



Cyberbezpieczeństwo i ochrona danych w organizacji – usługa szkoleniowa

Numer usługi 2026/10/26/180138/3905673

6 543,60 PLN brutto
5 320,00 PLN netto
163,59 PLN brutto/h
133,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

HC SPÓŁKA Z
OGRANICZONĄ
ODPOWIEDZIALNOŚ
CIĄ

★★★★★ 4,9 / 5

991 ocen

- 📄 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 📄 Zajęcia grupowe
- 🕒 40:00 h
- 📅 14.12.2026 do 18.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do pracowników oraz właścicieli i osób zarządzających mikro, małymi i średnimi przedsiębiorstwami, którzy w swojej pracy korzystają z komputerów, urządzeń mobilnych, poczty elektronicznej, Internetu oraz narzędzi i usług cyfrowych. Grupę docelową stanowią osoby chcące zwiększyć bezpieczeństwo wykonywanych zadań, lepiej chronić dane osobowe i informacje firmowe, rozpoznawać próby oszustw internetowych oraz ograniczać ryzyko związane z cyberatakami. Szkolenie jest odpowiednie dla osób bez specjalistycznego przygotowania informatycznego, posiadających podstawowe umiejętności obsługi komputera i korzystania z Internetu.
Minimalna liczba uczestników	2
Maksymalna liczba uczestników	30
Data zakończenia rekrutacji	13-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Celem edukacyjnym usługi jest rozwinięcie wiedzy i kompetencji uczestników w zakresie cyberbezpieczeństwa oraz bezpiecznego korzystania z technologii cyfrowych w środowisku zawodowym i prywatnym. Szkolenie przygotowuje do rozpoznawania zagrożeń cybernetycznych, stosowania zasad higieny cyfrowej, ochrony danych osobowych i informacji firmowych oraz podejmowania właściwych działań w przypadku podejrzenia incydentu bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Identyfikuje podstawowe pojęcia i zasady związane z cyberbezpieczeństwem oraz higieną cyfrową.	Rozpoznaje definicje pojęć: cyberbezpieczeństwo, malware, phishing, szyfrowanie danych i incydent bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje przykłady zagrożeń dla bezpieczeństwa informacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Dopasowuje rodzaje zagrożeń do ich charakterystyki.	Test teoretyczny z wynikiem generowanym automatycznie
Rozróżnia rodzaje zagrożeń cybernetycznych oraz metody stosowane przez cyberprzestępców.	Rozróżnia phishing, złośliwe oprogramowanie, ransomware, oszustwa finansowe i ataki socjotechniczne.	Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje charakterystyczne cechy podejrzanych wiadomości e-mail, SMS-ów i stron internetowych.	Test teoretyczny z wynikiem generowanym automatycznie
	Dopasowuje opis sytuacji do odpowiedniego rodzaju zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
	Rozróżnia hasła silne i słabe.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera zasady prawidłowego tworzenia unikalnych haseł.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera zasady tworzenia i zabezpieczania haseł oraz ochrony dostępu do kont.	Wskazuje zastosowanie menedżera haseł.	Test teoretyczny z wynikiem generowanym automatycznie
	Dobiera odpowiednie metody dodatkowego zabezpieczenia kont, w tym uwierzytelnianie dwuskładnikowe.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wskazuje sposoby zabezpieczania urządzeń i oprogramowania przed zagrożeniami cyfrowymi.	Wskazuje cel regularnego aktualizowania systemów operacyjnych i aplikacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Dopasowuje funkcje programów antywirusowych i zapory sieciowej do ich zastosowania.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera działania ograniczające ryzyko nieuprawnionego dostępu do urządzeń.	Test teoretyczny z wynikiem generowanym automatycznie
Dobiera sposoby ochrony danych osobowych, informacji firmowych i prywatności cyfrowej.	Wskazuje podstawowe zasady ochrony danych osobowych zgodnie z RODO.	Test teoretyczny z wynikiem generowanym automatycznie
	Dopasowuje metody szyfrowania do przykładowych zastosowań.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera właściwe sposoby tworzenia i przechowywania kopii zapasowych.	Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje działania ograniczające ryzyko kradzieży tożsamości i nieuprawnionego wykorzystania danych.	Test teoretyczny z wynikiem generowanym automatycznie
	Identyfikuje zagrożenia związane z korzystaniem z publicznych sieci Wi-Fi.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje zastosowanie i ograniczenia VPN.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera zasady bezpiecznego przechowywania i udostępniania plików w chmurze.	Test teoretyczny z wynikiem generowanym automatycznie
Wybiera zasady bezpiecznego korzystania z sieci publicznych, prywatnych i usług chmurowych.	Dopasowuje funkcje trybu prywatnego przeglądarki i ustawień cookies do ich zastosowania.	Test teoretyczny z wynikiem generowanym automatycznie
Rozpoznaje zagrożenia związane z wykorzystaniem sztucznej inteligencji do tworzenia fałszywych treści i oszustw internetowych.	Identyfikuje przykłady wykorzystania AI do tworzenia fałszywych wiadomości i materiałów.	Test teoretyczny z wynikiem generowanym automatycznie
	Rozróżnia wiarygodne informacje od treści, których autentyczność wymaga dodatkowej weryfikacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera sposoby sprawdzania wiarygodności informacji i źródeł.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wybiera właściwe działania w przypadku podejrzenia incydentu cyberbezpieczeństwa.	Rozpoznaje sytuacje wskazujące na możliwość wystąpienia incydentu bezpieczeństwa.	Test teoretyczny z wynikiem generowanym automatycznie
	Dobiera działania do przykładowego scenariusza zagrożenia.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje właściwe sposoby zgłaszania incydentów i ograniczania ich skutków.	Test teoretyczny z wynikiem generowanym automatycznie
Wskazuje działania wspierające rozwój kultury cyberbezpieczeństwa w organizacji.	Rozpoznaje przykłady odpowiedzialnych zachowań związanych z ochroną informacji.	Test teoretyczny z wynikiem generowanym automatycznie
	Wskazuje znaczenie procedur bezpieczeństwa i zgłaszania incydentów.	Test teoretyczny z wynikiem generowanym automatycznie
	Wybiera działania ograniczające ryzyko cyberataków w środowisku zawodowym.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje i kompetencje

