



SOFTRONIC
SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ
★★★★☆

Szkolenie CompTIA Security+ z egzaminem

Numer usługi 2025/03/10/142469/2611248

📍 zdalna w czasie rzeczywistym
🏠 Usługa szkoleniowa
🕒 43 h
📅 05.05.2025 do 06.06.2025

6 088,50 PLN brutto
4 950,00 PLN netto
141,59 PLN brutto/h
115,12 PLN netto/h

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 Security+ jest skierowane do profesjonalistów IT, którzy zajmują się zapewnianiem bezpieczeństwa informacji w organizacjach. Grupa docelowa obejmuje administratorów systemów, inżynierów bezpieczeństwa, specjalistów ds. sieci oraz wszystkich, którzy odpowiedzialni są za ochronę danych i infrastruktury przed zagrożeniami cybernetycznymi. Usługa adresowana również dla Uczestników Projektu Kierunek – Rozwój
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	7
Data zakończenia rekrutacji	21-04-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	43
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 Security+ przygotowuje Uczestników do samodzielnego skutecznego zapewniania bezpieczeństwa informacji w środowisku IT. Szkolenie koncentruje się na kluczowych aspektach ochrony danych, identyfikacji zagrożeń oraz stosowaniu skutecznych praktyk bezpieczeństwa, przygotowując profesjonalistów do skutecznego radzenia sobie z wyzwaniami związanymi z cyberbezpieczeństwem.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Rozumie podstawowe koncepcje bezpieczeństwa oraz typy zagrożeń.	Definiuje i wyjaśnia podstawowe terminy i koncepcje związane z bezpieczeństwem informacji. Identyfikuje i klasyfikuje różne typy zagrożeń (np. wirusy, malware, ataki DDoS). Porównuje skuteczność różnych strategii obrony przed zagrożeniami.	Test teoretyczny
Wyjaśnia i wdraża rozwiązania kryptograficzne.	Opisuje podstawowe mechanizmy kryptograficzne (np. szyfrowanie symetryczne, asymetryczne). Implementuje szyfrowanie danych za pomocą różnych metod. Wyjaśnia rolę certyfikatów cyfrowych i zarządza nimi.	Test teoretyczny
Wdraża zarządzanie tożsamością i dostępem.	Konfiguruje systemy zarządzania tożsamością (IAM). Definiuje i przyznaje role oraz uprawnienia użytkowników. Monitoruje i kontroluje dostęp do zasobów systemowych.	Test teoretyczny
Projektuje i implementuje architekturę bezpiecznej sieci korporacyjnej oraz w chmurze.	Opracowuje plan bezpiecznej architektury sieci korporacyjnej. Konfiguruje elementy bezpieczeństwa w sieci korporacyjnej (np. zapory ogniowe, VPN). Implementuje zasady bezpieczeństwa w środowisku chmurowym.	Test teoretyczny
Wyjaśnia koncepcje odporności, zarządzania podatnościami oraz oceny możliwości bezpieczeństwa.	Definiuje metody zwiększania odporności infrastruktury IT. Prowadzi procesy zarządzania podatnościami (np. skanowanie podatności, patch management). Przeprowadza ocenę możliwości w zakresie bezpieczeństwa sieci i punktów końcowych.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zwiększa bezpieczeństwo aplikacji oraz reaguje na incydenty i monitoruje bezpieczeństwo.	Implementuje rozwiązania zwiększające bezpieczeństwo aplikacji. Monitoruje systemy pod kątem incydentów bezpieczeństwa. Przeprowadza analizę i reakcję na incydenty bezpieczeństwa.	Test teoretyczny
Analizuje wskaźniki złośliwej aktywności oraz zarządza bezpieczeństwem.	Identyfikuje wskaźniki kompromitacji (IoC) i analizuje złośliwą aktywność. Opracowuje i wdraża polityki bezpieczeństwa organizacji. Monitoruje przestrzeganie polityk bezpieczeństwa.	Test teoretyczny
Wyjaśnia procesy zarządzania ryzykiem.	Definiuje i ocenia ryzyko związane z bezpieczeństwem informacji. Stosuje metody zarządzania ryzykiem (np. analiza ryzyka, plany awaryjne). Monitoruje i raportuje poziom ryzyka.	Test teoretyczny
Podsumowuje koncepcje ochrony danych oraz zgodności z przepisami.	Wyjaśnia koncepcje ochrony danych. Implementuje procedury zgodności z przepisami ochrony danych. Monitoruje i raportuje zgodność z przepisami.	Test teoretyczny
Korzysta z narzędzi pomocniczych i skryptowych oraz wdraża procedury operacyjne.	Używa narzędzi do monitorowania i analizowania bezpieczeństwa (np. SIEM, IDS). Implementuje i utrzymuje procedury operacyjne w zakresie bezpieczeństwa.	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

