Możliwość dofinansowania

Cyberbezpieczeństwo i analiza incydentów IT – studia podyplomowe.

Numer usługi 2026/08/27/18793/3771214
Logo Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej
Wyższa Szkoła Turystyki i Ekologii w Suchej Beskidzkiej
4,8 / 5
204 oceny
7 800,00 PLN
brutto
7 800,00 PLN
netto
43,98 PLN
brutto/h
43,98 PLN
netto/h
Sucha Beskidzka
Studia podyplomowe
mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Zajęcia grupowe
177:20 h
07.11.2026 do 29.08.2027

Informacje podstawowe

- Kategoria
  Informatyka i telekomunikacja / Bezpieczeństwo IT
- Grupa docelowa usługi

  Studia są skierowane do absolwentów studiów wyższych zainteresowanych rozpoczęciem lub rozwojem kariery w cyberbezpieczeństwie, w szczególności administratorów systemów i sieci, pracowników działów IT, helpdesk i service desk, osób przygotowujących się do pracy w SOC, specjalistów bezpieczeństwa informacji i GRC oraz osób odpowiedzialnych za zarządzanie ryzykiem i zgodność.

  Program przygotowuje przede wszystkim do rozwoju w kierunku Junior SOC Analyst / Security Operations Analyst, młodszego specjalisty cyberbezpieczeństwa lub reagowania na incydenty, Vulnerability Management Analyst, specjalisty bezpieczeństwa informacji/GRC oraz administratora rozwijającego się w kierunku security.

- Minimalna liczba uczestników
  10
- Maksymalna liczba uczestników
  20
- Data zakończenia rekrutacji
  26-10-2026
- Forma prowadzenia usługi
  mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
- Podstawa uzyskania wpisu do BUR

art. 163 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r. poz. 1571, z późn. zm.)

- Zakres uprawnień
  Studia podyplomowe

Cel

Cel edukacyjny

Usługa przygotowuje uczestnika do analizowania zdarzeń i incydentów bezpieczeństwa, pracy z logami, SIEM i EDR/XDR, priorytetyzowania podatności, doboru zabezpieczeń systemów, sieci, tożsamości, chmury i aplikacji, planowania reakcji na incydenty i działań naprawczych oraz oceny ryzyka i obowiązków regulacyjnych. Uczestnik przygotowuje także raport techniczny i komunikat dla kierownictwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się, kryteria weryfikacji i metody walidacji.

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
K_W01 – Charakteryzuje podstawowe mechanizmy bezpieczeństwa systemów, sieci, tożsamości i infrastruktury IT.	1. Rozróżnia funkcje protokołów, systemów, mechanizmów uwierzytelniania i kontroli dostępu istotnych dla bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Przyporządkowuje typowe zagrożenia i podatności do właściwych elementów infrastruktury.	Test teoretyczny z wynikiem generowanym automatycznie
K_W02 – Charakteryzuje procesy Security Operations, zarządzania podatnościami i reagowania na incydenty.	1. Rozróżnia role SIEM, EDR/XDR, threat intelligence, IOC, TTP i MITRE ATT&CK.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Wyjaśnia zastosowanie CVE, CWE, CVSS, EPSS, CISA KEV oraz etapów Incident Response i DFIR.	Test teoretyczny z wynikiem generowanym automatycznie
K_W03 – Charakteryzuje zasady zarządzania bezpieczeństwem, ryzykiem i zgodnością.	1. Rozróżnia elementy SZBI, ISO/IEC 27001, analizy ryzyka i ciągłości działania.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Identyfikuje podstawowe obowiązki wynikające z KSC/NIS2, DORA i CRA właściwe dla przedstawionej sytuacji.	Test teoretyczny z wynikiem generowanym automatycznie
K_U01 – Analizuje dane sieciowe, systemowe i telemetryczne w celu identyfikacji symptomów zagrożenia.	1. Interpretuje dane z ruchu sieciowego, logów systemowych, Sysmon, SIEM lub EDR/XDR.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Na podstawie danych wskazuje możliwy rodzaj zdarzenia i jego źródło.	Test teoretyczny z wynikiem generowanym automatycznie
K_U02 – Dobiera zabezpieczenia systemów, tożsamości i dostępu do rozpoznanego ryzyka.	1. Dobiera mechanizmy MFA, RBAC, Conditional Access, least privilege,	Test teoretyczny z wynikiem