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?

TAK

Program

DZIEŃ 1 – Audyt, podstawy prawne i rodzaje zagrożeń

08:00 – 09:15 | Moduł 1. Wprowadzenie i audyt cyberbezpieczeństwa (75 min)

- **Teoria (45 min):** Wprowadzenie do szkolenia i omówienie celów. Podstawowe terminy (triada CIA: poufność, integralność, dostępność). Metodologia audytu cyberbezpieczeństwa.
- **Praktyka (30 min):** Wstępna autodiagnoza stanu bezpieczeństwa cyfrowego na własnym stanowisku pracy.

09:15 – 10:15 | Moduł 2. Podstawy prawne i zalecenia ENISA – część teoretyczna (60 min)

- Krajowe i europejskie ramy prawne cyberbezpieczeństwa (NIS2, KSC). Wytyczne Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

10:15 – 10:30 | Przerwa kawowa (15 min)

10:30 – 11:30 | Moduł 2. Podstawy prawne i zalecenia ENISA – część praktyczna (60 min)

- **Praktyka:** Analiza przypadków (*case studies*) wdrażania zaleceń ENISA w organizacjach oraz audyt zgodności procedur firmowych.

11:30 – 12:30 | Moduł 3. Najpopularniejsze ataki cybernetyczne – część teoretyczna (60 min)

- Przegląd zagrożeń: Malware, Ransomware, DDoS, Man-in-the-Middle, BEC (*Business Email Compromise*). Mechanizmy infekcji i wektory ataków.

12:30 – 13:00 | Przerwa obiadowa (30 min)

13:00 – 14:30 | Moduł 3. Najpopularniejsze ataki cybernetyczne – część praktyczna (90 min)

- **Praktyka:** Analiza realnych incydentów i ataków Ransomware/DDoS na przykładowych firmach. Identyfikacja luk w zabezpieczeniach.

14:30 – 14:45 | Przerwa kawowa (15 min)

14:45 – 16:00 | Warsztat 1. Mapa podatności organizacji – część praktyczna (75 min)

- **Praktyka:** Praca warsztatowa nad stworzeniem wstępnej mapy podatności i zagrożeń cyfrowych dla własnego środowiska pracy. Podsumowanie Dnia 1.

