Możliwość dofinansowania

Certified Ethical Hacker (CEH) v13 - ELITE

Numer usługi 2026/06/12/202681/3623784

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)
- Zajęcia grupowe
- 40:00 h
- 27.07.2026 do 31.07.2026

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	25-07-2026
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

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: 62

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 62 01: Introduction to Ethical Hacking (Wprowadzenie do etycznego hacking-u)	Zajęcia	Krzysztof Bińkowski	27-07-2026	09:00	10:00	01:00	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
2 z 62 02: Footprinting and Reconnaissance (Footprinting i rekonesans / Zbieranie informacji o celu)	Zajęcia	Krzysztof Bińkowski	27-07-2026	10:00	10:45	00:45	Tak
3 z 62 -	Przerwa	-	27-07-2026	10:45	11:00	00:15	Tak
4 z 62 02: Footprinting and Reconnaissance (Footprinting i rekonesans / Zbieranie informacji o celu) - Laboratorium	Zajęcia	Krzysztof Bińkowski	27-07-2026	11:00	12:15	01:15	Tak
5 z 62 03: Scanning Networks (Skanowanie sieci)	Zajęcia	Krzysztof Bińkowski	27-07-2026	12:15	13:00	00:45	Tak
6 z 62 -	Przerwa	-	27-07-2026	13:00	13:30	00:30	Tak
7 z 62 03: Scanning Networks (Skanowanie sieci) - Laboratorium	Zajęcia	Krzysztof Bińkowski	27-07-2026	13:30	14:45	01:15	Tak
8 z 62 04: Enumeration (Enumeracja / Wyliczanie zasobów sieciowych)	Zajęcia	Krzysztof Bińkowski	27-07-2026	14:45	15:15	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
9 z 62 -	Przerwa	-	27-07-2026	15:15	15:30	00:15	Tak
10 z 62 04: Enumeration (Enumeracja / Wyliczanie zasobów sieciowych) - Laboratorium	Zajęcia	Krzysztof Bińkowski	27-07-2026	15:30	16:30	01:00	Tak
11 z 62 05: Vulnerability Analysis (Analiza podatności)	Zajęcia	Krzysztof Bińkowski	27-07-2026	16:30	17:00	00:30	Tak
12 z 62 05: Vulnerability Analysis (Analiza podatności) - Laboratorium	Zajęcia	Krzysztof Bińkowski	28-07-2026	09:00	09:45	00:45	Tak
13 z 62 06: System Hacking (Hacking systemowy)	Zajęcia	Krzysztof Bińkowski	28-07-2026	09:45	10:45	01:00	Tak
14 z 62 -	Przerwa	-	28-07-2026	10:45	11:00	00:15	Tak
15 z 62 06: System Hacking (Hacking systemowy)	Zajęcia	Krzysztof Bińkowski	28-07-2026	11:00	12:00	01:00	Tak
16 z 62 06: System Hacking (Hacking systemowy) - Laboratorium	Zajęcia	Krzysztof Bińkowski	28-07-2026	12:00	13:00	01:00	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
17 z 62 -	Przerwa	-	28-07-2026	13:00	13:30	00:30	Tak
18 z 62 06: System Hacking (Hacking systemowy) - Laboratorium	Zajęcia	Krzysztof Bińkowski	28-07-2026	13:30	15:00	01:30	Tak
19 z 62 07: Malware Threats (Zagrożenia ze strony złośliwego oprogramowania)	Zajęcia	Krzysztof Bińkowski	28-07-2026	15:00	15:15	00:15	Tak
20 z 62 -	Przerwa	-	28-07-2026	15:15	15:30	00:15	Tak
21 z 62 07: Malware Threats (Zagrożenia ze strony złośliwego oprogramowania)	Zajęcia	Krzysztof Bińkowski	28-07-2026	15:30	16:00	00:30	Tak
22 z 62 07: Malware Threats (Zagrożenia ze strony złośliwego oprogramowania) - Laboratorium	Zajęcia	Krzysztof Bińkowski	28-07-2026	16:00	17:00	01:00	Tak
23 z 62 08: Sniffing (Sniffing / Podsłuch ruchu sieciowego)	Zajęcia	Krzysztof Bińkowski	29-07-2026	09:00	09:30	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
24 z 62 08: Sniffing (Sniffing / Podsłuch ruchu sieciowego) - Laboratorium	Zajęcia	Krzysztof Bińkowski	29-07-2026	09:30	10:00	00:30	Tak
25 z 62 09: Social Engineering (Socjotechnika)	Zajęcia	Krzysztof Bińkowski	29-07-2026	10:00	10:30	00:30	Tak
26 z 62 09: Social Engineering (Socjotechnika) - Laboratorium	Zajęcia	Krzysztof Bińkowski	29-07-2026	10:30	10:45	00:15	Tak
27 z 62 -	Przerwa	-	29-07-2026	10:45	11:00	00:15	Tak
28 z 62 10: Denial-of-Service (Ataki typu DoS/DDoS – odmowa usługi)	Zajęcia	Krzysztof Bińkowski	29-07-2026	11:00	11:30	00:30	Tak
29 z 62 10: Denial-of-Service (Ataki typu DoS/DDoS – odmowa usługi) - Laboratorium	Zajęcia	Krzysztof Bińkowski	29-07-2026	11:30	12:00	00:30	Tak
30 z 62 11: Session Hijacking (Przejmowanie sesji)	Zajęcia	Krzysztof Bińkowski	29-07-2026	12:00	12:30	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
31 z 62 11: Session Hijacking (Przejmowanie sesji) - Laboratorium	Zajęcia	Krzysztof Bińkowski	29-07-2026	12:30	13:00	00:30	Tak
