaniu incydentami.
3. Procesy reagowania na incydenty
o Analiza danych z systemów SIEM i logów.
o Tworzenie raportów i eskalacja incydentów.
o Wdrażanie działań naprawczych i prewencyjnych.
II. Wywiad o zagrożeniach cybernetycznych (CTI)
1. Podstawy CTI
o Definicja i znaczenie Cyber Threat Intelligence w organizacji.
o Typy informacji wywiadowczych: taktyczne, operacyjne, strategiczne.
o Standardy wymiany informacji o zagrożeniach: STIX, TAXII, OpenIOC.
2. Platformy CTI
o Przegląd platform CTI: MISP, ThreatConnect, Anomali.
o Integracja danych z CTI z systemami SIEM.
o Automatyzacja analizy i priorytetyzacja zagrożeń.
3. Analiza zagrożeń
o Profilowanie zagrożeń i grup APT (Advanced Persistent Threat).
o Korelacja danych z różnych źródeł.
o Wykorzystanie CTI w planowaniu działań obronnych.
III. Projekt grupowy: zarządzanie incydentami z wykorzystaniem platform CTI
1. Scenariusze reagowania na incydenty
o Opracowanie i wdrożenie procedur reagowania na wybrany scenariusz incydentu.

o Analiza logów i danych z systemów SIEM w celu identyfikacji zagrożeń.
2. Wykorzystanie platform CTI
o Integracja platformy CTI z systemami operacyjnymi SOC.
o Analiza zagrożeń i priorytetyzacja działań na podstawie danych CTI.
3. Prezentacja wyników projektu
o Przygotowanie raportu końcowego.
o Omówienie zrealizowanego scenariusza, skuteczności wdrożonych działań i wniosków.

## Metody dydaktyczne

• Wykłady online z prezentacjami i przykładami praktycznymi.
• Projekt zespołowy realizowany z wykorzystaniem rzeczywistych narzędzi SOC i CTI.

## Literatura

Podstawowa:
1. "The Cyber Incident Response Handbook" - Jeff Bollinger, Brandon Enright, Matthew Valites. O'Reilly Media, 2015. ISBN-13: 978-1491949409. Amazon
2. "The Threat Intelligence Handbook" - Recorded Future, 2023. Recorded Future
3. NIST SP 800-61: "Computer Security Incident Handling Guide", National Institute of Standards and Technology, 2012. NIST
SANS Institute: "Incident Handler's Handbook", 2014. SANS

Uzupełniająca:
1. Materiały dotyczące platform CTI (np. MISP, ThreatConnect).

## Bilans nakładu pracy przeciętnego studenta

| | Godzin | ECTS |
|---|---|---|
| Łączny nakład pracy | 57 | 2,00 |
| Zajęcia wymagające bezpośredniego kontaktu z nauczycielem | 32 | 1,00 |
| Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu) | 25 | 1,00 |