

ALTKOM AKADEMIA  
SPÓŁKA AKCYJNA

## Warsztaty z CompTIA Cybersecurity Analyst (CySA+) wraz z egzaminem CS0-003 - szkolenie autoryzowane - forma zdalna w czasie rzeczywistym

Numer usługi 2024/11/13/120967/2409843

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 35 h

📅 12.05.2025 do 16.05.2025

7 380,00 PLN brutto

6 000,00 PLN netto

210,86 PLN brutto/h

171,43 PLN netto/h

## Informacje podstawowe

<b>Kategoria</b>	Informatyka i telekomunikacja / Bezpieczeństwo IT
<b>Sposób dofinansowania</b>	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
<b>Grupa docelowa usługi</b>	<p>Szkolenie skierowane jest dla osób pracujących na stanowiskach:</p> <ul style="list-style-type: none"><li>• Analityk bezpieczeństwa IT</li><li>• Analityk bezpieczeństwa cybernetycznego</li><li>• Analityk Security Operations Center (SOC)</li><li>• Inżynier bezpieczeństwa IT</li><li>• Specjalista ds. bezpieczeństwa cybernetycznego</li></ul> <p>Od uczestników wymagana jest wiedza z zakresu szkoleń:</p> <ul style="list-style-type: none"><li>• SPLUS+ – Warsztaty z CompTIA Security + (przygotowanie do egzaminu SY0-701)</li></ul> <p>oraz minimum 3-4 letnie doświadczenie pracy na stanowisku administratora bezpieczeństwa.</p>
<b>Minimalna liczba uczestników</b>	1
<b>Maksymalna liczba uczestników</b>	15
<b>Data zakończenia rekrutacji</b>	05-05-2025
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	35
<b>Podstawa uzyskania wpisu do BUR</b>	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

# Cel

## Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do korzystania z narzędzi i metod zarządzania ryzykiem cybernetycznym, rozpoznawania różnych rodzajów powszechnych zagrożeń, oceny poziomu bezpieczeństwa organizacji, zbierania i analizowania informacji o cyberprzestępczości, oraz radzenia sobie z sytuacjami kryzysowymi.

Uczestnik po szkoleniu będzie stosował wyszukiwanie i automatyzację, monitorował bezpieczeństwo ruchu sieciowego oraz wykorzystywał bezpieczeństwo oprogramowania i aplikacji.

## Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
- Stosuje koncepcje przywództwa ACCybersecurity	- definiuje typy i metody kontroli - charakteryzuje koncepcję zarządzania poprawkami	Test teoretyczny
- Wykorzystuje koncepcję analizy zagrożeń i wykrywania zagrożeń	- charakteryzuje sposoby badania koncepcji podmiotów zagrażających - definiuje aktywne zagrożenia - charakteryzuje sposoby badania koncepcji wykrywania zagrożeń („Threat-Hunting”)	Test teoretyczny
- Wykorzystuje koncepcje architektury systemu i sieci	- definiuje koncepcje architektury systemu i sieci - charakteryzuje zasady zarządzania tożsamością i dostępem (IAM) - definiuje sposoby utrzymania widoczności operacyjnej	Test teoretyczny
- Wykorzystuje zrozumienie i sposoby usprawniania procesów dotyczących operacji bezpieczeństwa	- charakteryzuje sposoby przywództwa w operacjach związanych z bezpieczeństwem - charakteryzuje technologię operacji bezpieczeństwa	Test teoretyczny
- Stosuje sposoby wdrażania metod skanowania podatności na zagrożenia	- definiuje wymagania dotyczące zgodności - charakteryzuje metody skanowania pod kątem luk w zabezpieczeniach - charakteryzuje specjalne kwestie związanych ze skanowaniem luk w zabezpieczeniach	Test teoretyczny
- Wykorzystuje analizy podatności na zagrożenia	- definiuje koncepcje punktacji podatności na zagrożenia - charakteryzuje sposoby badania zagadnień związanych z kontekstem luk w zabezpieczeniach	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
<p>- Stosuje sposoby przekazywania informacjami o podatnościach</p> <p>- Stosuje wyjaśnienie działań związanych z reagowaniem na incydenty</p>	<p>- definiuje koncepcje skutecznej komunikacji</p> <p>- charakteryzuje wyniki raportowania podatności na zagrożenia oraz rodzaje planów działania</p> <p>- definiuje sposoby planowania w reakcji na incydenty</p> <p>- charakteryzuje sposoby wykonywania działań związanych z reagowaniem na incydenty</p>	<p>Test teoretyczny</p> <p>Test teoretyczny</p>
<p>- Zarządza komunikacją w odpowiedzi na incydent</p>	<p>- definiuje sposoby komunikacji w odpowiedzi na incydent</p> <p>- charakteryzuje sposoby analizowania działań związanych z reagowaniem na incydenty</p>	<p>Test teoretyczny</p>
<p>- Stosuje narzędzia do identyfikacji złośliwej aktywności</p>	<p>- charakteryzuje złośliwą aktywność</p> <p>- definiuje ramy metodologii ataków</p> <p>- charakteryzuje techniki identyfikowania złośliwej aktywności</p>	<p>Test teoretyczny</p>
<p>- Wykorzystuje analizę potencjalnie złośliwej aktywności</p>	<p>-charakteryzuje sposoby badania wskaźników ataków sieciowych</p> <p>- charakteryzuje sposoby badania wskaźników ataku hosta</p> <p>- definiuje narzędzia oceny podatności</p>	<p>Test teoretyczny</p>
<p>- Wykorzystuje oceny podatności aplikacji</p>	<p>- charakteryzuje sposoby analizowania luk w zabezpieczeniach sieci Web</p> <p>- charakteryzuje sposoby analizowania luk w zabezpieczeniach chmury</p>	<p>Test teoretyczny</p>
<p>- Stosuje narzędzia skryptowe i koncepcje analizy</p> <p>- Wykorzystuje najlepsze praktyki w zakresie bezpieczeństwa aplikacji i ograniczania ataków</p>	<p>- definiuje języki skryptowe</p> <p>- charakteryzuje sposoby identyfikacji złośliwej aktywności z wykorzystaniem analizy</p> <p>- definiuje praktyki bezpiecznego tworzenia oprogramowania</p> <p>- charakteryzuje sposoby kontroli w celu ograniczenia skutecznych ataków na aplikacje</p> <p>- charakteryzuje sposoby wdrażania kontroli zapobiegających atakom</p>	<p>Test teoretyczny</p> <p>Test teoretyczny</p>

## 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

## Informacje

<b>Podstawa prawna dla Podmiotów / kategorii Podmiotów</b>	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
<b>Nazwa/Kategoria Podmiotu prowadzącego walidację</b>	PearsonVue
<b>Podmiot prowadzący walidację jest zarejestrowany w BUR</b>	Nie
<b>Nazwa/Kategoria Podmiotu certyfikującego</b>	PearsonVue
<b>Podmiot certyfikujący jest zarejestrowany w BUR</b>	Nie

# Program

## AGENDA SZKOLENIA

1. zrozumienie koncepcji przywództwa ACCybersecurity
  - Odkrywanie typów i metod kontroli
  - Wyjaśnienie koncepcji zarządzania poprawkami
2. Odkrywanie koncepcji analizy zagrożeń i wykrywania zagrożeń
  - Badanie koncepcji podmiotów zagrażających
  - Identyfikacja aktywnych zagrożeń
  - Badanie koncepcji wykrywania zagrożeń („Threat-Hunting”)
3. Wyjaśnienie koncepcji architektury systemu i sieci
  - Przegląd koncepcji architektury systemu i sieci
  - Odkrywanie zarządzania tożsamością i dostępem (IAM)
  - Utrzymanie widoczności operacyjnej
4. Zrozumienie i usprawnianie procesów dotyczących operacji bezpieczeństwa
  - Odkrywanie przywództwa w operacjach związanych z bezpieczeństwem
  - Zrozumienie technologii operacji bezpieczeństwa
5. Wdrażanie metod skanowania podatności na zagrożenia
  - Wyjaśnienie wymagań dotyczących zgodności
  - Zrozumienie metod skanowania pod kątem luk w zabezpieczeniach
  - Odkrywanie specjalnych kwestii związanych ze skanowaniem luk w zabezpieczeniach
6. Przeprowadzenie analizy podatności na zagrożenia
  - Zrozumienie koncepcji punktacji podatności na zagrożenia
  - Badanie zagadnień związanych z kontekstem luk w zabezpieczeniach
7. Przekazywanie informacji o podatnościach
  - Wyjaśnianie koncepcji skutecznej komunikacji
  - Zrozumienie wyników raportowania podatności na zagrożenia i planów działania

