

Automatyzacja Cyber-Reagowania: AI w Systemach SOAR

Kod przedmiotu: ACRS

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
- projekt – 35

Forma niestacjonarna

- wykłady – 10
- projekt – 10

Zajęcia prowadzone są w języku polskim.

Liczba punktów ECTS: 5

Osoby prowadzące:

wykład:

laboratorium/projekt:

1. Założenia i cele przedmiotu

Przedmiot uczy zautomatyzowanego podejścia do incydentów bezpieczeństwa. Kiedy systemy detekcji (np. SIEM) zgłaszają alert, do akcji wkraczają systemy klasy SOAR (Security Orchestration, Automation, and Response). Studenci nauczą się łączyć różne narzędzia bezpieczeństwa za pomocą interfejsów API oraz pisać „playbooki” (zautomatyzowane scenariusze reakcji). Głównym punktem kursu jest wykorzystanie modeli sztucznej inteligencji (w tym modeli językowych - LLM) do dynamicznej analizy alertów (np. oceny treści złośliwych e-maili) i podejmowania w ułamku sekundy autonomicznych decyzji obronnych, takich jak izolacja zainfekowanego hosta czy zablokowanie ataku na zaporze sieciowej bez udziału człowieka.

- Zrozumienie cyklu życia incydentu bezpieczeństwa (Incident Response Lifecycle) według standardów rynkowych (np. SANS, NIST) oraz miejsca systemów SOAR w architekturze SOC.
- Nabycie umiejętności integracji rozproszonych rozwiązań IT i Security za pomocą interfejsów programistycznych (REST API, Webhooks).

- Praktyczne projektowanie i programowanie zautomatyzowanych playbooków wspieranych przez algorytmy AI do odpierania najczęstszych wektorów ataków (np. phishing, infekcja malware).

2. Określenie przedmiotów wprowadzających wraz z wymaganiami wstępnymi

Wymogi wstępne dotyczą wiedzy i umiejętności z następujących obszarów:

- Dobra znajomość języka programowania Python (obsługa bibliotek do zapytań sieciowych, np. requests, przetwarzanie formatu JSON).
- Zrozumienie architektury klient-serwer oraz działania interfejsów REST API.
- Podstawowa wiedza z zakresu systemów operacyjnych i sieci komputerowych (znajomość pojęć takich jak firewall, Active Directory, endpoint).

3. Opis form zajęć

a) Wykłady

• Treści programowe:

1. Wprowadzenie do SOAR i Incident Response: Fazy obsługi incydentu (Przygotowanie, Identyfikacja, Powstrzymanie, Usunięcie, Przywrócenie, Wnioski). Przeciążenie analityków alertami (Alert Fatigue) a potrzeba automatyzacji.
2. Architektura Orkiestracji: Czym różni się orkiestracja od automatyzacji? Integracje (App/Plugins), struktura playbooków.
3. API i integracja systemów bezpieczeństwa: Protokoły komunikacyjne, uwierzytelnianie (OAuth, API Keys), formatowanie danych (JSON/XML).
4. AI jako wirtualny analityk SOC: Zastosowanie modeli LLM (np. GPT) do analizy języka naturalnego w wiadomościach phishingowych, streszczania alertów i proponowania akcji naprawczych.
5. Zarządzanie ryzykiem automatyzacji: „Human-in-the-loop” vs. pełna autonomia. Metody zapobiegania katastrofalnym błędom (np. odcięciu CEO od sieci).

• 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 - Ocena stopnia zaawansowania logiki, poprawności napisanych skryptów Python oraz odporności na błędy.

• Wykaz literatury podstawowej:

1. Islam, C. (2020). Security Automation with Cortex XSOAR. Packt Publishing.
2. Oficjalna dokumentacja wybranych narzędzi klasy SOAR (np. Tines, Shuffle, Palo Alto Cortex).
3. Dokument NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide.

• Wykaz literatury uzupełniającej:

1. Seitz, J. (2014). Black Hat Python: Python Programming for Hackers and Pentesters. No Starch Press (w zakresie wykorzystania języka Python do komunikacji sieciowej).
2. Publikacje i Whitepapery na temat integracji LLM w narzędziach zautomatyzowanego reagowania na incydenty (np. materiały z konferencji Black Hat / DEF CON).

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.
 - Ewaluacja rozwiązywania problemów integracyjnych
 - Wytlumaczenie zastosowanych ścieżek decyzyjnych oraz ról poszczególnych komponentów

• 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	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

Effekt przedmiotowy (Symbol)	Efekty uczenia się dla przedmiotu	Odniesienie do kierunkowych efektów uczenia się
ACRS_01	... Zna i rozumie zasady orkiestracji bezpieczeństwa oraz rolę sztucznej inteligencji w procesie kategoryzacji i obsługi incydentów (Triage).	K_W04, K_W06
ACRS_02	... Potrafi skonfigurować integracje między różnymi narzędziami (np.	K_U19,

	SIEM, Firewall, EDR) z wykorzystaniem API i skryptów w języku Python.	K_U23
ACRS_03	... Umie zaprojektować i wdrożyć kompletny, bezbłędny playbook w systemie SOAR, który wykorzystuje AI do analizy i automatycznie mityguje zagrożenie.	K_U19, K_U23
ACRS_04	... Ma świadomość ryzyka biznesowego związanego z nadmierną lub błędną automatyzacją (np. przypadkowe zablokowanie krytycznych usług produkcyjnych) i potrafi krytycznie testować swoje rozwiązania.	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:
ACRS_01	poprawnie wykonał sprawdzian końcowy, uzyskując wymaganą liczbę punktów;
ACRS_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
ACRS_03	wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe
ACRS_04	wykonał ćwiczenia laboratoryjne lub zadania projektowe zgodnie z wymaganiami prowadzącego; student potrafi omówić zastosowane rozwiązania, uzasadnić decyzje projektowe.