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
	PAM/PIM i hardening do przedstawionego przypadku.	generowanym automatycznie
	2. Rozpoznaje konfiguracje zwiększające ryzyko naruszenia bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
K_U03 – Priorytetyzuje podatności i dobiera działania naprawcze.	1. Łączy informacje CVSS, EPSS, CISA KEV, krytyczność zasobu i jego ekspozycję przy ustalaniu priorytetu.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Dobiera remediation, patch management oraz sposób weryfikacji skuteczności naprawy.	Test teoretyczny z wynikiem generowanym automatycznie
K_U04 – Analizuje alerty bezpieczeństwa i dobiera sposób prowadzenia triage oraz investigation.	1. Określa wagę i priorytet alertu na podstawie danych ze scenariusza.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Mapuje obserwowane działania do MITRE ATT&CK i dobiera dalsze kroki analizy, eskalacji lub strojenia detekcji.	Test teoretyczny z wynikiem generowanym automatycznie
K_U05 – Dobiera narzędzia automatyzacji do zadań analityka bezpieczeństwa.	1. Dobiera zastosowanie KQL, PowerShell, Python, regex, API lub SOAR do określonego zadania.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Rozpoznaje sytuacje, w których wynik automatyzacji lub AI wymaga dodatkowej weryfikacji przez analityka.	Test teoretyczny z wynikiem generowanym automatycznie
K_U06 – Planuje działania reagowania na incydent i zabezpieczenia materiału dowodowego.	1. Dobiera sposób zabezpieczenia dowodów, budowy timeline i zachowania chain of custody.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Ustala kolejność containment, eradication, remediation, recovery i lessons learned odpowiednią do scenariusza incydentu.	Test teoretyczny z wynikiem generowanym automatycznie
K_U07 – Ocenia bezpieczeństwo chmury, aplikacji, procesu DevSecOps i zastosowań AI.	1. Identyfikuje ryzyka związane z IAM, konfiguracją chmury, ochroną danych, API, zależnościami, SAST/DAST/SCA i SBOM.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Dobiera zabezpieczenia odpowiednie do rozpoznanego ryzyka, w tym zagrożeń związanych z AI, RAG, prompt injection i wyciekiem danych.	Test teoretyczny z wynikiem generowanym automatycznie
K_U08 – Integruje informacje dotyczące incydentu i dobiera pełny sposób postępowania z cyberatakiem na organizację.	1. Na podstawie scenariusza określa triage, timeline, techniki MITRE ATT&CK, zakres kompromitacji i źródła dowodowe.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Dobiera działania containment, remediation i recovery oraz ocenia	Test teoretyczny z wynikiem

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
	ryzyko i obowiązki raportowe.	generowanym automatycznie
	3. Rozróżnia zakres informacji wymaganych w raporcie technicznym i komunikacie dla kierownictwa.	Test teoretyczny z wynikiem generowanym automatycznie
K_K01 – Uwzględnia zasady etyki, legalności i odpowiedzialności zawodowej w działaniach związanych z cyberbezpieczeństwem.	1. Rozpoznaje działanie przekraczające zakres autoryzacji lub naruszające zasady odpowiedzialnego postępowania.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Wybiera sposób działania zgodny z zasadami etyki, legalności i ochrony informacji.	Test teoretyczny z wynikiem generowanym automatycznie
K_K02 – Uwzględnia ryzyko biznesowe i potrzeby interesariuszy podczas podejmowania decyzji dotyczących bezpieczeństwa.	1. Dobiera priorytet działania odpowiednio do wpływu incydentu na organizację.	Test teoretyczny z wynikiem generowanym automatycznie
	2. Dobiera zakres i sposób komunikacji do odbiorcy technicznego lub kierownictwa.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 1. Czy dokument jest wydany przez podmiot systemu oświaty lub szkolnictwa wyższego na podstawie odrębnych przepisów?
TAK
ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, 1871 i 1897)

Informacje

- Nazwa Podmiotu prowadzącego walidację
  Wyższa Szkoła Turystyki i Ekologii
- Nazwa Podmiotu certyfikującego
  Wyższa Szkoła Turystyki i Ekologii

Program

Program: **2 semestry, 200 godzin, minimum 30 ECTS, 130 godzin praktycznych (65%)**.