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

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	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
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 Security+** ma na celu wyposażenie uczestników w zaawansowaną wiedzę i umiejętności z zakresu bezpieczeństwa informacyjnego. Uczestnicy zdobędą umiejętności w identyfikacji, analizie i reakcji na różnorodne zagrożenia cybernetyczne. Szkolenie skupia się również na konfiguracji i zarządzaniu zabezpieczeniami systemów operacyjnych i aplikacji, umożliwiając profesjonalistom skuteczne ochrona organizacji przed atakami. Po ukończeniu szkolenia, uczestnicy będą przygotowani do pełnienia roli specjalistów ds. bezpieczeństwa informacyjnego oraz skutecznego zarządzania aspektami cyberbezpieczeństwa w organizacjach.

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.

Egzamin CompTIA Security+ 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.

Egzamin wpisany w harmonogramie ma prawdopodobny termin i godzinę. Dokładny termin egzaminu będzie ustalany indywidualnie z Uczestnikiem.

Uczestnik, który zda egzamin CompTIA Security+ SY0-701 otrzymuje międzynarodowy Certyfikat CompTIA Security+ w formie elektronicznej.

Szkolenie trwa 40 godzin dydaktycznych (1 godz. dydaktyczna = 45 minut) i jest realizowane w ciągu 5 dni + egzamin 3 godz.

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

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

Łączny czas trwania usługi: 43 godziny dydaktyczne

Szkolenie jest prowadzone na żywo (on-line), na platformie Microsoft Teams.

