

**CEH - Certified Ethical Hacker v13 AI**

Numer usługi 2026/06/01/17164/3601467

10 196,70 PLN brutto

8 290,00 PLN netto

254,92 PLN brutto/h

207,25 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Dagma sp. z o.o.

★★★★★ 4,5 / 5

461 ocen

📍 Katowice

🏢 Usługa szkoleniowa

📄 mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

👥 Zajęcia grupowe

🕒 40:00 h

📅 13.07.2026 do 17.07.2026

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie skierowane do pracowników sektora IT, w tym administratorów sieci, osób odpowiedzialnych za infrastrukturę informatyczną, tzw. security officers, audytorów, specjalistów ds. bezpieczeństwa informatycznego, administratorów witryn oraz każdego, kto planuje podniesienie poziomu bezpieczeństwa informatycznego swojej organizacji.

Minimalna liczba uczestników

5

Maksymalna liczba uczestników

12

Data zakończenia rekrutacji

06-07-2026

Forma prowadzenia usługi

mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

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 jest dostarczenie kompetencji, dzięki którym uczestnik będzie samodzielnie dokonywał kontrolowanych włamań do systemu „ofiary”, identyfikował słabe punkty organizacji, skanował, testował i przełamывał zabezpieczenia

systemów. Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekty dotyczące wiedzy: Uczestnik stosuje obowiązujące normy i standardy bezpieczeństwa.	Tworzy polityki na urządzeniach IDS/IPS dotyczących wykrywania włamań.	Obserwacja w warunkach symulowanych
Efekty dotyczące umiejętności: Uczestnik zapobiega metodom eskalacji uprawnień w systemach firmowych.	Skanuje, testuje i przełamuje zabezpieczenia systemów	Obserwacja w warunkach symulowanych
Efekty dotyczące wiedzy: uczestnik poprawnie identyfikuje podstawowe pojęcia	Uczestnik uzyska min. 80% poprawnych odpowiedzi na teście wiedzy teoretycznej	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyraźnie 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 wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1 Wprowadzenie do „Etycznego Hackingu - zajęcia teoretyczne (wykład)

Moduł 2 Wstępne zbieranie informacji o celu ataku - zajęcia teoretyczne (wykład)

Moduł 3 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci - zajęcia praktyczne (ćwiczenia)

- Aktywne odpytywanie usług/systemów w celu rozpoznania słabych punktów w infrastrukturze

Moduł 4 Enumeracja - zajęcia teoretyczne (wykład)

Moduł 5 Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru - zajęcia teoretyczne (wykład)

- Włamywanie się do systemów („Hakowanie” systemów)

Moduł 6 SYSTEM HACKING - zajęcia praktyczne (ćwiczenia)

- Zagrożenia malware – rodzaje niebezpiecznego oprogramowania i mechanizmy działania

Moduł 7 Podśluchiwanie sieci – przechwytywanie danych - zajęcia praktyczne (ćwiczenia)

Moduł 8 Socjotechniki (Inżynieria społeczna) - zajęcia teoretyczne (wykład)

Moduł 9 Ataki na odmowę dostępu do usługi - zajęcia teoretyczne (wykład)

Moduł 10 Przechwytywanie sesji – przejęcie komunikacji między ofiarą a systemem docelowym - zajęcia praktyczne (ćwiczenia)

Moduł 11 Omijanie systemów IDS, firewall’i, honeypot’ów - zajęcia praktyczne (ćwiczenia)

- Atakowanie serwerów webowych

Moduł 12 Atakowanie aplikacji webowych - zajęcia teoretyczne (wykład)

- SQL Injection – ataki z wykorzystaniem braku odpowiedniego filtrowania zapytań baz danych SQL

Moduł 13 Włamywanie się do sieci bezprzewodowych - zajęcia praktyczne (ćwiczenia)

Moduł 14 Hakowanie platform i urządzeń mobilnych - zajęcia praktyczne (ćwiczenia)

- Hakowanie "Internetu Rzeczy" (IoT)

Moduł 15 Koncepcje i bezpieczeństwo rozwiązań chmurowych (cloud computing) - zajęcia praktyczne (ćwiczenia)

- CRYPTOGRAPHY - Kryptografia
- **Walidacja**
- walidacja jest wliczona w czas szkolenia