## 8. Wyjaśnianie działań związanych z reagowaniem na incydenty

- Planowanie reagowania na incydenty
- Wykonywanie działań związanych z reagowaniem na incydenty

## 9. Komunikacja w odpowiedzi na incydent

- Zrozumienie komunikacji w odpowiedzi na incydent
- Analizowanie działań związanych z reagowaniem na incydenty

## 10. Stosowanie narzędzi do identyfikacji złośliwej aktywności

- Identyfikacja złośliwej aktywności
- Wyjaśnienie ram metodologii ataków Wyjaśnianie technik identyfikowania złośliwej aktywności

## 11. Analiza potencjalnie złośliwej aktywności

- Badanie wskaźników ataków sieciowych
- Badanie wskaźników ataku hosta
- Odkrywanie narzędzi oceny podatności

## 12. Zrozumienie oceny podatności aplikacji

- Analiza luk w zabezpieczeniach sieci Web
- Analiza luk w zabezpieczeniach chmury

## 13. Narzędzia skryptowe i koncepcja analizy

- Zrozumienie języków skryptowych
- Identyfikacja złośliwej aktywności poprzez analizę

## 14. Najlepsze praktyki w zakresie bezpieczeństwa aplikacji i ograniczania ataków

- Poznanie praktyk bezpiecznego tworzenia oprogramowania
- Poznanie zaleceń mających na celu ograniczenia skutecznych ataków na aplikacje
- Wdrażanie sposobów kontroli zapobiegających atakom

Od uczestników wymagana jest wiedza z zakresu szkoleń:

- SPLUS+ – Warsztaty z CompTIA Security + (przygotowanie do egzaminu SY0-701)

oraz minimum 3-4 letnie doświadczenie pracy na stanowisku administratora bezpieczeństwa.

Uczestnik po szkoleniu otrzymuje voucher na egzamin CS0-003. Egzamin można zdawać najpóźniej ostatniego dnia usługi. Egzamin w harmonogramie ma tylko prawdopodobny termin i godzinę. Uczestnik umawia się na egzamin indywidualnie z PearsonVue.

Egzamin online przeprowadzany jest w obecności proktora – osoby z firmy PeopleCert, która podcina się zdalnie pod pulpit kursanta i obserwuje przebieg egzaminu przez kamerkę. Zdający jest zobowiązany pokazać proktorowi za pośrednictwem kamerki pomieszczenie, w którym będzie zdawał egzamin. Proktor sprawdza, czy nie ma w pokoju osób trzecich i pomocy naukowych. Uczestnik loguje się do zewnętrznej platformy Pearson Vue uzyskując dostęp do egzaminu, zdaje egzamin i wysyła do Pearson Vue.

**Liczba godzin wpisana w pole "ogólna liczba godzin" obejmuje tylko czas szkolenia (35 godzin). Egzamin trwa 165 minut w związku z czym cała usługa szkolenie + egzamin trwa 37 godzi i 45 minut.**

### Informacje o egzaminie CS0-003:

Tytuł – The CompTIA Cybersecurity Analyst (CySA+)

Format testu: test wielokrotnego wyboru

Ilość pytań – max 85

Czas trwania – 165 min

### Szkolenie obejmuje:

- 5 dni pracy z trenerem
- Nadzór trenera
- Autoryzowany podręcznik: The Official CompTIA CySA+