Semestr	Przedmiot	Godz.	Praktyka
I	Wprowadzenie do cyberbezpieczeństwa, role zawodowe, etyka i środowisko laboratoryjne	6	2
I	Sieci komputerowe, protokoły i analiza ruchu sieciowego	16	10
I	Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	24	16
I	Cyberzagrożenia, phishing, malware i OSINT	12	8
I	Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	18	14
I	Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	24	8
	Razem I semestr	**100**	**58**
II	Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	24	17
II	Automatyzacja pracy analityka – KQL, PowerShell, Python i SOAR	10	8
II	Reagowanie na incydenty, informatyka śledcza i ransomware	24	17
II	Bezpieczeństwo chmury i Microsoft 365	14	9
II	Bezpieczeństwo aplikacji i DevSecOps	10	6
II	AI w cyberbezpieczeństwie i bezpieczeństwo systemów AI	6	3
II	**Projekt końcowy – symulacja cyberataku na organizację**	**12**	**12**
	Razem II semestr	**100**	**72**
	Łącznie	**200**	**130**

Projekt końcowy – symulacja cyberataku na organizację – 12 godz.

Uczestnicy zespołowo analizują scenariusz ataku na organizację. Na podstawie logów, alertów i innych śladów dokonują triage zdarzenia, budują timeline, mapują techniki do MITRE ATT&CK, identyfikują zakres kompromitacji i źródła dowodowe oraz dobierają działania containment, remediation i recovery. Projekt obejmuje również ocenę ryzyka i obowiązków raportowych, opracowanie raportu technicznego oraz przygotowanie informacji dla kierownictwa.

Organizacja walidacji

Walidacja efektów uczenia się jest realizowana za pomocą testów teoretycznych z wynikiem generowanym automatycznie na platformie elektronicznej. Testy zawierają pytania zamknięte, pytania sytuacyjne, analizę logów i danych, interpretację wskaźników oraz dobór prawidłowego sposobu postępowania do przedstawionych scenariuszy bezpieczeństwa.

