

AI w Cyber Threat Intelligence i Złożonej Analizie SIEM

Kod przedmiotu: CTIZ

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: 6

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 wprowadza studentów w świat zaawansowanych operacji bezpieczeństwa i polowania na zagrożenia (Threat Hunting) w środowiskach korporacyjnych klasy Enterprise. Skupia się na pracy z systemami SIEM (Security Information and Event Management) nowej generacji (np. Splunk, Microsoft Sentinel), w których gigabajty logów są na bieżąco analizowane przez algorytmy sztucznej inteligencji w celu identyfikacji ataków ukierunkowanych (APT). Studenci nauczą się, jak pisać złożone zapytania analityczne, redukować tzw. szum informacyjny (false positives) z wykorzystaniem AI oraz jak profilować zachowanie atakujących przy użyciu globalnych baz wiedzy o cyberzagrożeniach (Cyber Threat Intelligence) i frameworka MITRE ATT&CK.

- Zrozumienie architektury nowoczesnych systemów SIEM oraz roli sztucznej inteligencji w korelacji zdarzeń i analizie behawioralnej.
- Opanowanie w stopniu użytecznym specjalistycznych języków zapytań analitycznych (np. SPL - Splunk Processing Language lub KQL - Kusto Query Language).

- Nabycie umiejętności wykorzystywania platform Threat Intelligence (np. MISP) oraz frameworka MITRE ATT&CK do kategoryzowania incydentów i mapowania wektorów ataku.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Zrozumienie budowy sieci oraz działania usług katalogowych (np. Active Directory).
- Znajomość podstawowych wektorów ataków (np. phishing, malware, lateral movement).
- Umiejętność analizy logów systemowych (Windows Event Logs, logi z serwerów Linux i zapór sieciowych).

3. Opis form zajęć

a) Wykłady

• Treści programowe:

1. Architektura korporacyjnego SOC: Wprowadzenie do systemów SIEM (Splunk, Sentinel, QRadar). Centralizacja logów w modelu Zero Trust.
2. Cyber Threat Intelligence (CTI): Klasyfikacja danych o zagrożeniach (strategiczne, taktyczne, operacyjne). Wskaźniki kompromitacji (IoC) i TTPs (Tactics, Techniques, and Procedures). Platforma MISP.
3. Framework MITRE ATT&CK w praktyce: Mapowanie działań napastnika w poszczególnych fazach ataku (od Initial Access do Impact).
4. AI w analizie bezpieczeństwa: Rola uczenia maszynowego w wykrywaniu ukrytych kanałów komunikacji (C2 - Command & Control) i ataków "Living off the Land" (LotL). Metody punktacji ryzyka z pomocą AI.
5. Threat Hunting: Proaktywne poszukiwanie zagrożeń w środowisku IT zamiast pasywnego oczekiwania na alert.

• 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 oraz aktywny udział w dyskusjach dotyczących problematyki przedmiotu.

• Wykaz literatury podstawowej:

1. Dalziel, H. (2014). How to Define and Build an Effective Cyber Threat Intelligence Capability. Syngress.
2. Oficjalna dokumentacja: Splunk Enterprise Security, Microsoft Sentinel.
3. Baza wiedzy i matryce: MITRE ATT&CK® Framework (dostęp online).

• Wykaz literatury uzupełniającej:

1. Diogenes, Y., Ozkaya, E. (2018). Cybersecurity – Attack and Defense Strategies. Packt Publishing.
2. Shackelford, D. (2020). SANS Institute: AI and Machine Learning in Cybersecurity (Whitepapers).

b) Laboratorium

• Treści programowe:

1. Realizacja ćwiczeń praktycznych zgodnych z zakresem przedmiotu.
 - Ocenianie zaangażowania w praktyczne poszukiwanie zagrożeń i poprawność pisanych zapytań

- Wykonanie praktycznego "śledztwa" – wyłuskanie wskaźników ataku (IoC) za pomocą zapytań KQL/SPL

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 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, przygotowanie sprawozdań 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 zaliczenia	10
Laboratorium	Kontakt z nauczycielem	45
	Opracowanie sprawozdań i projektu	20
	Czytanie wskazanej literatury	10
	Wykonanie zadań laboratoryjnych	19
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
Całkowita ilość godzin aktywności studenta		150
Liczba punktów ECTS dla modułu/przedmiotu		6

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 zaliczenia	20
Laboratorium	Kontakt z nauczycielem	20

	Opracowanie sprawozdań i projektu	25
	Czytanie wskazanej literatury	24
	Wykonanie zadań laboratoryjnych	25
Konsultacje	Kontakt z nauczycielem	3
Zal./Egzamin	Kontakt z nauczycielem	3
Całkowita ilość godzin aktywności studenta		150
Liczba punktów ECTS dla modułu/przedmiotu		6

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

Efekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
CTIZ_01	... Zna i rozumie taktyki, techniki i procedury (TTPs) wykorzystywane przez cyberprzestępców oraz struktury platform wymiany informacji o zagrożeniach (CTI).	K_W04, K_W06
CTIZ_02	... Potrafi skonstruować zaawansowane zapytania w systemie SIEM (KQL/SPL), aby zidentyfikować wskaźniki kompromitacji (IoC) w rozproszonych źródłach logów.	K_U03, K_U11
CTIZ_03	... Umie wykorzystać możliwości algorytmów AI zagnieżdżonych w narzędziach SIEM do redukcji fałszywych alarmów oraz odtworzenia pełnej ścieżki ataku na matrycy MITRE ATT&CK.	K_U04, K_U23

CTIZ_04	... Potrafi analitycznie myśleć i syntetyzować złożone dane techniczne w celu raportowania incydentów na wyższe szczeble zarządzania organizacją (SOC Tier 2/3).	K_U02, 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		Sprawdzian końcowy,
DDSC_02	x	x	Sprawdzian końcowy, dyskusja na zajęciach, sprawozdanie z laboratorium/projektu, test lub zadanie praktyczne
DDSC_03		x	dyskusja na zajęciach, sprawozdanie z laboratorium/projektu, test lub zadanie praktyczne
DDSC_04		x	dyskusja na zajęciach, sprawozdanie z laboratorium/projektu, test lub zadanie praktyczne

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się

Efekt	Efekt jest uznawany za osiągnięty gdy:
CTIZ_01	student poprawnie wykonał sprawdzian końcowy, uzyskując wymaganą liczbę punktów;
CTIZ_02	student poprawnie wykonał sprawdzian końcowy, uzyskując wymaganą liczbę punktów; student wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe oraz odpowiedzieć na pytania dotyczące zakresu przedmiotu.
CTIZ_03	student poprawnie wykonał sprawdzian końcowy, uzyskując wymaganą liczbę punktów; student wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe oraz odpowiedzieć na pytania dotyczące zakresu przedmiotu.
CTIZ_04	student poprawnie wykonał sprawdzian końcowy, uzyskując wymaganą liczbę punktów; student wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe oraz odpowiedzieć na pytania dotyczące zakresu przedmiotu.