Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

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

Numer usługi 2024/09/19/120967/2316926

zdalna w czasie rzeczywistym
Usługa szkoleniowa
35 h
20.01.2025 do 20.02.2025

6 273,00 PLN brutto
5 100,00 PLN netto
179,23 PLN brutto/h
145,71 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 skierowane jest dla osób pracujących na stanowiskach: • Analityk bezpieczeństwa IT • Analityk bezpieczeństwa cybernetycznego • Analityk Security Operations Center (SOC) • Inżynier bezpieczeństwa IT • Specjalista ds. bezpieczeństwa cybernetycznego 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.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	13-01-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	35
Podstawa uzyskania wpisu do BUR	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 szkolenia 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 kwestii 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
- Stosuje sposoby przekazywania informacjami o podatnościach	- definiuje koncepcje skutecznej komunikacji - charakteryzuje wyniki raportowania podatności na zagrożenia oraz rodzaje planów działania	Test teoretyczny
- Stosuje wyjaśnienie działań związanych z reagowaniem na incydenty	- definiuje sposoby planowania w reakcji na incydenty - charakteryzuje sposoby wykonywania działań związanych z reagowaniem na incydenty	Test teoretyczny
- Zarządza komunikacją w odpowiedzi na incydent	- definiuje sposoby komunikacji w odpowiedzi na incydent - charakteryzuje sposoby analizowania działań związanych z reagowaniem na incydenty	Test teoretyczny
- Stosuje narzędzia do identyfikacji złośliwej aktywności	- charakteryzuje złośliwą aktywność - definiuje ramy metodologii ataków - charakteryzuje techniki identyfikowania złośliwej aktywności	Test teoretyczny
- Wykorzystuje analizę potencjalnie złośliwej aktywności	-charakteryzuje sposoby badania wskaźników ataków sieciowych - charakteryzuje sposoby badania wskaźników ataku hosta - definiuje narzędzia oceny podatności	Test teoretyczny
- Wykorzystuje oceny podatności aplikacji	- charakteryzuje sposoby analizowania luk w zabezpieczeniach sieci Web - charakteryzuje sposoby analizowania luk w zabezpieczeniach chmury	Test teoretyczny
- Stosuje narzędzia skryptowe i koncepcje analizy	- definiuje języki skryptowe - charakteryzuje sposoby identyfikacji złośliwej aktywności z wykorzystaniem analizy	Test teoretyczny
- Wykorzystuje najlepsze praktyki w zakresie bezpieczeństwa aplikacji i ograniczania ataków	- definiuje praktyki bezpiecznego tworzenia oprogramowania - charakteryzuje sposoby kontroli w celu ograniczenia skutecznych ataków na aplikacje - charakteryzuje sposoby wdrażania kontroli zapobiegających atakom	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

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa/Kategoria Podmiotu prowadzącego walidację	PearsonVue
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa/Kategoria Podmiotu certyfikującego	PearsonVue
Podmiot certyfikujący jest zarejestrowany w BUR	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 podpina 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: 16

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Podstawowe koncepcje bezpieczeństwa terminologia, koncepcje mechanizmy kontrolne bezpieczeństwa wykład	Dominik Węglarz	20-01-2025	10:00	13:00	03:00
2 z 16 Porównanie różnych typów zagrożeń wykład	Dominik Węglarz	20-01-2025	13:00	15:00	02:00
3 z 16 Omówienie podstawowych pojęć kryptografii wykład	Dominik Węglarz	20-01-2025	15:00	17:00	02:00
4 z 16 Wdrażanie zarządzania tożsamością i kontrolą dostępu ćwiczenia	Dominik Węglarz	21-01-2025	09:00	11:00	02:00
5 z 16 Zabezpieczanie architektury sieci korporacyjnej ćwiczenia	Dominik Węglarz	21-01-2025	11:00	13:00	02:00
6 z 16 Zabezpieczanie architektury sieci w usługach chmurowych ćwiczenia	Dominik Węglarz	21-01-2025	13:00	16:00	03:00
7 z 16 Omówienie koncepcji odporności wykład	Dominik Węglarz	22-01-2025	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
8 z 16 Zarządzanie podatnościami ćwiczenia	Dominik Węglarz	22-01-2025	11:00	13:00	02:00
9 z 16 Bezpieczeństwo sieciowe ćwiczenia	Dominik Węglarz	22-01-2025	13:00	16:00	03:00
10 z 16 Ocena bezpieczeństwa punktów końcowych wykład	Dominik Węglarz	23-01-2025	09:00	11:00	02:00
11 z 16 Wdrażanie zabezpieczeń aplikacji ćwiczenia	Dominik Węglarz	23-01-2025	11:00	13:00	02:00
12 z 16 Zarządzanie incydentami i monitorowanie środowiska ćwiczenia	Dominik Węglarz	23-01-2025	13:00	16:00	03:00
13 z 16 Po czym rozpoznać atak - wskaźniki kompromitacji wykład	Dominik Węglarz	24-01-2025	09:00	11:00	02:00
14 z 16 Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury ćwiczenia	Dominik Węglarz	24-01-2025	11:00	13:00	02:00
15 z 16 Podstawowe pojęcia związane zarządzania ryzykiem; Ochrona danych i dbałość o ich zgodność w organizacji wykład	Dominik Węglarz	24-01-2025	13:00	16:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 16 Egzamin	-	20-02-2025	10:00	12:45	02:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 273,00 PLN
Koszt przypadający na 1 uczestnika netto	5 100,00 PLN
Koszt osobogodziny brutto	179,23 PLN
Koszt osobogodziny netto	145,71 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 wciągu 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@altkom.pl
Telefon (+22) 801 258 566