DZIEŃ 2 – Phishing, przestępstwa finansowe i zarządzanie tożsamością

08:00 – 09:15 | Moduł 4. Przestępstwa finansowe w przestrzeni cyfrowej – część teoretyczna (75 min)

- Mechanizmy oszustw finansowych online (vishing, smishing, spoofing bankowy, wyłudzenia płatności). Bezpieczeństwo transakcji cyfrowych.

09:15 – 10:15 | Moduł 5. Ćwiczenie praktyczne: Phishing – część praktyczna (60 min)

- **Praktyka:** Rozpoznawanie sfałszowanych wiadomości e-mail, złośliwych linków i fałszywych domen. Analiza nagłówek wiadomości.

10:15 – 10:30 | Przerwa kawowa (15 min)

10:30 – 11:30 | Moduł 6. Standardy haseł i łamanie zabezpieczeń – część teoretyczna (60 min)

- Przyczyny łamania haseł przez hakerów (*brute-force*, *dictionary attack*, wycieki baz). Zasady tworzenia haseł według standardów NIST/ENISA.

11:30 – 12:30 | Moduł 6. Standardy haseł i menadżery haseł – część praktyczna (60 min)

- **Praktyka:** Testowanie siły haseł w bezpiecznych środowiskach. Jak działa i jak wybrać menadżer haseł? Konfiguracja i wdrażanie menadżera haseł.

12:30 – 13:00 | Przerwa obiadowa (30 min)

13:00 – 14:30 | Warsztat 2. Ochrona poświadczeń i bezpieczny menadżer haseł – część praktyczna (90 min)

- **Praktyka:** Tworzenie bezpiecznego magazynu poświadczeń, generowanie unikalnych haseł i migracja ze słabych zabezpieczeń.

14:30 – 14:45 | Przerwa kawowa (15 min)

14:45 – 16:00 | Audyt haseł i wycieków danych – część praktyczna (75 min)

- **Praktyka:** Sprawdzanie adresów e-mail w bazach wyciekowych oraz opracowanie spersonalizowanej polityki haseł. Podsumowanie Dnia 2.

DZIEŃ 3 - Uwierzytelnianie, szyfrowanie, RODO i kopie zapasowe

08:00 – 09:15 | Moduł 7. 2FA, szyfrowanie i ochrona RODO – część teoretyczna (75 min)

- Autoryzacja dwuskładnikowa (2FA/MFA) – aplikacje 2FA vs SMS vs klucze sprzętowe U2F/FIDO2. Ochrona danych osobowych zgodnie z RODO w ujęciu technicznym. Procedury usługi „Zastrzeż swój PESEL”.

09:15 – 10:15 | Moduł 7. Autoryzacja 2FA i zastrzeganie PESEL – część praktyczna (60 min)

- **Praktyka:** Wdrażanie i obsługa 2FA na kontach służbowych/prywatnych oraz praktyczna weryfikacja zastrzeżenia numeru PESEL.

10:15 – 10:30 | Przerwa kawowa (15 min)

10:30 – 11:30 | Moduł 8. Szyfrowanie i backup danych – część teoretyczna (60 min)

- Zasady szyfrowania danych statycznych i w transmisji (BitLocker, VeraCrypt, TLS/SSL). Tworzenie kopii zapasowych: zasada 3-2-1, rodzaje backupu (pełny, przyrostowy, różnicowy).

11:30 – 12:30 | Moduł 8. Szyfrowanie w praktyce – część praktyczna (60 min)

- **Praktyka:** Szyfrowanie plików, folderów i nośników przenośnych (pendrive'ów) w praktyce warsztatowej.

12:30 – 13:00 | Przerwa obiadowa (30 min)

13:00 – 14:30 | Warsztat 3. Tworzenie i testowanie kopii zapasowych – część praktyczna (90 min)

- **Praktyka:** Konfiguracja harmonogramu backupu, odzyskiwanie danych z pliku kopii zapasowej oraz testowanie spójności backupu.

