Możliwość dofinansowania

ALTKOM AKADEMIA SPÓŁKA AKCYJNA

★★★★½

# Warsztaty z CompTIA Security + ( przygotowanie do egzaminu SY0-701) - forma zdalna w czasie rzeczywistym TERMIN GWARANTOWANY

**Numer usługi** 2024/07/03/120967/2207271

5 535,00 PLN brutto
4 500,00 PLN netto
158,14 PLN brutto/h
128,57 PLN netto/h

- zdalna w czasie rzeczywistym
- Usługa szkoleniowa
- 35 h
- 05.08.2024 do 09.08.2024

# Informacje podstawowe

| | |
|---|---|
| **Kategoria** | Informatyka i telekomunikacja / Bezpieczeństwo IT |
| **Sposób dofinansowania** | wsparcie dla osób indywidualnych<br>wsparcie dla pracodawców i ich pracowników |
| **Grupa docelowa usługi** | Szkolenie skierowane do administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji.<br><br>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** | 1 |
| **Maksymalna liczba uczestników** | 15 |
| **Data zakończenia rekrutacji** | 29-07-2024 |
| **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 analizy ryzyka, planowania ciągłości działania, zachowania bezpieczeństwa informacyjnego, bezpieczeństwa systemów i sieci teleinformatycznych. Uczestnik po szkoleniu będzie analizował ryzyko, zabezpieczał architekturę sieci korporacyjnej, oceniał bezpieczeństwo punktów końcowych, zarządzał incydentami i monitorował środowisko.

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

| Efekty uczenia się | Kryteria weryfikacji | Metoda walidacji |
|---|---|---|
| Charakteryzuje różne typy zagrożeń | - definiuje typy zagrożeń<br>- rozróżnia przestrzenie ataku<br>- definiuje inżynierię społeczną | Test teoretyczny |
| Charakteryzuje podstawowe pojęcia kryptografii | - definiuje algorytmy kryptograficzne<br>- charakteryzuje infrastrukturę PKI<br>- rozróżnia rozwiązania kryptograficzne | Test teoretyczny |
| Wdraża zarządzanie tożsamością i kontrolą dostępu | - definiuje poprawne uwierzytelnianie<br>- definiuje właściwą autoryzację<br>- charakteryzuje zarządzanie tożsamością | Test teoretyczny |
| Ocenia bezpieczeństwo punktów końcowych | - charakteryzuje zabezpieczenia punktów końcowych<br>- definiuje zabezpieczenia urządzeń mobilnych | Test teoretyczny |
| Rozpoznaje atak | - charakteryzuje ataki złośliwym oprogramowaniem<br>- charakteryzuje ataki fizyczne i sieciowe<br>- rozróżnia ataki na aplikacje | Test teoretyczny |

# 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

AGENDA SZKOLENIA

- Role w bezpieczeństwie
- Analiza zagrożeń i ocena bezpieczeństwa
- Inżynieria społeczna i złośliwe oprogramowanie
- Podstawowe pojęcia i koncepcje kryptograficzne
- Infrastruktura klucza publicznego
- Bezpieczne uwierzytelnianie, kontrola zarządzania tożsamością i kontem
- Bezpieczna architektura sieciowa
- Urządzenia zabezpieczające sieć
- Bezpieczne protokoły sieciowe
- Bezpieczeństwo hosta
- Bezpieczeństwo rozwiązań mobilnych
- Koncepcja bezpiecznych aplikacji
- Bezpieczeństwo rozwiązań w chmurze
- Podstawowe pojęcia dotyczące prywatności i ochrony danych
- Reagowanie na incydent
- Kryminalistyka cyfrowa
- Zarządzanie ryzykiem i planowanie ciągłości działania
- Koncepcje budowania cyberodporności
- Bezpieczeństwo fizyczne
- Omówienie egzaminu CompTIA Security +

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.

Efekty uczenia zostaną zweryfikowane przed szkoleniem i po szkoleniu poprzez pre i post testy w formie testu teoretycznego zamkniętego w formie on-line.

