Możliwość dofinansowania

Szkolenie C CASP+ CompTIA Advanced Security Practitioner z egzaminem

Numer usługi 2024/05/22/142469/2158343

8 856,00 PLN brutto
7 200,00 PLN netto
253,03 PLN brutto/h
205,71 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
35 h
16.09.2024 do 20.09.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie **CompTIA Advanced Security Practitioner (CASP+)** jest przeznaczone dla doświadczonych profesjonalistów ds. bezpieczeństwa informatycznego, w tym analityków bezpieczeństwa, architektów systemów bezpieczeństwa i menedżerów ds. bezpieczeństwa. Grupa docelowa obejmuje osoby, które posiadają zaawansowaną wiedzę i doświadczenie w dziedzinie cyberbezpieczeństwa i chcą rozwijać umiejętności na poziomie zaawansowanym.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	26-08-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
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 Advanced Security Practitioner (CASP+) ma na celu dostarczenie doświadczonym profesjonalistom ds. bezpieczeństwa informatycznego zaawansowanej wiedzy i umiejętności w zakresie projektowania, wdrażania oraz zarządzania kompleksowymi strategiami bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykonuje działania związane z zarządzaniem ryzykiem.	Identyfikuje i ocenia ryzyka związane z IT. Planuje i wdraża strategie zarządzania ryzykiem. Monitoruje i raportuje wyniki zarządzania ryzykiem.	Test teoretyczny
Podsumowuje strategię zarządzania i zgodności z przepisami.	Analizuje i dokumentuje wymagania prawne i regulacyjne. Przeprowadza audyty zgodności. Tworzy raporty z wyników audytów i proponuje działania korygujące.	Test teoretyczny
Wdraża ciągłość działania i odzyskiwanie danych po awarii.	Opracowuje i wdraża plany ciągłości działania. Konfiguruje systemy do automatycznego tworzenia kopii zapasowych. Testuje procedury odzyskiwania danych po awarii.	Test teoretyczny
Identyfikuje usługi infrastrukturalne.	Wykazuje znajomość podstawowych usług infrastrukturalnych (np. DNS, DHCP, Active Directory). Konfiguruje i zarządza tymi usługami. Monitoruje dostępność i wydajność usług infrastrukturalnych.	Test teoretyczny
Przeprowadza integrację oprogramowania.	Planuje i realizuje procesy integracji różnych systemów. Testuje kompatybilność i wydajność zintegrowanych systemów. Rozwiązuje problemy wynikające z integracji oprogramowania.	Test teoretyczny
Wyjaśnia wirtualizację, chmurę i nowe technologie.	Definiuje pojęcia wirtualizacji i chmury. Opisuje korzyści i wyzwania związane z wdrażaniem nowych technologii. Wskazuje przykłady zastosowań wirtualizacji i chmury w przedsiębiorstwach.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Odkrywa bezpieczne konfiguracje i wzmacnianie systemu.	Konfiguruje systemy zgodnie z najlepszymi praktykami bezpieczeństwa. Przeprowadza audyty bezpieczeństwa systemów. Implementuje środki wzmacniające bezpieczeństwo systemów.	Test teoretyczny
Zrozumienie kwestii bezpieczeństwa chmury i wyspecjalizowanych platform.	Identyfikuje zagrożenia specyficzne dla środowisk chmurowych. Implementuje środki bezpieczeństwa w chmurze. Monitoruje i zarządza bezpieczeństwem wyspecjalizowanych platform.	Test teoretyczny
Wdraża kryptografię i infrastrukturę klucza publicznego (PKI).	Wyjaśnia podstawowe pojęcia kryptografii. Konfiguruje i zarządza PKI. Implementuje mechanizmy szyfrowania danych.	Test teoretyczny
Rozwija zdolności reagowania na incydenty.	Opracowuje plany reagowania na incydenty. Przeprowadza symulacje incydentów bezpieczeństwa. Analizuje i raportuje wyniki po incydentach.	Test teoretyczny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

Certyfikaty Comptia cieszą się globalnym uznaniem, potwierdzając umiejętności w obszarze powszechnie używanych technologii. Ich wartość wynika z rozległości produktów Comptia, uznawalności w branży, wymagań praktycznych i regularnych aktualizacji. To kwalifikacje cenione na poziomie globalnym.

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

Tak, certyfikat Comptia dla którego wypracowano system walidacji i certyfikacji na poziomie międzynarodowym.

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnionych do wydawania dokumentów potwierdzających uzyskanie kwalifikacji, w tym w zawodzie
Nazwa/Kategoria Podmiotu prowadzącego walidację	Pearson VUE
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	Comptia
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Szkolenie **CompTIA Advanced Security Practitioner (CASP+)** ma na celu dostarczenie doświadczonym profesjonalistom ds. bezpieczeństwa informatycznego zaawansowanych umiejętności i wiedzy. Program szkoleniowy skupia się na projektowaniu, wdrażaniu i zarządzaniu kompleksowymi strategiami bezpieczeństwa informatycznego, przygotowując uczestników do skutecznego kierowania zaawansowanymi inicjatywami bezpieczeństwa w organizacjach. Uczestnicy zdobywają umiejętności w identyfikacji i reakcji na zaawansowane zagrożenia cybernetyczne, a także w zarządzaniu ryzykiem bezpieczeństwa. Po ukończeniu szkolenia, absolwenci są gotowi do pełnienia roli zaawansowanych praktyków ds. bezpieczeństwa informatycznego, wykazując się kompleksową wiedzą i zdolnościami do skutecznego zarządzania bezpieczeństwem w dynamicznym środowisku cybernetycznym.

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.

Szkolenie trwa 35 godzin zegarowych i jest realizowane w ciągu 5 dni (po 7 godzin zegarowych dzinnie, wliczając w to przerwy - dwie przerwy kawowe po 15 minut i jedna lanchowa po 30 minut).

Program szkolenia

Wykonywanie działań związanych z zarządzaniem ryzykiem

Podsumowanie strategii zarządzania i zgodności z przepisami

Wdrażanie ciągłości działania i odzyskiwania danych po awarii

Identyfikacja usług infrastrukturalnych

Przeprowadzanie integracji oprogramowania

Wyjaśnienie wirtualizacji, chmury i nowych technologii

Odkrywanie bezpiecznych konfiguracji i wzmacnianie systemu

Zrozumienie kwestii bezpieczeństwa chmury i wyspecjalizowanych platform

Wdrażanie kryptografii

Wdrażanie infrastruktury klucza publicznego (PKI)

Zrozumienie działań związanych z zarządzaniem zagrożeniami i lukami w zabezpieczeniach

Rozwijanie zdolności reagowania na incydenty

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	8 856,00 PLN
Koszt przypadający na 1 uczestnika netto	7 200,00 PLN
Koszt osobogodziny brutto	253,03 PLN
Koszt osobogodziny netto	205,71 PLN
W tym koszt walidacji brutto	2 706,00 PLN
W tym koszt walidacji netto	2 200,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe Comptia.

Warunki uczestnictwa

Przed przystąpieniem do szkolenia warto, aby Uczestnik posiadał zaawansowaną wiedzę z zakresu bezpieczeństwa IT oraz doświadczenie w pracy na stanowisku związanych z cyberbezpieczeństwem. Zalecane jest również zrozumienie kwestii związanych z zarządzaniem ryzykiem i zgodnością z przepisami.

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.)

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

Ewa Kasprzak

E-mail ewa.kasprzak@softronic.pl
Telefon (+48) 618 658 840