Możliwość dofinansowania

CompTIA Security + wraz z egzaminem SY0-701 - szkolenie autoryzowane - forma zdalna w czasie rzeczywistym

Numer usługi 2026/02/25/120967/3362388

7 134,00 PLN brutto
5 800,00 PLN netto
198,17 PLN brutto/h
161,11 PLN netto/h
261,33 PLN cena rynkowa

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

4,4 / 5

2 693 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
36:00 h
08.06.2026 do 12.07.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji. Od Uczestników wymagana jest ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	14
Data zakończenia rekrutacji	27-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	36
Podstawa uzyskania wpisu do BUR	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

Cel

Cel edukacyjny

Usługa przygotowuje Uczestnika do analizy ryzyka, planowania ciągłości działania, zachowania bezpieczeństwa informacyjnego, bezpieczeństwa systemów i sieci teleinformatycznych. Uczestnik po szkoleniu charakteryzuje

podstawowe koncepcje bezpieczeństwa, rozróżnia typy zagrożeń, wdraża zarządzanie tożsamością i kontrolą dostępu, zabezpiecza architekturę sieci w usługach chmurowych, zarządza incydentami i monitoruje środowisko.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Charakteryzuje podstawowe koncepcje bezpieczeństwa	- charakteryzuje mechanizmy kontrolne bezpieczeństwa	Test teoretyczny
Rozróżnia typy zagrożeń	- charakteryzuje typy zagrożeń - definiuje przestrzenie ataku	Test teoretyczny
Wdraża zarządzanie tożsamością i kontrolą dostępu	- charakteryzuje uwierzytelnianie, autoryzację, zarządzanie tożsamością	Test teoretyczny
Zabezpiecza architekturę sieci w usługach chmurowych	- charakteryzuje infrastrukturę chmurową - charakteryzuje systemy wbudowane - charakteryzuje architekturę Zero Trust	Test teoretyczny
Zarządza incydentami i monitoruje środowisko	- charakteryzuje zasady reagowania na incydenty - charakteryzuje narzędzia do monitorowania	Test teoretyczny

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: https://www.comptia.org/en/certifications/security

Strona internetowa Instytucji Walidującej: https://www.pearsonvue.com/us/en/comptia

Informacje

Nazwa Podmiotu prowadzącego walidację	Pearson Vue
Nazwa Podmiotu certyfikującego	CompTIA

Program

Adresaci szkolenia

Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji.

Od Uczestników wymagana jest ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

Warunki organizacyjne

- Szkolenie realizowane jest w formule **zdalnej, w czasie rzeczywistym)**, z wykorzystaniem platformy wideokonferencyjnej (Zoom).
- Szkolenie realizowane jest w terminie 08-12.06.2026. Uczestnik ma 30 dni po szkoleniu na podejście do egzaminu.
- Grupa szkoleniowa liczy maksymalnie 14 uczestników, co pozwala na interaktywną pracę (zadania praktyczne, dyskusje) w komfortowych warunkach.
- W trakcie szkolenia uczestnicy wykonują samodzielnie ćwiczenia z możliwością konsultacji z trenerem.
- Każdy uczestnik powinien dysponować własnym stanowiskiem komputerowym z dostępem do Internetu – **dostawca usługi nie zapewnia sprzętu ani pomieszczenia do udziału w szkoleniu.**
- Materiały szkoleniowe (np. prezentacje, instrukcje do laboratoriów) są udostępniane w formie elektronicznej na dedykowanej platformie Altkom Akademii (dostęp wysyłany mailowo uczestnikom przed rozpoczęciem szkolenia).
- Efekty uczenia się zostaną zweryfikowane poprzez egzamin w formie testu.
- Uczestnik szkolenia otrzymuje Voucher na egzamin: CompTIA Security+ SY0-701.
- Po zakończeniu szkolenia uczestnik indywidualnie zapisuje się na egzamin na platformie PearsonVue, w dostępnym dniu i godzinie. Podana data i godzina w harmonogramie jest więc jedynie data orientacyjną. **Egzamin musi się odbyć najpóźniej do dnia zakończenia realizacji usługi opublikowanej w karcie usługi w BUR.**

Szkolenie obejmuje:

- 5 dni pracy z trenerem
- Nadzór trenera
- Kontakt ze społecznością
- Autoryzowany podręcznik: The Official CompTIA Security+ Self-Paced Study Guide (Exam SY0-701) eBook - w języku angielskim
- Środowisko laboratoryjne do pracy własnej – ważne 12 miesięcy
- Voucher na egzamin: CompTIA Security+ SY0-701

Liczba godzin usługi szkoleniowej

Szkolenie liczy łącznie: **36,5 godziny zegarowej** (35 godzin szkolenia + 90 minut egzaminu realizowanego przez zewnętrzny podmiot certyfikujący)**.** Przerwy wliczają się do czasu trwania usługi. Trener ma możliwość przesunięcia przerw, tak aby dostosować harmonogram do potrzeb uczestników.

