

KARTA PRZEDMIOTU

Nazwa w języku polskim: **Wykrywanie incydentów**

Nazwa w języku angielskim: **Incident detection**

Karta przedmiotu ważna od roku akademickiego: **2022/2023**

Kierunek studiów: **Informatyka**

Poziom studiów: **Studia I stopnia**

Forma studiów: **Niestacjonarne**

Profil: **Praktyczny**

Specjalność: **Cyberbezpieczeństwo**

Język wykładowy: **Polski**

Jednostka prowadząca: **Wydział Nauk Społecznych i Technicznych**

Prowadzący: **dr hab. inż. Bartłomiej Sulikowski**

OBciążENIE STUDENTA

	Wykład	Konwersatorium	Laboratorium	Projekt	Seminarium
Liczba godzin zajęć dydaktycznych organizowanych przez Uczelnię			20		
Liczba godzin całkowitego nakładu pracy studenta			50		
Forma zaliczenia			Zaliczenie z oceną		
Liczba punktów ECTS			2		

WYMAGANIA WSTĘPNE W ZAKRESIE WIEDZY, UMIEJĘTNOŚCI I INNYCH KOMPETENCJI

Wiedza i umiejętności z zakresu przedmiotów: Sieci komputerowe, Systemy operacyjne, Podstawy cyberbezpieczeństwa.

CELE PRZEDMIOTU

C1	Zdobycie wiedzy i umiejętności praktycznych związanych z wykrywaniem incydentów naruszenia bezpieczeństwa w systemach teleinformatycznych.
C2	Nabycie umiejętności skutecznego reagowania na incydenty naruszenia bezpieczeństwa komputerowego.
C3	Ugruntowanie świadomości, że zapewnianie i monitorowanie bezpieczeństwa systemów teleinformatycznych to proces ciągły, a nie jednorazowa procedura.

PRZEDMIOTOWE EFEKTY UCZENIA – PEU	
Z zakresu wiedzy:	
PEU_W01	Posiada wiedzę z zakresu wykrywania i klasyfikowania incydentów naruszających bezpieczeństwo komputerowe.
Z zakresu umiejętności:	
PEU_U01	Potrafi wykryć, scharakteryzować w odniesieniu do modelu ISO/OSI i określić stopień istotności incydentów naruszenia cyberbezpieczeństwa.
PEU_U02	W odniesieniu do wykrytych incydentów potrafi przeprowadzić analizę przypadku, wskazać źródło zagrożenia i zaproponować działania naprawcze i zabezpieczające.
Z zakresu kompetencji społecznych:	
PEU_K01	Rozumie konieczność współpracy z innymi osobami w jednostce organizacyjnej oraz pracownikami podmiotów zewnętrznych, np. ISP, podczas procedur wykrywania incydentów naruszających bezpieczeństwo, jak i wdrażania procedur naprawczych i zapobiegawczych.

TREŚCI PROGRAMOWE		
Forma zajęć – laboratorium		Liczba godzin
L1	Omówienie zasad zaliczenia przedmiotu. Alienvault – wprowadzenie.	2
L2	Alienvault – HIDS.	4
L3	Alienvault – wykrywanie ataków na warstwę II.	4
L4	Alienvault – wykrywanie malware, ransomware.	4
L5	Alienvault – wykrywanie ataków aplikacyjnych.	4
L6	Raportowanie i procedury postępowania w przypadku wykrycia incydentów. Podsumowanie, zaliczenie.	2
Razem		20

STOSOWANE NARZĘDZIA DYDAKTYCZNE	
1.	Praca własna/grupowa w laboratorium – wykonanie procedur umożliwiających wykrywanie incydentów naruszających bezpieczeństwo z wykorzystaniem środowiska Alienvault.
2.	Prezentacja treści z wykorzystaniem multimedialnych.

METODY I FORMY OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Formy oceny (F lub P)*	Numer efektu uczenia (przedmiotowego)	Metody oceny osiągnięcia efektu uczenia
F I	PEU_W01, PEU_U01, PU02, PEU_K01	Realizacja zestawu ćwiczeń grupowych.
P I	PEU_W01, PEU_U01, PU02, PEU_K01	Średnia z ocen cząstkowych wystawianych indywidualnie po wykonaniu każdego ćwiczenia.

