Możliwość dofinansowania

Zaawansowane Strategie Cyberbezpieczeństwa i Zarządzania Ryzykiem w Środowisku Cyfrowym - usługa szkoleniowa

Numer usługi 2025/07/17/180138/2885509

5 320,00 PLN brutto
5 320,00 PLN netto
166,25 PLN brutto/h
166,25 PLN netto/h

HC SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

5,0 / 5

642 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
32 h
04.09.2025 do 09.09.2025

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do: 1. **Pracowników Firm i Instytucji** • Osoby zatrudnione w działach administracji, kadr, marketingu czy innych obszarach, które w codziennych obowiązkach korzystają z urządzeń elektronicznych i internetu. 2. **Managerów i Kadr Zarządzających** • Osoby odpowiedzialne za polityki bezpieczeństwa danych w firmie, procedury wewnętrzne oraz zarządzanie ryzykiem cybernetycznym. 3. **Specjalistów IT i Pracowników Działów Technicznych** • Osoby techniczne, które chcą usystematyzować swoją wiedzę, pogłębić kompetencje oraz wdrożyć skuteczne zabezpieczenia w organizacjach. 4. **Osoby Odpowiedzialne za Zgodność Prawną (Compliance/Inspektorzy Ochrony Danych/RODO)** • Specjaliści zajmujący się realizacją wymogów prawnych związanych z ochroną danych osobowych i cyberbezpieczeństwem. 5. **Użytkownicy Internetu na Codzień** • Każda osoba, która chce chronić swoją tożsamość, finanse i prywatność w sieci, niezależnie od swojego poziomu zaawansowania technicznego.
Minimalna liczba uczestników	1
Maksymalna liczba uczestników	20

Data zakończenia rekrutacji	03-09-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do samodzielnego identyfikowania i neutralizowania zagrożeń cybernetycznych, wdrażania polityk bezpieczeństwa informatycznego oraz stosowania procedur zarządzania ryzykiem cyfrowym zgodnie z aktualnymi standardami i przepisami prawa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Definiuje podstawowe pojęcia z zakresu cyberbezpieczeństwa, w tym phishing, malware, szyfrowanie i backup.	wybiera poprawną definicję danego terminu spośród czterech opcji w pytaniu jednokrotnego wyboru,	Test teoretyczny z wynikiem generowanym automatycznie
	dopasowuje pojęcia do ich opisów w zadaniu typu „przeciągnij i upuść”.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje regulacje prawne dotyczące cyberbezpieczeństwa, ze szczególnym uwzględnieniem RODO i przestępstw finansowych w przestrzeni cyfrowej.	wskazuje właściwą regulację pasującą do opisu sytuacji w pytaniu jednokrotnego wyboru,	Test teoretyczny z wynikiem generowanym automatycznie
	odpowiada „prawda/fałsz” na twierdzenia dotyczące zastosowania przepisów prawnych.	Test teoretyczny z wynikiem generowanym automatycznie
Projektuje skuteczne strategie tworzenia kopii zapasowych z uwzględnieniem częstotliwości, lokalizacji i rodzaju danych.	wybiera optymalną strategię backupu spośród zaproponowanych wariantów w pytaniu scenariuszowym,	Test teoretyczny z wynikiem generowanym automatycznie
	klasyfikuje metody backupu jako różniące się częstotliwością i lokalizacją w pytaniach typu „przeciągnij i upuść”.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Ocenia poziom bezpieczeństwa danych na podstawie zastosowanych mechanizmów, takich jak autoryzacja dwuetapowa, szyfrowanie i użycie menedżera haseł.	zaznacza, które mechanizmy zwiększają bezpieczeństwo w pytaniu wielokrotnego wyboru,	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia, które z podanych opisów konfiguracji systemu spełniają wymogi bezpieczeństwa (pytania typu „prawda/fałsz”).	Test teoretyczny z wynikiem generowanym automatycznie
Uzasadnia znaczenie ochrony prywatności i świadomego zarządzania danymi w kontekście cyberzagrożeń.	odpowiada na pytania jednokrotnego wyboru z opisem sytuacji, wskazując najbardziej poprawne uzasadnienie potrzeby ochrony,	Test teoretyczny z wynikiem generowanym automatycznie
	rozpoznaje prawidłowe i nieprawidłowe praktyki ochrony prywatności (pytanie typu „prawda/fałsz”).	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia techniki socjotechniczne wykorzystywane przez hakerów oraz ich wpływ na zachowania użytkowników.	wybiera nazwę ataku socjotechnicznego pasującą do opisu sytuacji (pytanie jednokrotnego wyboru),	Test teoretyczny z wynikiem generowanym automatycznie
	dopasowuje typy socjotechnik do odpowiednich przykładów w pytaniu typu „przeciągnij i upuść”.	Test teoretyczny z wynikiem generowanym automatycznie

