Możliwość dofinansowania

Szkolenie CompTIA SecurityX

Numer usługi 2025/05/05/142469/2725155

6 150,00 PLN brutto
5 000,00 PLN netto
175,71 PLN brutto/h
142,86 PLN netto/h
261,33 PLN cena rynkowa

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

197 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
35:00 h
21.09.2026 do 25.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie **CompTIA SecurityX** 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, które chcą rozwijać umiejętności na poziomie zaawansowanym. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój oraz Projektu Zachodniopomorskie Bony Szkoleniowe
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	02-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
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 SecurityX 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
Projektuje i wdraża systemy bezpieczeństwa zgodne z wymaganiami zarządzania, ryzyka i zgodności (GRC)	• identyfikuje i wdraża komponenty zarządzania bezpieczeństwem, • przeprowadza analizę ryzyka i planuje działania zaradcze, • wyjaśnia wpływ przepisów i norm na strategie bezpieczeństwa informacji, • analizuje wyzwania bezpieczeństwa przy wdrażaniu sztucznej inteligencji.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje odporną architekturę systemów IT zgodnie z wymaganiami bezpieczeństwa	• analizuje wymagania w celu zapewnienia odporności systemów, • projektuje systemy zgodne z założeniami bezpieczeństwa, • integruje mechanizmy kontrolne w cyklu życia systemu.	Test teoretyczny z wynikiem generowanym automatycznie
Wdraża mechanizmy dostępu, uwierzytelniania i autoryzacji w systemach informatycznych	• projektuje bezpieczne systemy IAM, • stosuje zasady Zero Trust w projektowaniu architektury, • wdraża mechanizmy kontroli dostępu w środowiskach chmurowych i lokalnych.	Test teoretyczny
Analizuje i rozwiązuje problemy związane z infrastrukturą sieciową i systemową w kontekście bezpieczeństwa	• diagnozuje zagrożenia w sieci i serwerach, • projektuje i wdraża zabezpieczenia infrastruktury IT, • rozwiązuje złożone problemy związane z bezpieczeństwem sieci.	Test teoretyczny z wynikiem generowanym automatycznie
Zabezpiecza punkty końcowe, serwery i systemy specjalistyczne przed zagrożeniami	• analizuje wymagania bezpieczeństwa urządzeń końcowych, • wdraża zabezpieczenia dla systemów specjalistycznych i zastanych, • monitoruje skuteczność wdrożonych środków ochronnych.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje techniki i technologie zabezpieczeń sprzętowych	• instaluje i konfiguruje mechanizmy ochrony sprzętowej, • analizuje zastosowania sprzętowych funkcji bezpieczeństwa w środowisku organizacyjnym.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykorzystuje automatyzację w celu zwiększenia poziomu bezpieczeństwa organizacji	• identyfikuje procesy możliwe do automatyzacji, • projektuje i wdraża rozwiązania automatyzujące działania zabezpieczające, • ocenia skuteczność automatyzacji w kontekście bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Wyjaśnia i stosuje zaawansowane techniki kryptograficzne w systemach informatycznych	• charakteryzuje koncepcje kryptograficzne i ich zastosowania, • dobiera odpowiednie techniki kryptograficzne do określonych przypadków użycia, • ocenia poziom bezpieczeństwa zastosowanych metod szyfrowania.	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje dane w celu monitorowania zagrożeń i reagowania na incydenty	• analizuje logi, dane i artefakty w kontekście wykrywania incydentów, • identyfikuje podatności i proponuje działania minimalizujące ryzyko, • prowadzi działania z zakresu threat hunting i threat intelligence.	Test teoretyczny z wynikiem generowanym automatycznie
Rekomenduje rozwiązania zwiększające odporność organizacji na ataki cybernetyczne	• ocenia aktualny poziom bezpieczeństwa organizacji, • dobiera odpowiednie rozwiązania technologiczne i procesowe, • planuje i wdraża działania zwiększające odporność cybernetyczną.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Szkolenie **CompTIA SecurityX** 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.

