

ALTKOM AKADEMIA
SPÓŁKA AKCYJNA

Warsztaty z CompTIA Security + wraz z egzaminem SY0-701 - szkolenie autoryzowane

Numer usługi 2024/06/27/120967/2199862

zdalna w czasie rzeczywistym

Usługa szkoleniowa

35 h

04.11.2024 do 06.12.2024

7 380,00 PLN brutto

6 000,00 PLN netto

210,86 PLN brutto/h

171,43 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji. Od Uczestników wymagana jest ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	28-10-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do analizy ryzyka, planowania ciągłości działania, zachowania bezpieczeństwa informacyjnego, bezpieczeństwa systemów i sieci teleinformatycznych. Uczestnik po szkoleniu będzie analizował ryzyko, zabezpieczał architekturę sieci korporacyjnej, oceniał bezpieczeństwo punktów końcowych, zarządzał incydentami i monitorował środowisko.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe koncepcje bezpieczeństwa	- charakteryzuje mechanizmy kontrolne bezpieczeństwa	Test teoretyczny
Rozróżnia typy zagrożeń	- charakteryzuje typy zagrożeń - definiuje przestrzenie ataku	Test teoretyczny
Wdraża zarządzanie tożsamością i kontrolą dostępu	- charakteryzuje uwierzytelnianie, autoryzację, zarządzanie tożsamością	Test teoretyczny
Zabezpiecza architekturę sieci w usługach chmurowych	- charakteryzuje infrastrukturę chmurową - charakteryzuje systemy wbudowane - charakteryzuje architekturę Zero Trust	Test teoretyczny
Zarządza incydentami i monitorowaniem środowiska	- charakteryzuje zasady reagowania na incydenty - charakteryzuje narzędzia do monitorowania	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 5. Czy dokument jest certyfikatem, dla którego wypracowano system walidacji i certyfikowania efektów uczenia się na poziomie międzynarodowym?

tak

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa/Kategoria Podmiotu prowadzącego walidację	Pearson Vue
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie

Nazwa/Kategoria Podmiotu certyfikującego

Pearson Vue

Podmiot certyfikujący jest zarejestrowany w BUR

Nie

Program

Agenda szkolenia

1. Podstawowe koncepcje bezpieczeństwa

- terminologia, koncepcje
- mechanizmy kontrolne bezpieczeństwa

1. Porównanie różnych typów zagrożeń

- aktorzy-zagrozenia
- przestrzenie ataku
- inżynieria społeczna

1. Omówienie podstawowych pojęć kryptografii

- algorytmy kryptograficzne,
- infrastruktura PKI
- rozwiązania kryptograficzne

1. Wdrażanie zarządzania tożsamością i kontrolą dostępu

- uwierzytelnianie
- autoryzacja
- zarządzanie tożsamością

1. Zabezpieczanie architektury sieci korporacyjnej

- architektura sieci korporacyjnej
- urządzenia zabezpieczające sieć
- bezpieczna komunikacja

1. Zabezpieczanie architektury sieci w usługach chmurowych

- infrastruktura chmurowa
- systemy wbudowane
- architektura Zero Trust

1. Omówienie koncepcji odporności

- zarządzanie aktywami
- strategię redundancji
- bezpieczeństwo fizyczne

1. Zarządzanie podatnościami

- podatności w urządzeniach i systemach operacyjnych
- luki w oprogramowaniu i usługach chmurowych
- metody identyfikacji luk w zabezpieczeniach
- analiza i usuwanie luk w zabezpieczeniach

1. Bezpieczeństwo sieciowe

- podstawowe założenia dotyczące bezpieczeństwa sieci
- podnoszenie poziomu bezpieczeństwa sieci

1. Ocena bezpieczeństwa punktów końcowych

- wdrażanie zabezpieczeń punktów końcowych
- wdrażanie zabezpieczeń urządzeń mobilnych

