Możliwość dofinansowania

CompTIA Cybersecurity Analyst (CySA+) FORMA ZDALNA

Numer usługi 2026/07/29/5762/3716628

5 473,50 PLN brutto
4 450,00 PLN netto
156,39 PLN brutto/h
127,14 PLN netto/h
261,33 PLN cena rynkowa

Imperium Szkoleniowe
Targosiński Kamil

4,5 / 5
326 ocen

- Usługa szkoleniowa
- zdalna w czasie rzeczywistym
- Zajęcia grupowe
- 35:00 h
- 21.09.2026 do 25.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**CompTIA Security +** jest certyfikacją rozpoznawalną na całym świecie, która potwierdza podstawową wiedzę i umiejętności z zakresu bezpieczeństwa IT. Zwiększ swoje kompetencje na rynku IT. Zdobądź jeden z najbardziej cenionych certyfikatów z zakresu Bezpieczeństwa IT.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	14-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Uczestnik tego szkolenia poszerzy swoją dotychczasową wiedzę między innymi o: zarządzanue cyberbezpieczeństwem, identyfikowanie różnych typów zagrożeń, ocenę bezpieczeństwa organizacji, oraz obsługę incydentów w momencie ich wystąpienia.

Więcej informacji o szkoleniu: https://imperiumszkoleniowe.pl/szkolenie/comptia-cybersecurity-analyst-cysa/

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik poznaje metody zapobiegania, wykrywania i zwalczania zagrożeń cyberbezpieczeństwa.	Uczestnik potrafi wybrać odpowiednie konfiguracje oraz metody zabezpieczeń systemów.	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

CompTIA Cybersecurity Analyst (CySA+)

- Reagowanie na luki w zabezpieczeniach, obsługa i zarządzanie.
- Koncepcje; „Threat Intelligence” i „Threat Hunting”.
- Kluczowe koncepcje architektury systemów i sieci
- Usprawnianie procesów w operacjach bezpieczeństwa
- Wdrażanie metod skanowania podatności
- Wykonywanie analizy podatności
- Przekazywanie informacji o podatnościach.
- Wyjaśnienie działań związanych z reagowaniem na incydenty.
- Komunikacja w zakresie reagowania na incydenty.
- Narzędzia do identyfikacji złośliwej aktywności
- Analizowanie potencjalnie złośliwej aktywności.
- Ocena podatności aplikacji na zagrożenia.
- Ocena podatności aplikacji
- Najlepsze praktyki w zakresie bezpieczeństwa aplikacji i ograniczania ataków.
- Przygotowanie do egzaminu CompTIA Cybersecurity Analyst+ (egzamin CS0-003)

Harmonogram

Liczba pozycji harmonogramu: 36

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 dzień I COMPTIA CYSA + - Reagowanie na luki w zabezpieczeniach, obsługa i zarządzanie – część 1	Zajęcia	Miłosz Jaworski	21-09-2026	08:30	10:00	01:30
2 z 36 -	Przerwa	-	21-09-2026	10:00	10:20	00:20
3 z 36 dzień I COMPTIA CYSA + - Reagowanie na luki w zabezpieczeniach, obsługa i zarządzanie – część 2	Zajęcia	Miłosz Jaworski	21-09-2026	10:20	11:50	01:30
4 z 36 -	Przerwa	-	21-09-2026	11:50	12:10	00:20
5 z 36 dzień I COMPTIA CYSA + - Koncepcje Threat Intelligence	Zajęcia	Miłosz Jaworski	21-09-2026	12:10	13:40	01:30
6 z 36 -	Przerwa	-	21-09-2026	13:40	14:00	00:20
7 z 36 dzień I COMPTIA CYSA + - Koncepcje Threat Hunting	Zajęcia	Miłosz Jaworski	21-09-2026	14:00	15:30	01:30
8 z 36 dzień II COMPTIA CYSA + - Kluczowe koncepcje architektury systemów	Zajęcia	Miłosz Jaworski	22-09-2026	08:30	10:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 36 -	Przerwa	-	22-09-2026	10:00	10:20	00:20
10 z 36 dzień II COMPTIA CYSA + - Kluczowe koncepcje architektury sieci	Zajęcia	Miłosz Jaworski	22-09-2026	10:20	11:50	01:30
11 z 36 -	Przerwa	-	22-09-2026	11:50	12:10	00:20
12 z 36 dzień II COMPTIA CYSA + - Usprawnianie procesów w operacjach bezpieczeństwa	Zajęcia	Miłosz Jaworski	22-09-2026	12:10	13:40	01:30
13 z 36 -	Przerwa	-	22-09-2026	13:40	14:00	00:20
14 z 36 dzień II COMPTIA CYSA + - Wdrażanie metod skanowania podatności	Zajęcia	Miłosz Jaworski	22-09-2026	14:00	15:30	01:30
15 z 36 dzień III COMPTIA CYSA + - Wykonywanie analizy podatności	Zajęcia	Miłosz Jaworski	23-09-2026	08:30	10:00	01:30
16 z 36 -	Przerwa	-	23-09-2026	10:00	10:20	00:20
17 z 36 dzień III COMPTIA CYSA + - Przekazywanie informacji o podatnościach	Zajęcia	Miłosz Jaworski	23-09-2026	10:20	11:50	01:30
18 z 36 -	Przerwa	-	23-09-2026	11:50	12:10	00:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 36 dzień III COMPTIA CYSA + - Działania związane z reagowaniem na incydenty	Zajęcia	Miłosz Jaworski	23-09-2026	12:10	13:40	01:30
20 z 36 -	Przerwa	-	23-09-2026	13:40	14:00	00:20
21 z 36 dzień III COMPTIA CYSA + - Komunikacja w zakresie reagowania na incydenty	Zajęcia	Miłosz Jaworski	23-09-2026	14:00	15:30	01:30
22 z 36 dzień IV COMPTIA CYSA + - Narzędzia do identyfikacji złośliwej aktywności	Zajęcia	Miłosz Jaworski	24-09-2026	08:30	10:00	01:30
23 z 36 -	Przerwa	-	24-09-2026	10:00	10:20	00:20
24 z 36 dzień IV COMPTIA CYSA + - Analizowanie potencjalnie złośliwej aktywności	Zajęcia	Miłosz Jaworski	24-09-2026	10:20	11:50	01:30
25 z 36 -	Przerwa	-	24-09-2026	11:50	12:10	00:20
26 z 36 dzień IV COMPTIA CYSA + - Ocena podatności aplikacji na zagrożenia	Zajęcia	Miłosz Jaworski	24-09-2026	12:10	13:40	01:30
27 z 36 -	Przerwa	-	24-09-2026	13:40	14:00	00:20

