



## Zaawansowane techniki ochrony przed cyberatakami – bezpieczeństwo danych i infrastruktury IT

Numer usługi 2025/09/17/153767/3014597

1 472,00 PLN brutto

1 472,00 PLN netto

184,00 PLN brutto/h

184,00 PLN netto/h

K2 CONSULTING  
SPÓŁKA Z  
OGRANICZONĄ  
ODPOWIEDZIALNOŚĆ  
CIĄ

★★★★★ 5,0 / 5

1 585 ocen

📍 Klikawa / stacjonarna

🏠 Usługa szkoleniowa

🕒 8 h

📅 28.10.2025 do 28.10.2025

## Informacje podstawowe

### Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

### Grupa docelowa usługi

Szkolenie przeznaczone jest dla pracowników mających styczność z infrastrukturą IT i dokumentacją elektroniczną, korzystających z narzędzi teleinformatycznych w codziennej pracy. Skierowane jest do osób, które ukończyły podstawowy poziom szkolenia z cyberbezpieczeństwa i potrzebują pogłębionej wiedzy w zakresie ochrony danych i systemów.

Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.

### Minimalna liczba uczestników

1

### Maksymalna liczba uczestników

13

### Data zakończenia rekrutacji

27-10-2025

### Forma prowadzenia usługi

stacjonarna

### Liczba godzin usługi

8

### Podstawa uzyskania wpisu do BUR

Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

## Cel

### Cel edukacyjny

Celem szkolenia "Zaawansowane techniki ochrony przed cyberatakami – bezpieczeństwo danych i infrastruktury IT" jest wyposażenie uczestników w zaawansowaną wiedzę i umiejętności z zakresu ochrony przed cyberatakami, zarządzania incydentami bezpieczeństwa oraz wdrażania nowoczesnych strategii i technologii zabezpieczeń w organizacji.

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

| Efekty uczenia się                                                 | Kryteria weryfikacji                                                                                                     | Metoda walidacji |
|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|------------------|
| Uczestnik identyfikuje i analizuje zagrożenia cybernetyczne        | Wymienia i omawia nowoczesne metody ataków, w tym techniki AI-driven, oraz analizuje przykłady rzeczywistych cyberataków | Wywiad swobodny  |
| Uczestnik stosuje zaawansowane techniki ochrony                    | Wyjaśnia zasady działania systemów EDR/XDR i opisuje, jak wdrożyć skuteczne mechanizmy ochrony przed ransomware          | Wywiad swobodny  |
| Uczestnik zarządza bezpieczeństwem danych w chmurze                | Opisuje zasady Zero Trust i przedstawia sposoby zabezpieczania dostępu do systemów firmowych                             | Wywiad swobodny  |
| Uczestnik analizuje i przeciwdziała złośliwemu oprogramowaniu      | Omawia narzędzia do analizy malware oraz wskazuje sposoby reagowania na incydenty bezpieczeństwa                         | Wywiad swobodny  |
| Uczestnik przeprowadza testy penetracyjne i reaguje na incydenty   | Wyjaśnia, jak identyfikować słabe punkty infrastruktury IT oraz skutecznie reagować na cyberataki                        | Wywiad swobodny  |
| Uczestnik definiuje regulacje prawne dotyczące cyberbezpieczeństwa | Wskazuje kluczowe wymogi wynikające z NIS2, DORA i RODO oraz ich wpływ na organizację                                    | Wywiad swobodny  |
| Uczestnik planuje strategię długoterminowego cyberbezpieczeństwa   | Formułuje rekomendacje dla organizacji dotyczące zwiększenia odporności na zagrożenia                                    | Wywiad swobodny  |

**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. Nowoczesne zagrożenia i ewolucja cyberataków

- Przegląd najnowszych technik ataków stosowanych przez cyberprzestępców
- Cyberataki na poziomie międzynarodowym – analiza przypadków
- Ataki AI-driven (wykorzystanie sztucznej inteligencji do przeprowadzania ataków)

