Możliwość dofinansowania

Szkolenie: Cybersecurity Analyst (Analityk Cyberbezpieczeństwa)

Numer usługi 2026/03/12/22948/3401728

7 380,00 PLN brutto
6 000,00 PLN netto
147,60 PLN brutto/h
120,00 PLN netto/h
261,33 PLN cena rynkowa

Ernabo Adrian Flak

4,6 / 5

856 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
50:00 h
23.11.2026 do 17.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie skierowane jest do osób zainteresowanych zdobyciem podstawowych kompetencji w zakresie **analizy cyberbezpieczeństwa oraz pracy w obszarze SOC (Security Operations Center)**. Wymagania wstępne: Od uczestników oczekuje się: • podstawowej znajomości obsługi komputera i systemów operacyjnych • podstawowej wiedzy o działaniu sieci komputerowych (mile widziana, ale niekonieczna) • zainteresowania tematyką bezpieczeństwa IT. Szkolenie przeznaczone jest również dla uczestników projektu **Kierunek Rozwój** realizowany przez WUP w Toruniu. • Usługa również adresowana dla Uczestników Projektu **Małopolski Pociąg do Kariery sezon 1** • Usługa skierowana również dla uczestników projektu " **Zachodniopomorskie bony szkoleniowe"** • Oraz dla uczestników projektów dofinansowanych **w całej Polsce** • Szkolenie skierowane jest zarówno do **osób indywidualnych, jak i pracodawców i pracowników**
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	8
Data zakończenia rekrutacji	18-11-2026

Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	50
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

Szkolenie przygotowujee uczestników do pracy na stanowisku analityka cyberbezpieczeństwa poprzez rozwinięcie wiedzy i praktycznych umiejętności w zakresie identyfikacji, analizy oraz reagowania na incydenty bezpieczeństwa w środowisku IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik charakteryzuje podstawowe pojęcia i zagrożenia związane z cyberbezpieczeństw m.	definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa	Test teoretyczny
	opisuje model bezpieczeństwa informacji (CIA: poufność, integralność, dostępność)	Test teoretyczny
	wymienia najczęstsze typy zagrożeń cybernetycznych	Test teoretyczny
	opisuje rolę analityka bezpieczeństwa w strukturze SOC	Test teoretyczny
Uczestnik opisuje podstawowe elementy infrastruktury IT istotne w analizie bezpieczeństwa.	wyjaśnia działanie podstawowych protokołów sieciowych (TCP/IP, DNS, HTTP/HTTPS)	Test teoretyczny
	rozpoznaje elementy infrastruktury sieciowej	Test teoretyczny
	opisuje rolę logów systemowych w monitorowaniu bezpieczeństwa	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wyjaśnia zasady analizy ruchu sieciowego i identyfikacji zagrożeń.	wskazuje zastosowanie narzędzi do analizy ruchu sieciowego	Test teoretyczny
	wyjaśnia pojęcie wskaźników kompromitacji (IOC)	Test teoretyczny
	rozpoznaje przykłady nietypowych zdarzeń w ruchu sieciowym	Test teoretyczny
Uczestnik opisuje podstawowe etapy reagowania na incydenty bezpieczeństwa.	wymienia etapy procesu reagowania na incydent	Test teoretyczny
	opisuje znaczenie dokumentowania incydentów	Test teoretyczny
	wskazuje elementy raportu z incydentu bezpieczeństwa	Test teoretyczny

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

Program szkolenia jest dostosowany do potrzeb uczestników usługi oraz głównego celu usługi i jej charakteru oraz obejmuje zakres tematyczny usługi. Uczestnik nie musi spełniać dodatkowych wymagań dot. poziomu zaawansowania.

Usługa prowadzona jest w godzinach dydaktycznych. **Przerwy nie są wliczone w ogólny czas usługi rozwojowej.** Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazuje nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Szkolenie będzie realizowane **zdalnie w czasie rzeczywistym** za pomocą platformy **ClickMeeting**, co umożliwia aktywny udział uczestników w warsztatach i ćwiczeniach grupowych.

Szkolenie realizowane jest przez platformę umożliwiającą:

- udostępnianie ekranu,
- czat, komunikację audio-wideo,
- współdzielenie materiałów i plików,
- interaktywną prezentację kodu i analiz danych.

Każdy uczestnik pracuje indywidualnie na swoim komputerze z bieżącym wsparciem trenera.

