Możliwość dofinansowania

Szkolenie C CySA+ CompTIA Cybersecurity Analyst

Numer usługi 2024/09/09/142469/2299099

5 535,00 PLN brutto
4 500,00 PLN netto
141,92 PLN brutto/h
115,38 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
39 h
25.11.2024 do 29.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Grupa docelowa dla szkolenia CompTIA CySA+ obejmuje osoby, które chcą rozwijać zaawansowane umiejętności w dziedzinie cyberbezpieczeństwa i monitorowania bezpieczeństwa sieci oraz infrastruktury. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	11-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	39
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 CompTIA CySA+ ma na celu przekazanie uczestnikom zaawansowanych umiejętności w zakresie analizy bezpieczeństwa, monitorowania sieci i infrastruktury oraz wykrywania i reagowania na incydenty bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozróżnia różne typy zagrożeń dla systemów informatycznych.	Potrafi wymienić i opisać rodzaje zagrożeń, takie jak ataki typu DDoS, malware, phishing oraz potrafi zidentyfikować odpowiednie kroki reakcji na każde z nich.	Test teoretyczny
Definiuje proces analizy i polowania na zagrożenia w kontekście cyberbezpieczeństwa.	Potrafi wyjaśnić etapy analizy zagrożeń oraz techniki wykorzystywane do wykrywania i śledzenia potencjalnych incydentów.	Test teoretyczny
Charakteryzuje podstawowe elementy architektury systemów i sieci.	Potrafi opisać role i funkcje takie jak serwery, routery, firewall'e oraz ich wpływ na bezpieczeństwo IT.	Test teoretyczny
Uzasadnia znaczenie ciągłego doskonalenia procesów bezpieczeństwa.	Przedstawia przykłady narzędzi lub metodologii używanych do doskonalenia operacyjnych procesów bezpieczeństwa.	Test teoretyczny
Implementuje narzędzia do skanowania podatności w systemach informatycznych.	Demonstruje umiejętność użycia narzędzi do identyfikacji i klasyfikacji podatności w środowisku IT.	Test teoretyczny
Przeprowadza analizę słabych punktów w infrastrukturze IT.	Potrafi wykonać test penetracyjny lub audyt bezpieczeństwa, identyfikując istniejące słabe punkty.	Test teoretyczny
Komunikuje znalezione podatności i zalecane działania naprawcze.	Potrafi sporządzić raport z wynikami skanowania lub audytu, opisujący znalezione podatności i zalecenia.	Test teoretyczny
Reaguje na incydenty bezpieczeństwa w sposób zgodny z procedurami.	Potrafi opisać kroki podejmowane podczas reakcji na incydent, w tym zarządzanie zdarzeniami i odzyskiwanie danych.	Test teoretyczny
Przedstawia jasną i skuteczną komunikację podczas incydentów bezpieczeństwa.	Potrafi opisać procesy informacyjne i komunikacyjne, które są stosowane podczas zarządzania incydentami bezpieczeństwa.	Test teoretyczny
Używa narzędzi do detekcji i analizy złośliwej aktywności.	Demonstruje umiejętność korzystania z systemów detekcji złośliwego oprogramowania oraz interpretuje wyniki analizy złośliwych aktywności.	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, Uczestnik szkolenia, poza certyfikatem, otrzymuje zaświadczenie o ukończeniu szkolenia z zawartym opisem efektów uczenia się.

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

Szkolenie **C CySA+ CompTIA Cybersecurity Analyst** przygotowuje uczestników do analizy i reagowania na zagrożenia cybernetyczne w środowiskach IT. Szkolenie ma na celu dostarczenie uczestnikom niezbędnych umiejętności i wiedzy do skutecznego monitorowania, identyfikowania oraz reagowania na incydenty bezpieczeństwa informatycznego.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy Uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności. W trakcie szkolenia omawiane jest również studium przypadków, w którym Uczestnicy wspólnie wymieniają się doświadczeniami. Nad case-study czuwa autoryzowany Trener, który przekazuje informację na temat przydatnych narzędzi oraz najlepszych praktyk do rozwiązania omawianego zagadnienia.

