Możliwość dofinansowania

Certified Ethical Hacker (CEH) v13 - ELITE

Numer usługi 2026/02/05/202681/3311174

9 999,90 PLN brutto
8 130,00 PLN netto
250,00 PLN brutto/h
203,25 PLN netto/h
261,33 PLN cena rynkowa

KRZYSZTOF BIŃKOWSKI NET COMPUTER

Brak ocen dla tego dostawcy

Warszawa
Usługa szkoleniowa
mieszana (stacjonarna połączona z usługą zdalną 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 EC-Council CEH to flagowy program dla specjalistów IT, którzy chcą poznać narzędzia cyberprzestępców, aby skuteczniej chronić infrastrukturę. Główną grupą docelową są administratorzy sieci i systemów oraz inżynierowie wsparcia IT, dla których zrozumienie wektorów ataków jest kluczowe w proaktywnym łataniu luk. Kurs to również fundament rozwoju dla przyszłych pentesterów i analityków w zespołach SOC (Security Operations Center). Z wiedzy z zakresu ofensywnego bezpieczeństwa korzystają audytorzy IT, oficerowie bezpieczeństwa oraz konsultanci oceniający ryzyko technologiczne. Spojrzenie na system z perspektywy atakującego pozwala im rzetelnie weryfikować wdrożone zabezpieczenia. Od kandydatów oczekuje się praktycznych podstaw administracji sieciami (np. TCP/IP) oraz systemami Windows i Linux.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	15-05-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną 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

Szkolenie Certified Ethical Hacker (CEH) v13 przygotowuje do samodzielnego planowania i przeprowadzania testów penetracyjnych infrastruktury IT z wykorzystaniem narzędzi wspieranych przez sztuczną inteligencję (AI). Uczestnik będzie gotowy do identyfikacji podatności, oceny ryzyka oraz wdrażania środków zaradczych przeciwko nowoczesnym cyberzagrożeniom.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik zna i rozumie wektory ataków na systemy informatyczne oraz fazy procesu etycznego hackingu (rozpoznanie, skanowanie, uzyskanie dostępu, utrzymanie dostępu, zacieranie śladów).	Uczestnik potrafi poprawnie zdefiniować wszystkie 5 faz etycznego hackingu oraz wskazać różnice pomiędzy poszczególnymi rodzajami złośliwego oprogramowania i atakami sieciowymi.	Test teoretyczny
Uczestnik potrafi przeprowadzić skanowanie podatności sieci i systemów przy użyciu dedykowanych narzędzi (np. Nmap) w celu identyfikacji luk w zabezpieczeniach.	Uczestnik samodzielnie konfiguruje i uruchamia skanowanie wybranej puli adresów IP, a następnie na podstawie wyników poprawnie identyfikuje otwarte porty, uruchomione usługi oraz potencjalne podatności.	Obserwacja w warunkach symulowanych
Uczestnik umie zastosować techniki przełamywania zabezpieczeń aplikacji webowych (np. ataki SQL Injection, XSS) oraz systemów operacyjnych.	Uczestnik skutecznie wykorzystuje lukę w zabezpieczeniach testowej aplikacji lub maszyny wirtualnej, uzyskując zaplanowany, nieautoryzowany dostęp do danych w wyznaczonym czasie.	Obserwacja w warunkach symulowanych
Uczestnik potrafi ocenić ryzyko biznesowe wynikające ze znalezionych podatności oraz zaproponować rekomendacje naprawcze zgodnie z zasadami etyki "białego wywiadu" (White Hat).	Uczestnik w sposób zrozumiały przedstawia wpływ zidentyfikowanych zagrożeń na ciągłość działania organizacji oraz proponuje adekwatne metody ich mitygacji (złagodzenia).	Prezentacja
		Wywiad ustrukturyzowany

