Możliwość dofinansowania

Certified Ethical Hacker (CEH)® v13 AI - akredytowane szkolenie z egzaminem (S_52172)

Numer usługi 2026/03/07/7629/3388146

8 597,70 PLN brutto
6 990,00 PLN netto
268,68 PLN brutto/h
218,44 PLN netto/h
261,33 PLN cena rynkowa

ASSECO DATA SYSTEMS SPÓŁKA AKCYJNA

4,4 / 5

154 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
32:00 h
22.06.2026 do 25.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	• Specjaliści ds. cyberbezpieczeństwa i osoby aspirujące do tej roli • Administratorzy sieci • Administratorzy odpowiedzialni za infrastrukturę IT • Inżynierzy systemowi • Pracownicy SOC • Administratorzy witryn www • Pracownicy IT chcący rozwijać swoją karierę dzięki najbardziej pożądanemu certyfikatowi bezpieczeństwa cybernetycznego na świecie – Certified Ethical Hacker • Typowe role zawodowe dla CEH: Security/ Cybersecurity Auditor; Security/ IT Security Administrator; Cyber Defense Analyst; Vulnerability Assessment Analyst; Warning Analyst; Security / Cybersecurity Analyst; Network Security Engineer; SOC Security Analyst; Security/ Cybersecurity Consultant; Information Security Manager; Solution Architect.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	15-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
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 rozwój kompetencji uczestników w zakresie identyfikowania podatności, analizowania zagrożeń oraz stosowania technik testów penetracyjnych i etycznego hackingu w celu oceny poziomu bezpieczeństwa systemów informatycznych i sieci. Uczestnicy poznają metody wykorzystywane przez cyberprzestępców oraz sposoby ich wykrywania i przeciwdziałania, zgodnie ze standardem zdefiniowanym w programie Certified Ethical Hacker - (CEH)®.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik opisuje podstawowe koncepcje etycznego hackingu, typy cyberataków oraz metody wykorzystywane do identyfikowania podatności w systemach informatycznych.	Wyjaśnia pojęcia związane z testami penetracyjnymi i etycznym hackingiem Identyfikuje typowe techniki ataków na systemy i sieci Wskazuje etapy procesu testów penetracyjnych	Test teoretyczny
WIEDZA: Uczestnik wyjaśnia metody wykorzystywane do wykrywania podatności w infrastrukturze IT oraz znaczenie testów bezpieczeństwa dla ochrony systemów informatycznych.	Opisuje metody identyfikacji podatności w systemach i aplikacjach Wskazuje rolę testów penetracyjnych w ocenie bezpieczeństwa organizacji Wyjaśnia znaczenie monitorowania zagrożeń cybernetycznych	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik identyfikuje potencjalne podatności i zagrożenia w systemach informatycznych oraz sieciach komputerowych.	Analizuje przykładowe scenariusze ataków cybernetycznych Wskazuje możliwe luki bezpieczeństwa w infrastrukturze IT Interpretuje wyniki podstawowych narzędzi do analizy bezpieczeństwa	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik stosuje podstawowe techniki testów penetracyjnych w celu oceny poziomu bezpieczeństwa systemów informatycznych.	Dobiera narzędzia do testowania bezpieczeństwa Przeprowadza podstawową analizę podatności w środowisku testowym Formułuje wnioski dotyczące poziomu bezpieczeństwa badanych systemów	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
KOMPETECJE SPOŁECZNE: Uczestnik rozumie znaczenie etyki i odpowiedzialności w prowadzeniu testów bezpieczeństwa systemów informatycznych.	Stosuje zasady etycznego hackingu podczas analiz scenariuszy bezpieczeństwa Rozróżnia działania legalne i nielegalne w obszarze testów bezpieczeństwa Wskazuje zasady odpowiedzialnego ujawniania podatności	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik dostrzega znaczenie współpracy między zespołami IT, bezpieczeństwa i zarządzania ryzykiem w budowaniu cyberbezpieczeństwa organizacji.	Wskazuje rolę specjalistów bezpieczeństwa w organizacji Proponuje działania wspierające poprawę poziomu cyberbezpieczeństwa Formułuje rekomendacje dotyczące ograniczania ryzyka cyberzagrożeń	Test teoretyczny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

TAK

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Certified Ethical Hacker Elite v13 – 20 modułów, które pomogą Ci opanować sztuczną inteligencję, by zautomatyzować etyczne hakowanie:

- **Moduł 01**: Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking) – Learn the fundamentals and key issues in information security, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.
- **Moduł 02**: Zbieranie informacji o ataku i rekonesans (Footprinting and Reconnaissance) – Learn how to use the latest techniques and tools for footprinting and reconnaissance, a critical pre-attack phase of ethical hacking.
- **Moduł 03**: Skanowanie sieci (Scanning Networks) – Learn different network scanning techniques and countermeasures.