Szkolenie trwa 35 godzin zegarowych (tj. 40 godz. dydaktycznych + przerwy) i jest realizowane w ciągu 5 dni (po 8 godzin dydaktycznych dziennie).

Trener ma możliwość przesunięcia przerw, tak aby dostosować harmonogram do potrzeb uczestników.

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 (test teoretyczny z wynikiem generowanym automatycznie)

Program szkolenia

Zarządzanie, ryzyko i zgodność (GRC)

wdrażanie odpowiednich komponentów zarządzania

przeprowadzanie działań związanych z zarządzaniem ryzykiem

wyjaśnienie, jak zgodność wpływa na strategie bezpieczeństwa informacji

działania związane z modelowaniem zagrożeń

podsumowanie wyzwań związanych z bezpieczeństwem informacji w kontekście wdrażania sztucznej inteligencji (AI)

Architektura bezpieczeństwa

analiza wymagań w celu projektowania odpornych systemów

wdrażanie zabezpieczeń na wczesnych i kolejnych etapach cyklu życia systemów

integracja odpowiednich mechanizmów kontrolnych w projektowaniu bezpiecznej architektury

zastosowanie koncepcji bezpieczeństwa w projektowaniu systemów dostępu, uwierzytelniania i autoryzacji

bezpieczne wdrażanie funkcji chmurowych w środowisku przedsiębiorstwa

integracja koncepcji Zero Trust w projektowaniu architektury systemu

Inżynieria bezpieczeństwa

diagnozowanie typowych problemów z komponentami zarządzania tożsamością i dostępem (IAM) w środowisku przedsiębiorstwa

analiza wymagań w celu zwiększenia bezpieczeństwa punktów końcowych i serwerów

rozwiązywanie złożonych problemów związanych z bezpieczeństwem infrastruktury sieciowej

wdrażanie technologii i technik zabezpieczeń sprzętowych

zabezpieczanie systemów specjalistycznych i tzw. „systemów zastanych” przed zagrożeniami

wykorzystanie automatyzacji do zabezpieczania przedsiębiorstwa

wyjaśnienie znaczenia zaawansowanych koncepcji kryptograficznych oraz zastosowanie odpowiednich przypadków użycia i technik kryptograficznych

Operacje bezpieczeństwa

analiza danych w celu umożliwienia monitorowania i działań reagowania

analiza podatności i ataków oraz rekomendowanie rozwiązań w celu zmniejszenia powierzchni ataku

zastosowanie koncepcji wyszukiwania zagrożeń (threat hunting) i wywiadu o zagrożeniach (threat intelligence)

analiza danych i artefaktów w ramach działań związanych z reagowaniem 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.

Uczestnik/Uczestniczka ma obowiązek uczestnictwa w **minimum 80%** czasu trwania UR.

Sposób potwierdzania frekwencji na szkoleniu: raport z logowań na platformie Microsoft Teams.

