



Ernst & Young

spółka z

ograniczoną

odpowiedzialnością

Academy of

Business sp. k.

★★★★★ 4,6 / 5

459 ocen

Cyberbezpieczeństwo – podstawy

Numer usługi 2026/07/29/10940/3717178

📅 Usługa szkoleniowa

📺 zdalna w czasie rzeczywistym

👥 Zajęcia grupowe

🕒 23:00 h

📅 26.08.2026 do 28.08.2026

4 305,00 PLN brutto

3 500,00 PLN netto

187,17 PLN brutto/h

152,17 PLN netto/h

261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Grupa docelowa usługi

Szkolenie skierowane jest do:

- Specjalistów ds. IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Dyrektorów i menedżerów pionów IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników branży IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników działów nowych technologii
- Pracowników działów zarządzania ryzykiem
- Audytorów wewnętrznych
- Audytorów systemów
- Użytkowników końcowych nowych technologii
- Pracowników biurowych.

Minimalna liczba uczestników

6

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji

21-08-2026

Forma prowadzenia usługi

zdalna 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 "Cyberbezpieczeństwo-podstawy" przygotowuje uczestników do samodzielnego reagowania na cyberzagrożenia, poprzez dokonywanie prawidłowej oceny własnych zabezpieczeń oraz wykorzystanie technik i sposobów walki z hakerami.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się podstawową wiedzą w zakresie cyberbezpieczeństwa	* identyfikuje role uczestników ekosystemu cyberbezpieczeństwa (white hat, black hat, etc.)	Test teoretyczny z wynikiem generowanym automatycznie
	* definiuje bezpieczne hasła	Test teoretyczny z wynikiem generowanym automatycznie
	* omawia metody uwierzytelnienia wieloskładnikowego	Test teoretyczny z wynikiem generowanym automatycznie
	* charakteryzuje podstawowe zasady bezpieczeństwa informacji: poufność, integralność i dostępność	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wykorzystuje techniki i sposoby walki z cyberzagrożeniem	* rozpoznaje sytuacje kiedy stosuje się szyfrowanie symetryczne, a kiedy asymetryczne	Test teoretyczny z wynikiem generowanym automatycznie
	* definiuje czym jest powierzchnia ataku i jak wpływa na bezpieczeństwo systemu	Test teoretyczny z wynikiem generowanym automatycznie
	* identyfikuje zagrożenia wynikające ze złośliwego oprogramowania	Test teoretyczny z wynikiem generowanym automatycznie
	* charakteryzuje się świadomością roli aktualizacji w ochronie systemów przed zagrożeniami	Test teoretyczny z wynikiem generowanym automatycznie
	* wdraża rozwiązania pozwalające na identyfikowanie prób manipulacji wykorzystujących techniki inżynierii społecznej	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

PROGRAM

1. Zrozumienie podstawowych zasad bezpieczeństwa

- Poufność; integralność; dostępność; wpływ zagrożenia i ryzyka; zasada najmniejszego przywileju; inżynieria społeczna; analiza powierzchni ataku; modelowanie zagrożeń

2. Zrozumienie struktur, procesów i audytów cyberbezpieczeństwa w firmie lub organizacji

- Obszary specjalizacji w zakresie cyberbezpieczeństwa; role w zespole ds. bezpieczeństwa; audyty cyberbezpieczeństwa; zasoby oraz audyty wewnętrzne i zewnętrzne

3. Zrozumienie bezpieczeństwa fizycznego

- Bezpieczeństwo obiektu; bezpieczeństwo komputera; wymienne urządzenia; kontrola dostępu; bezpieczeństwo urządzeń mobilnych; keyloggery

4. Zrozumienie bezpieczeństwa w Internecie

- Ustawienia bezpieczeństwa przeglądarki; bezpieczne strony internetowe

5. Zrozumienie bezpieczeństwa sieci bezprzewodowej

- Zalety i wady konkretnych typów zabezpieczeń; Klucze; SSID; Filtry MAC

6. Zrozumienie bezpieczeństwa komputerów

- Zrozumienie uwierzytelniania użytkowników
- Uwierzytelnianie wieloskładnikowe; fizyczne i wirtualne smart cardy; Usługa zdalnego uwierzytelniania użytkowników (RADIUS); biometria; użycie opcji „Uruchom jako”, do wykonywania zadań administracyjnych

7. Zrozumienie uprawnień

- Uprawnienia systemu plików; uprawnienia udostępniania; włączanie i wyłączanie dziedziczenia; zachowanie podczas przenoszenia lub kopiowania plików na tym samym dysku lub na inny dysk; wiele grup z różnymi uprawnieniami; uprawnienia podstawowe i uprawnienia zaawansowane; przejęcie własności; delegacja; dziedziczenie; znaczenie Registry i Active Directory;

8. Zrozumienie zasad dotyczących haseł

- Złożoność hasła; blokada konta; długość hasła; historia haseł; czas między zmianami hasła; egzekwowanie za pomocą zasad grupy; powszechne metody ataku; procedury resetowania hasła; ochrona haseł do kont użytkowników domeny

9. Zrozumienie zasad protokołowania

- Rodzaje protokołów; co może być protokołowane; włączanie protokołowania; co zapisywać w określonych celach; gdzie zapisywać informacje; jak zabezpieczać informacje

10. Zrozumienie szyfrowania

- System szyfrowania plików (EFS); wpływ folderów zaszyfrowanych przez EFS na przenoszenie / kopiowanie plików; BitLocker (To Go); TPM; szyfrowanie oparte na oprogramowaniu; Szyfrowanie i podpisywanie poczty mail; wirtualna sieć prywatna (VPN); klucz publiczny / klucz prywatny; algorytmy szyfrowania; właściwości certyfikatu; usługi certyfikujące; Infrastruktura PKI / usługi certyfikacyjne; tokeny sprzętowe, ograniczenie urządzeń, aby uruchamiały tylko zaufane aplikacje