# Harmonogram

Liczba przedmiotów/zajęć: 15

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 1 z 15 **Podstawowe koncepcje bezpieczeństwa terminologia, koncepcje mechanizmy kontrolne bezpieczeństwa wykład** | Paweł Stobiecki | 05-08-2024 | 10:00 | 11:00 | 01:00 |
| 2 z 15 **Porównanie różnych typów zagrożeń wykład** | Paweł Stobiecki | 05-08-2024 | 11:00 | 12:30 | 01:30 |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 3 z 15 Omówienie podstawowych pojęć kryptografii wykład | Paweł Stobiecki | 05-08-2024 | 12:30 | 17:00 | 04:30 |
| 4 z 15 Wdrażanie zarządzania tożsamością i kontrolą dostępu ćwiczenia | Paweł Stobiecki | 06-08-2024 | 09:00 | 11:00 | 02:00 |
| 5 z 15 Zabezpieczanie architektury sieci korporacyjnej ćwiczenia | Paweł Stobiecki | 06-08-2024 | 11:00 | 13:00 | 02:00 |
| 6 z 15 Zabezpieczanie architektury sieci w usługach chmurowych ćwiczenia | Paweł Stobiecki | 06-08-2024 | 13:00 | 16:00 | 03:00 |
| 7 z 15 Omówienie koncepcji odporności wykład | Paweł Stobiecki | 07-08-2024 | 09:00 | 11:00 | 02:00 |
| 8 z 15 Zarządzanie podatnościami ćwiczenia | Paweł Stobiecki | 07-08-2024 | 11:00 | 13:00 | 02:00 |
| 9 z 15 Bezpieczeństwo sieciowe ćwiczenia | Paweł Stobiecki | 07-08-2024 | 13:00 | 16:00 | 03:00 |
| 10 z 15 Ocena bezpieczeństwa punktów końcowych wykład | Paweł Stobiecki | 08-08-2024 | 09:00 | 11:00 | 02:00 |
| 11 z 15 Wdrażanie zabezpieczeń aplikacji ćwiczenia | Paweł Stobiecki | 08-08-2024 | 11:00 | 13:00 | 02:00 |

| Przedmiot / temat zajęć | Prowadzący | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|---|---|---|---|---|---|
| 12 z 15 Zarządzanie incydentami i monitorowanie środowiska ćwiczenia | Paweł Stobiecki | 08-08-2024 | 13:00 | 16:00 | 03:00 |
| 13 z 15 Po czym rozpoznać atak - wskaźniki kompromitacji wykład | Paweł Stobiecki | 09-08-2024 | 09:00 | 11:00 | 02:00 |
| 14 z 15 Zarządzania bezpieczeństwem w organizacji poprzez polityki, standardy i procedury ćwiczenia | Paweł Stobiecki | 09-08-2024 | 11:00 | 13:00 | 02:00 |
| 15 z 15 Podstawowe pojęcia związane zarządzania ryzykiem; Ochrona danych i dbałość o ich zgodność w organizacji wykład | Paweł Stobiecki | 09-08-2024 | 13:00 | 16:00 | 03:00 |

# 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** | 158,14 PLN |
| **Koszt osobogodziny netto** | 128,57 PLN |

# Prowadzący

Liczba prowadzących: 1

1 z 1

## Paweł Stobiecki

Wykształcenie:
Akademia Obrony Narodowej
• stacjonarne studia III stopnia: nauki o bezpieczeństwie;
Wyższa Szkoła Menedżerska
• studia podyplomowe, Ochrona informacji niejawnych i administrowanie bezpieczeństwem informacji;
Akademia Obrony Narodowej
• studia I i II stopnia: bezpieczeństwo narodowe, specjalność: zarządzanie bezpieczeństwem.
Specjalizacja:
• Bezpieczeństwo sieci bezprzewodowych;
• Bezpieczeństwo Informacyjne;
• Testy penetracyjne/etyczny hacking;
• Modyfikowanie urządzeń sieciowych;
• świadomości bezpieczeństwa użytkownika w Internecie.
Doświadczenie trenerskie: Obecnie trener Altkom Akademii. Posiada ponad 3-letnie doświadczenie trenerskie.
Zakres tematyczny prowadzonych szkoleń:
• Bezpieczeństwo sieci bezprzewodowych;
• Bezpieczeństwo Informacyjne;
• Testy penetracyjne/etyczny hacking;
• Modyfikowanie urządzeń sieciowych;
• świadomości bezpieczeństwa użytkownika w Internecie.

# 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.

## 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.

OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

Ogólna znajomość zagadnień informatycznych oraz pojęć związanych z sieciami komputerowymi i umiejętność sprawnej obsługi komputera. Wymagana podstawowa znajomość systemów operacyjnych Windows oraz Linux.

# 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