32 z 62 -	Przerwa	-	29-07-2026	13:00	13:30	00:30	Tak
33 z 62 12: Evading IDS, Firewalls, and Honeypots (Omijanie systemów IDS, firewalli i honeypotów)	Zajęcia	Krzysztof Bińkowski	29-07-2026	13:30	14:30	01:00	Tak
34 z 62 12: Evading IDS, Firewalls, and Honeypots (Omijanie systemów IDS, firewalli i honeypotów) - Laboratorium	Zajęcia	Krzysztof Bińkowski	29-07-2026	14:30	15:15	00:45	Tak
35 z 62 -	Przerwa	-	29-07-2026	15:15	15:30	00:15	Tak
36 z 62 13: Hacking Web Servers (Hacking serwerów WWW)	Zajęcia	Krzysztof Bińkowski	29-07-2026	15:30	17:00	01:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
37 z 62 13: Hacking Web Servers (Hacking serwerów WWW) - Laboratorium	Zajęcia	Krzysztof Bińkowski	30-07-2026	09:00	09:45	00:45	Tak
38 z 62 14: Hacking Web Applications (Hacking aplikacji internetowych)	Zajęcia	Krzysztof Bińkowski	30-07-2026	09:45	10:45	01:00	Tak
39 z 62 -	Przerwa	-	30-07-2026	10:45	11:00	00:15	Tak
40 z 62 14: Hacking Web Applications (Hacking aplikacji internetowych) - Laboratorium	Zajęcia	Krzysztof Bińkowski	30-07-2026	11:00	12:30	01:30	Tak
41 z 62 15: SQL Injection (Wstrzykiwanie kodu SQL)	Zajęcia	Krzysztof Bińkowski	30-07-2026	12:30	13:00	00:30	Tak
42 z 62 -	Przerwa	-	30-07-2026	13:00	13:30	00:30	Tak
43 z 62 15: SQL Injection (Wstrzykiwanie kodu SQL)	Zajęcia	Krzysztof Bińkowski	30-07-2026	13:30	14:00	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
44 z 62 15: SQL Injection (Wstrzykiwanie kodu SQL) - Laboratorium	Zajęcia	Krzysztof Bińkowski	30-07-2026	14:00	14:45	00:45	Tak
45 z 62 16: Hacking Wireless Networks (Hacking sieci bezprzewodowych)	Zajęcia	Krzysztof Bińkowski	30-07-2026	14:45	15:15	00:30	Tak
46 z 62 -	Przerwa	-	30-07-2026	15:15	15:30	00:15	Tak
47 z 62 16: Hacking Wireless Networks (Hacking sieci bezprzewodowych) - Laboratorium	Zajęcia	Krzysztof Bińkowski	30-07-2026	15:30	16:00	00:30	Tak
48 z 62 17: Hacking Mobile Platforms (Hacking platform mobilnych)	Zajęcia	Krzysztof Bińkowski	30-07-2026	16:00	17:00	01:00	Tak
49 z 62 17: Hacking Mobile Platforms (Hacking platform mobilnych) - Laboratorium	Zajęcia	Krzysztof Bińkowski	31-07-2026	09:00	10:00	01:00	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
50 z 62 18: IoT Hacking (Hacking internetu rzeczy - IoT)	Zajęcia	Krzysztof Bińkowski	31-07-2026	10:00	10:45	00:45	Tak
51 z 62 -	Przerwa	-	31-07-2026	10:45	11:00	00:15	Tak
52 z 62 18: IoT Hacking (Hacking internetu rzeczy - IoT)	Zajęcia	Krzysztof Bińkowski	31-07-2026	11:00	11:30	00:30	Tak
53 z 62 18: IoT Hacking (Hacking internetu rzeczy - IoT) - Laboratorium	Zajęcia	Krzysztof Bińkowski	31-07-2026	11:30	12:15	00:45	Tak
54 z 62 19: Cloud Computing (Przetwarzanie w chmurze / Bezpieczeństwo chmury)	Zajęcia	Krzysztof Bińkowski	31-07-2026	12:15	13:00	00:45	Tak
55 z 62 -	Przerwa	-	31-07-2026	13:00	13:30	00:30	Tak
56 z 62 19: Cloud Computing (Przetwarzanie w chmurze / Bezpieczeństwo chmury)	Zajęcia	Krzysztof Bińkowski	31-07-2026	13:30	14:00	00:30	Tak

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
57 z 62 19: Cloud Computing (Przetwarzanie w chmurze / Bezpieczeństwo chmury) - Laboratorium	Zajęcia	Krzysztof Bińkowski	31-07-2026	14:00	14:45	00:45	Tak
58 z 62 20: Cryptography (Kryptografia)	Zajęcia	Krzysztof Bińkowski	31-07-2026	14:45	15:15	00:30	Tak
59 z 62 -	Przerwa	-	31-07-2026	15:15	15:30	00:15	Tak
60 z 62 20: Cryptography (Kryptografia)	Zajęcia	Krzysztof Bińkowski	31-07-2026	15:30	16:00	00:30	Tak
61 z 62 20: Cryptography (Kryptografia) - Laboratorium	Zajęcia	Krzysztof Bińkowski	31-07-2026	16:00	16:45	00:45	Tak
62 z 62 -	Walidacja	-	31-07-2026	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
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 za 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	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	1,23 PLN
W tym koszt walidacji netto	1,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

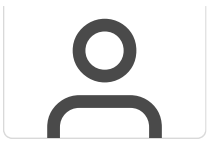
Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

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 pojedyczne 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