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

Program Szkolenia

Dzień Pierwszy: Fundamenty Cyberbezpieczeństwa

- Wprowadzenie do cyberbezpieczeństwa:
  - Definicja i podstawowe terminy.
  - Podstawy prawne cyberbezpieczeństwa.
- Najpopularniejsze ataki cybernetyczne:
  - Phishing i inne formy oszustw.
  - Klasyfikacja najpopularniejszych ataków cybernetycznych

Dzień Drugi: Ochrona Danych i Autoryzacja

- Przestępstwa finansowe w przestrzeni cyfrowej.
- Zarządzanie hasłami:
  - Standardy bezpieczeństwa.
  - Wybór menedżera haseł.
- Zabezpieczenia przed cyberatakami:
  - Autoryzacja dwuetapowa.
  - Szyfrowanie danych.

Dzień Trzeci: Zabezpieczenia Systemowe

- Backup danych:
  - Skuteczne strategie tworzenia kopii zapasowych.
- Ochrona sprzętu i prywatności:
  - Antywirusy, firewally, tryb incognito.
  - Socjotechniki wykorzystywane przez hakerów.
- Prawne aspekty cyberbezpieczeństwa:
  - Regulacje RODO.

Dzień Czwarty: Aktualne Zagrożenia i Reakcje

- Fake newsy i narzędzia AI:
  - Mechanizmy generowania fałszywych treści.
- Legalne metody pozyskiwania danych (OSINT).
- Procedury reagowania na ataki cybernetyczne:
  - Formalne i komunikacyjne kroki.
- Podsumowanie
- Test teoretyczny z wynikiem generowanym automatycznie - walidacja

Szkolenie odbywa się w godzinach dydaktycznych, czyli 1 godzina szkolenia równa się 45 minut.

W ciągu dnia zostały uwzględnione 2 przerwy po 30 minut które nie są wliczane do czasu trwania usługi.

Prowadzone w ramach szkolenia zajęcia realizowane są metodami interaktywnymi i aktywizującymi, rozumianymi jako metody umożliwiające uczenie się w oparciu o doświadczenie i pozwalające uczestnikom na ćwiczenie umiejętności.

Warunki organizacyjne: grupa maksymalnie 20 osobowa gdzie każdy ma dostęp do swojego komputera

W szkoleniu wykorzystywane są tylko zajęcia teoretyczne.

Harmonogram

Liczba przedmiotów/zajęć: 35

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 35 Wprowadzenie do cyberbezpieczeństwa (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	08:00	09:00	01:00
2 z 35 Definicja i podstawowe terminy (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	09:00	10:30	01:30
3 z 35 Przerwa	Joanna Dubisz	04-09-2025	10:30	11:00	00:30
4 z 35 Podstawy prawne cyberbezpieczeństwa (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	11:00	12:00	01:00
5 z 35 Najpopularniejsze ataki cybernetyczne (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	12:00	13:00	01:00
6 z 35 Przerwa	Joanna Dubisz	04-09-2025	13:00	13:30	00:30
7 z 35 Phishing i inne formy oszustw (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	13:30	14:15	00:45
8 z 35 Klasyfikacja najpopularniejszych ataków cybernetycznych (współdzielenie ekranu)	Joanna Dubisz	04-09-2025	14:15	15:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 35 Przestępstwa finansowe w przestrzeni cyfrowej (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	08:00	09:00	01:00
10 z 35 Zarządzanie hasłami (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	09:00	10:00	01:00
11 z 35 Standardy bezpieczeństwa (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	10:00	11:00	01:00
12 z 35 Przerwa	Joanna Dubisz	05-09-2025	11:00	11:30	00:30
13 z 35 Wybór menedżera haseł (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	11:30	12:30	01:00
14 z 35 Zabezpieczenia przed cyberatakami (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	12:30	13:30	01:00
15 z 35 Przerwa	Joanna Dubisz	05-09-2025	13:30	14:00	00:30
16 z 35 Autoryzacja dwuetapowa (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	14:00	14:30	00:30
17 z 35 Szyfrowanie danych (współdzielenie ekranu)	Joanna Dubisz	05-09-2025	14:30	15:00	00:30
18 z 35 Backup danych (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 35 Skuteczne strategie tworzenia kopii zapasowych (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	09:00	10:00	01:00
20 z 35 Ochrona sprzętu i prywatności (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	10:00	11:00	01:00
21 z 35 Przerwa	Joanna Dubisz	08-09-2025	11:00	11:30	00:30
22 z 35 Antywirusy, firewally, tryb incognito (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	11:30	12:30	01:00
23 z 35 Socjotechniki wykorzystywane przez hakerów (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	12:30	13:30	01:00
24 z 35 Przerwa	Joanna Dubisz	08-09-2025	13:30	14:00	00:30
25 z 35 Prawne aspekty cyberbezpieczeństwa (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	14:00	14:30	00:30
26 z 35 Regulacje RODO (współdzielenie ekranu)	Joanna Dubisz	08-09-2025	14:30	15:00	00:30
27 z 35 Fake newsy i narzędzia AI (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	08:00	09:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 35 Mechanizmy generowania fałszywych treści (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	09:00	10:00	01:00
29 z 35 Legalne metody pozyskiwania danych (OSINT) (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	10:00	11:00	01:00
30 z 35 Przerwa	Joanna Dubisz	09-09-2025	11:00	11:30	00:30
31 z 35 Procedury reagowania na ataki cybernetyczne (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	11:30	12:30	01:00
32 z 35 Formalne i komunikacyjne kroki (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	12:30	13:30	01:00
33 z 35 Przerwa	Joanna Dubisz	09-09-2025	13:30	14:00	00:30
34 z 35 Podsumowanie (współdzielenie ekranu)	Joanna Dubisz	09-09-2025	14:00	14:30	00:30
35 z 35 Test teoretyczny z wynikiem generowanym automatycznie - walidacja	Joanna Dubisz	09-09-2025	14:30	15:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena

Koszt przypadający na 1 uczestnika brutto	5 320,00 PLN
Koszt przypadający na 1 uczestnika netto	5 320,00 PLN
Koszt osobogodziny brutto	166,25 PLN
Koszt osobogodziny netto	166,25 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Joanna Dubisz

Joanna Dubisz to doświadczona szkoleniowiec specjalizująca się w obszarach sprzedaży oraz obsługi klienta. Swoją edukację rozpoczęła od ukończenia liceum profilowanego o kierunku socjalnym, co dało jej solidne podstawy w zakresie pracy z ludźmi i zrozumienia ich potrzeb. Karierę szkoleniowca rozpoczęła w 2018 roku i od tego czasu nieustannie rozwija swoje umiejętności, zdobywając liczne certyfikaty, w tym z zakresu pracy w zespole oraz radzenia sobie z trudnymi klientami.

Joanna zrealizowała ponad 300 godzin szkoleń, prowadząc warsztaty zarówno dla firm, jak i klientów indywidualnych. Jej szkolenia cechują się praktycznym podejściem i są dostosowane do rzeczywistych potrzeb uczestników, dzięki czemu potrafi efektywnie przekazywać wiedzę, jednocześnie budując zaangażowanie i motywację w zespole. Dzięki swojemu doświadczeniu oraz umiejętnościom w zarządzaniu relacjami z klientem, Joanna cieszy się opinią eksperta w zakresie rozwijania kompetencji sprzedażowych i obsługi klienta."
Joanna Dubisz posiada udokumentowane doświadczenie w zakresie cyberbezpieczeństwa zdobyte w ciągu ostatnich 5 lat. W latach 2020–2024 realizowała szkolenia i projekty wdrożeniowe w obszarze ochrony danych i zarządzania ryzykiem IT

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Komplet materiałów zostanie wysłany w wiadomości e-mail dla każdego z uczestników szkolenia.

Zestaw materiałów szkoleniowych składa się z prezentacji oraz skryptu szkolenia.

Informacje dodatkowe

Uczestnik otrzyma zaświadczenie o ukończeniu szkolenia zawierające efekty uczenia się oraz potwierdzenie przeprowadzenia walidacji zgodnie z wymaganiami Załącznika nr 4 do Regulaminu BUR

Szkolenie jest zwolnione z podatku VAT na podstawie§3 ust.l 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)).

Jeśli dofinansowanie za szkolenie ze środków publicznych wyniesie poniżej 70%, do kwoty faktury zostanie doliczona stawka podatku VAT (23%).

Do wybranej metody walidacji nie jest potrzebny walidator, ponieważ uczestnicy dostają link do wypełnienia testu

Warunki techniczne

1. Platforma komunikacyjna – Microsoft Teams

2. Wymagania sprzętowe: komputer stacjonarny/laptop, kamera, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/Mac

3. Sieć: łącze internetowe minimum 50 kb/s;

4. System operacyjny: minimum Windows XP/MacOS High Sierra, przeglądarka internetowa (marka nie ma znaczenia)

5. Okres ważności linku: od 1 h przed godziną rozpoczęcia szkolenia w dniu pierwszym do godziny po zakończeniu szkoleń w dniu ostatnim.

Kontakt

Dominik Hamera

E-mail office@hameracapital.eu
Telefon (+48) 888 677 422