- **Moduł 04**: Enumeracja (Enumeration) – Learn various enumeration techniques, including Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits and associated countermeasures.
- **Moduł 05**: Analiza podatności (Vulnerability Analysis) – Learn how to identify security loopholes in a target organization's network, communication infrastructure, and end systems. Different types of vulnerability assessment and vulnerability assessment tools are also included.
- **Moduł 06**: Hakowanie systemów (System Hacking) – Learn about the various system hacking methodologies used to discover system and network vulnerabilities, including steganography, steganalysis attacks, and how to cover tracks.
- **Moduł 07**: Złośliwe oprogramowanie (Malware Threats) – Learn about different types of malware (Trojan, viruses, worms, etc.), APT and fileless malware, malware analysis procedures, and malware countermeasures.
- **Moduł 08**: Monitorowanie i przechwytywanie danych (Sniffing) – Learn about packet sniffing techniques and their uses for discovering network vulnerabilities, plus countermeasures to defend against sniffing attacks.
- **Moduł 09**: Socjotechnika (Social Engineering) – Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
- **Moduł 10**: Ataki DDoS (Denial-of-Service) – Learn about different Denial of Service (DoS) and Distributed DoS (DDoS) attack techniques, plus the tools used to audit a target and devise DoS and DDoS countermeasures and protections.
- **Moduł 11**: Przejmowanie sesji (Session Hijacking) – Learn the various session-hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures.
- **Moduł 12**: Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots) – Learn about firewalls, intrusion detection systems (IDS), and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.
- **Moduł 13**: Hakowanie serwerów sieciowych (Hacking Web Servers) – Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.
- **Moduł 14**: Hakowanie aplikacji internetowych (Hacking Web Applications) – Learn about web application attacks, including a comprehensive hacking methodology for auditing vulnerabilities in web applications and countermeasures.
- **Moduł 15**: Ataki przez zapytania w SQL (SQL Injection) – Learn about SQL injection attack techniques, evasion techniques, and SQL injection countermeasures.
- **Moduł 16**: Hakowanie sieci bezprzewodowych (Hacking Wireless Networks) – Learn about different types of encryption, threats, hacking methodologies, hacking tools, security tools, and countermeasures for wireless networks.
- **Moduł 17**: Hakowanie platform mobilnych (Hacking Mobile Platforms) – Learn mobile platform attack vectors, Android and iOS hacking, mobile device management, mobile security guidelines, and security tools.
- **Moduł 18**: Hakowanie urządzeń IoT (IoT Hacking) – Learn different types of Internet of Things (IoT) and operational technology (OT) attacks, hacking methodologies, hacking tools, and countermeasures.
- **Moduł 19**: Bezpieczeństwo chmury (Cloud Computing) – Learn different cloud computing concepts, such as container technologies and serverless computing, various cloud computing threats, attacks, hacking methodologies, and cloud security techniques and tools.
- **Moduł 20**: Kryptografia (Cryptography) – Learn about encryption algorithms, cryptography tools, Public Key Infrastructure (PKI), email encryption, disk encryption, cryptography attacks, and cryptanalysis tools.

Harmonogram

Liczba pozycji harmonogramu: 20

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 20 Moduł 01: Wprowadzenie do etycznego hakingu (Introduction to Ethical Hacking)	academy@assecods.pl	22-06-2026	09:00	10:30	01:30
2 z 20 Moduł 02: Zbieranie informacji o ataku i rekonesans (Footprinting and Reconnaissance)	academy@assecods.pl	22-06-2026	10:30	11:45	01:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 20 Moduł 03: Skanowanie sieci (Scanning Networks)	academy@assecods.pl	22-06-2026	11:45	13:00	01:15
4 z 20 Moduł 04: Enumeracja (Enumeration)	academy@assecods.pl	22-06-2026	13:00	14:15	01:15
5 z 20 Moduł 05: Analiza podatności (Vulnerability Analysis)	academy@assecods.pl	22-06-2026	14:15	15:30	01:15
6 z 20 Moduł 06: Hakowanie systemów (System Hacking)	academy@assecods.pl	23-06-2026	09:00	10:30	01:30
7 z 20 Moduł 07: Złośliwe oprogramowanie (Malware Threats)	academy@assecods.pl	23-06-2026	10:30	11:45	01:15
8 z 20 Moduł 08: Monitorowanie i przechwytywanie danych (Sniffing)	academy@assecods.pl	23-06-2026	11:45	13:00	01:15
9 z 20 Moduł 09: Socjotechnika (Social Engineering)	academy@assecods.pl	23-06-2026	13:00	14:15	01:15
10 z 20 Moduł 10: Ataki DDoS (Denial-of-Service)	academy@assecods.pl	23-06-2026	14:15	15:30	01:15
11 z 20 Moduł 11: Przejmowanie sesji (Session Hijacking)	academy@assecods.pl	24-06-2026	09:00	10:30	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 20 Moduł 12: Omijanie IDS, zapór Firewall i Honeypots (Evading IDS, Firewalls, and Honeypots)	academy@assecods.pl	24-06-2026	10:30	11:45	01:15
13 z 20 Moduł 13: Hakowanie serwerów sieciowych (Hacking Web Servers)	academy@assecods.pl	24-06-2026	11:45	13:00	01:15
14 z 20 Moduł 14: Hakowanie aplikacji internetowych (Hacking Web Applications)	academy@assecods.pl	24-06-2026	13:00	14:15	01:15
15 z 20 Moduł 15: Ataki przez zapytania w SQL (SQL Injection)	academy@assecods.pl	24-06-2026	14:15	15:30	01:15
16 z 20 Moduł 16: Hakowanie sieci bezprzewodowych (Hacking Wireless Networks)	academy@assecods.pl	25-06-2026	09:00	10:30	01:30
17 z 20 Moduł 17: Hakowanie platform mobilnych (Hacking Mobile Platforms)	academy@assecods.pl	25-06-2026	10:30	11:45	01:15
18 z 20 Moduł 18: Hakowanie urządzeń IoT (IoT Hacking)	academy@assecods.pl	25-06-2026	11:45	13:00	01:15
19 z 20 Moduł 19: Bezpieczeństwo chmury (Cloud Computing)	academy@assecods.pl	25-06-2026	13:00	14:15	01:15