14:30 – 14:45 | Przerwa kawowa (15 min)

14:45 – 16:00 | Audyt ochrony danych na stanowisku – część praktyczna (75 min)

- **Praktyka:** Przygotowanie checklisty RODO i zabezpieczeń fizycznych/cyfrowych na własnym stanowisku pracy. Podsumowanie Dnia 3.

DZIEŃ 4 – Chmura, sztuczna inteligencja, higiena cyfrowa i reagowanie na incydenty

08:00 – 09:15 | Moduł 9. Bezpieczeństwo chmury, socjotechnika i AI – część teoretyczna (75 min)

- Modele bezpieczeństwa chmurowego (SaaS/PaaS/IaaS) i odpowiedzialność dzielona. Wykorzystywanie AI przez cyberprzestępców – deepfake głosowy/wideo, advanced-phishing. Socjotechniki hakerskie (wywieranie presji, autorytet).

09:15 – 10:15 | Moduł 9. Detekcja ataków AI i socjotechniki – część praktyczna (60 min)

- **Praktyka:** Analiza prób manipulacji socjotechnicznej i identyfikacja materiałów syntetycznych generowanych przez AI (deepfake).

10:15 – 10:30 | Przerwa kawowa (15 min)

10:30 – 11:30 | Moduł 10. Ochrona sprzętu i prywatności – część teoretyczna (60 min)

- Ochrona sprzętu: programy antywirusowe (EDR/XDR), firewall, tryb incognito, pliki cookies, VPN. Cyfrowy ślad i ochrona prywatności w sieci.

11:30 – 12:30 | Moduł 10. Konfiguracja narzędzi prywatności i ochrony – część praktyczna (60 min)

- **Praktyka:** Konfiguracja zapory sieciowej, ustawień prywatności w przeglądarkach, czyszczenie śladów i obsługa bezpiecznego połączenia VPN.

12:30 – 13:00 | Przerwa obiadowa (30 min)

13:00 – 14:30 | Moduł 11. Reagowanie na incydenty – część teoretyczna i praktyczna (90 min)

- **Teoria (45 min):** Pierwsi responderzy. Procedura formalna (zgłaszanie do CSIRT Polska/UODO/policji) i komunikacyjna (komunikacja kryzysowa).
- **Praktyka (45 min):** Tworzenie ścieżki reagowania na incydent dla własnego zespołu.

14:30 – 14:45 | Przerwa kawowa (15 min)

14:45 – 16:00 | Symulacja zgłoszenia incydentu – część praktyczna (75 min)

- **Praktyka:** Odgrywanie ról i wypełnianie formularzy zgłoszeniowych incydentu bezpieczeństwa. Podsumowanie Dnia 4.

DZIEŃ 5 – Kultura bezpieczeństwa, fake newsy, symulacje i walidacja

08:00 – 09:15 | Moduł 12. Kultura cyberbezpieczeństwa i dezinformacja AI – część teoretyczna (75 min)

- Budowanie kultury bezpieczeństwa w organizacji („ludzki firewall”). Jak rodzą się fake newsy przy użyciu AI? Weryfikacja informacji (*fact-checking*).

09:15 – 10:15 | Moduł 12. Fact-checking i weryfikacja informacji – część praktyczna (60 min)

- **Praktyka:** Warsztat weryfikacji informacji, wykrywanie dezinformacji oraz obsługa narzędzi do wstecznego wyszukiwania obrazem i tekstem.

10:15 – 10:30 | Przerwa kawowa (15 min)

10:30 – 11:30 | Moduł 13. Narzędzia wzmacniające bezpieczeństwo cyfrowe – część teoretyczna (60 min)

- Przegląd bezpłatnych i komercyjnych narzędzi wspierających higienę cyfrową (skanery podatności, menadżery tożsamości, analizatory linków).

11:30 – 12:30 | Moduł 13. Praca z narzędziami bezpieczeństwa – część praktyczna (60 min)

- **Praktyka:** Testowanie i wdrażanie wybranych narzędzi wspierających ochronę systemu na własnych urządzeniach.

12:30 – 13:00 | Przerwa obiadowa (30 min)

13:00 – 14:30 | Moduł 14. Symulacje ataków cybernetycznych – część praktyczna (90 min)

- **Praktyka:** Zaawansowana symulacja skoordynowanego ataku na organizację (wyciek danych + Ransomware + atak socjotechniczny). Praca w zespołach nad opanowaniem kryzysu.