Harmonogram

Liczba pozycji harmonogramu: 139

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 139 Wprowadzenie do cyberbezpieczeństwa, role zawodowe, etyka i środowisko laboratoryjne	Zajęcia	Prowadzący	07-11-2026	08:30	11:30	03:00	Nie
2 z 139 -	Przerwa	-	07-11-2026	11:30	11:45	00:15	Nie
3 z 139 Wprowadzenie do cyberbezpieczeństwa, role zawodowe, etyka i środowisko laboratoryjne	Zajęcia	Prowadzący	07-11-2026	11:45	13:15	01:30	Nie
4 z 139 -	Przerwa	-	07-11-2026	13:15	14:00	00:45	Nie
5 z 139 Sieci komputerowe, protokoły i analiza ruchu sieciowego	Zajęcia	Prowadzący 1	07-11-2026	14:00	16:15	02:15	Nie
6 z 139 Sieci komputerowe, protokoły i analiza ruchu sieciowego	Zajęcia	Prowadzący 1	08-11-2026	08:30	11:30	03:00	Nie
7 z 139 -	Przerwa	-	08-11-2026	11:30	11:45	00:15	Nie
8 z 139 Sieci komputerowe, protokoły i analiza ruchu sieciowego	Zajęcia	Prowadzący 1	08-11-2026	11:45	13:15	01:30	Nie
9 z 139 -	Przerwa	-	08-11-2026	13:15	14:00	00:45	Nie
10 z 139 Sieci komputerowe, protokoły	Zajęcia	Prowadzący 1	08-11-2026	14:00	15:30	01:30	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
i analiza ruchu sieciowego							
11 z 139 Sieci komputerowe, protokoły i analiza ruchu sieciowego	Zajęcia	Prowadzący 1	21-11-2026	08:30	11:30	03:00	Nie
12 z 139 -	Przerwa	-	21-11-2026	11:30	11:45	00:15	Nie
13 z 139 Sieci komputerowe, protokoły i analiza ruchu sieciowego	Zajęcia	Prowadzący 1	21-11-2026	11:45	12:30	00:45	Nie
14 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	21-11-2026	12:30	13:15	00:45	Nie
15 z 139 -	Przerwa	-	21-11-2026	13:15	14:00	00:45	Nie
16 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	21-11-2026	14:00	16:15	02:15	Nie
17 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	22-11-2026	08:30	11:30	03:00	Nie
18 z 139 -	Przerwa	-	22-11-2026	11:30	11:45	00:15	Nie
19 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	22-11-2026	11:45	13:15	01:30	Nie
20 z 139 -	Przerwa	-	22-11-2026	13:15	14:00	00:45	Nie
21 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	22-11-2026	14:00	15:30	01:30	Nie
22 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	05-12-2026	08:30	11:30	03:00	Tak
23 z 139 -	Przerwa	-	05-12-2026	11:30	11:45	00:15	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
24 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	05-12-2026	11:45	13:15	01:30	Tak
25 z 139 -	Przerwa	-	05-12-2026	13:15	14:00	00:45	Tak
26 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	05-12-2026	14:00	16:15	02:15	Tak
27 z 139 Bezpieczeństwo Windows, Linux, Active Directory i Entra ID – IAM i hardening	Zajęcia	Prowadzący 1	06-12-2026	08:30	10:45	02:15	Tak
28 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	06-12-2026	10:45	11:30	00:45	Tak
29 z 139 -	Przerwa	-	06-12-2026	11:30	11:45	00:15	Tak
30 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	06-12-2026	11:45	13:15	01:30	Tak
31 z 139 -	Przerwa	-	06-12-2026	13:15	14:00	00:45	Tak
32 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	06-12-2026	14:00	15:30	01:30	Tak
33 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	09-01-2027	08:30	11:30	03:00	Nie
34 z 139 -	Przerwa	-	09-01-2027	11:30	11:45	00:15	Nie
35 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	09-01-2027	11:45	13:15	01:30	Nie
36 z 139 -	Przerwa	-	09-01-2027	13:15	14:00	00:45	Nie
37 z 139 Cyberzagrożenia, phishing, malware i OSINT	Zajęcia	Prowadzący 2	09-01-2027	14:00	14:45	00:45	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
38 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	09-01-2027	14:45	16:15	01:30	Nie
39 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	10-01-2027	08:30	11:30	03:00	Nie
40 z 139 -	Przerwa	-	10-01-2027	11:30	11:45	00:15	Nie
41 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	10-01-2027	11:45	13:15	01:30	Nie
42 z 139 -	Przerwa	-	10-01-2027	13:15	14:00	00:45	Nie
43 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	10-01-2027	14:00	15:30	01:30	Nie
44 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	23-01-2027	08:30	11:30	03:00	Nie
45 z 139 -	Przerwa	-	23-01-2027	11:30	11:45	00:15	Nie
46 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	23-01-2027	11:45	13:15	01:30	Nie
47 z 139 -	Przerwa	-	23-01-2027	13:15	14:00	00:45	Nie
48 z 139 Zarządzanie podatnościami i ekspozycją oraz podstawy testów penetracyjnych	Zajęcia	Prowadzący 2	23-01-2027	14:00	15:30	01:30	Nie
49 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	24-01-2027	08:30	11:30	03:00	Nie
50 z 139 -	Przerwa	-	24-01-2027	11:30	11:45	00:15	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
51 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	24-01-2027	11:45	13:15	01:30	Nie
52 z 139 -	Przerwa	-	24-01-2027	13:15	14:00	00:45	Nie
53 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	24-01-2027	14:00	15:30	01:30	Nie
54 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	06-02-2027	08:30	11:30	03:00	Nie
55 z 139 -	Przerwa	-	06-02-2027	11:30	11:45	00:15	Nie
56 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	06-02-2027	11:45	13:15	01:30	Nie
57 z 139 -	Przerwa	-	06-02-2027	13:15	14:00	00:45	Nie
58 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	06-02-2027	14:00	15:30	01:30	Nie
59 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	07-02-2027	08:30	11:30	03:00	Nie
60 z 139 -	Przerwa	-	07-02-2027	11:30	11:45	00:15	Nie
61 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	07-02-2027	11:45	13:15	01:30	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