Łączny czas realizacji usługi szkoleniowej rozłożony jest na **5 dni roboczych.**

- **21 godzin – część teoretyczna** (wykłady, prezentacje, omówienie przykładów),
- **14 godzin – część praktyczna** (ćwiczenia laboratoryjne, case study, konfiguracje w środowisku testowym).

PROGRAM SZKOLENIA

1. Podstawowe koncepcje bezpieczeństwa

- terminologia, koncepcje
- mechanizmy kontrolne bezpieczeństwa

1. Porównanie różnych typów zagrożeń

- aktorzy-zagrożenia
- przestrzenie ataku
- inżynieria społeczna

1. Omówienie podstawowych pojęć kryptografii

- algorytmy kryptograficzne,
- infrastruktura PKI
- rozwiązania kryptograficzne

1. Wdrażanie zarządzania tożsamością i kontrolą dostępu

- uwierzytelnianie
- autoryzacja
- zarządzanie tożsamością

1. Zabezpieczanie architektury sieci korporacyjnej

- architektura sieci korporacyjnej
- urządzenia zabezpieczające sieć
- bezpieczna komunikacja

1. Zabezpieczanie architektury sieci w usługach chmurowych

- infrastruktura chmurowa
- systemy wbudowane
- architektura Zero Trust

1. Omówienie koncepcji odporności

- zarządzanie aktywami
- strategie redundancji
- bezpieczeństwo fizyczne

1. Zarządzanie podatnościami

- podatności w urządzeniach i systemach operacyjnych
- luki w oprogramowaniu i usługach chmurowych
- metody identyfikacji luk w zabezpieczeniach
- analiza i usuwanie luk w zabezpieczeniach

1. Bezpieczeństwo sieciowe

- podstawowe założenia dotyczące bezpieczeństwa sieci
- podnoszenie poziomu bezpieczeństwa sieci

1. Ocena bezpieczeństwa punktów końcowych

- wdrażanie zabezpieczeń punktów końcowych
- wdrażanie zabezpieczeń urządzeń mobilnych

1. Wdrażanie zabezpieczeń aplikacji

- wytyczne dla zabezpieczania aplikacji
- koncepcje bezpieczeństwa aplikacji w chmurze i sieci Web

1. Zarządzanie incydentami i monitorowanie środowiska

- reagowanie na incydenty
- informatyka śledcza
- narzędzia do monitorowania

1. Po czym rozpoznać atak – wskaźniki kompromitacji

- ataki złośliwym oprogramowaniem
- ataki fizyczne i sieciowe
- ataki na aplikacje

1. Egzamin

Metoda egzaminacyjna:

- Do egzaminu można przystąpić w Pearson Vue.
    - Tytuł – CompTIA Security+
- Format testu: Kombinacja pytań wielokrotnego wyboru, ćwiczenia drag and drops, oraz elementów opartych na rozwiązywaniu problemu – wynikach
- Ilość pytań – max 90
- Czas trwania – 90 min
- Szczegółowe informacje dotyczące egzaminu znajdują się na stronie Comptia: https://www.comptia.org/en-eu/blog/what-is-on-the-comptia-security-exam/

Harmonogram

Liczba pozycji harmonogramu: 26

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Podstawowe koncepcje bezpieczeństwa_wykład	Adam Przybysz	08-06-2026	10:00	11:40	01:40
2 z 26 Przerwa	Adam Przybysz	08-06-2026	11:40	11:55	00:15
3 z 26 Porównanie różnych typów zagrożeń_wykład	Adam Przybysz	08-06-2026	11:55	14:00	02:05
4 z 26 Przerwa	Adam Przybysz	08-06-2026	14:00	14:30	00:30
5 z 26 Omówienie podstawowych pojęć kryptografii_wykład	Adam Przybysz	08-06-2026	14:30	17:00	02:30
6 z 26 Wdrażanie zarządzania tożsamością i kontrolą dostępu_wykład	Adam Przybysz	09-06-2026	09:00	10:45	01:45
7 z 26 Przerwa	Adam Przybysz	09-06-2026	10:45	11:00	00:15
8 z 26 Zabezpieczanie architektury sieci korporacyjnej_wykład + ćwiczenia praktyczne	Adam Przybysz	09-06-2026	11:00	13:30	02:30
9 z 26 Przerwa	Adam Przybysz	09-06-2026	13:30	14:00	00:30
10 z 26 Zabezpieczanie architektury sieci w usługach chmurowych_wykład	Adam Przybysz	09-06-2026	14:00	16:00	02:00