14:30 – 14:45 | Przerwa kawowa (15 min)

14:45 – 15:00 | Podsumowanie dydaktyczne (15 min)

- Omówienie wniosków z symulacji, podsumowanie kluczowych zasad i przygotowanie do cyfrowego testu końcowego.

15:00 – 16:00 | Moduł 15. Walidacja efektów uczenia się (60 min)

1) Czas trwania oraz format zajęć

Łączny wymiar godzinowy wynosi **40 godzin zegarowych** (gdzie 1 godzina odpowiada 60 minutom), włączając w to przewidziane w harmonogramie przerwy. Zajęcia odbywają się w formie zdalnej na żywo za pośrednictwem platformy wideokonferencyjnej. Grupa warsztatowa liczy od 2 do maksymalnie 30 uczestników.

2) Sposób prowadzenia zajęć

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 praktyczne ćwiczenie umiejętności.

3) Sposób weryfikacji wiedzy (Walidacja)

Walidacja efektów uczenia się jest w pełni niezależna od procesu dydaktycznego i od osoby trenera prowadzącego szkolenie. Weryfikacja odbywa się na zakończenie szkolenia za pośrednictwem zewnętrznego, automatycznego systemu cyfrowego (Microsoft Forms).

Przebieg i zasady walidacji:

- 1. **Automatyczna weryfikacja (Niezależny algorytm):** Test teoretyczno-praktyczny ma formę cyfrowego testu wiedzy i umiejętności. Baza pytań oraz klucz odpowiedzi są ze sobą powiązane w sposób sztywny, a wynik wyliczany jest automatycznie przez algorytm systemu bez jakiegokolwiek ingerencji człowieka.
- 2. **Rola trenera:** Trener prowadzący szkolenie nie jest egzaminatorem i nie ocenia prac. W module walidacyjnym pełni wyłącznie rolę moderatora technicznego (przekazuje uczestnikom link do zewnętrznego arkusza egzaminacyjnego i nadzoruje przebieg techniczny). Trener nie ma możliwości edycji pytań, modyfikacji klucza odpowiedzi, ręcznego sprawdzania prac ani wpływania na wynik końcowy.
- 3. **Próg zaliczenia:** Minimum 80% punktów możliwych do zdobycia.
- 4. **Bezstronność i obiektywizm:** Dzięki zastosowaniu algorytmicznego sprawdzania w zewnętrznym narzędziu cyfrowym zagwarantowane jest pełne rozdzielenie funkcji dydaktycznej od funkcji walidującej oraz bezstronność oceny.

