Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

Warsztaty z CompTIA Security + (przygotowanie do egzaminu SY0-701) - szkolenie autoryzowane - forma zdalna w czasie rzeczywistym

Numer usługi 2024/10/08/120967/2349353

- zdalna w czasie rzeczywistym
- Usługa szkoleniowa
- 35 h
- 09.12.2024 do 13.12.2024

5 535,00 PLN brutto
4 500,00 PLN netto
158,14 PLN brutto/h
128,57 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	02-12-2024
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 przygotowuje Uczestnika do analizy ryzyka, planowania ciągłości działania, zachowania bezpieczeństwa informacyjnego, bezpieczeństwa systemów i sieci teleinformatycznych. Uczestnik po szkoleniu charakteryzuje podstawowe koncepcje bezpieczeństwa, rozróżnia typy zagrożeń, wdraża zarządzanie tożsamością i kontrolą dostępu, zabezpiecza architekturę sieci w usługach chmurowych, zarządza incydentami i monitoruje 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 monitoruje środowisko	- charakteryzuje zasady reagowania na incydenty - charakteryzuje narzędzia do monitorowania	Test teoretyczny

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

Agenda szkolenia

1. Podstawowe koncepcje bezpieczeństwa

- terminologia, koncepcje
- mechanizmy kontrolne bezpieczeństwa

1. Porównanie różnych typów zagrożeń

- aktorzy-zagrożenia
- 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
- strategie 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

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.

Efekty uczenia zostaną zweryfikowane przed szkoleniem i po szkoleniu poprzez pre i post testy w formie testu teoretycznego zamkniętego w formie online.

Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 15 **Podstawowe koncepcje bezpieczeństwa terminologia, koncepcje mechanizmy kontrolne bezpieczeństwa wykład**	**Dominik Węglarz**	**09-12-2024**	**10:00**	**13:00**	**03:00**
2 z 15 **Porównanie różnych typów zagrożeń wykład**	**Dominik Węglarz**	**09-12-2024**	**13:00**	**15:00**	**02:00**

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 15 Omówienie podstawowych pojęć kryptografii wykład	Dominik Węglarz	09-12-2024	15:00	17:00	02:00
4 z 15 Wdrażanie zarządzania tożsamością i kontrolą dostępu ćwiczenia	Dominik Węglarz	10-12-2024	09:00	11:00	02:00
5 z 15 Zabezpieczanie architektury sieci korporacyjnej ćwiczenia	Dominik Węglarz	10-12-2024	11:00	13:00	02:00
6 z 15 Zabezpieczanie architektury sieci w usługach chmurowych ćwiczenia	Dominik Węglarz	10-12-2024	13:00	16:00	03:00
7 z 15 Omówienie koncepcji odporności wykład	Dominik Węglarz	11-12-2024	09:00	11:00	02:00
8 z 15 Zarządzanie podatnościami ćwiczenia	Dominik Węglarz	11-12-2024	11:00	13:00	02:00
9 z 15 Bezpieczeństwo sieciowe ćwiczenia	Dominik Węglarz	11-12-2024	13:00	16:00	03:00
10 z 15 Ocena bezpieczeństwa punktów końcowych wykład	Dominik Węglarz	12-12-2024	09:00	11:00	02:00
11 z 15 Wdrażanie zabezpieczeń aplikacji ćwiczenia	Dominik Węglarz	12-12-2024	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 15 Zarządzanie incydentami i monitorowanie środowiska ćwiczenia	Dominik Węglarz	12-12-2024	13:00	16:00	03:00
13 z 15 Po czym rozpoznać atak - wskaźniki kompromitacji wykład	Dominik Węglarz	13-12-2024	09:00	11:00	02:00
14 z 15 Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury ćwiczenia	Dominik Węglarz	13-12-2024	11:00	13:00	02:00
15 z 15 Podstawowe pojęcia związane zarządzania ryzykiem; Ochrona danych i dbałość o ich zgodność w organizacji wykład	Dominik Węglarz	13-12-2024	13:00	16:00	03:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	158,14 PLN
Koszt osobogodziny netto	128,57 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: Obecnie trener Altkom Akademii. Posiada doświadczenie trenerskie zdobyte w ostatnich 5 latach.
Prowadzi autoryzowane szkolenia z technologii VMware, z bezpieczeństwa EC Council, z zakresu wirtualizacji i bezpieczeństwa.
Był prelegentem wielu seminariów i webinariów. 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.

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.

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt

Adrianna Kukurudz

E-mail adrianna.kukurudz@altkom.pl
Telefon (+22) 801 258 566