

ALTKOM AKADEMIA  
SPÓŁKA AKCYJNA**Security/Wprowadzenie do zagadnień  
bezpieczeństwa IT - forma zdalna w czasie  
rzeczywistym TERMIN GWARANTOWANY**

Numer usługi 2024/06/24/120967/2196091

📍 zdalna w czasie rzeczywistym

📄 Usługa szkoleniowa

🕒 21 h

📅 15.07.2024 do 17.07.2024

**3 198,00 PLN** brutto

2 600,00 PLN netto

152,29 PLN brutto/h

123,81 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>	Szkolenie dla osób z branży IT, które zajmują się bezpieczeństwem systemów informatycznych w firmie, a w szczególności dla osób, które będą pełniły funkcję Security Managera.  OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY:  Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.
<b>Minimalna liczba uczestników</b>	1
<b>Maksymalna liczba uczestników</b>	15
<b>Data zakończenia rekrutacji</b>	08-07-2024
<b>Forma prowadzenia usługi</b>	zdalna w czasie rzeczywistym
<b>Liczba godzin usługi</b>	21
<b>Podstawa uzyskania wpisu do BUR</b>	Standard Usługi Szkoleniowo-Rozwojowej PIFS SUS 2.0

## Cel

### Cel edukacyjny

Usługa potwierdza przygotowanie Uczestnika do samodzielnego tworzenia procedur, zarządzania bezpieczeństwem w przedsiębiorstwie. Uczestnik tworzy protokoły i mechanizmy zabezpieczające transmisję danych, zapobiega atakom, wykrywa włamanie IDS/IPS.

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

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zarządza bezpieczeństwem	- definiuje procedury bezpieczeństwa - charakteryzuje zagrożenia i zabezpieczenia	Test teoretyczny
Korzysta z protokołów i mechanizmów zabezpieczających transmisję danych	- charakteryzuje tunelowanie danych	Test teoretyczny
Zarządza sieciami I TCP/IP	- charakteryzuje metody uwierzytelniania w sieciach LAN - charakteryzuje bezpieczeństwo sieci bezprzewodowych	Test teoretyczny
Skanuje sieci	- charakteryzuje porty	Test teoretyczny
Zarządza systemami wykrywania włamań IDS/IPS	- charakteryzuje host IDS - charakteryzuje typy firewalli	Test teoretyczny
Stosuje dobre praktyki zapewniające bezpieczeństwo	- charakteryzuje sposoby weryfikacji spójności systemów - charakteryzuje sposoby składowania i ochrona logów	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

## 1. Wprowadzenie do tematyki bezpieczeństwa

- Czym jest bezpieczeństwo IT?
- Terminologia

## 2. Organizacje i normy

- Kryteria oceny poziomu bezpieczeństwa

## 3. Zarządzanie bezpieczeństwem

- Inicjowanie procesów bezpieczeństwa IT
- Tworzenie procedur bezpieczeństwa
- Zagrożenia i zabezpieczenia rozważane przy tworzeniu polityki bezpieczeństwa

## 4. Kryptografia oraz środowisko PKI

- Terminologia i organizacje standaryzujące
- Algorytmy
- Funkcje skrótu

## 5. Protokoły i mechanizmy zabezpieczające transmisję danych

- SSH
- PGP
- SSL/TLS
- Tunelowanie danych

## 6. Metody autentykacji użytkowników

- LDAP
- Kerberos

## 7. Sieć I TCP/IP

- Wprowadzenie do TCP/IP
- Metody uwierzytelniania w sieciach LAN
- Bezpieczeństwo sieci bezprzewodowych

## 8. Skanowanie sieci

- Mapowanie sieci
- Skanowanie portów
- Wykrywanie systemu operacyjnego

## 9. Opis typowych i aktualnych trendów ataków

- Typy ataków
- Zapobieganie
- Źródła informacji o nowych typach ataków

## 10. Systemy wykrywania włamań IDS/IPS

- Host IDS
- Network IDS
- Firewalle
- Typy firewalli
- Działanie i implementacje

## 11. Sieci VPN

- SSL VPN
- IPsec VPN

## 12. Dobre praktyki

- Sposoby weryfikacji spójności systemów
- Sposoby składowania i ochrona logów
- Co i jak monitorujemy?

## OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY:

Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

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: 12

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>1 z 12</b> Wprowadzenie do tematyki bezpieczeństwa Czym jest bezpieczeństwo IT? Terminologia wykład	Paweł Stobiecki	15-07-2024	10:00	11:00	01:00
<b>2 z 12</b> Organizacje i normy Kryteria oceny poziomu bezpieczeństwa wykład	Paweł Stobiecki	15-07-2024	11:00	13:00	02:00
<b>3 z 12</b> Zarządzanie bezpieczeństwem Inicjowanie procesów bezpieczeństwa IT Tworzenie procedur bezpieczeństwa Zagrożenia i zabezpieczenia rozważane przy tworzeniu polityki bezpieczeństwa wykład	Paweł Stobiecki	15-07-2024	13:00	14:00	01:00
<b>4 z 12</b> Kryptografia oraz środowisko PKI Terminologia i organizacje standaryzujące Algorytmy Funkcje skrótu wykład	Paweł Stobiecki	15-07-2024	14:00	17:00	03:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>5 z 12</b> Protokoły i mechanizmy zabezpieczające transmisję danych SSH PGP SSL/TLS Tunelowanie danych ćwiczenia	Paweł Stobiecki	16-07-2024	09:00	11:00	02:00
<b>6 z 12</b> Metody autentykacji użytkowników LDAP Kerberos wykład	Paweł Stobiecki	16-07-2024	11:00	13:00	02:00
<b>7 z 12</b> Sieć I TCP/IP Wprowadzenie do TCP/IP Metody uwierzytelniania w sieciach LAN Bezpieczeństwo sieci bezprzewodowych wykład	Paweł Stobiecki	16-07-2024	13:00	14:00	01:00
<b>8 z 12</b> Skanowanie sieci Mapowanie sieci Skanowanie portów Wykrywanie systemu operacyjnego wykład	Paweł Stobiecki	16-07-2024	14:00	16:00	02:00
<b>9 z 12</b> Opis typowych i aktualnych trendów ataków Typy ataków Zapobieganie Źródła informacji o nowych typach ataków wykład	Paweł Stobiecki	17-07-2024	09:00	11:00	02:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
<b>10 z 12</b> Systemy wykrywania włamań IDS/IPS Host IDS Network IDS Firewalle Typy firewalli Działanie i implementacje wykład	Paweł Stobiecki	17-07-2024	11:00	13:00	02:00
<b>11 z 12</b> Sieci VPN SSL VPN IPsec VPN wykład	Paweł Stobiecki	17-07-2024	13:00	14:00	01:00
<b>12 z 12</b> Dobre praktyki Sposoby weryfikacji spójności systemów Sposoby składowania i ochrona logów Co i jak monitorujemy? Wykład	Paweł Stobiecki	17-07-2024	14:00	16:00	02:00

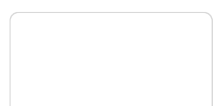
## Cennik

### Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 198,00 PLN
Koszt przypadający na 1 uczestnika netto	2 600,00 PLN
Koszt osobogodziny brutto	152,29 PLN
Koszt osobogodziny netto	123,81 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: Altkom Akademia S.A. – współpraca od 3 lat.

Prowadzenie szkoleń z zakresu:

- BS.IT 01 - Wprowadzenie do zagadnień bezpieczeństwa IT

- BS.IT 02 - Warsztaty z wybranych elementów bezpieczeństwa IT

- BS.IT 02-IT - Zarządzanie cyberbezpieczeństwem

- BS.IT CS - Warsztaty z Cyberbezpieczeństwa

- BS-WiFi 01 - Wi-Fi Security Essentials – Wprowadzenie do bezpieczeństwa sieci bezprzewodowych

- BS-WiFi 02 - Wi-Fi Security Testing – Testowanie bezpieczeństwa sieci bezprzewodowych

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://altkom.sharepoint.com/sites/Sprzedaz/SitePages/Karty-zg%C5%82oszenia.aspx?csf=1&web=1&e=AD94u3&CID=72b4df7a-33bb-461a-b23f-e9b58ac84b2c>

### 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:

Wymagana ogólna wiedza informatyczna z zakresu systemów operacyjnych i zagadnień sieciowych.

## 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](mailto:adrianna.kukurudz@altkom.pl)

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