Możliwość dofinansowania

Szkolenie CySA+ CompTIA Cybersecurity Analyst

Numer usługi 2025/07/02/142469/2852481

5 535,00 PLN brutto
4 500,00 PLN netto
138,38 PLN brutto/h
112,50 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

4,3 / 5

162 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
23.02.2026 do 27.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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,*** *projektu* ***Małopolski Pociąg do Kariery - sezon 1,*** *oraz projektu* ***Zachodniopomorskie Bony Szkoleniowe.***
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	23-01-2026
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 CompTIA CySA+ przygotowuje uczestników do samodzielnej 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
Definiuje proces analizy i polowania na zagrożenia w kontekście cyberbezpieczeństwa.	Wyjaśna etapy analizy zagrożeń oraz techniki wykorzystywane do wykrywania i śledzenia potencjalnych incydentów.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje podstawowe elementy architektury systemów i sieci.	Opisuje role i funkcje takie jak serwery, routery, firewall'e oraz ich wpływ na bezpieczeństwo IT.	Test teoretyczny z wynikiem generowanym automatycznie
Uzasadnia znaczenie ciągłego doskonalenia procesów bezpieczeństwa.	Przedstawia przykłady narzędzi lub metodologii używanych do doskonalenia operacyjnych procesów bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Implementuje narzędzia do skanowania podatności w systemach informatycznych.	Używa narzędzi do identyfikacji i klasyfikacji podatności w środowisku IT.	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza analizę słabych punktów w infrastrukturze IT.	Wykonuje test penetracyjny lub audyt bezpieczeństwa, identyfikując istniejące słabe punkty.	Test teoretyczny z wynikiem generowanym automatycznie
Komunikuje znalezione podatności i zalecane działania naprawcze.	Sporządza raport z wynikami skanowania lub audytu, opisujący znalezione podatności i zalecenia.	Test teoretyczny z wynikiem generowanym automatycznie
Reaguje na incydenty bezpieczeństwa w sposób zgodny z procedurami.	Opisuje kroki podejmowane podczas reakcji na incydent, w tym zarządzanie zdarzeniami i odzyskiwanie danych.	Test teoretyczny z wynikiem generowanym automatycznie
Przedstawia jasną i skuteczną komunikację podczas incydentów bezpieczeństwa.	Opisuje procesy informacyjne i komunikacyjne, które są stosowane podczas zarządzania incydentami bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
Używa narzędzi do detekcji i analizy złośliwej aktywności.	Korzysta z systemów detekcji złośliwego oprogramowania oraz interpretuje wyniki analizy złośliwych aktywności.	Test teoretyczny z wynikiem generowanym automatycznie
Współpracuje z innymi członkami zespołu w organizacji, korzystając z narzędzi do pracy grupowej w celu realizacji wyznaczonego celu lub projektu.	Identyfikuje wyzwania związane z wyznaczonym celem, planuje etapy ich realizacji, monitoruje ich wykonanie oraz ocenia ich efektywność. Współdzieli informacje z innym współpracownikami i wykorzystuje narzędzia do pracy nad danymi w ramach zespołów.	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

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 **CySA+ CompTIA Cybersecurity Analyst** przygotowuje uczestników do samodzielnej 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.

Szkolenie trwa 40 godzin dydaktycznych (1 godz. dydaktyczna = 45 minut) i jest realizowane w ciągu 5 dni.

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

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:

Operacje związane z bezpieczeństwem

Architektura systemu i sieci

Wskaźniki złośliwej aktywności

Narzędzia i techniki

Analiza zagrożeń i wykrywanie

Ulepszanie procesów

Zarządzanie podatnością na zagrożenia

Skanowanie podatności

Ocena i wyniki

Priorytetyzacja podatności

Środki ograniczające ryzyko

Reagowanie na podatności

Zarządzanie reagowaniem na incydenty

Ramy metodologii ataków

Działania w odpowiedzi na incydenty

Cykl życia zarządzania incydentami

Raportowanie i komunikacja

Raportowanie zarządzania podatnościami

Raportowanie 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. 5 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	138,38 PLN
Koszt osobogodziny netto	112,50 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdemu Uczestnikowi zostaną przekazane autoryzowane materiały szkoleniowe CompTIA w formie elektronicznej oraz dostęp do środowiska laboratoryjneg online.

Warunki uczestnictwa

Posiadanie certyfikatu CompTIA Network+, Security+ lub posiadanie równoważnej wiedzy. Co najmniej 4 lata praktycznego doświadczenia jako analityk reagowania na incydenty lub analityk centrum operacji bezpieczeństwa (SOC) lub doświadczenie równoważne.

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.

Zawarto umowę z WUP w Szczecinie na świadczenie usług rozwojowych z wykorzystaniem elektronicznych bonów szkoleniowych w ramach projektu Zachodniopomorskie Bony Szkoleniowe”.

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

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