



Szkolenie CompTIA Security+ z egzaminem

Numer usługi 2024/11/12/142469/2407304

6 088,50 PLN brutto

4 950,00 PLN netto

160,22 PLN brutto/h

130,26 PLN netto/h

SOFTRONIC

SPÓŁKA Z

OGRANICZONĄ

ODPOWIEDZIALNOŚĆ

CIA



📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 38 h

📅 10.03.2025 do 10.04.2025

Informacje podstawowe

| | |
|--|--|
| Kategoria | Informatyka i telekomunikacja / Bezpieczeństwo IT |
| Identyfikator projektu | Kierunek - Rozwój |
| Sposób dofinansowania | wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników |
| Grupa docelowa usługi | Szkolenie CompTIA Security+ jest skierowane do profesjonalistów IT, którzy zajmują się zapewnianiem bezpieczeństwa informacji w organizacjach. Grupa docelowa obejmuje administratorów systemów, inżynierów bezpieczeństwa, specjalistów ds. sieci oraz wszystkich, którzy odpowiedzialni są za ochronę danych i infrastruktury przed zagrożeniami cybernetycznymi. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój |
| Minimalna liczba uczestników | 3 |
| Maksymalna liczba uczestników | 7 |
| Data zakończenia rekrutacji | 31-01-2025 |
| Forma prowadzenia usługi | zdalna w czasie rzeczywistym |
| Liczba godzin usługi | 38 |
| 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 Security+ ma na celu dostarczenie uczestnikom umiejętności i wiedzy niezbędnej do skutecznego zapewniania bezpieczeństwa informacji w środowisku IT. Szkolenie koncentruje się na kluczowych aspektach ochrony danych, identyfikacji zagrożeń oraz stosowaniu skutecznych praktyk bezpieczeństwa, przygotowując profesjonalistów do skutecznego radzenia sobie z wyzwaniami związanymi z cyberbezpieczeństwem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|--|---|------------------|
| Rozumie podstawowe koncepcje bezpieczeństwa oraz typy zagrożeń. | Definiuje i wyjaśnia podstawowe terminy i koncepcje związane z bezpieczeństwem informacji. Identyfikuje i klasyfikuje różne typy zagrożeń (np. wirusy, malware, ataki DDoS). Porównuje skuteczność różnych strategii obrony przed zagrożeniami. | Test teoretyczny |
| Wyjaśnia i wdraża rozwiązania kryptograficzne. | Opisuje podstawowe mechanizmy kryptograficzne (np. szyfrowanie symetryczne, asymetryczne). Implementuje szyfrowanie danych za pomocą różnych metod. Wyjaśnia rolę certyfikatów cyfrowych i zarządza nimi. | Test teoretyczny |
| Wdraża zarządzanie tożsamością i dostępem. | Konfiguruje systemy zarządzania tożsamością (IAM). Definiuje i przyznaje role oraz uprawnienia użytkowników. Monitoruje i kontroluje dostęp do zasobów systemowych. | Test teoretyczny |
| Projektuje i implementuje architekturę bezpiecznej sieci korporacyjnej oraz w chmurze. | Opracowuje plan bezpiecznej architektury sieci korporacyjnej. Konfiguruje elementy bezpieczeństwa w sieci korporacyjnej (np. zapory ogniowe, VPN). Implementuje zasady bezpieczeństwa w środowisku chmurowym. | Test teoretyczny |
| Wyjaśnia koncepcje odporności, zarządzania podatnościami oraz oceny możliwości bezpieczeństwa. | Definiuje metody zwiększania odporności infrastruktury IT. Prowadzi procesy zarządzania podatnościami (np. skanowanie podatności, patch management). Przeprowadza ocenę możliwości w zakresie bezpieczeństwa sieci i punktów końcowych. | Test teoretyczny |

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|--|---|------------------|
| Zwiększa bezpieczeństwo aplikacji oraz reaguje na incydenty i monitoruje bezpieczeństwo. | Implementuje zabezpieczenia w cyklu życia aplikacji (DevSecOps). Monitoruje systemy pod kątem incydentów bezpieczeństwa. Przeprowadza analizę i reakcję na incydenty bezpieczeństwa. | Test teoretyczny |
| Analizuje wskaźniki złośliwej aktywności oraz zarządza bezpieczeństwem. | Identyfikuje wskaźniki kompromitacji (IoC) i analizuje złośliwą aktywność. Opracowuje i wdraża polityki bezpieczeństwa organizacji. Monitoruje przestrzeganie polityk bezpieczeństwa. | Test teoretyczny |
| Wyjaśnia procesy zarządzania ryzykiem. | Definiuje i ocenia ryzyko związane z bezpieczeństwem informacji. Stosuje metody zarządzania ryzykiem (np. analiza ryzyka, plany awaryjne). Monitoruje i raportuje poziom ryzyka. | Test teoretyczny |
| Podsumowuje koncepcje ochrony danych oraz zgodności z przepisami. | Wyjaśnia zasady ochrony danych osobowych (np. RODO, HIPAA). Implementuje procedury zgodności z przepisami ochrony danych. Monitoruje i raportuje zgodność z przepisami. | Test teoretyczny |
| Korzysta z narzędzi pomocniczych i skryptowych oraz wdraża procedury operacyjne. | Używa narzędzi do monitorowania i analizowania bezpieczeństwa (np. SIEM, IDS). Tworzy skrypty automatyzujące zadania związane z bezpieczeństwem. Implementuje i utrzymuje procedury operacyjne w zakresie bezpieczeństwa. | 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 Security+** ma na celu wyposażenie uczestników w zaawansowaną wiedzę i umiejętności z zakresu bezpieczeństwa informacyjnego. Uczestnicy zdobędą umiejętności w identyfikacji, analizie i reakcji na różnorodne zagrożenia cybernetyczne. Szkolenie skupia się również na konfiguracji i zarządzaniu zabezpieczeniami systemów operacyjnych i aplikacji, umożliwiając profesjonalistom skuteczne ochrona organizacji przed atakami. Po ukończeniu szkolenia, uczestnicy będą przygotowani do pełnienia roli specjalistów ds. bezpieczeństwa informacyjnego oraz skutecznego zarządzania aspektami cyberbezpieczeństwa w organizacjach.