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 36 dzień IV COMPTIA CYSA + - Ocena podatności aplikacji	Zajęcia	Miłosz Jaworski	24-09-2026	14:00	15:30	01:30
29 z 36 dzień V COMPTIA CYSA + - Najlepsze praktyki w zakresie bezpieczeństwa aplikacji	Zajęcia	Miłosz Jaworski	25-09-2026	08:30	10:00	01:30
30 z 36 -	Przerwa	-	25-09-2026	10:00	10:20	00:20
31 z 36 dzień V COMPTIA CYSA + - Ograniczanie ataków na aplikacje	Zajęcia	Miłosz Jaworski	25-09-2026	10:20	11:50	01:30
32 z 36 -	Przerwa	-	25-09-2026	11:50	12:10	00:20
33 z 36 dzień V COMPTIA CYSA + - Przygotowanie do egzaminu CompTIA Cybersecurity Analyst+ CS0-003 – część 1	Zajęcia	Miłosz Jaworski	25-09-2026	12:10	13:40	01:30
34 z 36 -	Przerwa	-	25-09-2026	13:40	14:00	00:20
35 z 36 dzień V COMPTIA CYSA + - Przygotowanie do egzaminu CompTIA Cybersecurity Analyst+ CS0-003 – część 2	Zajęcia	Miłosz Jaworski	25-09-2026	14:00	15:15	01:15
36 z 36 -	Walidacja	Miłosz Jaworski	25-09-2026	15:15	15:30	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	35:00
w tym suma godzin zajęć	29:45
w tym suma godzin walidacji	00:15
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	40:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 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, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 473,50 PLN
Koszt przypadający na 1 uczestnika netto	4 450,00 PLN
Koszt osobogodziny brutto	156,39 PLN
Koszt osobogodziny netto	127,14 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	35:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Miłosz Jaworski

Trener CompTIA

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

materiały zostaną przesłane drogą mailową do uczestników

Warunki uczestnictwa

Przed przystąpieniem do szkolenia konieczne jest posiadanie ogólnej wiedzy dotyczącej bezpieczeństwa IT.

Informacje dodatkowe

Podczas szkolenia gwarantujemy:

- Materiały szkoleniowe
- 30 dniową Opiekę Mentorską
- Certyfikat ukończenia szkolenia

Uczestnik szkolenia otrzyma podręcznik szkoleniowy, dyplom w dwóch wersjach językowych oraz zostanie objęty 30-dniową opieką mentorską.

Warunki techniczne

Warunki techniczne

Platforma /rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa: MS Teams.

Minimalne wymagania sprzętowe i oprogramowanie jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

Komputer , laptop z systemem Operacyjnym WindowsPrzeglądarka internetowa Google Chrome (preferowana) lub Mozilla Firefox .

Oprogramowanie umożliwiające dostęp do prezentowanych treści i materiałów (czytnik plików pdf oraz doc i xls) (MS Office- MS Excel).

Kamera o rozdzielczości min 640 x 480 pix.

Mikrofon, głośnik.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

Łącze inernetowe: min download: 10 Mb/s, min upload: 10 Mb/s (zalecamy korzystanie z łącza stałego).

Usługa będzie rejestrowana na potrzeby kontroli (monitoringu) odpowiednich instytucji, w ramach rozliczenia usługi.

Link do szkolenia jest ważny w ciągu 5 dni, w których trwa szkolenie.

Kontakt

Karolina Banaszczyk

E-mail banaszczyk@imperiumszkoleniowe.pl
Telefon (+48) 535 201 087