## 2. Zaawansowane techniki ochrony przed atakami

- Systemy EDR/XDR – jak działają i dlaczego są kluczowe?
- Nowoczesne metody ochrony przed ransomware (segregacja uprawnień, honeypoty, air-gapped backups)
- Sztuczna inteligencja w cyberbezpieczeństwie – automatyczna analiza zagrożeń

## 3. Cyberbezpieczeństwo w chmurze i model Zero Trust

- Zasady Zero Trust i ich wdrażanie w organizacji
- Bezpieczeństwo danych w środowisku chmurowym – strategie i narzędzia
- Ochrona dostępu do systemów firmowych z różnych lokalizacji

## 4. Inżynieria wsteczna i analiza złośliwego oprogramowania

- Jak cyberprzestępcy analizują luki w systemach?
- Praktyczne przykłady reverse engineeringu
- Narzędzia do analizy malware i reagowania na incydenty

## 5. Reagowanie na incydenty i testy penetracyjne

- Symulacja ataków na infrastrukturę firmy
- Praktyczne testy penetracyjne – identyfikacja słabych punktów
- Ćwiczenia z reagowania na atak i minimalizacji strat

## 6. Ochrona danych w kontekście regulacji prawnych

- Nowe regulacje dotyczące cyberbezpieczeństwa (NIS2, DORA, RODO)
- Wymogi prawne dla firm w zakresie ochrony infrastruktury IT
- Cyberbezpieczeństwo jako element compliance

## 7. Warsztaty praktyczne i podsumowanie

- Analiza rzeczywistych przypadków ataków – wnioski i lekcje
- Rekomendacje dla organizacji – planowanie strategii długoterminowej

- 
- Szkolenie ma charakter praktyczny i aktywizujący w celu wypracowania najkorzystniejszego podejścia oraz rozwiązań dla organizacji.
  - Warunki niezbędne do spełnienia, aby realizacja usługi pozwoliła na osiągnięcie głównego celu: Aby osiągnąć główny cel usługi, uczestnicy muszą wziąć udział w całym szkoleniu (100% frekwencji), aktywnie uczestniczyć w szkoleniu.
  - Szkolenie przeznaczone jest dla pracowników mających styczność z infrastrukturą IT i dokumentacją elektroniczną, korzystających z narzędzi teleinformatycznych w codziennej pracy. Skierowane jest do osób, które ukończyły podstawowy poziom szkolenia z cyberbezpieczeństwa i potrzebują pogłębionej wiedzy w zakresie ochrony danych i systemów. Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.
  - Trener na bieżąco - w trakcie trwania usługi weryfikuje postępy i ocenia efekty uczenia. Po zakończonej usłudze zostaje przeprowadzona walidacja, oparta o założone kryteria weryfikacji efektów uczenia się, realizowana jest z zachowaniem rozdzielności funkcji.

- W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.
- Usługa realizowana jest w godzinach zegarowych (1 godzina zegarowa = 60 minut).
- Przerwy wliczone są w czas trwania szkolenia.