Harmonogram

Liczba pozycji harmonogramu: 46

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 46 Moduł 1. Wprowadzenie i audyt cyberbezpieczeństwa – część teoretyczna i praktyczna (współdzielenie ekranu/ćwiczenia)	Zajęcia	DOMINIK HAMERA	14-12-2026	08:00	09:15	01:15
2 z 46 Moduł 2. Podstawy prawne i zalecenia ENISA – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	14-12-2026	09:15	10:15	01:00
3 z 46 -	Przerwa	-	14-12-2026	10:15	10:30	00:15
4 z 46 Moduł 2. Podstawy prawne i zalecenia ENISA – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	14-12-2026	10:30	11:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 46 Moduł 3. Najpopularniejsze ataki cybernetyczne – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	14-12-2026	11:30	12:30	01:00
6 z 46 -	Przerwa	-	14-12-2026	12:30	13:00	00:30
7 z 46 Moduł 3. Najpopularniejsze ataki cybernetyczne – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	14-12-2026	13:00	14:30	01:30
8 z 46 -	Przerwa	-	14-12-2026	14:30	14:45	00:15
9 z 46 Warsztat 1. Mapa podatności organizacji – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	14-12-2026	14:45	16:00	01:15
10 z 46 Moduł 4. Przestępstwa finansowe w przestrzeni cyfrowej – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	15-12-2026	08:00	09:15	01:15
11 z 46 Moduł 5. Ćwiczenie praktyczne: Phishing – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	15-12-2026	09:15	10:15	01:00
12 z 46 -	Przerwa	-	15-12-2026	10:15	10:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 46 Moduł 6. Standardy haseł i łamanie zabezpieczeń – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	15-12-2026	10:30	11:30	01:00
14 z 46 Moduł 6. Standardy haseł i menadżery haseł – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	15-12-2026	11:30	12:30	01:00
15 z 46 -	Przerwa	-	15-12-2026	12:30	13:00	00:30
16 z 46 Warsztat 2. Ochrona poświadczeń i bezpieczny menadżer haseł – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	15-12-2026	13:00	14:30	01:30
17 z 46 -	Przerwa	-	15-12-2026	14:30	14:45	00:15
18 z 46 Audyt haseł i wycieków danych – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	15-12-2026	14:45	16:00	01:15
19 z 46 Moduł 7. 2FA, szyfrowanie i ochrona RODO – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	16-12-2026	08:00	09:15	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 46 Moduł 7. Autoryzacja 2FA i zastrzeganie PESEL – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	16-12-2026	09:15	10:15	01:00
21 z 46 -	Przerwa	-	16-12-2026	10:15	10:30	00:15
22 z 46 Moduł 8. Szyfrowanie i backup danych – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	16-12-2026	10:30	11:30	01:00
23 z 46 Moduł 8. Szyfrowanie w praktyce – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	16-12-2026	11:30	12:30	01:00
24 z 46 -	Przerwa	-	16-12-2026	12:30	13:00	00:30
25 z 46 Warsztat 3. Tworzenie i testowanie kopii zapasowych – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	16-12-2026	13:00	14:30	01:30
26 z 46 -	Przerwa	-	16-12-2026	14:30	14:45	00:15
27 z 46 Audyt ochrony danych na stanowisku – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	16-12-2026	14:45	16:00	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
28 z 46 Moduł 9. Bezpieczeństwo chmury, socjotechnika i AI – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	17-12-2026	08:00	09:15	01:15
29 z 46 Moduł 9. Detekcja ataków AI i socjotechniki – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	17-12-2026	09:15	10:15	01:00
30 z 46 -	Przerwa	-	17-12-2026	10:15	10:30	00:15
31 z 46 Moduł 10. Ochrona sprzętu i prywatności – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	17-12-2026	10:30	11:30	01:00
32 z 46 Moduł 10. Konfiguracja narzędzi prywatności i ochrony – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	17-12-2026	11:30	12:30	01:00
33 z 46 -	Przerwa	-	17-12-2026	12:30	13:00	00:30
34 z 46 Moduł 11. Reagowanie na incydenty – część teoretyczna i praktyczna (współdzielenie ekranu/ćwiczenia)	Zajęcia	DOMINIK HAMERA	17-12-2026	13:00	14:30	01:30
35 z 46 -	Przerwa	-	17-12-2026	14:30	14:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
36 z 46 Symulacja zgłoszenia incydentu – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	17-12-2026	14:45	16:00	01:15
37 z 46 Moduł 12. Kultura cyberbezpieczeństwa i dezinformacja AI – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	18-12-2026	08:00	09:15	01:15
38 z 46 Moduł 12. Fact-checking i weryfikacja informacji – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	18-12-2026	09:15	10:15	01:00
39 z 46 -	Przerwa	-	18-12-2026	10:15	10:30	00:15
40 z 46 Moduł 13. Narzędzia wzmacniające bezpieczeństwo cyfrowe – część teoretyczna (współdzielenie ekranu)	Zajęcia	DOMINIK HAMERA	18-12-2026	10:30	11:30	01:00
41 z 46 Moduł 13. Praca z narzędziami bezpieczeństwa – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	18-12-2026	11:30	12:30	01:00
42 z 46 -	Przerwa	-	18-12-2026	12:30	13:00	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
43 z 46 Moduł 14. Symulacje ataków cybernetycznych – część praktyczna (warsztaty)	Zajęcia	DOMINIK HAMERA	18-12-2026	13:00	14:30	01:30
44 z 46 -	Przerwa	-	18-12-2026	14:30	14:45	00:15
45 z 46 Podsumowanie dydaktyczne – część praktyczna (ćwiczenia)	Zajęcia	DOMINIK HAMERA	18-12-2026	14:45	15:00	00:15
46 z 46 -	Walidacja	DOMINIK HAMERA	18-12-2026	15:00	16:00	01:00