Harmonogram

Liczba pozycji harmonogramu: 30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
<div style="background-color: #e00000; color: white; padding: 2px; display: inline-block;">1 z 30</div> Moduł 1 Wprowadzenie do „Etycznego Hackingu” - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	13-07-2026	09:00	10:30	01:30	Tak
<div style="background-color: #e00000; color: white; padding: 2px; display: inline-block;">2 z 30</div> -	Przerwa	-	13-07-2026	10:30	10:45	00:15	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
3 z 30 Moduł 2 Wstępne zbieranie informacji o celu ataku - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	13-07-2026	10:45	13:00	02:15	Tak
4 z 30 -	Przerwa	-	13-07-2026	13:00	13:30	00:30	Tak
5 z 30 Moduł 3 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	13-07-2026	13:30	16:00	02:30	Tak
6 z 30 -	Przerwa	-	13-07-2026	16:00	16:15	00:15	Tak
7 z 30 Moduł 3 Skanowanie sieci - identyfikacja systemów, portów, usług działających w sieci - zajęcia praktyczne (ćwiczenia cz 2)	Zajęcia	Tomasz Gębicki	13-07-2026	16:15	17:00	00:45	Tak
8 z 30 Moduł 4 Enumeracja - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	14-07-2026	09:00	10:30	01:30	Tak
9 z 30 -	Przerwa	-	14-07-2026	10:30	10:45	00:15	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
10 z 30 Moduł 5 Analiza podatności - omówienie narzędzi do wykonywania skanowania oraz kryteriów ich doboru - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	14-07-2026	10:45	13:00	02:15	Tak
11 z 30 -	Przerwa	-	14-07-2026	13:00	13:30	00:30	Tak
12 z 30 Moduł 6 SYSTEM HACKING - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	14-07-2026	13:30	16:45	03:15	Tak
13 z 30 -	Przerwa	-	14-07-2026	16:45	17:00	00:15	Tak
14 z 30 Moduł 7 Podśluchiwanie sieci – przechwytywanie danych - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	15-07-2026	09:00	11:15	02:15	Tak
15 z 30 -	Przerwa	-	15-07-2026	11:15	11:30	00:15	Tak
16 z 30 Moduł 8 Socjotechniki (Inżynieria społeczna) - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	15-07-2026	11:30	13:00	01:30	Tak
17 z 30 -	Przerwa	-	15-07-2026	13:00	13:30	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
18 z 30 Moduł 9 Ataki na odmowę dostępu do usługi - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	15-07-2026	13:30	16:45	03:15	Tak
19 z 30 -	Przerwa	-	15-07-2026	16:45	17:00	00:15	Tak
20 z 30 Moduł 10 Przechwytywanie sesji – przejęcie komunikacji i między ofiarą a systemem docelowym - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	16-07-2026	09:00	10:45	01:45	Tak
21 z 30 -	Przerwa	-	16-07-2026	10:45	11:00	00:15	Tak
22 z 30 Moduł 11 Omijanie systemów IDS, firewall'i, honeypot'ów - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	16-07-2026	11:00	13:00	02:00	Tak
23 z 30 -	Przerwa	-	16-07-2026	13:00	13:45	00:45	Tak
24 z 30 Moduł 12 Atakowanie aplikacji webowych - zajęcia teoretyczne (wykład)	Zajęcia	Tomasz Gębicki	16-07-2026	13:45	17:00	03:15	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
25 z 30 Moduł 13 Włamywani e się do sieci bezprzewo dowych - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	17-07-2026	09:00	11:00	02:00	Tak
26 z 30 Moduł 14 Hakowanie platform i urządzeń mobilnych - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	17-07-2026	11:00	13:00	02:00	Tak
27 z 30 -	Przerwa	-	17-07-2026	13:00	13:45	00:45	Tak
28 z 30 Moduł 15 Koncepcje i bezpieczeń stwo rozwiązań chmurowyc h (cloud computing) - zajęcia praktyczne (ćwiczenia)	Zajęcia	Tomasz Gębicki	17-07-2026	13:45	16:30	02:45	Tak
29 z 30 -	Przerwa	-	17-07-2026	16:30	16:45	00:15	Tak
30 z 30 -	Walidacja	-	17-07-2026	16:45	17:00	00:15	Tak

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00
w tym suma godzin zajęć	34:45
w tym suma godzin walidacji	00:15
w tym suma przerw	05:00

Rodzaj godzin

Liczba godzin

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 2024 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

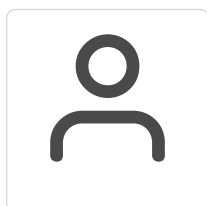
Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 196,70 PLN
Koszt przypadający na 1 uczestnika netto	8 290,00 PLN
Koszt osobogodziny brutto	254,92 PLN
Koszt osobogodziny netto	207,25 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Tomasz Gębicki

Trener IT w Dagma Szkolenia IT od 2015 roku. Quality Assurance w firmie programistycznej, specjalista, a następnie inżynier systemowy. Prowadzący szkolenia z dziedziny cyberbezpieczeństwa, w tym autoryzowanych szkoleń CEH oraz ESET. Obszar specjalizacji: Aplikacje typu Antywirus, szyfrowanie, DLP, MDM, Antyspam dla serwera pocztowego. Certyfikowany

trener CEH oraz produktów ESET. Wykształcenie: wyższe, magister inżynier Informatyki. Absolwent Politechniki Śląskiej na wydziale AEI w Gliwicach.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (materiały dydaktyczne dostępne na platformie EC COUNCIL, do których dostęp jest przesyłany na e-mail uczestnika)
- dostęp do przygotowanego środowiska wirtualnego (dane dostępowe przesłane na wskazany przez uczestnika adres e-mail)

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową <https://szkolenia.dagma.eu/pl> w celu rezerwacji miejsca.

Wymagania sprzętowe:

- komputer z aktualnym systemem operacyjnym Microsoft Windows lub macOS.
- aktualna wersja przeglądarki internetowej zgodnej z HTML5,

Opcjonalnie:

- minimalna rozdzielczość ekranu 1920 x 1080,
- tablet lub inne urządzenie, na którym będziesz mógł przeglądać materiały.

Informacje dodatkowe

- W cenę szkolenia nie wchodzi koszty związane z dojazdem, wyżywieniem oraz noclegiem.
- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA Sp. z o.o.
- Podstawa zwolnienia z VAT: dofinansowanie w co najmniej 70% - zgodnie z treścią § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)

Warunki techniczne

WARUNKI TECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM**

- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępnić sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: <https://szkolenia.dagma.eu/pl/training-list>

Adres

ul. Bażantów 6a/3

40-668 Katowice

woj. śląskie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi

Kontakt



Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 32 7931 180