Możliwość dofinansowania

Szkolenie CompTIA SecurityX

Numer usługi 2025/05/05/142469/2725103

6 150,00 PLN brutto
5 000,00 PLN netto
153,75 PLN brutto/h
125,00 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
23.06.2025 do 27.06.2025

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 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 i chcą rozwijać umiejętności na poziomie zaawansowanym. Usługa adresowana również dla uczestników Projektu Kierunek – Rozwój oraz Projektu Małopolski Pociąg do Kariery - sezon 1.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	09-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40

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 przygotowuje uczestników do samodzielnego skuteczne zarządzania ryzykiem, opracowywania architektury bezpieczeństwa i wzmacniania odporności organizacji na cyberzagrożenia.

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	• projektuje bezpieczne systemy IAM, • stosuje zasady Zero Trust w projektowaniu architektury, • wdraża mechanizmy kontroli dostępu w środowiskach chmurowych i lokalnych.	Test teoretyczny z wynikiem generowanym automatycznie
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 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 **CompTIA SecurityX**zostało zaprojektowane, aby umożliwić uczestnikom rozwijanie zaawansowanych umiejętności w zakresie bezpieczeństwa IT. Uczestnicy zdobędą praktyczną wiedzę oraz kompetencje, umożliwiające skuteczne zarządzanie ryzykiem, opracowanie architektury bezpieczeństwa, wzmocnienie odporności organizacji na cyberzagrożenia, z uwzględnieniem aktualnych regulacji dotyczących cyberbezpieczeństwa, zaawansowane zarządzanie zagrożeniami, zarządzanie podatnościami, taktyką reagowania na incydenty. W trakcie szkolenia zostaną również omówione zagadnienia dotyczące konfiguracji kontroli bezpieczeństwa punktów końcowych, środowisk w chmurze/hybrydowych oraz rozwiązań PKI i kryptograficznych w całym przedsiębiorstwie.

Szkolenie składa się z wykładu wzbogaconego o prezentację. W trakcie szkolenia każdy uczestnik wykonuje indywidualne ćwiczenia - laboratoria, dzięki czemu zyskuje praktyczne umiejętności.

Szkolenie trwa **40 godzin dydaktycznych** i jest realizowane w ciągu 5 następujących po sobie dni.

Czas trwania przerw nie wlicza się do ogólnej liczby godzin trwania usługi szkoleniowej.

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.

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.

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	6 150,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	153,75 PLN
Koszt osobogodziny netto	125,00 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe CompTIA: ebook oraz dostęp do laboratoriów.

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;

Usługa skierowana również do uczestników Projektu Małopolski Pociąg do Kariery - sezon 1.

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 lub tel. 61 865 88 40

Chcesz nabyć kwalifikacje - prosimy o kontakt **tel. 61 865 88 40**

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, 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