Przed dokonaniem zapisu i złożeniem karty uczestnictwa do Operatora, zachęcamy do **kontaktowania się z nami telefonicznie, SMS-em lub e-mailem** pod adresem/numerem wskazanym w zakładce **„Kontakt”**.

Pozwoli to **potwierdzić dostępność miejsca** w grupie szkoleniowej oraz rozwiać ewentualne wątpliwości.

Moduł I: Wprowadzenie do cyberbezpieczeństwa i pracy analityka (6h dyd., 4h teoria, 2h praktyka)

Moduł otwierający szkolenie wprowadza uczestników w świat współczesnych zagrożeń cybernetycznych oraz realiów pracy analityka bezpieczeństwa. Omawiany jest aktualny krajobraz zagrożeń, najczęściej występujące wektory ataków oraz mechanizmy obronne stosowane w organizacjach.

Uczestnicy poznają rolę i odpowiedzialności analityka w strukturze SOC (Security Operations Center), a także podstawowe modele bezpieczeństwa informacji, takie jak poufność, integralność i dostępność (CIA).

Moduł II: Podstawy infrastruktury IT w analizie bezpieczeństwa (8h dyd, 2h teoria, 6h praktyka)

Moduł koncentruje się na praktycznym zrozumieniu działania sieci komputerowych i systemów operacyjnych — w zakresie niezbędnym do skutecznej analizy zdarzeń bezpieczeństwa.

Omawiane są kluczowe protokoły komunikacyjne (TCP/IP, DNS, HTTP/HTTPS) oraz ich znaczenie w kontekście monitorowania ruchu i wykrywania anomalii. Uczestnicy uczą się interpretować logi systemowe generowane przez systemy takie jak Windows oraz Linux.

Szczególny nacisk kładziony jest na identyfikację zdarzeń mogących wskazywać na próbę nieautoryzowanego dostępu, eskalację uprawnień lub obecność złośliwego oprogramowania.

Moduł III: Analiza ruchu sieciowego i wykrywanie zagrożeń (8h dyd, 2h teoria, 6h praktyka)

Moduł warsztatowy, w którym uczestnicy zdobywają praktyczne umiejętności analizy ruchu sieciowego oraz identyfikacji podejrzanych aktywności.

Praca odbywa się z wykorzystaniem narzędzi takich jak **Wireshark**, umożliwiającego szczegółową analizę pakietów sieciowych, oraz **Nmap**, wykorzystywanego do identyfikacji aktywnych hostów i usług.

Ćwiczenia obejmują analizę prób skanowania, rozpoznawanie anomalii komunikacyjnych, identyfikację wskaźników kompromitacji (IOC), interpretację nietypowych zachowań w ruchu sieciowym..

Moduł IV: Analiza logów i systemy klasy SIEM (12h,)

Moduł szkolenia skupiony na pracy z logami i narzędziami wykorzystywanymi w środowisku.

Uczestnicy poznają koncepcję systemów SIEM oraz uczą się pracy Zakres obejmuje tworzenie zapytań, filtrowanie danych, korelację zdarzeń oraz identyfikację nieprawidłowości w dużych zbiorach logów.

Szczególny nacisk położony jest na logiczne myślenie analityczne oraz budowanie procesu dochodzenia – od alertu do wniosków.

Efekt modułu:

Uczestnik potrafi analizować logi w środowisku SIEM oraz identyfikować zdarzenia wymagające eskalacji.

Moduł V Reagowanie na incydenty i raportowanie (8h dyd, 4h teoria, 4h praktyka))

Moduł poświęcony procesowi reagowania na incydenty bezpieczeństwa — od momentu wykrycia zdarzenia do przygotowania raportu końcowego.

Omawiany jest cykl reagowania zgodny z dobrymi praktykami branżowymi (m.in. NIST), zabezpieczanie materiału dowodowego oraz współpraca z zespołami IT i zarządem. Uczestnicy uczą się tworzyć raport techniczny oraz streszczenie biznesowe incydentu.

Moduł obejmuje symulację incydentu.

Moduł VI Projekt końcowy – analiza scenariusza incydentu (7h dyd. praktyka)

Szkolenie kończy się kompleksowym ćwiczeniem projektowym, integrującym wiedzę i umiejętności zdobyte podczas wszystkich modułów.

Uczestnicy pracują na scenariuszu incydentu obejmującym analizę logów, ruchu sieciowego oraz alertów systemowych. Celem jest identyfikacja źródła zagrożenia, określenie jego zakresu oraz przygotowanie rekomendacji działań naprawczych.