62 z 139 -	Przerwa	-	07-02-2027	13:15	14:00	00:45	Nie
63 z 139 Zarządzanie bezpieczeństwem i ryzykiem – ISO/IEC 27001, KSC/NIS2, DORA, CRA i ciągłość działania	Zajęcia	Prowadzący 3	07-02-2027	14:00	15:30	01:30	Nie
64 z 139 -	Walidacja	Prowadzący 3	07-02-2027	15:30	16:10	00:40	Nie
65 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	13-03-2027	08:30	11:30	03:00	Nie
66 z 139 -	Przerwa	-	13-03-2027	11:30	11:45	00:15	Nie
67 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	13-03-2027	11:45	13:15	01:30	Nie
68 z 139 -	Przerwa	-	13-03-2027	13:15	14:00	00:45	Nie
69 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	13-03-2027	14:00	15:30	01:30	Nie
70 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	14-03-2027	08:30	11:30	03:00	Nie
71 z 139 -	Przerwa	-	14-03-2027	11:30	11:45	00:15	Nie
72 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	14-03-2027	11:45	13:15	01:30	Nie
73 z 139 -	Przerwa	-	14-03-2027	13:15	14:00	00:45	Nie
74 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	14-03-2027	14:00	15:30	01:30	Nie
75 z 139 Security Operations – SOC,	Zajęcia	Prowadzący 3	10-04-2027	08:30	11:30	03:00	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
SIEM, EDR/XDR, threat intelligence i detection engineering							
76 z 139 -	Przerwa	-	10-04-2027	11:30	11:45	00:15	Nie
77 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	10-04-2027	11:45	13:15	01:30	Nie
78 z 139 -	Przerwa	-	10-04-2027	13:15	14:00	00:45	Nie
79 z 139 Security Operations – SOC, SIEM, EDR/XDR, threat intelligence i detection engineering	Zajęcia	Prowadzący 3	10-04-2027	14:00	15:30	01:30	Nie
80 z 139 Automatyzacja pracy analityka bezpieczeństwa – KQL, PowerShell, Python i SOAR	Zajęcia	Prowadzący 5	11-04-2027	08:30	11:30	03:00	Nie
81 z 139 -	Przerwa	-	11-04-2027	11:30	11:45	00:15	Nie
82 z 139 Automatyzacja pracy analityka bezpieczeństwa – KQL, PowerShell, Python i SOAR	Zajęcia	Prowadzący 5	11-04-2027	11:45	13:15	01:30	Nie
83 z 139 -	Przerwa	-	11-04-2027	13:15	14:00	00:45	Nie
84 z 139 Automatyzacja pracy analityka bezpieczeństwa – KQL, PowerShell, Python i SOAR	Zajęcia	Prowadzący 5	11-04-2027	14:00	15:30	01:30	Nie
85 z 139 Automatyzacja pracy analityka bezpieczeństwa – KQL, PowerShell, Python i SOAR	Zajęcia	Prowadzący 5	24-04-2027	08:30	10:00	01:30	Tak
86 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	24-04-2027	10:00	11:30	01:30	Tak
87 z 139 -	Przerwa	-	24-04-2027	11:30	11:45	00:15	Tak
88 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	24-04-2027	11:45	13:15	01:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
89 z 139 -	Przerwa	-	24-04-2027	13:15	14:00	00:45	Tak
90 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	24-04-2027	14:00	14:45	00:45	Tak
91 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	25-04-2027	08:30	11:30	03:00	Tak
92 z 139 -	Przerwa	-	25-04-2027	11:30	11:45	00:15	Tak
93 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	25-04-2027	11:45	13:15	01:30	Tak
94 z 139 -	Przerwa	-	25-04-2027	13:15	14:00	00:45	Tak
95 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	25-04-2027	14:00	14:45	00:45	Tak
96 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	08-05-2027	08:30	11:30	03:00	Nie
97 z 139 -	Przerwa	-	08-05-2027	11:30	11:45	00:15	Nie
98 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	08-05-2027	11:45	13:15	01:30	Nie
99 z 139 -	Przerwa	-	08-05-2027	13:15	14:00	00:45	Nie
100 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	08-05-2027	14:00	14:45	00:45	Nie
101 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	09-05-2027	08:30	11:30	03:00	Nie
102 z 139 -	Przerwa	-	09-05-2027	11:30	11:45	00:15	Nie
103 z 139 Reagowanie na incydenty, informatyka śledcza i ransomware	Zajęcia	Prowadzący 4	09-05-2027	11:45	12:30	00:45	Nie
104 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	09-05-2027	12:30	13:15	00:45	Nie
105 z 139 -	Przerwa	-	09-05-2027	13:15	14:00	00:45	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
106 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący	09-05-2027	14:00	14:45	00:45	Nie
107 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	22-05-2027	08:30	11:30	03:00	Nie
108 z 139 -	Przerwa	-	22-05-2027	11:30	11:45	00:15	Nie
109 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	22-05-2027	11:45	13:15	01:30	Nie
110 z 139 -	Przerwa	-	22-05-2027	13:15	14:00	00:45	Nie
111 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	22-05-2027	14:00	14:45	00:45	Nie
112 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	23-05-2027	08:30	11:30	03:00	Nie
113 z 139 -	Przerwa	-	23-05-2027	11:30	11:45	00:15	Nie
114 z 139 Bezpieczeństwo chmury i Microsoft 365	Zajęcia	Prowadzący 2	23-05-2027	11:45	12:30	00:45	Nie
115 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący 2	23-05-2027	12:30	13:15	00:45	Nie
116 z 139 -	Przerwa	-	23-05-2027	13:15	14:00	00:45	Nie
117 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący 2	23-05-2027	14:00	14:45	00:45	Nie
118 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący	05-06-2027	08:30	11:30	03:00	Nie
119 z 139 -	Przerwa	-	05-06-2027	11:30	11:45	00:15	Nie
120 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący	05-06-2027	11:45	13:15	01:30	Nie
121 z 139 -	Przerwa	-	05-06-2027	13:15	14:00	00:45	Nie
122 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący	05-06-2027	14:00	14:45	00:45	Nie
123 z 139 Bezpieczeństwo aplikacji i DevSecOps	Zajęcia	Prowadzący	06-06-2027	08:30	09:15	00:45	Nie

