

**CEH - Certified Ethical Hacker v13 AI**

Numer usługi 2026/01/13/17164/3254175

8 966,70 PLN brutto
7 290,00 PLN netto
224,17 PLN brutto/h
182,25 PLN netto/h

Dagma sp. z o.o.

★★★★★ 4,5 / 5

454 oceny

- 📄 Usługa szkoleniowa
- 📄 zdalna w czasie rzeczywistym
- 🕒 40:00 h
- 📅 18.05.2026 do 22.05.2026

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	11-05-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	40
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 kompetencji społecznych: uczestnik buduje relacje społeczne.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny

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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1: Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)

Moduł 2: Zbieranie informacji o ataku (Footprinting and Reconnaissance)

Moduł 3: Skanowanie sieci (Scanning Networks)

Moduł 4: Enumeracja (Enumeration)

Moduł 5: Analiza podatności (Vulnerability Analysis)

Moduł 6: Hackowanie systemu (System Hacking)

Moduł 7: Złośliwe oprogramowanie (Malware Threats)

Moduł 8: Monitorowanie i przechwytywanie danych (Sniffing)

Moduł 9: Inżynieria społeczna – socjotechnika (Social Engineering)

Moduł 10: Ataki DDoS (Denial-of-Service)

Moduł 11: Przejęcie/przechwytywanie sesji (Session Hijacking)

Moduł 12: Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)

Moduł 13: Hakowanie serwerów sieciowych (Hacking Web Servers)

Moduł 14: Hakowanie aplikacji internetowych (Hacking Web Applications)

Moduł 15: Ataki przez zapytania w SQL (SQL Injection)

Moduł 16: Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)

Moduł 17: Hakowanie mobilnych platform (Hacking Mobile Platforms)

Moduł 18: Hakowanie Internetu Rzeczy (IoT Hacking)

Moduł 19: Bezpieczeństwo chmury (Cloud Computing)

Moduł 20: Kryptografia (Cryptography)

- Walidacja

Razem 40 godzin lekcyjnych, (30 godzin zegarowych):

- walidacja jest wliczona w czas szkolenia / przerwy
- nie są
- wliczone w czas trwania szkolenia.

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Moduł 1-2	Tomasz Gębicki	18-05-2026	09:00	13:00	04:00
2 z 16 Przerwa obiadowa	Tomasz Gębicki	18-05-2026	13:00	13:30	00:30
3 z 16 Moduł 3-4	Tomasz Gębicki	18-05-2026	13:30	17:00	03:30
4 z 16 Moduł 5-6	Tomasz Gębicki	19-05-2026	09:00	13:00	04:00
5 z 16 Przerwa obiadowa	Tomasz Gębicki	19-05-2026	13:00	13:30	00:30
6 z 16 Moduł 7-8	Tomasz Gębicki	19-05-2026	13:30	17:00	03:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 16 Moduł 9-11	Tomasz Gębicki	20-05-2026	09:00	13:00	04:00
8 z 16 Przerwa obiadowa	Tomasz Gębicki	20-05-2026	13:00	13:30	00:30
9 z 16 Moduł 12-13	Tomasz Gębicki	20-05-2026	13:30	17:00	03:30
10 z 16 Moduł 14-15	Tomasz Gębicki	21-05-2026	09:00	13:00	04:00
11 z 16 Przerwa obiadowa	Tomasz Gębicki	21-05-2026	13:00	13:30	00:30
12 z 16 Moduł 16-17	Tomasz Gębicki	21-05-2026	13:30	17:00	03:30
13 z 16 Moduł 18-19	Tomasz Gębicki	22-05-2026	09:00	13:00	04:00
14 z 16 Przerwa obiadowa	Tomasz Gębicki	22-05-2026	13:00	13:30	00:30
15 z 16 Moduł 20	Tomasz Gębicki	22-05-2026	13:30	16:45	03:15
16 z 16 Walidacja	-	22-05-2026	16:45	17:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 966,70 PLN
Koszt przypadający na 1 uczestnika netto	7 290,00 PLN
Koszt osobogodziny brutto	224,17 PLN
Koszt osobogodziny netto	182,25 PLN

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

- **Jedna godzina szkolenia to 45 minut**
- W cenę szkolenia nie wchodzi koszt związany 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>

Kontakt



Mateusz Szwarc

E-mail szwarc.m@damga.pl

Telefon (+48) 539 069 649