Możliwość dofinansowania

Szkolenie C PenTest+ CompTIA z egzaminem

Numer usługi 2024/11/13/142469/2409533

7 644,45 PLN brutto
6 215,00 PLN netto
196,01 PLN brutto/h
159,36 PLN netto/h

SOFTRONIC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
39 h
03.02.2025 do 17.02.2025

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 PenTest+** jest skierowane do profesjonalistów ds. bezpieczeństwa informatycznego, testerów penetracyjnych oraz analityków bezpieczeństwa, którzy zajmują się identyfikacją i zwalczaniem zagrożeń cybernetycznych. Grupa docelowa obejmuje osoby z zaawansowaną wiedzą i doświadczeniem w dziedzinie testów penetracyjnych, które chcą rozwijać umiejętności w zakresie penetracji sieci i aplikacji. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	27-01-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	39
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 PenTest+ ma na celu dostarczenie zaawansowanej wiedzy i umiejętności testerom penetracyjnym oraz specjalistom ds. bezpieczeństwa informatycznego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje i charakteryzuje wymagania organizacyjne oraz klienta.	Analizuje i dokumentuje potrzeby organizacyjne i oczekiwania klienta. Przeprowadza wywiady i zbiera dane dotyczące wymagań. Uzasadnia wybrane metody identyfikacji wymagań.	Test teoretyczny
Tworzy i uzasadnia zasady zaangażowania w projekty bezpieczeństwa.	Opracowuje zasady i procedury zaangażowania dla różnych typów projektów. Komunikuje zasady zaangażowania zespołowi i interesariuszom. Monitoruje i ocenia zgodność działań z ustalonymi zasadami.	Test teoretyczny
Przeprowadza proces footprintingu i zbierania informacji.	Stosuje techniki footprintingu do identyfikacji zasobów organizacji. Zbiera i analizuje informacje z publicznie dostępnych źródeł. Dokumentuje wyniki procesu zbierania informacji.	Test teoretyczny
Analizuje i ocenia ludzkie oraz fizyczne słabe punkty w zabezpieczeniach.	Identyfikuje i klasyfikuje słabe punkty ludzkie i fizyczne. Przeprowadza testy symulacyjne w celu oceny tych słabych punktów. Dokumentuje i uzasadnia wyniki oceny.	Test teoretyczny
Przeprowadza skanowanie podatności logicznych systemów.	Konfiguruje i uruchamia narzędzia do skanowania podatności. Analizuje wyniki skanowania i identyfikuje podatności. Dokumentuje znalezione podatności i proponuje środki zaradcze.	Test teoretyczny
Stosuje techniki unikania wykrycia i zacierania śladów.	Przeprowadza testy penetracyjne z zastosowaniem technik unikania wykrycia. Stosuje metody zacierania śladów po przeprowadzonych atakach. Dokumentuje zastosowane techniki i ocenia ich skuteczność.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza testy bezpieczeństwa sieci bezprzewodowych.	Konfiguruje narzędzia do testowania sieci bezprzewodowych. Wykonuje testy penetracyjne na sieciach bezprzewodowych. Analizuje wyniki testów i proponuje środki zaradcze.	Test teoretyczny
Przeprowadza ataki na aplikacje internetowe w celach testowych.	Identyfikuje podatności aplikacji internetowych. Stosuje techniki ataków, takie jak SQL injection, XSS. Dokumentuje wyniki ataków i proponuje środki zaradcze.	Test teoretyczny
Pisze skrypty i oprogramowanie do celów testowania penetracyjnego.	Projektuje i implementuje skrypty automatyzujące testy bezpieczeństwa. Testuje i debugguje stworzone oprogramowanie. Dokumentuje skrypty i ich zastosowanie w testach.	Test teoretyczny
Proponuje środki zaradcze na podstawie przeprowadzonych testów.	Analizuje wyniki testów penetracyjnych i identyfikuje luki bezpieczeństwa. Opracowuje i uzasadnia rekomendacje dotyczące środków zaradczych. Przedstawia raport z rekomendacjami interesariuszom i klientom.	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 PenTest+** skupia się na zaawansowanych umiejętnościach z zakresu testów penetracyjnych. Uczestnicy zdobywają głęboką wiedzę z identyfikacji, oceny i eksploatacji potencjalnych luk w zabezpieczeniach sieci i aplikacji, wykorzystując różnorodne narzędzia i techniki. Program szkoleniowy umożliwia skuteczne przeprowadzanie testów penetracyjnych oraz dostarczanie szczegółowych raportów z zaleceniami bezpieczeństwa. Po ukończeniu szkolenia, absolwenci są przygotowani do roli specjalistów ds. testów penetracyjnych, oferując wartościowy wkład w zabezpieczanie organizacji przed cyberzagrożeniami.

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 Pentest+ **PT0-002**

Czas trwania egzaminu: 250 minut

Łączny czas realizacji usługi szkoleniowej wraz z egzaminem to 39 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

Określanie zakresu wymagań organizacyjnych/klienta

Definiowanie zasad zaangażowania

Footprinting i zbieranie informacji

Ocena ludzkich i fizycznych słabych punktów

Przygotowanie skanowania podatności

Skanowanie podatności logicznych

Analiza wyników skanowania

Unikanie wykrycia i zacieranie śladów

Wykorzystywanie sieci LAN i chmury

Testowanie sieci bezprzewodowych

Ataki na urządzenia mobilne

Atakowanie wyspecjalizowanych systemów

Ataki oparte na aplikacjach internetowych

Przeprowadzanie włamań do systemów

Tworzenie skryptów i oprogramowania

Wykorzystanie ataku: Obrót i penetracja

Komunikacja podczas procesu testowania penetracyjnego

Podsumowanie komponentów raportu

Rekomendowanie środków zaradczych

Wykonywanie działań po dostarczeniu raportu

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	7 644,45 PLN
Koszt przypadający na 1 uczestnika netto	6 215,00 PLN
Koszt osobogodziny brutto	196,01 PLN
Koszt osobogodziny netto	159,36 PLN

W tym koszt walidacji brutto	2 109,45 PLN
W tym koszt walidacji netto	1 715,00 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 Uczestnik powinien posiadać podstawową wiedzę z zakresu bezpieczeństwa informatycznego oraz znajomość podstawowych pojęć związanych z sieciami komputerowymi. Doświadczenie w administracji systemami oraz podstawowa znajomość protokołów sieciowych będzie również korzystne.

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;

kwalifikacja 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 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