- Środowisko laboratoryjne
- voucher na egzamin CS0-003

# Harmonogram

Liczba przedmiotów/zajęć: 15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 15</b> Podstawowe koncepcje bezpieczeństwa terminologia, koncepcje mechanizmy kontrolne bezpieczeństwa wykład	Dominik Węglarz	12-05-2025	10:00	11:00	01:00
<b>2 z 15</b> Porównanie różnych typów zagrożeń wykład	Dominik Węglarz	12-05-2025	11:00	12:30	01:30
<b>3 z 15</b> Omówienie podstawowych pojęć kryptografii wykład	Dominik Węglarz	12-05-2025	12:30	17:00	04:30
<b>4 z 15</b> Wdrażanie zarządzania tożsamością i kontrolą dostępu ćwiczenia	Dominik Węglarz	13-05-2025	09:00	11:00	02:00
<b>5 z 15</b> Zabezpieczanie architektury sieci korporacyjnej ćwiczenia	Dominik Węglarz	13-05-2025	11:00	13:00	02:00
<b>6 z 15</b> Zabezpieczanie architektury sieci w usługach chmurowych ćwiczenia	Dominik Węglarz	13-05-2025	13:00	16:00	03:00
<b>7 z 15</b> Omówienie koncepcji odporności wykład	Dominik Węglarz	14-05-2025	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>8 z 15</b> Zarządzanie podatnościami ćwiczenia	Dominik Węglarz	14-05-2025	11:00	13:00	02:00
<b>9 z 15</b> Bezpieczeństwo sieciowe ćwiczenia	Dominik Węglarz	14-05-2025	13:00	16:00	03:00
<b>10 z 15</b> Ocena bezpieczeństwa punktów końcowych wykład	Dominik Węglarz	15-05-2025	09:00	11:00	02:00
<b>11 z 15</b> Wdrażanie zabezpieczeń aplikacji ćwiczenia	Dominik Węglarz	15-05-2025	11:00	13:00	02:00
<b>12 z 15</b> Zarządzanie incydentami i monitorowanie środowiska ćwiczenia	Dominik Węglarz	15-05-2025	13:00	16:00	03:00
<b>13 z 15</b> Po czym rozpoznać atak - wskaźniki kompromitacji wykład	Dominik Węglarz	16-05-2025	09:00	11:00	02:00
<b>14 z 15</b> Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury ćwiczenia	Dominik Węglarz	16-05-2025	11:00	13:00	02:00
<b>15 z 15</b> Podstawowe pojęcia związane zarządzania ryzykiem; Ochrona danych i dbałość o ich zgodność w organizacji wykład	Dominik Węglarz	16-05-2025	13:00	16:00	03:00

# Cennik

## Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	7 380,00 PLN
Koszt przypadający na 1 uczestnika netto	6 000,00 PLN
Koszt osobogodziny brutto	210,86 PLN
Koszt osobogodziny netto	171,43 PLN
W tym koszt walidacji brutto	1 845,00 PLN
W tym koszt walidacji netto	1 500,00 PLN
W tym koszt certyfikowania brutto	1,23 PLN
W tym koszt certyfikowania netto	1,00 PLN

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Dominik Węglarz

Wykształcenie: XIX Liceum Ogólnokształcące Profil Informatyczny w Poznaniu

Uniwersytet im. Adama Mickiewicza w Poznaniu

- Absolwent Wydziału Matematyki i Informatyki.
- Zdobył tytuł Licencjata Informatyki.

Uniwersytet im. Adama Mickiewicza w Poznaniu

- Studia uzupełniające magisterskie II-go stopnia na Wydziale Matematyki i Informatyki UAM.

Wyższa Szkoła Komunikacji i Zarządzania w Poznaniu

- Cisco Networking Academy (4 semestry Akademii Sieci Komputerowej)

Specjalizacja: Infrastruktura IT, wirtualizacja, bezpieczeństwo IT.

Doświadczenie trenerskie: Obecnie trener Altkom Akademii. Posiada doświadczenie trenerskie zdobyte w ciągu ostatnich 5 lat.

Zakres tematyczny prowadzonych szkoleń:

- VV6ICM



- VV6.5ICM
- VV6.5FT
- VV6FT
- VV6.5WN
- VV6WN
- VV6.7ICM
- VV6.7FT
- VV7ICM
- VV7FT
- BS.IT01
- BS.IT02
- CEHv9
- CEHv10
- CEHv11
- CSCU

## 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. Platformą do kontaktu z trenerami, grupą i całą społecznością absolwentów jest portal Moja Akademia.

### Warunki uczestnictwa

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, do którego składają Państwo dokumenty o dofinansowanie do usługi rozwojowej.

Ogólne warunki uczestnictwa w zajęciach zostały zamieszczone 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. Informacja o przerwach będzie umieszczona na slajdzie.

## Warunki techniczne

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.

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



**Adrianna Kukurudz**

**E-mail** [adrianna.kukurudz@alkom.pl](mailto:adrianna.kukurudz@alkom.pl)

**Telefon** (+22) 801 258 566