



Cyberbezpieczeństwo – usługa szkoleniowa

Numer usługi 2026/05/20/180138/3573650

6 642,00 PLN brutto
5 400,00 PLN netto
189,77 PLN brutto/h
154,29 PLN netto/h
261,33 PLN cena rynkowa ⓘ

HC SPÓŁKA Z
OGRA NICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,9 / 5

990 ocen

- 🏠 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 35:00 h
- 📅 16.11.2026 do 20.11.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• pracownicy i/lub właściciele pracujący z komputerem, Internetem oraz urządzeniami mobilnymi • pracownicy z sektora MSP Szkolenie jest przeznaczone przede wszystkim dla osób chcących chronić dane firmy, rozpoznawać oszustwa np. w mediach społecznościowych oraz odpowiednio reagować na nie.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	15-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Usługa ma na celu zwiększenie świadomości i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz higieny w sieci, z naciskiem na rozumienie i praktyczne stosowanie najlepszych praktyk i strategii obrony przed zagrożeniami cybernetycznymi w środowisku zawodowym i osobistym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Omawia podstawowe pojęcia związane z cyberbezpieczeństwem i higieną w sieci, takie jak malware, phishing, bezpieczne hasła i szyfrowanie danych.	Uczestnik poprawnie definiuje wymienione pojęcia i opisuje ich znaczenie w kontekście bezpieczeństwa sieciowego.	Test teoretyczny z wynikiem generowanym automatycznie
Charakteryzuje różne typy zagrożeń cyfrowych oraz metody ich rozpoznawania.	Uczestnik wymienia i opisuje co najmniej trzy różne typy zagrożeń, podając przykłady oraz sposoby ich identyfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
Definiuje znaczenie aktualizacji oprogramowania w kontekście zabezpieczeń cyfrowych.	Uczestnik wyjaśnia, dlaczego regularne aktualizacje oprogramowania są kluczowe dla zachowania bezpieczeństwa systemów i danych.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje praktyki tworzenia i zarządzania bezpiecznymi hasłami.	Uczestnik demonstruje umiejętność tworzenia silnych haseł i korzystania z menedżerów haseł do ich przechowywania.	Test teoretyczny z wynikiem generowanym automatycznie
Identyfikuje i reaguj na próby phishingu i inne oszustwa internetowe.	Uczestnik poprawnie identyfikuje fałszywe wiadomości e-mail i strony internetowe oraz zna procedury reagowania na te zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
Stosuje zasady bezpiecznego korzystania z sieci publicznych i prywatnych.	Uczestnik potrafi skonfigurować bezpieczne połączenie sieciowe i stosuje praktyki ochrony prywatności podczas korzystania z sieci publicznych.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Program

Dzień 1:

1. wprowadzenie do szkolenia
2. audyt cyberbezpieczeństwa
3. istota i podstawowe terminy w zakresie cyberbezpieczeństwa
4. podstawy prawne cyberbezpieczeństwa i zalecenia ENISA
5. najpopularniejsze ataki cybernetyczne

Dzień 2:

1. ćwiczenie: phishing
2. przestępstwa finansowe w przestrzeni cyfrowej
3. zasady ustalania haseł zgodnie z obecnymi standardami bezpieczeństwa cyfrowego
4. jak działa i jak wybrać menadżera haseł?
5. dlaczego tak często hakerzy łamią hasła?

Dzień 3:

1. dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce
2. szyfrowanie plików, folderów i pendrive'ów w praktyce
3. jak chronić dane osobowe zgodnie z RODO?
4. zastrzeż swój PESEL
5. jak robić backup danych?

Dzień 4:

1. dlaczego warto korzystać z „chmur”?
2. wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?
3. jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN
4. co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów
5. co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna

Dzień 5:

1. jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?
2. jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?
3. ćwiczenie grupowe: symulacje ataków cybernetycznych
4. narzędzia i programy wzmacniające bezpieczeństwo cyfrowe
5. Podsumowanie
6. Test teoretyczny z wynikiem generowanym automatycznie - walidacja

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

Przerwy ujęte w harmonogramie nie są wliczane w czas trwania szkolenia.

