Możliwość dofinansowania

Analiza incydentów bezpieczeństwa IT - szkolenie

Numer usługi 2026/07/08/172284/3678263

3 800,00 PLN brutto
3 800,00 PLN netto
237,50 PLN brutto/h
237,50 PLN netto/h
261,33 PLN cena rynkowa

UKNOW EDU SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

2 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
16:00 h
24.09.2026 do 25.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za bezpieczeństwo IT, administrację systemami i sieciami oraz monitorowanie infrastruktury teleinformatycznej w organizacji. W szczególności adresatami szkolenia są: administratorzy systemów i sieci, specjaliści IT, pracownicy działów bezpieczeństwa informacji, osoby zajmujące się monitoringiem infrastruktury, analizą logów, obsługą incydentów bezpieczeństwa oraz członkowie zespołów IT/SOC. Szkolenie jest przeznaczone również dla osób, które chcą rozwinąć praktyczne umiejętności w zakresie identyfikowania, analizowania i reagowania na incydenty bezpieczeństwa IT, w tym analizy logów, ruchu sieciowego, zagrożeń malware, ransomware oraz ataków ukierunkowanych.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	18-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem edukacyjnym szkolenia jest przygotowanie uczestników do samodzielnego identyfikowania, analizowania i klasyfikowania incydentów bezpieczeństwa IT oraz podejmowania właściwych działań w zakresie reagowania na zagrożenia w środowisku teleinformatycznym.

Po zakończeniu szkolenia uczestnik będzie potrafił rozpoznawać rodzaje incydentów bezpieczeństwa, analizować logi systemowe i zdarzenia bezpieczeństwa, interpretować ruch sieciowy, identyfikować symptomy złośliwej komunikacji oraz oceniać pr

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia podstawowe rodzaje incydentów bezpieczeństwa IT oraz wskazuje ich możliwe źródła.	Poprawnie wskazuje przykładowe rodzaje incydentów oraz źródła informacji o incydentach.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wyjaśnia etapy cyberataku zgodnie z metodologią Cyber Kill Chain.	Poprawnie porządkuje lub opisuje podstawowe etapy ataku według Cyber Kill Chain.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik analizuje logi i zdarzenia bezpieczeństwa w celu identyfikacji anomalii oraz podejrzanych aktywności.	Poprawnie wskazuje, które wpisy lub zdarzenia mogą świadczyć o incydencie bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik identyfikuje podstawowe symptomy zagrożeń w ruchu sieciowym i dobiera adekwatne działania reakcji na incydent.	Poprawnie rozpoznaje przykładowe symptomy złośliwej komunikacji oraz wskazuje właściwe działania Incident Response.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Metodologia Cyber Kill Chain i podstawy incydentów

- rodzaje incydentów bezpieczeństwa,
- źródła informacji o incydentach,
- wprowadzenie do metodologii Cyber Kill Chain.

1. Narzędzia i podstawy monitoringu

- narzędzia do analizy incydentów,
- monitoring i analiza logów w środowiskach IT,
- podstawowa konfiguracja systemów monitoringu.

1. Analiza logów i korelacja zdarzeń

- techniki analizy logów systemowych,
- identyfikacja wzorców ataków na podstawie zebranych danych,
- korelacja zdarzeń bezpieczeństwa / SIEM.

1. Analiza ruchu sieciowego

- analiza ruchu sieciowego w kontekście incydentów,
- techniki przechwytywania ruchu,
- analiza protokołów sieciowych pod kątem bezpieczeństwa,
- praca z plikami pcap i narzędziami do analizy pakietów.

1. Identyfikacja zagrożeń w sieci

- wykrywanie anomalii w ruchu,
- identyfikacja złośliwej komunikacji, w tym C2 i exfiltration.

1. Praktyczna analiza zagrożeń

- analiza przebiegu ataku ransomware,
- podstawy analizy złośliwego oprogramowania,
- ocena wektorów infekcji,
- analiza ataków ukierunkowanych APT.

1. Reagowanie na incydenty

- techniki Incident Response,
- dobór działań reakcji do rodzaju incydentu,
- podsumowanie szkolenia i wnioski końcowe.

1. Walidacja efektów uczenia się

- test teoretyczny z wynikiem generowanym automatycznie.

Harmonogram

Liczba pozycji harmonogramu: 15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 Metodologia Cyber Kill Chain i podstawy incydentów	Zajęcia	Monika Bienies	24-09-2026	08:00	10:00	02:00
2 z 15 -	Przerwa	-	24-09-2026	10:00	10:15	00:15
3 z 15 Narzędzia i podstawy monitoringu	Zajęcia	Monika Bienies	24-09-2026	10:15	12:00	01:45
4 z 15 -	Przerwa	-	24-09-2026	12:00	12:30	00:30
5 z 15 Zaawansowana analiza logów i korelacja zdarzeń	Zajęcia	Monika Bienies	24-09-2026	12:30	14:15	01:45
6 z 15 -	Przerwa	-	24-09-2026	14:15	14:30	00:15
7 z 15 Wstęp do analizy ruchu sieciowego	Zajęcia	Monika Bienies	24-09-2026	14:30	16:00	01:30
8 z 15 Techniki przechwytywania i analizy ruchu	Zajęcia	Monika Bienies	25-09-2026	08:00	10:00	02:00
9 z 15 -	Przerwa	-	25-09-2026	10:00	10:15	00:15
10 z 15 Identyfikacja zagrożeń w sieci	Zajęcia	Monika Bienies	25-09-2026	10:15	12:00	01:45
11 z 15 -	Przerwa	-	25-09-2026	12:00	12:30	00:30
12 z 15 Praktyczna analiza zagrożeń	Zajęcia	Monika Bienies	25-09-2026	12:30	14:15	01:45
13 z 15 -	Przerwa	-	25-09-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 15 Praktyczna analiza zagrożeń – Część 2 i reagowanie	Zajęcia	Monika Bienies	25-09-2026	14:30	15:45	01:15
15 z 15 -	Walidacja	Monika Bienies	25-09-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	16:00
w tym suma godzin zajęć	13:45
w tym suma godzin walidacji	00:15
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	18:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 800,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	3 800,00 PLN
Koszt osobogodziny brutto	237,50 PLN
Koszt osobogodziny netto	237,50 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin

Liczba godzin zegarowych usługi	16:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Monika Bienies

Prowadzący merytoryczny zostanie przypisany do usługi przed rozpoczęciem szkolenia, zgodnie z zakresem tematycznym usługi oraz wymaganiami dotyczącymi doświadczenia w obszarze bezpieczeństwa IT i analizy incydentów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymają materiały szkoleniowe wyłącznie w formie elektronicznej, najpóźniej w pierwszym dniu szkolenia. Materiały zostaną udostępnione w języku polskim.

Warunki techniczne

Szkolenie będzie realizowane w formie zdalnej, za pośrednictwem platformy szkoleniowej / komunikatora internetowego udostępnionego przez Wykonawcę.

Uczestnik powinien posiadać komputer lub laptop z dostępem do Internetu, aktualną przeglądarką internetową, głośnikami lub słuchawkami oraz mikrofonem. Zalecane jest stabilne łącze internetowe umożliwiające udział w wideokonferencji oraz odbiór obrazu i dźwięku w czasie rzeczywistym.

Kontakt

Monika Bienies

E-mail szkolenia@uknowedu.pl

Telefon (+48) 693 708 705