

Inteligentny Cyber-Monitoring i Detekcja Anomalii Oparta na AI

Kod przedmiotu: ICMD

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 ukazuje ewolucję od klasycznego, opartego na sygnaturach monitorowania sieci do nowoczesnych systemów NDR (Network Detection and Response). Studenci koncentrują się na wykorzystaniu modeli uczenia maszynowego (ML) do analizy ruchu sieciowego i logów. Zamiast uczyć się na pamięć statycznych reguł, poznają metody tworzenia "bazylinii" (normalnego zachowania systemu) wspierane przez algorytmy sztucznej inteligencji, które natychmiast alarmują o anomaliami i odchyleniach świadczących o potencjalnym cyberataku. Kurs ma charakter wybitnie praktyczny, oparty na analizie rzeczywistych zrzutów ruchu i logów w środowiskach typu ELK.

- Zrozumienie architektury oraz mechanizmów działania nowoczesnych systemów monitorowania bezpieczeństwa sieci i agregacji logów (np. stos ELK).
- Zapoznanie z podstawowymi algorytmami sztucznej inteligencji (uczenie nadzorowane i nienadzorowane) stosowanymi do wykrywania anomalii w ruchu sieciowym.

- Nabycie praktycznych umiejętności w analizie powłamaniowej i detekcji zagrożeń na podstawie dostarczonych danych (zrzuty PCAP, logi systemowe) w warunkach symulowanych incydentów.

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Znajomość modelu OSI/TCP/IP oraz protokołów sieciowych (HTTP, DNS, TCP, UDP).
- Podstawowa umiejętność programowania (znajomość struktur danych, pisanie prostych skryptów).
- Biegłość w poruszaniu się po systemie operacyjnym Linux (wiersz poleceń).

3. Opis form zajęć

a) Wykłady

• Treści programowe:

1. Od IDS do NDR: Ewolucja systemów detekcji intruzów. Ograniczenia systemów sygnaturowych a zalety analizy behawioralnej.
2. Architektura systemów zbierania logów: Omówienie stosu ELK (Elasticsearch, Logstash, Kibana) oraz lekkich agentów (Beats). Metody normalizacji logów.
3. Podstawy uczenia maszynowego w cyberbezpieczeństwie: Uczenie nadzorowane vs nienadzorowane. Algorytmy klasteryzacji i izolacji (np. Isolation Forest) w detekcji anomalii.
4. Analiza zachowań użytkowników i encji (UEBA): Jak AI buduje profil "normalności" dla użytkowników i systemów.
5. Zarządzanie szumem informacyjnym: Problem fałszywych alarmów (False Positives) w modelach ML i metody ich redukcji.

• 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 praktyczny - Samodzielna analiza incydentu bezpieczeństwa na podstawie dostarczonych logów i ruchu sieciowego.

• Wykaz literatury podstawowej:

1. Collins, M. (2017). Network Security Through Data Analysis: Building Situational Awareness. O'Reilly Media.
2. Chuvakin, A., Schmidt, K., Phillips, C. (2013). Data-Driven Security: Analysis, Visualization and Dashboards. Wiley.
3. Oficjalna dokumentacja systemów Elastic Stack (ELK) oraz Zeek Network Security Monitor.

• Wykaz literatury uzupełniającej:

1. O'Connor, T. (2012). Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers. Syngress. (w zakresie bibliotek analizy danych).
2. Artykuły naukowe i whitepapery dotyczące zastosowań algorytmów Isolation Forest oraz Deep Learningu w detekcji anomalii sieciowych.

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 ćwiczeń, a następnie studenci samodzielnie lub zespołowo realizują zadania określone przez prowadzącego.

Metoda laboratoryjna –ćwiczenia laboratoryjne z wykorzystaniem komputerów

• **Forma i warunki zaliczenia:**

Sprawozdania laboratoryjne - Ocena poprawności konfiguracji narzędzi oraz jakości wniosków wyciąganych z analizy danych

Ocena i weryfikacja aktywności i zaangażowania studenta w rozwiązywanie problemów analitycznych podczas zajęć

• **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	39
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 egzaminu	20
Laboratorium	Kontakt z nauczycielem	20
	Czytanie wskazanej literatury	24
	Wykonanie zadań laboratoryjnych	50
	Konsultacje	Kontakt z nauczycielem
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

- 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
- 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
ICMD_01	... Zna i rozumie różnice między klasycznymi systemami IDS/IPS a systemami opartymi na analizie behawioralnej i AI. Zna procesy agregacji i parsowania logów.	K_W02, K_W06
ICMD_02	... Potrafi wdrożyć i skonfigurować narzędzia do analizy ruchu sieciowego (Zeek/Suricata) oraz scentralizowanego zarządzania logami (np. Elasticsearch, Kibana).	K_U02, K_U09
ICMD_03	... Umie zastosować podstawowe biblioteki Data Science (np. Scikit-Learn) do trenowania modeli wykrywających anomalie w zebranych	K_U02, K_U09

	pakietach i zdarzeniach.	
ICMD_04	... Rozumie wagę ciągłego monitorowania infrastruktury krytycznej i potrafi zachować opanowanie oraz analityczne podejście podczas presji czasu (symulacja ataku).	K_K01, K_K03

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	<i>x</i>		Egzamin końcowy
DDSC_02	<i>x</i>	<i>x</i>	Egzamin końcowy, dyskusja na zajęciach, realizacja zadania praktycznych
DDSC_03		<i>x</i>	dyskusja na zajęciach, realizacja zadania praktycznych
DDSC_04		<i>x</i>	dyskusja na zajęciach, realizacja zadania praktycznych

8. Kryteria uznania osiągnięcia przez studenta efektów uczenia się

Efekt	Efekt jest uznawany za osiągnięty gdy:
ICMD_01	Zrealizował zadanie
ICMD_02	Zrealizował zadanie Poprawnie wykonuje zadania w czasie zajęć.
ICMD_03	Poprawnie wykonuje zadania w czasie zajęć.
ICMD_04	Poprawnie wykonuje zadania w czasie zajęć.