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.

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

Po zakończeniu szkolenia zostanie przeprowadzany egzamin CompTIA Security+ (SY0-701). Czas trwania egzaminu to 165 minut.

Łączny czas realizacji usługi szkoleniowej wraz z egzaminem to 38 godzin zegarowych.

Egzamin odbędzie się stacjonarnie, najpóźniej do dnia zakończenia trwania usługi rozwojowej, w jednym z autoryzowanych ośrodków egzaminacyjnym Pearson VUE: SOFTRONIC Poznań lub SOFTRONIC Warszawa. Przed zapisaniem się na szkolenie, Uczestnik jest proszony o kontakt z SOFTRONIC w celu ustalenia możliwego terminu egzaminu.

Program szkolenia

Podsumowanie podstawowych koncepcji bezpieczeństwa

Porównanie typów zagrożeń

Wyjaśnienie rozwiązań kryptograficznych

Wdrażanie zarządzania tożsamością i dostępem

Architektura bezpiecznej sieci korporacyjnej

Architektura bezpiecznej sieci w chmurze

Wyjaśnienie koncepcji odporności i bezpieczeństwa witryny

Wyjaśnianie zarządzania podatnościami

Ocena możliwości w zakresie bezpieczeństwa sieci

Ocena możliwości w zakresie bezpieczeństwa punktów końcowych

Zwiększenie możliwości w zakresie bezpieczeństwa aplikacji

Analiza koncepcji reagowania na incydenty i monitorowania

Analizowanie wskaźników złośliwej aktywności

Podsumowanie koncepcji zarządzania bezpieczeństwem

Wyjaśnienie procesów zarządzania ryzykiem

Podsumowanie koncepcji ochrony danych i zgodności z przepisami

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 | 6 088,50 PLN |
| Koszt przypadający na 1 uczestnika netto | 4 950,00 PLN |
| Koszt osobogodziny brutto | 160,22 PLN |
| Koszt osobogodziny netto | 130,26 PLN |
| W tym koszt walidacji brutto | 1 918,80 PLN |
| W tym koszt walidacji netto | 1 560,00 PLN |

| | |
|-----------------------------------|----------|
| W tym koszt certyfikowania brutto | 0,00 PLN |
|-----------------------------------|----------|

| | |
|----------------------------------|----------|
| W tym koszt certyfikowania netto | 0,00 PLN |
|----------------------------------|----------|

Prowadzący

Liczba prowadzących: 1



1 z 1

Adam Kornacki

Trener z ponad 25 letnim doświadczeniem, Posiada tytuł Microsoft Certified Trainer oraz Trener CompTIA.

Prowadzi szkolenia z zakresu Serwerów Microsoft, Office 365, Cyberbezpieczeństwo, Azure, Exchange, SharePoint, SCCM, SCOM.

Posiada liczne referencje od Klientów z sektora publicznego oraz prywatnego. W roku 2022 przeprowadził ponad 60 szkoleń dla ponad 300 Uczestników. W zewnętrznym systemie badania satysfakcji Uczestników MTM uzyskał wysoką ocenę 8,54 w 9 stopniowej skali. Uczestnicy szczególnie cenią sobie przygotowanie merytoryczne do prowadzenia zajęć oraz sposób przekazywania wiedzy. Adam Kornacki profesjonalnie i ambitnie podchodzi do powierzonych zadań. W swojej karierze zdobył kilkadziesiąt autoryzowanych certyfikatów potwierdzających jego kompetencje.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe CompTIA. Uczestnik uzyskuje również dostęp do laboratoriów CompTIA, z których korzysta w dowolny sposób i w dowolnym momencie, za pośrednictwem przeglądarki internetowej.

Poza dostępnymi przekazywanymi Uczestnikowi, w trakcie szkolenia, Trener przedstawia i omawia autoryzowaną prezentację.

Informacje dodatkowe

Istnieje możliwość zastosowania zwolnienia z podatku VAT dla szkoleń mających charakter kształcenia zawodowego lub służących przekwalifikowaniu zawodowemu pracownikom, 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. zmieniającego 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;

kwalfikacja 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 odbywa się za pośrednictwem platformy **Microsoft Teams**, która umożliwia transmisję dwukierunkową, dzięki czemu 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 20Mb/s.
- wbudowane lub peryferyjne urządzenia do obsługi audio - słuchawki/głośniki 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