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.

Harmonogram

Liczba pozycji harmonogramu: 36

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Wprowadzenie do szkolenia	Zajęcia	DOMINIK HAMERA	16-11-2026	08:00	09:00	01:00
2 z 36 Audyt cyberbezpieczeństwa	Zajęcia	DOMINIK HAMERA	16-11-2026	09:00	10:00	01:00
3 z 36 -	Przerwa	-	16-11-2026	10:00	10:30	00:30
4 z 36 Istota i podstawowe terminy w zakresie cyberbezpieczeństwa	Zajęcia	DOMINIK HAMERA	16-11-2026	10:30	11:30	01:00
5 z 36 Podstawy prawne cyberbezpieczeństwa i zalecenia ENISA	Zajęcia	DOMINIK HAMERA	16-11-2026	11:30	12:30	01:00
6 z 36 -	Przerwa	-	16-11-2026	12:30	13:00	00:30
7 z 36 Najpopularniejsze ataki cybernetyczne	Zajęcia	DOMINIK HAMERA	16-11-2026	13:00	15:00	02:00
8 z 36 Ćwiczenie: phishing	Zajęcia	DOMINIK HAMERA	17-11-2026	08:00	09:00	01:00
9 z 36 Przestępstwa finansowe w przestrzeni cyfrowej	Zajęcia	DOMINIK HAMERA	17-11-2026	09:00	10:00	01:00
10 z 36 -	Przerwa	-	17-11-2026	10:00	10:30	00:30
11 z 36 Zasady ustalania hasel zgodnie z obecnymi standardami bezpieczeństwa cyfrowego	Zajęcia	DOMINIK HAMERA	17-11-2026	10:30	11:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 36 Jak działa i jak wybrać menadżera haseł?	Zajęcia	DOMINIK HAMERA	17-11-2026	11:30	12:30	01:00
13 z 36 -	Przerwa	-	17-11-2026	12:30	13:00	00:30
14 z 36 Dlaczego tak często hakerzy łamią hasła?	Zajęcia	DOMINIK HAMERA	17-11-2026	13:00	15:00	02:00
15 z 36 Dlaczego samo hasło nie wystarczy? Autoryzacja dwuskładnikowa w praktyce	Zajęcia	DOMINIK HAMERA	18-11-2026	08:00	09:00	01:00
16 z 36 Szyfrowanie plików, folderów i pendrive'ów w praktyce	Zajęcia	DOMINIK HAMERA	18-11-2026	09:00	10:00	01:00
17 z 36 -	Przerwa	-	18-11-2026	10:00	10:30	00:30
18 z 36 Jak chronić dane osobowe zgodnie z RODO?	Zajęcia	DOMINIK HAMERA	18-11-2026	10:30	11:30	01:00
19 z 36 Zastrzeż swój PESEL	Zajęcia	DOMINIK HAMERA	18-11-2026	11:30	12:30	01:00
20 z 36 -	Przerwa	-	18-11-2026	12:30	13:00	00:30
21 z 36 Jak robić backup danych?	Zajęcia	DOMINIK HAMERA	18-11-2026	13:00	15:00	02:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
22 z 36 Dlaczego warto korzystać z „chmury”?	Zajęcia	DOMINIK HAMERA	19-11-2026	08:00	09:00	01:00
23 z 36 Wykorzystywanie AI przez cyberprzestępców – jak nie dać się nabrać?	Zajęcia	DOMINIK HAMERA	19-11-2026	09:00	10:00	01:00
24 z 36 -	Przerwa	-	19-11-2026	10:00	10:30	00:30
25 z 36 Jak zabezpieczyć swój sprzęt i prywatność? Programy antywirusowe, firewall, tryb incognito, cookies, VPN	Zajęcia	DOMINIK HAMERA	19-11-2026	10:30	11:30	01:00
26 z 36 Co o nas wiedzą? - socjotechniki wykorzystywane przez hakerów	Zajęcia	DOMINIK HAMERA	19-11-2026	11:30	12:30	01:00
27 z 36 -	Przerwa	-	19-11-2026	12:30	13:00	00:30
28 z 36 Co zrobić, gdy zostanę zaatakowany? Procedura formalna i komunikacyjna	Zajęcia	DOMINIK HAMERA	19-11-2026	13:00	15:00	02:00
29 z 36 Jak wzmocnić kulturę cyberbezpieczeństwa w organizacji?	Zajęcia	DOMINIK HAMERA	20-11-2026	08:00	09:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
30 z 36 Jak rodzą się fake newsy przez wykorzystywanie narzędzi AI?	Zajęcia	DOMINIK HAMERA	20-11-2026	09:00	10:00	01:00
31 z 36 -	Przerwa	-	20-11-2026	10:00	10:30	00:30
32 z 36 Ćwiczenie grupowe: symulacje ataków cybernetycznych	Zajęcia	DOMINIK HAMERA	20-11-2026	10:30	11:30	01:00
33 z 36 Narzędzia i programy wzmacniające bezpieczeństwo cyfrowe	Zajęcia	DOMINIK HAMERA	20-11-2026	11:30	12:30	01:00
34 z 36 -	Przerwa	-	20-11-2026	12:30	13:00	00:30
35 z 36 Podsumowanie	Zajęcia	DOMINIK HAMERA	20-11-2026	13:00	14:00	01:00
36 z 36 -	Walidacja	DOMINIK HAMERA	20-11-2026	14:00	15:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	35:00
w tym suma godzin zajęć	29:00
w tym suma godzin walidacji	01:00
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	40:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeżeli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	6 642,00 PLN
Koszt przypadający na 1 uczestnika netto	5 400,00 PLN
Koszt osobogodziny brutto	189,77 PLN
Koszt osobogodziny netto	154,29 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	35:00