1. Wdrażanie zabezpieczeń aplikacji

- wytyczne dla zabezpieczania aplikacji
- koncepcje bezpieczeństwa aplikacji w chmurze i sieci Web

1. Zarządzanie incydentami i monitorowanie środowiska

- reagowanie na incydenty
- informatyka śledcza
- narzędzia do monitorowania

1. Po czym rozpoznać atak – wskaźniki kompromitacji

- ataki złośliwym oprogramowaniem
- ataki fizyczne i sieciowe
- ataki na aplikacje

1. Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury

- polityki, standardy i procedury
- zarządzanie zmianami
- automatyzacja i orkiestracja

1. Podstawowe pojęcia związane zarządzania ryzykiem

- koncepcje zarządzania ryzykiem
- audyty i ocena ryzyka

1. Ochrona danych i dbałość o ich zgodność w organizacji

- klasyfikacja danych i zgodność
- polityki personalne

Od Uczestników wymagana jest ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Szkolenie jest prowadzone całościowo w formule distance learning, natomiast egzamin jest przeprowadzany stacjonarnie.

Uczestnik po szkoleniu otrzymuje voucher na egzamin do wykorzystania max. 30 dni po szkoleniu. Egzamin w harmonogramie ma tylko prawdopodobny termin i godzinę. Uczestnik umawia się na egzamin indywidualnie z Administratorami Egzaminów w wybranym ośrodku egzaminacyjnym Altkom Akademia.

Egzamin jest przeprowadzany stacjonarnie w centrum egzaminacyjnym pod adresem Szczyśliwa 33 53-445 Wrocław (Sky Tower).

Uczestnik podchodzi do egzaminu w centrum egzaminacyjnym. Dedykowana osoba z Altkom Akademii sprawdza tożsamość Uczestnika, następnie Uczestnik loguje się do zewnętrznej platformy Pearson Vue uzyskując dostęp do egzaminu, zdaje egzamin i wysyła do Pearson Vue. Podczas trwania całego egzaminu jest nadzorowany przez dedykowaną osobę z Altkom Akademii, która sprawdza czy nie korzysta z niedozwolonych pomocy naukowych. Pomieszczenie, w którym zdaje egzamin Uczestnik jest monitorowane.

Uczestnik w ciągu trzech tygodni otrzymuje od firmy Pearson Vue wyniki egzaminu i certyfikat.

Liczba godzin wpisana w pole "ogólna liczba godzin" obejmuje tylko czas szkolenia (35 godzin). Egzamin trwa 1,5 godziny w związku z czym cała usługa szkolenie + egzamin trwa 36 godzin i 30 minut.

Informacje o egzaminie SY0-701:

Tytuł – CompTIA Security+

Format testu: Kombinacja pytań wielokrotnego wyboru, ćwiczenia drag and drops, oraz elementów opartych na rozwiązywaniu problemu – wynikach.

Ilość pytań – max 90

Czas trwania – 90 min

Szkolenie obejmuje:

5 dni pracy z trenerem

Nadzór trenera

Kontakt ze społecznością

Autoryzowany podręcznik: The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-701) eBook