Aby Uczestnik osiągnął zamierzony cel szkolenia niezbędne jest wykonanie przez niego zadanych laboratoriów. Pomocne będzie również ugruntowanie wiedzy i wykonywanie ćwiczeń po zakończonej usłudze. Każdy Uczestnik dysponuje dostępem do laboratoriów przez okres 180 dni.

Przed rozpoczęciem szkolenia Uczestnik rozwiązuje pre-test badający poziom wiedzy na wstępie.

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy.

Szkolenie trwa 35 godzin zegarowych i jest realizowane w ciągu 5 dni.

W trakcie każdego dnia szkolenia przewidziane są dwie krótkie przerwy "kawowe" oraz przerwa lunchowa.

Program szkolenia:

Wyjaśnienie znaczenia kontroli bezpieczeństwa i wywiadu bezpieczeństwa

Wykorzystywanie danych i analizy zagrożeń

Analiza danych monitorowania bezpieczeństwa

Zbieranie i wysyłanie zapytań do danych monitorowania bezpieczeństwa

Wykorzystanie kryminalistyki cyfrowej i technik analizy wskaźników

Stosowanie procedur reagowania na incydenty

Stosowanie ram ograniczania ryzyka i bezpieczeństwa

Zarządzanie lukami w zabezpieczeniach

Stosowanie rozwiązań zabezpieczających do zarządzania infrastrukturą

Zrozumienie prywatności i ochrony danych

Stosowanie rozwiązań zabezpieczających w ramach pakietu Software Assurance

Stosowanie rozwiązań zabezpieczających w chmurze i automatyzacji

SOFTRONIC Sp. z o. o. zastrzega sobie prawo do zmiany terminu szkolenia lub jego odwołania w przypadku niezebrania się minimalnej liczby Uczestników tj. 3 osób.

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	5 535,00 PLN
Koszt przypadający na 1 uczestnika netto	4 500,00 PLN
Koszt osobogodziny brutto	141,92 PLN
Koszt osobogodziny netto	115,38 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe, które są dostępne na koncie Uczestnika na dedykowanym portalu. Uczestnik uzyskuje również 180-dniowy dostęp do laboratoriów CompTIA, z których korzysta w dowolny sposób i w dowolnym momencie, za pośrednictwem przeglądarki internetowej.
Poza dostępami przekazywanymi Uczestnikowi, w trakcie szkolenia, Trener przedstawia i omawia autoryzowaną prezentację.

Warunki uczestnictwa

Aby wziąć udział w szkoleniu CompTIA CySA+, rekomendowane jest posiadanie podstawowej wiedzy i doświadczenia w dziedzinie cyberbezpieczeństwa. Warto mieć wcześniejsze doświadczenie w bezpieczeństwie informatycznym lub być posiadaczem certyfikatu CompTIA Security+

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracowników, których poziom dofinansowania ze środków publicznych wynosi co najmniej 70% (na podstawie § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. zmieniające rozporządzenie w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Zawarto umowę z WUP w Toruniu w ramach Projektu Kierunek – Rozwój;

kwalifikacja związana z cyfrową transformacją;

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział z każdego miejsca na świecie.

Szkolenie obywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu Uczestnik może zadawać pytania i aktywnie uczestniczyć w dyskusji. Uczestnik, ktory potwierdzi swój udziałw szkoleniu, przed rozpoczęciem szkolenia, drogą mailową, otrzyma link do spotkania wraz z hasłami dostępu.

Wymagania sprzętowe:
- komputer z dostępem do internetu o minimalnej przepustowości 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/glosniki oraz mikrofon.
- zainstalowana przeglądarka internetowa - Microsoft Edge/ Internet Explorer 10+ / **Google Chrome** 39+ (sugerowana) / Safari 7+
- aplikacja MS Teams może zostać zainstalowana na komputerze lub można z niej korzystać za pośrednictwem przeglądarki internetowej

Kontakt

Agata Wojciechowska

E-mail agata.wojciechowska@softronic.pl
Telefon (+48) 618 658 840