Możliwość dofinansowania

Szkolenie CompTIA PenTest+

Numer usługi 2025/12/04/142469/3191114

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

166 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
40 h
02.02.2026 do 06.02.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
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 Małopolski Pociąg do Kariery - sezon 1*oraz projektu* ***Zachodniopomorskie Bony Szkoleniowe.***
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	09-01-2026
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 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.	Test teoretyczny z wynikiem generowanym automatycznie
	• Opracowuje plan testu penetracyjnego zgodnie z określonym zakresem i wymaganiami prawnymi.	Test teoretyczny z wynikiem generowanym automatycznie
	• Dobiera odpowiednie narzędzia i metody testowania.	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje chmurę do symulacji i testowania zewnętrznych ataków, analizuje zalety i wyzwania związane z wykorzystaniem sieci LAN i chmury w testowaniu.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje techniki zbierania informacji o docelowej infrastrukturze IT, identyfikuje punkty wejścia i potencjalne podatności.	• Wykorzystuje techniki pasywnego i aktywnego rozpoznania (np. OSINT, skanowanie sieci).	Test teoretyczny z wynikiem generowanym automatycznie
	• Identyfikuje usługi, protokoły i systemy operacyjne działające w docelowym środowisku.	Test teoretyczny z wynikiem generowanym automatycznie
	• Dokumentuje wyniki rozpoznania w strukturze raportu testu penetracyjnego.	Test teoretyczny z wynikiem generowanym automatycznie
Przeprowadza testy podatności, ocenia poziom zagrożenia i wykonuje kontrolowane ataki.	• Wykonuje skanowanie podatności przy użyciu specjalistycznych narzędzi (np. Nessus, OpenVAS).	Test teoretyczny z wynikiem generowanym automatycznie
	• Selekcjonuje i klasyfikuje podatności według stopnia krytyczności.	Test teoretyczny z wynikiem generowanym automatycznie
	• Wdraża kontrolowane ataki (np. SQL Injection, XSS, brute-force) w bezpiecznym środowisku testowym.	Test teoretyczny z wynikiem generowanym automatycznie

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.	Test teoretyczny z wynikiem generowanym automatycznie
	• Ocenia skuteczność przeprowadzonych ataków i proponuje środki zaradcze.	Test teoretyczny z wynikiem generowanym automatycznie
	• Dokumentuje przebieg ataku w raporcie technicznym.	Test teoretyczny z wynikiem generowanym automatycznie
Sporządza raport z testu penetracyjnego, rekomenduje działania korygujące i komunikuje wyniki zainteresowanym stronom.	• Strukturyzuje raport zawierający opis metodyki, wyniki testów i rekomendacje.	Test teoretyczny z wynikiem generowanym automatycznie
	• Przedstawia wyniki w sposób zrozumiały dla różnych grup odbiorców (zarząd, dział IT, audytorzy).	Test teoretyczny z wynikiem generowanym automatycznie
	• Proponuje środki zabezpieczające eliminujące wykryte podatności.	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 **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.

Walidacja będzie miała formę testu teoretycznego z wynikiem generowanym automatycznie.

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.