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00
w tym suma godzin zajęć	34:00
w tym suma godzin walidacji	01:00
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	46:30

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 ze 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, jeśli 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	6 543,60 PLN
Koszt przypadający na 1 uczestnika netto	5 320,00 PLN
Koszt osobogodziny brutto	163,59 PLN
Koszt osobogodziny netto	133,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

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

Komplet materiałów zostanie wysłany w wiadomości e-mail przed rozpoczęciem szkolenia do każdego z Uczestników. Będzie to skrypt wraz z prezentacją (w formacie PDF).

Warunki uczestnictwa

Wymagania formalne i sprzętowe:

- Pełnoletniość (ukończone 18 lat).
- Dostęp do komputera/laptopa z aktualną przeglądarką i połączeniem z siecią.
- Aktywna skrzynka e-mail do rejestracji w usługach cyfrowych.

Wymagania kompetencyjne i postawa:

- Elementarna umiejętność obsługi środowiska komputerowego oraz Internetu.
- Gotowość do aktywnej pracy na warsztatach i wykonywania zadań praktycznych.

Informacje dodatkowe

Informacje o podatku VAT:

- W przypadku dofinansowania usługi ze środków publicznych na poziomie co najmniej 70%, stosuje się zwolnienie z podatku VAT na podstawie aktualnych przepisów prawa (§ 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r.).
- Dla pozostałych form płatności usługa zostanie powiększona o podatek VAT według należnej stawki.

Kryteria zaliczenia:

Gwarancją ukończenia udziału w usłudze jest:

- obecność na co najmniej 80% czasu trwania modułów merytorycznych (nie uwzględniając przerw w harmonogramie),
- przystąpienie do automatycznego testu sprawdzającego wiedzę i umiejętności (walidacja).

Warunki techniczne

1. Sposób realizacji i platforma zajęć

Szkolenie odbywa się na żywo w formie wideokonferencji w środowisku **Microsoft Teams** (organizator zapewnia licencję komercyjną). Egzamin końcowy (automatycznie oceniany test) realizowany jest w aplikacji **Microsoft Forms**.

2. Sprzęt i oprogramowanie

Uczestnik powinien korzystać z komputera (stacjonarnego lub laptopa) wyposażonego w:

- procesor min. 2-rdzeniowy oraz co najmniej 4 GB RAM,
- sprawny zestaw do komunikacji audio-wideo (kamera, mikrofon, głośniki/słuchawki),
- aktualny system operacyjny (Windows 10/11, macOS, Linux lub Chrome OS),
- nowoczesną przeglądarkę internetową (np. MS Edge lub Google Chrome) z zezwoleniem na użycie kamery/mikrofonu i obsługę plików cookies.

3. Łącze internetowe

Do płynnego odbioru obrazu i dźwięku wymagany jest dostawca Internetu gwarantujący transfer na poziomie minimum 4 Mb/s (pobieranie) i 3,2 Mb/s (wysyłanie). Rekomendujemy połączenie kablowe lub silny sygnał Wi-Fi.

4. Dostęp do materiałów i wymogi e-mail

Każda osoba musi podać ważny adres e-mail, na który przesłane zostaną:

- zaproszenie wraz z odnośnikiem do wirtualnej sali w MS Teams,
- zestaw materiałów do zajęć i odnośnik do testu sprawdzającego,
- informacje o uzyskanej punktacji oraz dostęp do nagrań wideo.

Dostęp do pokoju spotkaniowego otwiera się na godzinę przed pierwszymi zajęciami i wygasa godzinę po zakończeniu całego kursu. Test w MS Forms udostępniany jest wyłącznie w czasie przewidzianym w planie na walidację.

5. Test techniczny przed startem

Przed pierwszym modułem uczestnik zobowiązany jest zweryfikować sprawność sprzętu: przetestować mikrofon, głośniki, kamerę, stabilność Internetu oraz możliwość otwarcia linków do MS Teams i MS Forms.

Kontakt



DOMINIK HAMERA

E-mail office@hameracapital.eu

Telefon (+48) 888 677 422