Walidacja (test z wynikiem gen automatycznie, analiza dowodów i deklaracji)

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 380,00 PLN
Koszt przypadający na 1 uczestnika netto	6 000,00 PLN
Koszt osobogodziny brutto	147,60 PLN
Koszt osobogodziny netto	120,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma materiały dydaktyczne oraz prezentację w formie e-mail.

Trener prowadzący szkolenie na bieżąco będzie przesyłał zadania oraz ćwiczenia.

Warunki uczestnictwa

Warunkiem zdobycia certyfikatu potwierdzającego zdobyte kompetencje jest przystąpienie do Egzaminu. Na egzamin uczestnik nie musi dokonywać osobnego zapisu oraz jest w koszt usługi.

Wymagana jest obecność min 80% lub zgodna ze wskazaniami Operatora. Obecność na usłudze weryfikowana będzie na podstawie raportu logowań wygenerowanego z platformy.

Uczestnicy przyjmują do wiadomości, że usługa może być poddana monitoringowi z ramienia Operatora lub PARP i wyrażają na to zgodę.

Uczestnik ma obowiązek zapisania się na usługę przez BUR co najmniej w dniu zakończenia rekrutacji.

Organizator zapewnia dostępność osobom ze szczególnymi potrzebami podczas realizacji usług rozwojowych zgodnie z Ustawą z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz.U. 2022 poz. 2240) oraz „Standardami dostępności dla polityki spójności 2021-2027”. **W przypadku potrzeby zapewnienia specjalnych udogodnień prosimy o kontakt przed zapisem na usługę!**

Informacje dodatkowe

- **Zapis BUR nie jest jednoznaczny z zarezerwowaniem miejsca**. W celu potwierdzenia miejsca prosimy o dodatkowy kontakt telefoniczny/sms lub mailowy na adres/numer wskazany w zakładce " kontakt"
- zawarto umowę z WUP w Szczecinie w ramach projektu Zachodniopomorskie Bony Szkoleniowe
- usługi dedykowane również uczestnikom innych programów dofinansowań

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 3 ust. 1 pkt. 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień - w przypadku dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

Warunki techniczne szkolenia zdalnego

1. Sprzęt uczestnika:

- Komputer stacjonarny lub laptop z minimum:
  - Procesor: Intel i5 / AMD Ryzen 5 lub wyższy
  - RAM: 8 GB (zalecane 16 GB)
  - Dysk SSD minimum 256 GB
- Monitor o rozdzielczości minimum 1920x1080
- Kamera i mikrofon (wbudowane lub zewnętrzne)
- Słuchawki z mikrofonem dla lepszej jakości dźwięku

Obowiązkowe:

- **Kamera:**Uczestnik powinien posiadać działającą kamerę (wbudowaną w laptop/komputer lub zewnętrzną). Kamera umożliwia aktywny udział w sesjach, prezentację ćwiczeń grupowych oraz interakcję z prowadzącym.
- **Mikrofon:** Niezbędny jest sprawny mikrofon (wbudowany lub zewnętrzny, np. w zestawie słuchawkowym).Umożliwia zadawanie pytań, udział w dyskusjach i ćwiczeniach grupowych.
- Zalecane użycie słuchawek z mikrofonem, aby zredukować echo i poprawić jakość dźwięku.

2. Oprogramowanie:

- Przeglądarka internetowa aktualnej wersji (Chrome, Edge, Firefox)
- Szkolenie prowadzone będzie na platformie ClickMeeting

3. Łącze internetowe:

- Minimum 10 Mbps download / 5 Mbps upload
- Stabilne połączenie bez dużych przerw i opóźnień

4. Środowisko pracy:

- Ciche miejsce do pracy i nauki
- Dostęp do powierzchni roboczej umożliwiającej komfortowe używanie komputera
- Możliwość dzielenia ekranu w trakcie sesji praktycznych i konsultacji

5. Dodatkowe wymagania:

- Podstawowa znajomość obsługi komputera i przeglądarki internetowej
- Znajomość podstawowych pojęć graficznych i interfejsowych będzie dodatkowym atutem
- Uczestnicy powinni przygotować przykłady projektów lub inspiracje, do projektu praktycznego

Kontakt

AGATA FLAK

E-mail kontakt@dofinansowanekursy.pl

Telefon (+48) 530 642 270