SYLABUS PRZEDMIOTU

Wykrywanie Incydentów

I. Informacje ogólne

Nazwa przedmiotu	*Wykrywanie incydentów*
Kod przedmiotu	WYI
Rodzaj przedmiotu	specjalistyczny
Kierunek studiów	Informatyka
Poziom kształcenia	II stopień
Profil kształcenia	Ogólnoakademicki
Rok studiów	drugi
Rodzaje zajęć i liczba godzin	
Wykład	0
Ćwiczenia	0
Laboratoria	30
Praktyki	0
Liczba punktów ECTS	3

Imię, nazwisko, tytuł/stopień naukowy, adres e-mail wykładowcy (wykładowców)/ prowadzących zajęcia

- mgr inż. Konrad Popławski konrad.poplawski@pm.me

Język wykładowy	polski
Przedmiot prowadzony zdalnie (e-learning)	tak, częściowo

II. Informacje szczegółowe

1. Cele przedmiotu

Przedmiot stawia następujące cele:

- poznanie metodyk obsługi incydentów bezpieczeństwa

- poszerzenie wiedzy o technikach wykorzystywanych przez cyberprzestępców

- nabycie umiejętności wykrywania incydentów bezpieczeństwa

- doskonalenie zdolności analitycznych

- zapoznanie ze środowiskiem i technologiami wykorzystywanymi do wykrywania i zarządzania incydentami bezpieczeństwa

- zapoznanie się z możliwościami zastosowań wywiadu zagrożeń w wykrywaniu i obsłudze incydentów

- doskonalenie zdolności do pracy w zespole

- wskazanie możliwych specjalizacji i kierunków samorozwoju.

2. Wymagania wstępne w zakresie wiedzy, umiejętności oraz kompetencji społecznych

Znajomość budowy i funkcjonowania sieci TCP/IP w szczególności protokołów TCP/UDP oraz protokołów aplikacyjnych http(s), DNS, FTP, telnet, SSH, SMB.

Podstawowa umiejętność administracji systemami Linux i Windows.

Podstawowe umiejętności z zakresu bezpieczeństwa informacji.

Znajomość funkcjonowania aplikacji webowych oraz baz danych.

3. Efekty uczenia się (EU) dla zajęć i odniesienie do efektów uczenia się (EK) dla kierunku studiów

Symbol EU dla przedmiotu	Symbol EK dla kierunku studiów	Po zakończeniu modułu i potwierdzeniu osiągnięcia EU student/ka:
WY_01	KINF2_U05 KINF2_U07	Potrafi określić cechy incydentu bezpieczeństwa.
WY_02	KINF2_W03 KINF2_W04	Zna metodyki zarządzania incydentami i przedstawić ich etapy.
WY_03	KINF_U10	Potrafi przygotować raport opisujący incydent bezpieczeństwa.
WY_04	KINF_U11 KINF_K01	Potrafi wykorzystać wywiad zagrożeń do wykrywania incydentów.
WY_05	KINF2_U05 KINF2_U07	Potrafi odwzorować incydent wykorzystując modele zagrożeń.
WY_06	KINF2_W03 KINF2_W04	Zna metody i technologie wykorzystywane do wykrywania ataków cybernetycznych.
WY_07	KINF2_U03 KINF2_U05 KINF2_U07	Potrafi scharakteryzować technologię SIEM i jej zastosowanie w wykrywaniu incydentów.
WY_08	KINF2_U05 KINF2_U07	Potrafi zidentyfikować ataki na zewnętrzne usługi sieciowe.
WY_09	KINF2_U05 KINF2_U07	Potrafi rozpoznać i dokonać analizy ataków typu *phishing*.
WY_10	KINF2_U05 KINF2_U07	Potrafi przeprowadzić podstawową analizę złośliwych dokumentów elektronicznych.
WY_11	KINF2_W03 KINF2_W04	Rozumie techniki rekonesansu i techniki ich wykrywania.