*F – ocena formująca (w trakcie semestru), P – ocena podsumowująca (na koniec semestru)

KRYTERIA OCENY
OSIĄGNIĘCIA PRZEDMIOTOWYCH EFEKTÓW UCZENIA

Nr PEU	Ocena dostateczna	Ocena dobra	Ocena bardzo dobra
PEU_W01	Wie jak zidentyfikować najczęstsze incydenty naruszające cyberbezpieczeństwo.	Wie jak zidentyfikować incydenty naruszające cyberbezpieczeństwo oraz scharakteryzować procedury i narzędzia służące do ich wykrywania.	Posiada specjalistyczną i zaawansowaną wiedzę z zakresu identyfikowania szerokiej gamy incydentów oraz stosowania procedur i narzędzi służących do ich wykrywania.
PEU_U01	Wie jak wykryć i scharakteryzować najczęściej występujące incydenty naruszające bezpieczeństwo systemu teleinformatycznego.	Wie jak wykryć i scharakteryzować szeroką gamę incydentów naruszających bezpieczeństwo systemu teleinformatycznego.	Wie jak wykryć i scharakteryzować szeroką gamę incydentów naruszających bezpieczeństwo systemu teleinformatycznego oraz określić stopień ich istotności.
PEU_U02	Bazując na analizie danych pochodzących z systemu teleinformatycznego potrafi wykryć i scharakteryzować szeroką gamę incydentów naruszających bezpieczeństwo tego systemu.	Bazując na analizie danych pochodzących z systemu teleinformatycznego potrafi wykryć i scharakteryzować szeroką gamę incydentów naruszających bezpieczeństwo tego systemu oraz wskazać ich potencjalne źródła.	Bazując na analizie danych pochodzących z systemu teleinformatycznego potrafi wykryć i scharakteryzować szeroką gamę incydentów naruszających bezpieczeństwo tego systemu, wskazać ich potencjalne źródła oraz zaproponować działania naprawcze i zabezpieczające.
PEU_K01	Rozumie konieczność współpracy z innymi osobami w jednostce organizacyjnej oraz pracownikami podmiotów zewnętrznych, np. ISP podczas procesu wykrywania incydentów.	Rozumie konieczność współpracy z innymi osobami w jednostce organizacyjnej oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno podczas procesu wykrywania incydentów, jak i reagowania na ich wystąpienie.	Rozumie konieczność współpracy z innymi osobami w jednostce organizacyjnej oraz pracownikami podmiotów zewnętrznych, np. ISP, zarówno podczas procesu wykrywania incydentów jak i reagowania na ich wystąpienie. Rozumie konieczność stosowania przepisów prawa (Ustawa o ochronie informacji niejawnej) w zakresie

			obowiązków pracowników podczas wykrycia wystąpienia incydentów i wdrażania postępowania naprawczego.
--	--	--	--

LITERATURA PODSTAWOWA
Jason Luttgens, Matthew Pepe, Kevin Mandia, Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, wyd. Helion, 2016. Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego, Narodowy Standard Cyberbezpieczeństwa, wersja obowiązująca podczas realizacji kursu. Dokumentacja projektu AlienVault.
LITERATURA UZUPEŁNIAJĄCA
Colby A Clark, Cybersecurity incident management - masters guide. Vol. 1-2, wyd. Independently published, 2020.

**MACIERZ POWIĄZANIA
EFEKTÓW UCZENIA DLA PRZEDMIOTU WYKRYWANIE INCYDENTÓW
Z EFEKTAMI UCZENIA NA KIERUNKU INFORMATYKA**

Przedmiotowy efekt uczenia	Odniesienie przedmiotowego efektu do efektów uczenia zdefiniowanych dla kierunku studiów i specjalności	Cele przedmiotu	Treści programowe	Numer narzędzia dydaktycznego
PEU_W01	K_W02, K_W03	C1, C2	L1-L6	1,2
PEU_U01	K_U04	C1, C2, C3	L1-L6	1,2
PEU_U02	K_U08	C1, C2, C3	L1-L6	1,2
PEU_K01	K_K01, K_K04	C3	L6	1,2