Harmonogram

Liczba pozycji harmonogramu: 36

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Zarządzanie, ryzyko i zgodność (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	21-09-2026	09:00	10:45	01:45
2 z 36 -	Przerwa	-	21-09-2026	10:45	11:00	00:15
3 z 36 Zarządzanie, ryzyko i zgodność (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	21-09-2026	11:00	13:00	02:00
4 z 36 -	Przerwa	-	21-09-2026	13:00	13:30	00:30
5 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	21-09-2026	13:30	14:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 36 -	Przerwa	-	21-09-2026	14:30	14:45	00:15
7 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	21-09-2026	14:45	16:00	01:15
8 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	22-09-2026	09:00	10:45	01:45
9 z 36 -	Przerwa	-	22-09-2026	10:45	11:00	00:15
10 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	22-09-2026	11:00	13:00	02:00
11 z 36 -	Przerwa	-	22-09-2026	13:00	13:30	00:30
12 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	22-09-2026	13:30	14:30	01:00
13 z 36 -	Przerwa	-	22-09-2026	14:30	14:45	00:15
14 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	22-09-2026	14:45	16:00	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 36 Architektura bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	23-09-2026	09:00	10:45	01:45
16 z 36 -	Przerwa	-	23-09-2026	10:45	11:00	00:15
17 z 36 Architektura bezpieczeństwa, Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	23-09-2026	11:00	13:00	02:00
18 z 36 -	Przerwa	-	23-09-2026	13:00	13:30	00:30
19 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	23-09-2026	13:30	14:30	01:00
20 z 36 -	Przerwa	-	23-09-2026	14:30	14:45	00:15
21 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	23-09-2026	14:45	16:00	01:15
22 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	24-09-2026	09:00	10:45	01:45
23 z 36 -	Przerwa	-	24-09-2026	10:45	11:00	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	24-09-2026	11:00	13:00	02:00
25 z 36 -	Przerwa	-	24-09-2026	13:00	13:30	00:30
26 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	24-09-2026	13:30	14:30	01:00
27 z 36 -	Przerwa	-	24-09-2026	14:30	14:45	00:15
28 z 36 Inżynieria bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	24-09-2026	14:45	16:00	01:15
29 z 36 Operacje bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	25-09-2026	09:00	10:45	01:45
30 z 36 -	Przerwa	-	25-09-2026	10:45	11:00	00:15
31 z 36 Operacje bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	25-09-2026	11:00	13:00	02:00
32 z 36 -	Przerwa	-	25-09-2026	13:00	13:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 36 Operacje bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	25-09-2026	13:30	14:30	01:00
34 z 36 -	Przerwa	-	25-09-2026	14:30	14:45	00:15
35 z 36 Operacje bezpieczeństwa (on-line, na żywo, wykład + ćwiczenia)	Zajęcia	Zdzisław Knap	25-09-2026	14:45	15:45	01:00
36 z 36 -	Walidacja	-	25-09-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	35:00
w tym suma godzin zajęć	29:45
w tym suma godzin walidacji	00:15
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	40:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 150,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	175,71 PLN
Koszt osobogodziny netto	142,86 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	35:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Zdzisław Knap

Doświadczony trener i wykładowca, z 20-letnim doświadczeniem. Certyfikowany Akademicki Instruktor Novell NAI w zakresie Novell Netware i Suse Linux.
Poza branżowymi certyfikatami produktowymi posiada akredytacje trenerskie m.in Microsoft Certified Trainer MCT , Novell Academic Instruktor, Certyfikowany Trener CompTIA, Linux Professional Institute (LPI). Specjalizuje się w technologiach Linux, Microsoft oraz w zakresie cyberbezpieczeństwa. Jego umiejętności interpersonalne oraz szeroka wiedza merytoryczna jest wysoko oceniana przez uczestników.

Doświadczenie zawodowe zdobyte nie wcześniej niż 5 lat przed datą wprowadzenia szczegółowych danych dotyczących oferowanej usługi.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe CompTIA w formie elektronicznej:

- podręcznik w formie ebooka
- dostęp do środowiska laboratoryjnego

Warunki uczestnictwa

Przed przystąpieniem do szkolenia uczestnik powinien posiadać certyfikaty Network+, Security+, CySA+, Cloud+ i PenTest+ lub równoważną wiedzą. Wymagane co najmniej 10-letnie ogólne doświadczenie praktycznego w zakresie IT, w tym 5 lat doświadczenia praktycznego w zakresie bezpieczeństwa.

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;

Zawarto umowę z Wojewódzkim Urzędem Pracy w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe

kompetencja związana z cyfrową transformacją

UWAGA! Przed dokonaniem zgłoszenia / złożeniem wniosku o dofinansowanie prosimy o kontakt z SOFTRONIC w celu potwierdzenia terminu szkolenia oraz dostępności miejsc: e-mail: softronic@softronic.pl

Warunki techniczne

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/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