WY_12	KINF2_W03 KINF2_W04	Rozumie charakterystykę ruchu Command & Control i możliwości jego identyfikacji.
WY_13	KINF2_U05 KINF2_U07	Potrafi zidentyfikować próby eskalacji uprawnień.
WY_14	KINF2_U05 KINF2_U07	Potrafi przedstawić metody utrwalania dostępu i sposoby na ich rozpoznanie.
WY_15	KINF2_U05 KINF2_U07	Potrafi przedstawić przykłady technik ruchu poprzecznego i metody ich detekcji.
WY_16	KINF2_W03 KINF2_W04	Zna techniki eksfiltracji danych i metody ich wykrycia.
WY_17	KINF2_W03 KINF2_W04	Zna charakterystykę ataków w środowisku chmurowym i możliwości ich identyfikacji.

4. Treści programowe zapewniające uzyskanie efektów uczenia się (EU) z odniesieniem do odpowiednich efektów uczenia się (EU) dla przedmiotu

Lp.	Symbol EU dla przedmiotu	Godzin Wykład	Godzin ĆW/ LAB/ SEM	Godzin pracy własnej	Opis treści kształcenia modułu zajęć/przedmiotu
Suma		0	30	45	
1.	WY_01 WY_02 WY_03		2	3	**Wprowadzenie do wykrywania incydentów bezpieczeństwa:** Charakterystyka incydentu bezpieczeństwa. Porównanie metodyk zarządzania incydentami.
2	WY _04 WY_05		2	3	**Modelowanie i wywiad zagrożeń:** Wykrywanie incydentów w oparciu o wywiad zagrożeń oraz wykorzystanie modeli „Cyber Kill Chain" i Mitre „Att&ck" do przedstawienia cyklu ataku cybernetycznego.
3.	WY _06		1	2	**Metody i systemy wykrywania ataków:** Zapoznanie z podstawowymi metodami wykrywania ataków. Porównanie możliwości systemów IDS, EDR, WAF oraz UBA.
4.	WY _07		2	4	**Technologia SIEM:** Zapoznanie się z możliwościami wykorzystania rozwiązań SIEM do identyfikacji ataków cybernetycznych.
5.	WY _08		2	4	**Ataki na perymetr sieci:** Przegląd wybranych technik ataków na zewnętrzne usługi sieciowe i aplikacje webowe oraz ich detekcji.
6.	WY _09 WY _10		4	4	**Ataki typu phishing i złośliwe dokumenty:** Analiza wybranych wariantów ataków wykorzystujących pocztę elektroniczną i złośliwe dokumenty elektroniczne.
7.	WY _11		2	3	**Rekonesans:** Wykrywanie aktywności cyberprzestępców związanych z rozpoznaniem otoczenia skompromitowanych systemów informatycznych.
8.	WY _12		3	4	**Ruch Command & Control:** Poznanie wybranych metod komunikacji z serwerami C2 i opracowanie sposobu ich identyfikacji.
9.	WY _13		2	4	**Eskalacja uprawnień:** Przedstawienie metod podnoszenia uprawnień oraz ich detekcji.
10.	WY _14		3	4	**Techniki utrwalania dostępu:** Prezentacja sposobów na zapewnienie trwałego dostępu

					do skompromitowanych systemów i ich identyfikację.
11.	WY _15		3	4	**Techniki ruchu poprzecznego:** Omówienie kluczowych technik poruszania się po skompromitowanej sieci oraz generowanych przez nie śladów.
12.	WY _16		1	3	**Eksfiltracja danych:** Poznanie technik eksfiltracji danych oraz metod ich detekcji.
13.	WY _17		2	3	**Ataki w chmurze:** Metody wykrywania incydentów w środowisku chmurowym.
14.	WY _03		1	0	Podsumowanie kursu

5. Zalecana literatura

1) Steve Anson, "Applied Incident Response", Wiley, 2020
2) Gerard Johansen, "Digital Forensics and Incident Response: Incident response techniques and procedures to respond to modern cyber threats", Packt, 2020
3) Yuri Diogenes, Erdal Ozkaya, "Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics", Packt, 2019
4) Chris Sanders, "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems", No Starch Press, 2017
5) Chris Sanders Jason Smith, "Applied Network Security Monitoring: Collection, Detection, and Analysis", Syngress, 2014
6) Richard Bejtlich, "The Practice of Network Security Monitoring: Understanding Incident Detection and Response", No Starch Press, 2013

