Możliwość dofinansowania

CompTIA Security+ Prep Course

Numer usługi 2026/02/02/10100/3301871

6 000,00 PLN brutto
6 000,00 PLN netto
171,43 PLN brutto/h
171,43 PLN netto/h

Compendium - Centrum Edukacyjne Spółka z o.o.

4,3 / 5

190 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
35 h
30.03.2026 do 03.04.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe
Grupa docelowa usługi	Minimum 2-letnie doświadczenie praktyczne związane z administracją systemami IT ze szczególnym uwzględnieniem elementów technicznych związanych z bezpieczeństwem systemów i informacji oraz wiedza na temat ogólnych koncepcji bezpieczeństwa.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	25
Data zakończenia rekrutacji	29-03-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
Podstawa uzyskania wpisu do BUR	Znak Jakości Małopolskich Standardów Usług Edukacyjno-Szkoleniowych (MSUES) - wersja 2.0

Cel

Cel edukacyjny

Certyfikat CompTIA Security+ jest międzynarodowym standardem w branży IT potwierdzającym wiedzę i umiejętności dotyczące zagadnień bezpieczeństwa IT. Jest wykorzystywany przez wiele organizacji i specjalistów ds. bezpieczeństwa na całym świecie.

CompTIA Security+ jest zgodny ze standardami ISO 17024 i zatwierdzony przez Departament Obrony Stanów

Zjednoczonych (DoD) jako spełniający wymagania dyrektywy 8140/8570.01-M. Szereg krajowych organów regulujących i urzędów polegają na akredytacji ANSI,

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi zidentyfikować i opisać główne typy zagrożeń, podatności oraz wektory ataków w środowiskach IT (w tym w chmurze, IoT, urządzeniach mobilnych).	potrafi wskazać co najmniej 5 różnych typów aktorów zagrożeń oraz ich motywacje; potrafi opisać co najmniej 3 typowe wektory ataku oraz związane z nimi podatności;	Wywiad swobodny
Uczestnik potrafi reagować na incydenty i zdarzenia bezpieczeństwa — identyfikować, analizować dane, koordynować działania reagowania i oceny po-incydentalnej, zgodnie z dobrymi praktykami bezpieczeństwa.	w przypadku symulowanego incydentu uczestnik identyfikuje źródła danych (np. logi, alerty, zdarzenia) i przedstawia co najmniej 2 możliwe techniki dochodzenia oraz sposób ich zastosowania;	Wywiad swobodny
Uczestnik potrafi zaproponować i wdrożyć odpowiednie środki bezpieczeństwa (kontrole, architekturę, procedury) w celu ochrony środowiska organizacji, uwzględniając hybrydowe środowiska (znajomość chmury, IoT, OT) oraz zasady zarządzania ryzykiem, zgodności i ładu korporacyjnego.	sporządza propozycję planu kontrolnego, uwzględniającego co najmniej 3 obszary (np. chmura, urządzenia mobilne, IoT) oraz określa sposób monitorowania i reagowania na incydenty;	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

- Ogólne koncepcje bezpieczeństwa
- Zagrożenia, luki w zabezpieczeniach i sposoby ich ograniczania
- Architektura bezpieczeństwa
- Operacje bezpieczeństwa
- Zarządzanie programem bezpieczeństwa i nadzór nad nim

Harmonogram

Liczba przedmiotów/zajęć: 0

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

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 000,00 PLN
Koszt przypadający na 1 uczestnika netto	6 000,00 PLN
Koszt osobogodziny brutto	171,43 PLN
Koszt osobogodziny netto	171,43 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Zbigniew Jakubowsi

Od 2004 pracuje w Compendium CE jako wykładowca i „content developer”. Główne kierunki zainteresowań to technologie sieciowe, szeroko pojęte bezpieczeństwo informacji oraz sieci i technologie radiowe. Posiada autoryzację trenerską wielu znanych firm takich jak Alvarion, CWNP, Check Point, Proxim, Extreme Networks i wielu innych. Okazyjnie współpracuje z producentami przy tworzeniu nowych kursów. Nie prowadzi żadnego bloga, nie udziela się w żadnym serwisie społecznościowym z wyjątkiem LinkedIn. Przed podjęciem współpracy z Compendium pracował w wielu firmach branży IT, zarówno w kraju, jak i za granicą.

Absolwent Uniwersytetu Jagiellońskiego w Krakowie, Wydział Matematyki, Fizyki i Chemii. Doktorat z fizyki cząstek elementarnych DESY Hamburg/Instytut Fizyki Jądrowej w Krakowie. Jest również autorem kilkudziesięciu publikacji naukowych.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Autoryzowane materiały szkoleniowe.

Warunki techniczne

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams.**

Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, który potwierdzi swój udział w szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:

- komputer z dostępem do internetu o minimalnej przepustowości 10Mb/s.

- urządzenie do obsługi audio - słuchawki/glosniki oraz mikrofon.

- zainstalowana dowolna przeglądarka internetowa - np. **Google Chrome**

Kontakt

Michał Dobrzański

E-mail michal.dobrzanski@compendium.pl
Telefon (+48) 122 984 777