Środowisko laboratoryjne

Voucher na egzamin: CompTIA Security+ SY0-701

Harmonogram

Liczba przedmiotów/zajęć: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Podstawowe koncepcje bezpieczeństwa terminologia, koncepcyjemechanizmy kontrolne bezpieczeństwa wykład	Dominik Węglarz	04-11-2024	10:00	11:00	01:00
2 z 16 Porównanie różnych typów zagrożeń wykład	Dominik Węglarz	04-11-2024	11:00	12:30	01:30
3 z 16 Omówienie podstawowych pojęć kryptografii wykład	Dominik Węglarz	04-11-2024	12:30	17:00	04:30
4 z 16 Wdrażanie zarządzania tożsamością i kontrolą dostępu ćwiczenia	Dominik Węglarz	05-11-2024	09:00	11:00	02:00
5 z 16 Zabezpieczanie architektury sieci korporacyjnej ćwiczenia	Dominik Węglarz	05-11-2024	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 16 Zabezpieczanie architektury sieci w usługach chmurowych ćwiczenia	Dominik Węglarz	05-11-2024	13:00	16:00	03:00
7 z 16 Omówienie koncepcji odporności wykład	Dominik Węglarz	06-11-2024	09:00	11:00	02:00
8 z 16 Zarządzanie podatnościami ćwiczenia	Dominik Węglarz	06-11-2024	11:00	13:00	02:00
9 z 16 Bezpieczeństwo sieciowe ćwiczenia	Dominik Węglarz	06-11-2024	13:00	16:00	03:00
10 z 16 Ocena bezpieczeństwa punktów końcowych wykład	Dominik Węglarz	07-11-2024	09:00	11:00	02:00
11 z 16 Wdrażanie zabezpieczeń aplikacji ćwiczenia	Dominik Węglarz	07-11-2024	11:00	13:00	02:00
12 z 16 Zarządzanie incydentami i monitorowanie środowiska ćwiczenia	Dominik Węglarz	07-11-2024	13:00	16:00	03:00
13 z 16 Po czym rozpoznać atak - wskaźniki kompromitacji wykład	Dominik Węglarz	08-11-2024	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
14 z 16 Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury ćwiczenia	Dominik Węglarz	08-11-2024	11:00	13:00	02:00
15 z 16 Podstawowe pojęcia związane zarządzania ryzykiem; Ochrona danych i dbałość o ich zgodność w organizacji wykład	Dominik Węglarz	08-11-2024	13:00	16:00	03:00
16 z 16 Egzamin	-	21-11-2024	11:00	12:30	01:30

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	210,86 PLN
Koszt osobogodziny netto	171,43 PLN
W tym koszt walidacji brutto	1 845,00 PLN
W tym koszt walidacji netto	1 500,00 PLN
W tym koszt certyfikowania brutto	1,23 PLN
W tym koszt certyfikowania netto	1,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Dominik Węglarz

Wykształcenie: XIX Liceum Ogólnokształcące Profil Informatyczny w Poznaniu

Uniwersytet im. Adama Mickiewicza w Poznaniu

- Absolwent Wydziału Matematyki i Informatyki.
- Zdobył tytuł Licencjata Informatyki.

Uniwersytet im. Adama Mickiewicza w Poznaniu

- Studia uzupełniające magisterskie II-go stopnia na Wydziale Matematyki i Informatyki UAM.

Wyższa Szkoła Komunikacji i Zarządzania w Poznaniu

- Cisco Networking Academy (4 semestry Akademii Sieci Komputerowej)

Specjalizacja: Infrastruktura IT, wirtualizacja, bezpieczeństwo IT.

Doświadczenie trenerskie: Trener Altkom Akademii od 2017r.

Prowadzi autoryzowane szkolenia z technologii VMware; autoryzowane szkolenia bezpieczeństwa EC Council; autorskie szkolenia z zakresu wirtualizacji i bezpieczeństwa. Był prelegentem wielu seminariów i webinarów. Opracowywał nowe szkolenia.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Warunki uczestnictwa

Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych, do którego składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Ogólne warunki uczestnictwa w zajęciach zostały zamieszczone na stronie: <https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/>

Informacje dodatkowe

Po szkoleniu Uczestnik otrzyma zaświadczenie o ukończeniu szkolenia.

Trener podczas szkolenia będzie organizował krótkie przerwy. Informacja o przerwach będzie umieszczona na slajdzie.

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

Ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Warunki techniczne

Wymagania ogólne realizacji szkolenia w formule distance learning (online): Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt



Adrianna Kukurudz

E-mail adrianna.kukurudz@altkom.pl

Telefon (+22) 801 258 566