Zarządzanie zaangażowaniem

Planowanie i określanie zakresu

Zgodność z przepisami prawnymi i zasadami etycznymi

Współpraca i komunikacja

Raporty z testów penetracyjnych

Rozpoznanie i enumeracja

Rozpoznanie aktywne i pasywne

Techniki enumeracji

Narzędzia rozpoznawcze

Modyfikacja skryptów

Wykrywanie i analiza podatności

Skanowanie podatności

Analiza wyników

Narzędzia wykrywające

Ataki i exploity

Ataki sieciowe

Ataki uwierzytelniające

Ataki oparte na hoście

Ataki na aplikacje internetowe

Ataki oparte na chmurze

Ataki AI

Wykorzystanie luk i ruch boczny

Działania po wykorzystaniu luk

Dokumentacja

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: 36

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Zarządzanie zaangażowaniem (on-line, na żywo, wykład)	Zdzisław Knap	02-02-2026	09:00	10:45	01:45
2 z 36 Przerwa	Zdzisław Knap	02-02-2026	10:45	11:00	00:15
3 z 36 Zarządzanie zaangażowaniem (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	02-02-2026	11:00	13:00	02:00
4 z 36 Przerwa	Zdzisław Knap	02-02-2026	13:00	13:30	00:30
5 z 36 Zarządzanie zaangażowaniem (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	02-02-2026	13:30	14:30	01:00
6 z 36 Przerwa	Zdzisław Knap	02-02-2026	14:30	14:45	00:15
7 z 36 Zarządzanie zaangażowaniem (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	02-02-2026	14:45	16:00	01:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 36 Rekonesans i enumeracja (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	03-02-2026	09:00	10:45	01:45
9 z 36 Przerwa	Zdzisław Knap	03-02-2026	10:45	11:00	00:15
10 z 36 Rekonesans i enumeracja (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	03-02-2026	11:00	13:00	02:00
11 z 36 Przerwa	Zdzisław Knap	03-02-2026	13:00	13:30	00:30
12 z 36 Wykrywanie i analiza podatności (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	03-02-2026	13:30	14:30	01:00
13 z 36 Przerwa	Zdzisław Knap	03-02-2026	14:30	14:45	00:15
14 z 36 Wykrywanie i analiza podatności (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	03-02-2026	14:45	16:00	01:15
15 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	04-02-2026	09:00	10:45	01:45
16 z 36 Przerwa	Zdzisław Knap	04-02-2026	10:45	11:00	00:15
17 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	04-02-2026	11:00	13:00	02:00
18 z 36 Przerwa	Zdzisław Knap	04-02-2026	13:00	13:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	04-02-2026	13:30	14:30	01:00
20 z 36 Przerwa	Zdzisław Knap	04-02-2026	14:30	14:45	00:15
21 z 36 Ataki i exploity(on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	04-02-2026	14:45	16:00	01:15
22 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	05-02-2026	09:00	10:45	01:45
23 z 36 Przerwa	Zdzisław Knap	05-02-2026	10:45	11:00	00:15
24 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	05-02-2026	11:00	13:00	02:00
25 z 36 Przerwa	Zdzisław Knap	05-02-2026	13:00	13:30	00:30
26 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	05-02-2026	13:30	14:30	01:00
27 z 36 Przerwa	Zdzisław Knap	05-02-2026	14:30	14:45	00:15
28 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	05-02-2026	14:45	16:00	01:15
29 z 36 Ataki i exploity (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	06-02-2026	09:00	10:45	01:45
30 z 36 Przerwa	Zdzisław Knap	06-02-2026	10:45	11:00	00:15
31 z 36 Wykorzystanie luk i ruch boczny (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	06-02-2026	11:00	13:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
32 z 36 Przerwa	Zdzisław Knap	06-02-2026	13:00	13:30	00:30
33 z 36 Wykorzystanie luk i ruch boczny (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	06-02-2026	13:30	14:30	01:00
34 z 36 Przerwa	Zdzisław Knap	06-02-2026	14:30	14:45	00:15
35 z 36 Wykorzystanie luk i ruch boczny (on-line, na żywo, wykład + ćwiczenia)	Zdzisław Knap	06-02-2026	14:45	15:45	01:00
36 z 36 Walidacja: post-test (test teoretyczny z wynikiem generowanym automatycznie)	-	06-02-2026	15:45	16:00	00:15

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 - ebook
- 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**;

Zawarto umowę z WUP w Szczecinie na świadczenie usług rozwojowych w ramach **Projektu Zachodniopomorskie Bony Szkoleniowe.**

Usługa jest skierowana do Uczestników Projektu MP.

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 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