Możliwość dofinansowania

Szkolenie CompTIA PenTest+

Numer usługi 2025/03/10/142469/2611177

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

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
30.06.2025 do 04.07.2025

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	02-06-2025
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 CompTIA PenTest+ przygotowuje Uczestników do samodzielnego planowania i określania zakresu testów penetracyjnych zgodnie z wymaganiami zgodności, przeprowadzania działań związanych z enumeracją i rozpoznaniem, analizowania podatności, przeprowadzania ataków, eksfiltrowania danych oraz przygotowywania pisemnych raportów z technikami naprawczymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje zakres i cele testów penetracyjnych, uwzględniając wymagania organizacyjne, prawne i etyczne.	• Analizuje i interpretuje regulacje dotyczące testów penetracyjnych. • Opracowuje plan testu penetracyjnego zgodnie z określonym zakresem i wymaganiami prawnymi. • Dobiera odpowiednie narzędzia i metody testowania. wykorzystuje chmurę do symulacji i testowania zewnętrznych ataków, analizuje zalety i wyzwania związane z wykorzystaniem sieci LAN i chmury w testowaniu.	Test teoretyczny
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
Stosuje techniki zbierania informacji o docelowej infrastrukturze IT, identyfikuje punkty wejścia i potencjalne podatności.	• Wykorzystuje techniki pasywnego i aktywnego rozpoznania (np. OSINT, skanowanie sieci). • Identyfikuje usługi, protokoły i systemy operacyjne działające w docelowym środowisku. • Dokumentuje wyniki rozpoznania w strukturze raportu testu penetracyjnego.	Test teoretyczny
Przeprowadza testy podatności, ocenia poziom zagrożenia i wykonuje kontrolowane ataki.	• Wykonuje skanowanie podatności przy użyciu specjalistycznych narzędzi (np. Nessus, OpenVAS). • Selekcjonuje i klasyfikuje podatności według stopnia krytyczności. • Wdraża kontrolowane ataki (np. SQL Injection, XSS, brute-force) w bezpiecznym środowisku testowym.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Przeprowadza ataki w celu uzyskania nieautoryzowanego dostępu, analizuje skutki naruszenia oraz stosuje techniki ukrywania śladów.	• Wykorzystuje techniki ataków, takie jak privilege escalation, pass-the-hash, pivoting. • Ocenia skuteczność przeprowadzonych ataków i proponuje środki zaradcze. • Dokumentuje przebieg ataku w raporcie technicznym.	Test teoretyczny
Sporządza raport z testu penetracyjnego, rekomenduje działania korygujące i komunikuje wyniki zainteresowanym stronom.	• Strukturyzuje raport zawierający opis metodyki, wyniki testów i rekomendacje. • Przedstawia wyniki w sposób zrozumiały dla różnych grup odbiorców (zarząd, dział IT, audytorzy). • Proponuje środki zabezpieczające eliminujące wykryte podatności.	Test teoretyczny

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 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.

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.

Kurs obejmuje **40 godzin dydaktycznych** (45 min), prowadzonych na żywo (on-line), na platformie Microsoft Teams, w formie wirtualnej klasy na żywo z trenerem. Czas trwania przerw nie wlicza się do ogólnej liczby godzin trwania usługi.

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

Szkolenie jest realizowane w ciągu 5 dni.

Program szkolenia

Przed rozpoczęciem szkolenia Uczestnik rozwiązuje pre-test badający poziom wiedzy na wstępie.

Działania wstępne

Zastosowanie działań przedtestowych

Rekonesans i enumeracja

Skanowanie i identyfikacja podatności

Przeprowadzanie ataków pentestowych

Ataki webowe

Ataki na środowiska korporacyjne

Ataki specjalistyczne

Wykonywanie zadań testów penetracyjnych

Raportowanie i rekomendacje

Walidacja: Na koniec usługi Uczestnik wykonuje post-test w celu dokonania oceny wzrostu poziomu wiedzy.

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	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: 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:

- dostęp do podręcznika w wersji elektronicznej
- dostęp do środowiska laboratoryjnego

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

Warunki uczestnictwa

Przed przystąpieniem do szkolenia uczestnik powinien ukończyć kurs CompTIA Network+, CompTIA Security+ lub posiadać wiedzę równoważną. Zalecane posiadanie doświadczenia: 3-4 lata na stanowisku testera penetracyjnego.

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;

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

Warunki techniczne

Szkolenie realizowane jest w formule distance learning - szkolenie **on-line w czasie rzeczywistym**, w którym możesz wziąć udział zkażdego 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