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 26 Omówienie koncepcji odporności_wykład	Adam Przybysz	10-06-2026	09:00	10:45	01:45
12 z 26 Przerwa	Adam Przybysz	10-06-2026	10:45	11:00	00:15
13 z 26 Zarządzanie podatnościami_ćwiczenia	Adam Przybysz	10-06-2026	11:00	13:30	02:30
14 z 26 Przerwa	Adam Przybysz	10-06-2026	13:30	14:00	00:30
15 z 26 Bezpieczeństwo sieciowe_ćwiczenia	Adam Przybysz	10-06-2026	14:00	16:00	02:00
16 z 26 Ocena bezpieczeństwa punktów końcowych_wykład	Adam Przybysz	11-06-2026	09:00	10:45	01:45
17 z 26 Przerwa	Adam Przybysz	11-06-2026	10:45	11:00	00:15
18 z 26 Wdrażanie zabezpieczeń aplikacji_ćwiczenia	Adam Przybysz	11-06-2026	11:00	13:30	02:30
19 z 26 Przerwa	Adam Przybysz	11-06-2026	13:30	14:00	00:30
20 z 26 Wdrażanie zabezpieczeń aplikacji cd._ćwiczenia	Adam Przybysz	11-06-2026	14:00	16:00	02:00
21 z 26 Zarządzanie incydentami i monitorowanie środowiska_ćwiczenia	Adam Przybysz	12-06-2026	09:00	10:45	01:45
22 z 26 Przerwa	Adam Przybysz	12-06-2026	10:45	11:00	00:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
23 z 26 Po czym rozpoznać atak – wskaźniki kompromitacji_ćwiczenia	Adam Przybysz	12-06-2026	11:00	13:30	02:30
24 z 26 Przerwa	Adam Przybysz	12-06-2026	13:30	14:00	00:30
25 z 26 Po czym rozpoznać atak – wskaźniki kompromitacji cd._ćwiczenia	Adam Przybysz	12-06-2026	14:00	16:00	02:00
26 z 26 Egzamin	-	12-07-2026	10:00	11:30	01:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 134,00 PLN
Koszt przypadający na 1 uczestnika netto	5 800,00 PLN
Koszt osobogodziny brutto	198,17 PLN
Koszt osobogodziny netto	161,11 PLN
W tym koszt walidacji brutto	1,23 PLN
W tym koszt walidacji netto	1,00 PLN
W tym koszt certyfikowania brutto	1 943,40 PLN
W tym koszt certyfikowania netto	1 580,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Przybysz

Certyfikowany trener i specjalista IT. Na co dzień projektuje, konfiguruje i administruje systemami informatycznymi oraz środowiskami chmurowymi Microsoft Azure i MS365, zapewniając ich bezpieczeństwo i efektywność działania. Posiada wieloletnie doświadczenie w zarządzaniu infrastrukturą IT w środowiskach wysokiego ryzyka i odpowiedzialności, w tym systemach wsparcia dowodzenia oraz taktycznych systemach transmisji danych.

Jako trener współpracuje z sektorem publicznym i prywatnym, prowadząc specjalistyczne szkolenia z zakresu technologii Microsoft: Windows Server, PowerShell, MS365, Azure, a także Cisco i Red Hat. Wspiera organizacje we wdrażaniu systemów IT, automatyzacji procesów oraz podnoszeniu poziomu bezpieczeństwa informacji.

Łączy wiedzę techniczną z doświadczeniem dydaktycznym, co pozwala mu efektywnie szkolić zarówno początkujących, jak i zaawansowanych administratorów.

Ukończył studia wojskowe inżynierskie i magisterskie na kierunku informatyka, specjalność systemy wspomagania dowodzenia. Uzupełnił wykształcenie studiami podyplomowymi z zakresu zarządzania bezpieczeństwem informatycznym.