Prowadzący

Liczba prowadzących: 1



1 z 1

DOMINIK HAMERA

Jestem doświadczonym szkoleniowcem i doradcą biznesowym z 10-letnim stażem, specjalizującym się w pozyskiwaniu funduszy (ponad 200 mln zł dla klientów) oraz kompleksowym wsparciu w zarządzaniu, motywacji i optymalizacji procesów organizacyjnych. Absolwent AWF Warszawa (kierunek: Wychowanie Fizyczne, specjalność: Menedżer), łączę wiedzę akademicką z praktyką biznesową, prowadząc szkolenia z zakresu tworzenia dokumentów unijnych, automotywacji, radzenia sobie ze stresem oraz skutecznego zarządzania dla właścicieli firm, kadry kierowniczej i sektora MŚP. Z ponad 2000 godzin szkoleń i 3000 przeszkolonych osób, oferuję spersonalizowane rozwiązania, które przekładają się na mierzalne sukcesy – od pozyskania finansowania po wzrost efektywności zespołów. Moja misja? Przekazywać wiedzę, która napędza rozwój zarówno firm, jak i ich zespołów.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały zostaną przesłane drogą mailową w formacie pdf. Uczestnik otrzyma:

1. skrypty
2. materiały video

Informacje dodatkowe

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

Szkolenie skierowane do osób korzystających z bonów rozwojowych

Warunki techniczne

1. platforma komunikacyjna – Microsoft Teams.
2. wymagania sprzętowe: komputer stacjonarny/laptop, mikrofon, słuchawki/ głośniki, system operacyjny minimum Windows XP/MacOS High Sierra, min 2 GB pamięci RAM, pamięć dysku minimum 10GB,
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