PROGRAM SZKOLENIA

Podsumowanie podstawowych koncepcji bezpieczeństwa

Porównanie typów zagrożeń

Wyjaśnienie rozwiązań kryptograficznych

Wdrażanie zarządzania tożsamością i dostępem

Architektura bezpiecznej sieci korporacyjnej

Architektura bezpiecznej sieci w chmurze

Wyjaśnienie koncepcji odporności i bezpieczeństwa witryny

Wyjaśnianie zarządzania podatnościami

Ocena możliwości w zakresie bezpieczeństwa sieci

Ocena możliwości w zakresie bezpieczeństwa punktów końcowych

Zwiększenie możliwości w zakresie bezpieczeństwa aplikacji

Analiza koncepcji reagowania na incydenty i monitorowania

Analizowanie wskaźników złośliwej aktywności

Podsumowanie koncepcji zarządzania bezpieczeństwem

Wyjaśnienie procesów zarządzania ryzykiem

Podsumowanie koncepcji ochrony danych i zgodności z przepisami

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 Podsumowanie podstawowych koncepcji bezpieczeństwa (on-line, na żywo, wykład)	Patryk Łączny	05-05-2025	09:00	10:30	01:30
2 z 36 Przerwa	Patryk Łączny	05-05-2025	10:30	10:45	00:15
3 z 36 Porównanie typów zagrożeń (on-line, na żywo, wykład)	Patryk Łączny	05-05-2025	10:45	12:15	01:30
4 z 36 Przerwa	Patryk Łączny	05-05-2025	12:15	12:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 36 Porównanie typów zagrożeń (on-line, na żywo, wykład)	Patryk Łączny	05-05-2025	12:30	14:00	01:30
6 z 36 Przerwa	Patryk Łączny	05-05-2025	14:00	14:30	00:30
7 z 36 Wyjaśnienie rozwiązań kryptograficznych (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	05-05-2025	14:30	16:00	01:30
8 z 36 Wdrażanie zarządzania tożsamością i dostępem (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	06-05-2025	09:00	10:30	01:30
9 z 36 Przerwa	Patryk Łączny	06-05-2025	10:30	10:45	00:15
10 z 36 Wdrażanie zarządzania tożsamością i dostępem (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	06-05-2025	10:45	12:15	01:30
11 z 36 Przerwa	Patryk Łączny	06-05-2025	12:15	12:30	00:15
12 z 36 Architektura bezpiecznej sieci korporacyjnej (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	06-05-2025	12:30	14:00	01:30
13 z 36 Przerwa	Patryk Łączny	06-05-2025	14:00	14:30	00:30
14 z 36 Architektura bezpiecznej sieci w chmurze (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	06-05-2025	14:30	16:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 36 Wyjaśnienie koncepcji odporności i bezpieczeństwa witryny (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	07-05-2025	09:00	10:30	01:30
16 z 36 Przerwa	Patryk Łączny	07-05-2025	10:30	10:45	00:15
17 z 36 Wyjaśnianie zarządzania podatnościami (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	07-05-2025	10:45	12:15	01:30
18 z 36 Przerwa	Patryk Łączny	07-05-2025	12:15	12:30	00:15
19 z 36 Wyjaśnianie zarządzania podatnościami (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	07-05-2025	12:30	14:00	01:30
20 z 36 Przerwa	Patryk Łączny	07-05-2025	14:00	14:30	00:30
21 z 36 Ocena możliwości w zakresie bezpieczeństwa sieci (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	07-05-2025	14:30	16:00	01:30
22 z 36 Ocena możliwości w zakresie bezpieczeństwa punktów końcowych (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	08-05-2025	09:00	10:30	01:30
23 z 36 Przerwa	Patryk Łączny	08-05-2025	10:30	10:45	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 36 Zwiększenie możliwości w zakresie bezpieczeństwa aplikacji (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	08-05-2025	10:45	12:15	01:30
25 z 36 Przerwa	Patryk Łączny	08-05-2025	12:15	12:30	00:15
26 z 36 Analiza koncepcji reagowania na incydenty i monitorowania (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	08-05-2025	12:30	14:00	01:30
27 z 36 Przerwa	Patryk Łączny	08-05-2025	14:00	14:30	00:30
28 z 36 Analizowanie wskaźników złośliwej aktywności (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	08-05-2025	14:30	16:00	01:30
29 z 36 Analizowanie wskaźników złośliwej aktywności (on-line, na żywo, wykład + ćwiczenia)	Patryk Łączny	09-05-2025	09:00	10:30	01:30
30 z 36 Przerwa	Patryk Łączny	09-05-2025	10:30	10:45	00:15
31 z 36 Podsumowanie koncepcji zarządzania bezpieczeństwem (on-line, na żywo, wykład)	Patryk Łączny	09-05-2025	10:45	12:15	01:30
32 z 36 Przerwa	Patryk Łączny	09-05-2025	12:15	12:30	00:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 36 Wyjaśnienie procesów zarządzania ryzykiem (online, na żywo, wykład)	Patryk Łączny	09-05-2025	12:30	14:00	01:30
34 z 36 Przerwa	Patryk Łączny	09-05-2025	14:00	14:30	00:30
35 z 36 Podsumowanie koncepcji ochrony danych i zgodności z przepisami (online, na żywo, wykład)	Patryk Łączny	09-05-2025	14:30	16:00	01:30
36 z 36 Egzamin CompTIA Security SY0-701	-	06-06-2025	09:00	11:15	02:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 088,50 PLN
Koszt przypadający na 1 uczestnika netto	4 950,00 PLN
Koszt osobogodziny brutto	141,59 PLN
Koszt osobogodziny netto	115,12 PLN
W tym koszt walidacji brutto	1 918,80 PLN
W tym koszt walidacji netto	1 560,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Patryk Łączny

certyfikowany trener Microsoft (MCT), absolwent Politechniki Warszawskiej – Wydział Elektryczny. Posiada ponad 10-letnie doświadczenie zawodowe w prowadzeniu szkoleń informatycznych. Zdobył m.in. certyfikaty Microsoft Certified Trainer, Microsoft Office Specialist, Microsoft 365 Certified Modern Desktop Administrator Associate, CompTIA IT Fundamentals, Microsoft Certified Professional. Specjalizuje się w prowadzeniu szkoleń z zakresu Microsoft Office, systemy klienckie Windows oraz Windows Server. Zrealizował szkolenia dla setek Klientów z sektora publicznego oraz prywatnego, co potwierdzają liczne referencje. 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:

- podręcznik w formie ebooka
- dostęp do środowiska laboratoryjnego

Warunki uczestnictwa

Przed przystąpieniem do szkolenia zaleca się posiadanie Certyfikatu CompTIA Network+ lub wiedzy równoważnej i dwuletniego doświadczenie na stanowisku administratora systemów/zabezpieczeń

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;

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 z każdego miejsca na świecie.

Szkolenie odbywa 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