W ciągu ostatnich 5 lat przeszkolił dla Altkom Akademii ponad 270 osób

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Na platformie Wirtualna Klasa Altkom Akademii udostępnione zostaną bezterminowo materiały szkoleniowe (tj. np. podręczniki/prezentacje/materiały dydaktyczne niezbędne do odbycia szkolenia/ebooki itp.), zasoby bazy wiedzy portalu oraz dodatkowe informacje od trenera. Uczestnicy zachowują bezterminowy dostęp do zasobów Mojej Akademii i materiałów szkoleniowych zgromadzonych w Wirtualnej Klasie szkolenia. Platforma do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

Usługa prowadzona jest z wykorzystaniem metod interaktywnych i aktywizujących, w szczególności: wykładu interaktywnego, moderowanej dyskusji, pytań i odpowiedzi, analizy przypadków (case study), ćwiczeń praktycznych i laboratoryjnych, samodzielnego wykonywania zadań w środowisku testowym oraz bieżących konsultacji z trenerem.

Warunki uczestnictwa

1. Niezbędnym warunkiem uczestnictwa w szkoleniach dofinansowanych z funduszy europejskich jest założenie konta w Bazie Usług Rozwojowych, zapis na szkolenie za pośrednictwem Bazy oraz spełnienie warunków przedstawionych przez danego Operatora, dysponenta funduszy publicznych.
2. Przez uczestnictwo w usłudze rozwojowej rozumie się aktywny udział Uczestnika w szkoleniu wyłącznie przy włączonej kamerze skierowanej na osobę uczestniczącą i umożliwiającej jej identyfikację.
3. Warunkiem uznania uczestnictwa w szkoleniu jest obecność podczas co najmniej 80% czasu trwania szkolenia (lub zgodnie z warunkami określonymi w umowie z Operatorem). Uczestnik, który nie spełni tego wymagania, traktowany jest jako nieobecny.
4. Frekwencja będzie potwierdzana na podstawie raportów logowań z platformy Zoom oraz bieżącej obserwacji uczestnika przez trenera.
5. Ogólne warunki uczestnictwa w szkoleniach Altkom Akademii zamieszczone są na stronie: https://www.altkomakademia.pl/ogolne-warunki-uczestnictwa-w-szkoleniach/

Informacje dodatkowe

Po szkoleniu uczestnik otrzyma zaświadczenie o ukończeniu szkolenia. Trener podczas szkolenia będzie organizował krótkie przerwy w porozumieniu z Uczestnikami, po zakończeniu danego modułu tematycznego.

Uwaga! W przypadku, gdy liczba zapisów na szkolenie nie osiągnie minimalnej liczby Uczestników, usługa może zostać niezrealizowana.

Informacja dot. podatku VAT:

Zwolnienie z podatku VAT może mieć zastosowanie wyłącznie w przypadku spełnienia przesłanek określonych w art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług – w przypadku finansowania usługi w całości ze środków publicznych – albo w § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień – w przypadku finansowania usługi w co najmniej 70% ze środków publicznych. W przypadku zastosowania zwolnienia obowiązuje cena netto, a w pozostałych przypadkach doliczany jest VAT 23%.

Warunki techniczne

Szkolenie realizowane jest w formule **zdalnej, w czasie rzeczywistym)**, z wykorzystaniem platformy wideokonferencyjnej (Zoom).

Każdy uczestnik powinien dysponować własnym stanowiskiem komputerowym z dostępem do Internetu – **dostawca usługi nie zapewnia sprzętu ani pomieszczenia do udziału w szkoleniu uczestnikom.**

Wymagania ogólne realizacji szkolenia w formule distance learning (online):

Komputer stacjonarny lub notebook wyposażony w mikrofon, głośniki i kamerę internetową z przeglądarką internetową z obsługą HTML 5. Monitor o rozdzielczości FullHD. Szerokopasmowy dostęp do Internetu o przepustowości co najmniej 25/5 (download/upload) Mb/s. W przypadku szkoleń z laboratoriami zalecamy: sprzęt wyposażony w dwa ekrany o rozdzielczości minimum HD (lub dwa komputery), kamerę internetową USB, zewnętrzne głośniki lub słuchawki.

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć.

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na: https://www.altkomakademia.pl/distance-learning/#FAQ

Platforma komunikacji – ZOOM

Oprogramowanie – zdalny pulpit, aplikacja ZOOM

Link do szkolenia zgodnie z regulaminem zostanie wysłany na 2 dni przed rozpoczęciem usługi.

Link do szkolenia jest ważny w trakcie trwania całej usługi szkoleniowej.

Kontakt

AGNIESZKA SIPURA

E-mail agnieszka.sipura@altkom.pl

Telefon (+48) 609 191 281