# Harmonogram

Liczba przedmiotów/zajęć: 8

| Przedmiot / temat zajęć                                                     | Prowadzący   | Data realizacji zajęć | Godzina rozpoczęcia | Godzina zakończenia | Liczba godzin |
|-----------------------------------------------------------------------------|--------------|-----------------------|---------------------|---------------------|---------------|
| <div>1 z 8</div> 1. Nowoczesne zagrożenia i ewolucja cyberataków            | Kamil Kamola | 28-10-2025            | 08:00               | 09:00               | 01:00         |
| <div>2 z 8</div> 2. Zaawansowane techniki ochrony przed atakami             | Kamil Kamola | 28-10-2025            | 09:00               | 10:30               | 01:30         |
| <div>3 z 8</div> 3. Cyberbezpieczeństwo w chmurze i model Zero Trust        | Kamil Kamola | 28-10-2025            | 10:30               | 11:15               | 00:45         |
| <div>4 z 8</div> 4. Inżynieria wsteczna i analiza złośliwego oprogramowania | Kamil Kamola | 28-10-2025            | 11:15               | 12:00               | 00:45         |
| <div>5 z 8</div> Przerwa                                                    | Kamil Kamola | 28-10-2025            | 12:00               | 12:15               | 00:15         |
| <div>6 z 8</div> 5. Reagowanie na incydenty i testy penetracyjne            | Kamil Kamola | 28-10-2025            | 12:15               | 13:30               | 01:15         |
| <div>7 z 8</div> 6. Ochrona danych w kontekście regulacji prawnych          | Kamil Kamola | 28-10-2025            | 13:30               | 14:30               | 01:00         |
| <div>8 z 8</div> 7. Warsztaty praktyczne i podsumowanie                     | Kamil Kamola | 28-10-2025            | 14:30               | 16:00               | 01:30         |

# Cennik

## Cennik

| Rodzaj ceny                               | Cena         |
|-------------------------------------------|--------------|
| Koszt przypadający na 1 uczestnika brutto | 1 472,00 PLN |
| Koszt przypadający na 1 uczestnika netto  | 1 472,00 PLN |
| Koszt osobogodziny brutto                 | 184,00 PLN   |
| Koszt osobogodziny netto                  | 184,00 PLN   |

## Prowadzący

Liczba prowadzących: 1



1 z 1

### Kamil Kamola

Przedsiębiorca posiadający 13-letnie doświadczenie zawodowe w branży IT. W trakcie swojej pracy zawodowej kładzie nacisk na rozwój praktycznych umiejętności w zakresie bezpieczeństwa systemów informatycznych pod kątem zgodności z obecnie obowiązującymi przepisami prawa międzynarodowego oraz krajowego. W swojej codziennej pracy koordynuje działania związane z funkcjonowaniem sektora IT przedsiębiorstw prywatnych jak i podmiotów publicznych, świadczy usługi z zakresu m.in. modelowania procesów biznesowych, audytów oraz analiz przedwdrożeniowych. W przeszłości zdobywał doświadczenie zawodowe na stanowisku programisty aplikacji webowych. Osoba posiadająca bogate doświadczenie zawodowe zbudowane na praktyce, a nie jedynie samej teorii. Posiada średnie wykształcenie. Posiada co najmniej 250 godzin doświadczenia w realizacji szkoleń w podobnej tematyce zrealizowanych w ostatnich pięciu latach (60 miesiącach) wstecz od dnia rozpoczęcia szkolenia.

## Informacje dodatkowe

### Informacje o materiałach dla uczestników usługi

W ramach realizacji szkolenia uczestnicy otrzymują materiały merytoryczne w formie prezentacji. Materiały wysyłane są na adresy mailowe uczestników szkolenia.

### Warunki uczestnictwa

Szkolenie przeznaczone jest dla pracowników mających styczność z infrastrukturą IT i dokumentacją elektroniczną, korzystających z narzędzi teleinformatycznych w codziennej pracy. Skierowane jest do osób, które ukończyły podstawowy poziom szkolenia z cyberbezpieczeństwa i potrzebują pogłębionej wiedzy w zakresie ochrony danych i systemów.

Wymagany jest minimalny staż pracy wynoszący 1 miesiąc.

Koszt szkolenia nie zawiera kosztów dojazdu, zakwaterowania oraz wyżywienia, a także kosztów środków trwałych.

## Informacje dodatkowe

Usługa zwolniona z VAT na podstawie §3 ust.1 pkt 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz.U. z 2015 r., poz.736)

## Adres

ul. Leśna 5  
24-100 Klikawa  
woj. lubelskie

Szkolenie odbędzie się w siedzibie firmy ZPH Krzaczek Sp. z o. o.

## Kontakt



**Kamil Kamola**

**E-mail** [bur@k2c.com.pl](mailto:bur@k2c.com.pl)

**Telefon** (+48) 533 552 510