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: https://www.eccouncil.org

Informacje

Nazwa Podmiotu prowadzącego walidację	Nazwa: EC-Council (lub International Council of E-Commerce Consultants) Kraj: USA (Stany Zjednoczone) Adres strony www: www.eccouncil.org
Nazwa Podmiotu certyfikującego	Nazwa: EC-Council (lub International Council of E-Commerce Consultants) Kraj: USA (Stany Zjednoczone) Adres strony www: www.eccouncil.org

Program

Zakres wiedzy omawiany na szkoleniu:

- **Module 01: Introduction to Ethical Hacking** (Wprowadzenie do etycznego hacking-u)
- **Module 02: Footprinting and Reconnaissance** (Footprinting i rekonesans / Zbieranie informacji o celu)
- **Module 03: Scanning Networks** (Skanowanie sieci)
- **Module 04: Enumeration** (Enumeracja / Wyliczanie zasobów sieciowych)
- **Module 05: Vulnerability Analysis** (Analiza podatności)
- **Module 06: System Hacking** (Hacking systemowy)
- **Module 07: Malware Threats** (Zagrożenia ze strony złośliwego oprogramowania)
- **Module 08: Sniffing** (Sniffing / Podsłuch ruchu sieciowego)
- **Module 09: Social Engineering** (Socjotechnika)
- **Module 10: Denial-of-Service** (Ataki typu DoS/DDoS – odmowa usługi)
- **Module 11: Session Hijacking** (Przejmowanie sesji)
- **Module 12: Evading IDS, Firewalls, and Honeypots** (Omijanie systemów IDS, firewalli i honeypotów)
- **Module 13: Hacking Web Servers** (Hacking serwerów WWW)
- **Module 14: Hacking Web Applications** (Hacking aplikacji internetowych)
- **Module 15: SQL Injection** (Wstrzykiwanie kodu SQL)
- **Module 16: Hacking Wireless Networks** (Hacking sieci bezprzewodowych)
- **Module 17: Hacking Mobile Platforms** (Hacking platform mobilnych)
- **Module 18: IoT Hacking** (Hacking internetu rzeczy - IoT)
- **Module 19: Cloud Computing** (Przetwarzanie w chmurze / Bezpieczeństwo chmury)
- **Module 20: Cryptography** (Kryptografia)

Harmonogram

Liczba pozycji harmonogramu: 0

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
Brak wyników.						

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 999,90 PLN
Koszt przypadający na 1 uczestnika netto	8 130,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	203,25 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Krzysztof Bińkowski

Autoryzowany trener/instruktor Ec-Council.
CEI - Certified Ec-Council Instructor (od 2014r.)

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- Szkolenie w języku polskim.
- Materiały szkoleniowe w języku angielskim.
- Egzamin w języku angielskim.

Egzamin 312-50 (ECC EXAM):

Po szkoleniu uczestnik otrzymuje voucher na **bezpłatny** egzamin w centrum ECC

Na egzamin można umówić się do ośrodka Netcomputer w Warszawie kontaktując się na szkolenia@netcomputer.pl

- Liczba pytań: 125
- Czas trwania: 4 godziny
- Format testu: pytania pojedyncze i wielokrotnego wyboru
- Exam Prefix: 312-50 (ECC EXAM)
- Termin ważności: **Rok od otrzymania vouchera**

Warunki uczestnictwa

- Silnie rekomendowana znajomość podstaw informatyki oraz sieci.
- Rekomendowane co najmniej dwa lata doświadczenia w zakresie cyberbezpieczeństwa.

Warunki techniczne

Szkolenie jest prowadzone w formie BYOD (Bring Your Own Device).

Wymagany jest komputer z dostępem do:

- Internetu,
- platformy MS Teams.

Adres

ul. Daniszewska 27/117

03-230 Warszawa

woj. mazowieckie

Udogodnienia w miejscu realizacji usługi

- Klimatyzacja
- Wi-fi
- Laboratorium komputerowe
- Bezpłatny parking przed budynkiem

Kontakt

Krzysztof Bińkowski

E-mail szkolenia@netcomputer.pl

Telefon (+48) 516 502 351