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
124 z 139 AI w cyberbezpieczeństwie i bezpieczeństwo systemów AI	Zajęcia	Prowadzący	06-06-2027	09:15	11:30	02:15	Nie
125 z 139 -	Przerwa	-	06-06-2027	11:30	11:45	00:15	Nie
126 z 139 AI w cyberbezpieczeństwie i bezpieczeństwo systemów AI	Zajęcia	Prowadzący	06-06-2027	11:45	13:15	01:30	Nie
127 z 139 -	Przerwa	-	06-06-2027	13:15	14:00	00:45	Nie
128 z 139 AI w cyberbezpieczeństwie i bezpieczeństwo systemów AI	Zajęcia	Prowadzący	06-06-2027	14:00	14:45	00:45	Nie
129 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	12-06-2027	08:30	10:00	01:30	Nie
130 z 139 -	Przerwa	-	12-06-2027	10:00	10:15	00:15	Nie
131 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	12-06-2027	10:15	11:45	01:30	Nie
132 z 139 -	Przerwa	-	12-06-2027	11:45	12:30	00:45	Nie
133 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	12-06-2027	12:30	14:00	01:30	Nie
134 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	13-06-2027	08:30	10:00	01:30	Nie
135 z 139 -	Przerwa	-	13-06-2027	10:00	10:15	00:15	Nie
136 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	13-06-2027	10:15	11:45	01:30	Nie
137 z 139 -	Przerwa	-	13-06-2027	11:45	12:30	00:45	Nie
138 z 139 Projekt końcowy – symulacja cyberataku na organizację	Zajęcia	Prowadzący	13-06-2027	12:30	14:00	01:30	Nie
139 z 139 -	Walidacja	Prowadzący	13-06-2027	14:00	14:40	00:40	Nie