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 20 Moduł 20: Kryptografia (Cryptography)	academy@assecods.pl	25-06-2026	14:15	15:30	01:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	8 597,70 PLN
Koszt przypadający na 1 uczestnika netto	6 990,00 PLN
Koszt osobogodziny brutto	268,68 PLN
Koszt osobogodziny netto	218,44 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

academy@assecods.pl

Trener z co najmniej 5 letnim doświadczeniem w prowadzeniu szkoleń, w tym z obszaru merytorycznego, którego dotyczy. W przypadku szkoleń akredytowanych i autoryzowanych nasi trenerzy posiadają stosowne uprawnienia do ich prowadzenia.

2 z 2

Koordynator walidacji efektów uczenia się

Pracownik Asseco Academy, który przeprowadza i zarządza procesem walidacji efektów uczenia w oparciu o przygotowane narzędzia diagnostyczne

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Podstawowy pakiet CEH Lite integruje wszystkie 4 etapy etycznego hakowania – Learn, Certify, Engage i Compete, i obejmuje:

- Udział w 4-dniowym akredytowanym szkoleniu Certified Ethical Hacker (CEH)® v13 prowadzonym na żywo przez trenera eksperta ds. cyberbezpieczeństwa

- Dostęp do akredytowanych materiałów szkoleniowych eCourseware przez 2 lata, w tym do nowszych wersji materiałów, gdy zostaną opublikowane
- Voucher na egzamin CEH ważny przez 12 miesięcy
- Dostęp do Ethical Hacking Video Library przez 12 miesięcy
- Zaświadczenie Asseco Academy o ukończeniu szkolenia.

Opcjonalnie do szkolenia można zakupić upgrade do pakietu **CEH Elite**, który obejmuje dodatkowo:

- Dostęp do oficjalnych laboratoriów iLabs przez 6 miesięcy
- Dostęp do platformy Live Cyber Range – CEH Engage przez 12 miesięcy
- Dostęp do zawodów CEH Global Challenge Pass przez 12 miesięcy
- Voucher na egzamin CEH Practical ważny przez 12 miesięcy
- 1 darmowe podejście do egzaminu poprawkowego CEH.

Egzamin CEH można zdać stacjonarnie w jednym z ośrodków EC-Council Test Center (wg cennika ECT) lub zdalnie po wykupieniu usługi Remote Proctoring Service (obowiązuje dodatkowa opłata do EC-Council) .

Organizacja szkolenia

- Rodzaj szkolenia: otwarte lub dla grup zamkniętych
- Forma realizacji: stacjonarnie lub zdalnie; więcej informacji: Formy Szkoleń Asseco Academy
- Język szkolenia: polski
- Język materiałów: angielski
- Wielkość grupy: do 20 uczestników

Organizacja szkolenia w Wirtualnej Klasie

- Szkolenie jest realizowane w godz. 9:00-15:30
- Każdy uczestnik powinien dokonać rejestracji do zdalnej sesji szkoleniowej w godz. 8:30-8:50
- W trakcie dnia szkoleniowego przewidujemy kilka przerw, w tym 60-minutową na lunch, a także po każdej godzinie szkolenia 10-minutowe przerwy; szczegółowy rozkład przerw każdy trener ustala indywidualnie z grupą
- Jedna godzina lekcyjna to 45 minut
- Komplet akredytowanych materiałów szkoleniowych dystrybuowany jest w formie elektronicznej.

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową https://academy.asseco.pl/szkolenie/certified-ethical-hacker-ceh-v13-ai/ w celu rezerwacji miejsca.

UWAGA! Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Asseco Academy academy@assecods.pl Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%.

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny, laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe:

- Komputer PC z systemem Windows 7 lub nowszym, Max OX 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem"). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łączy GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia.
- Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt

Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl
Telefon (+48) 801 303 030