V. Informacje dodatkowe

1. Metody i formy prowadzenia zajęć umożliwiające osiągnięcie założonych EU (proszę wskazać z proponowanych metod właściwe dla opisywanych zajęć lub/i zaproponować inne)

Realizacja	Metody i formy prowadzenia zajęć
	Wykład z prezentacją multimedialną wybranych zagadnień
	Wykład konwersatoryjny
	Wykład problemowy
	Dyskusja
	Praca z tekstem
✔	Metoda analizy przypadków
✔	Uczenie problemowe (Problem-based learning)
✔	Gra dydaktyczna/symulacyjna
✔	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych)
	Metoda ćwiczeniowa
✔	Metoda laboratoryjna
	Metoda badawcza (dociekania naukowego)
	Metoda warsztatowa
✔	Metoda projektu
✔	Pokaz i obserwacja
	Demonstracje dźwiękowe i/lub video
	Metody aktywizujące (np.: „burza mózgów", technika analizy SWOT, technika drzewka decyzyjnego, metoda „kuli śniegowej", konstruowanie „map myśli")
✔	Praca w grupach
	Wykład zdalny w czasie rzeczywistym
	Wykład zdalny asynchroniczny uzupełniony spotkaniem w czasie rzeczywistym
	Wykład zdalny asynchroniczny z aktywnością studenta uzupełniony spotkaniem w czasie rzeczywistym
✔	Ćwiczenia/laboratoria/konwersatoria zdalne w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą indywidualną studenta uzupełnione spotkaniem w czasie rzeczywistym
	Ćwiczenia zdalne asynchroniczne z pracą grupową studentów uzupełnione spotkaniem w czasie rzeczywistym
✔	Laboratorium cyfrowe zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Konwersatorium asynchroniczne zdalne uzupełnione spotkaniem w czasie rzeczywistym
	Seminarium zdalne w czasie rzeczywistym
	Seminarium asynchroniczne zdalne ze spotkaniem w czasie rzeczywistym
	Inne (jakie?) -

2. Sposoby oceniania stopnia osiągnięcia EU (proszę wskazać z proponowanych sposobów właściwe dla danego EU lub/i zaproponować inne

	Symbole EU dla modułu zajęć/przedmiotu

Sposoby oceniania

			WY: 01, 02, 03, 04, 05, 06, 07, 08, 09, 10, 11, 12, 13, 14, 15, 16, 17							

Egzamin pisemny										
Egzamin ustny										
Egzamin z „otwartą książką”										
Kolokwium pisemne										
Kolokwium ustne										
Test										
Projekt										
Esej										
Raport										
Prezentacja multimedialna										
Egzamin praktyczny (obserwacja wykonawstwa)										
Portfolio										
Zadania cząstkowe na wykładzie										
Zadania cząstkowe na laboratorium			✔							

3. Nakład pracy studenta i punkty ECTS

Forma aktywności		Średnia liczba godzin na zrealizowanie aktywności
Godziny zajęć (wg planu studiów) z nauczycielem		30
Praca własna studenta*	Przygotowanie do zajęć	5
	Czytanie wskazanej literatury	5
	Przygotowanie pracy pisemnej, raportu, prezentacji, itp.	10
	Przygotowanie projektu	0
	Przygotowanie pracy semestralnej	0
	Przygotowanie do egzaminu/zaliczenia	0
	Praca z materiałem do samokształcenia (np. Jupyter Notebook)	5
	Praca z laboratorium cyfrowym (np. Code Runner)	20
	Inne (jakie?)	
SUMA GODZIN		75

LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3

* proszę wskazać z proponowanych przykładów pracy własnej studenta właściwe dla opisywanego modułu lub/i zaproponować inne

4. Kryteria oceniania wg skali stosowanej w UAM

Ocena	Kryterium
bardzo dobry (bdb; 5,0)	od 88% punktów
dobry plus (+db; 4,5)	od 80% punktów
dobry (db; 4,0)	od 70% punktów
dostateczny plus (+dst; 3,5)	od 60% punktów
dostateczny (dst; 3,0)	od 50% punktów
niedostateczny (ndst; 2,0)	poniżej 50% punktów