Podsumowanie

Rodzaj godzin	Liczba godzin
Rodzaj godzin Suma godzin zegarowych usługi	Liczba godzin 177:20
Rodzaj godzin w tym suma godzin zajęć	Liczba godzin 150:00
Rodzaj godzin w tym suma godzin walidacji	Liczba godzin 01:20
Rodzaj godzin w tym suma przerw	Liczba godzin 26:00
Rodzaj godzin Suma godzin dydaktycznych bez przerw	Liczba godzin 201:35

Cennik

Cennik

- Rodzaj ceny
  Cena
- Koszt przypadający na 1 uczestnika brutto
  7 800,00 PLN

  Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT

- Koszt przypadający na 1 uczestnika netto
  7 800,00 PLN
- Koszt osobogodziny brutto
  43,98 PLN
- Koszt osobogodziny netto
  43,98 PLN
- W tym koszt walidacji brutto
  88,00 PLN
- W tym koszt walidacji netto
  88,00 PLN
- W tym koszt certyfikowania brutto
  0,00 PLN
- W tym koszt certyfikowania netto
  0,00 PLN

Liczba godzin usługi

- Rodzaj godzin
  Liczba godzin
- Liczba godzin zegarowych usługi
  177:20

Prowadzący

Liczba prowadzących: 6
1 z 6

Prowadzący

Specjalista ds. cyberbezpieczeństwa
2 z 6

Prowadzący 1

Specjalista ds. sieci i systemów komputerowych
3 z 6

Prowadzący 2

Specjalista ds. zagrożeń w sieci
4 z 6

Prowadzący 3

Specjalista ds. zarządzania bezpieczeństwem i ryzykiem
5 z 6

Prowadzący 4

Specjalista ds. informatyki śledczej
6 z 6

Prowadzący 5

Specjalista ds. automatyzacji pracy

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzymuje materiały dydaktyczne w formie elektronicznej, instrukcje laboratoryjne, zestawy logów i danych do analizy, scenariusze case study, wzory dokumentacji incydentowej i rejestru ryzyka, materiały dotyczące MITRE ATT&CK, KQL i zarządzania podatnościami oraz dostęp do przygotowanych środowisk i kont laboratoryjnych niezbędnych do wykonania ćwiczeń.

Warunki uczestnictwa

Obowiązkowo: ukończone studia I stopnia, II stopnia lub jednolite studia magisterskie

Wskazane jest posiadanie podstawowej znajomości systemów Windows/Linux oraz sieci komputerowych. Osoby bez podstaw informatycznych mogą zostać skierowane na test diagnostyczny i kurs przygotowawczy realizowany przed rozpoczęciem zasadniczego programu studiów.

Informacje dodatkowe

Walidacja odbywa się poprzez testy egzaminacyjne udostępniane słuchaczom na platformie e-learningowej WSTiE. Wynik testów jest generowany automatycznie przez system.

Walidacja jest ustalana indywidualnie z uczestnikiem usługi i odbędzie się **w okresie od ..... do ..... (I semestr)** oraz **w okresie od ..... do ..... (II semestr)** Termin walidacji dostępny będzie u osoby nadzorującej usługę po stronie Dostawcy Usług.

Do ceny usługi została wliczona opłata wpisowa w wysokości 300 zł.

Zaakceptowano regulamin projektu "Małopolski Pociąg do Kariery - sezon I" dla Instytucji Szkoleniowych.

Warunki techniczne

Zajęcia zdalne w czasie rzeczywistym prowadzone są na platformie Webex.

Wymagania techniczne:

komputer / laptop ze stałym dostępem do Internetu (Szybkość pobierania/przesyłania: minimalna

2 Mb/s / 128 kb/s; zalecana 4 Mb/s / 512 kb/s)

przeglądarka internetowa – zalecane: Google Chrome, Mozilla Firefox

słuchawki lub dobrej jakości głośniki

mikrofon

zalecane: kamera (w przypadku komputerów stacjonarnych)

spokojne miejsce, odizolowane od zewnętrznych czynników rozpraszających

Adres

ul. Zamkowa 1
34-200 Sucha Beskidzka
woj. małopolskie

Udogodnienia w miejscu realizacji usługi

- Wi-fi
- Laboratorium komputerowe

Kontakt

Anna Oleksa-Kaźmierczak

E-mail
szkola@wste.edu.pl
Telefon
(+48) 338 744 605