11. Zrozumienie złożonego oprogramowania

- Przepelnienie bufora; wirusy, wirusy polimorficzne; robaki; konie trojańskie; programy szpiegujące; oprogramowanie ransomware; oprogramowanie reklamowe; rootkity; tylne drzwi; ataki zero day

12. Zrozumienie dedykowanych zapór ogniowych

- Rodzaje zapór sprzętowych i ich charakterystyka; kiedy używać zapory sprzętowej zamiast zapory opartej na oprogramowaniu; inspekcja stanowa i bezstanowa

13. Zrozumienie izolacji sieci

- Trasowanie; honeypot; sieci obwodowe; translacja adresów sieciowych (NAT); VPN; IPsec; izolacja serwerów i domen

14. Zrozumienie zabezpieczenia protokołów

- Spoofing protokołów; IPsec; tunelowanie; DNSsec; podsłuchiwanie sieci; ataki typu DoS; powszechne metody ataku

15. Zrozumienie ochrony stacji klienckich

- Antywirus; ochrona przed niechcianymi instalacjami oprogramowania; Kontrola konta użytkownika (UAC); aktualizacja systemu operacyjnego klienta i oprogramowania klienta; szyfrowanie folderów offline; zasady ograniczeń oprogramowania; zasada najmniejszego przywileju

16. Zrozumienie ochrony poczty elektronicznej

- Antyspam, oprogramowanie antywirusowe, spoofing, phishing i pharming; ochrona klienta a ochrona serwera; Rekordy Sender Policy Framework (SPF); Rekordy PTR

17. Zrozumienie ochrony serwera

- Rozdzielenie usług; hartowanie (hardening); aktualizacje serwera; bezpieczne aktualizacje dynamicznego systemu nazw domen (DNS); dezaktywacja niezabezpieczonych protokołów uwierzytelniania; Kontrolery domeny tylko do odczytu (RODC).

INFORMACJE DODATKOWE:

Szkolenie skierowane jest do:

- Specjalistów ds. IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Dyrektorów i menedżerów pionów IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników branży IT bez doświadczenia w temacie Cyberbezpieczeństwa
- Pracowników działów nowych technologii
- Pracowników działów zarządzania ryzykiem
- Audytorów wewnętrznych
- Audytorów systemów
- Użytkowników końcowych nowych technologii
- Pracowników biurowych.

Czas trwania szkolenia:

Szkolenie trwa **23 godzin zegarowych, w tym: 9 godzin stanowi część praktyczna, 9 godzin i 45 minut część teoretyczna, 30 min. walidacja.** Podana ilość godzin zegarowych szkolenia zawiera czas przerw.

Walidacja:

Po szkoleniu przeprowadzana będzie walidacja w formie testu teoretycznego. Pytania testowe przygotowane zostały przez niezależnego walidatora, zapewniając rozdzielenie funkcji uczenia od walidacji. Test przeprowadzany będzie w formie online, poprzez wykorzystanie platformy zewnętrznej. Osoba walidująca nie jest obecna w części szkoleniowej. W harmonogramie szkolenia, został wskazany przybliżony czas

przeprowadzenia walidacji usługi rozwojowej.

Informacje techniczne:

W trakcie szkolenia online korzystamy z platformy Zoom. Każdy uczestnik otrzymuje przed szkoleniem link do platformy internetowej (na wskazany adres mailowy), na której znajdować się będzie transmisja online. Uczestnictwo w streamingu nie wymaga żadnych, specjalnych oprogramowań: wystarczy, że komputer jest podłączony do Internetu (należy korzystać z przeglądarek: Google Chrome, Mozilla Firefox lub Safari). Uczestnicy oglądają i słuchają na żywo tego, co dzieje się w sali szkoleniowej oraz śledzą treści wyświetlane na komputerze prowadzącego. Dodatkowo, wszyscy mogą zadawać pytania za pośrednictwem chatu online. W przypadku mniejszych szkoleń uczestnicy mogą przez mikrofon komunikować się z trenerem i innymi uczestnikami kursu. Link do szkolenia online generowany jest przed szkoleniem i ważny jest przez cały czas trwania szkolenia (uczestnik może połączyć się w dowolnym momencie).

Podczas szkoleń online wykorzystujemy następujące funkcjonalności:

1) Praca w grupach (breakout rooms)

- trener może podzielić uczestników automatycznie lub manualnie
- trener ustala czas trwania pracy w grupach
- pojawia się krótki komunikat na ekranie uczestnika, który informuje, że gospodarz zaprasza do podpokoju
- prowadzący może wysłać wiadomość do wszystkich pokoi jednocześnie, np. z opisem zadania do wykonania.

2) Narzędzia dostępne podczas sesji w breakout rooms:

- tablica, możliwość pisania mają wszyscy uczestnicy, efekt pracy można zapisać i pokazać w pokoju szkoleniowym, wszystkim uczestnikom szkolenia
- pokazywanie ekranu, każdy uczestnik może udostępnić swój ekran
- czat
- użytkownik pracujący w pokoju, może w dowolnym momencie zaprosić prowadzącego do pokoju grupowego.

Harmonogram

Liczba pozycji harmonogramu: 26

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 26 Zrozumienie podstawowych zasad bezpieczeństwa ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	26-08-2026	09:00	10:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 26 Zrozumienie struktur, procesów i audytów cyberbezpieczeństwa w firmie lub organizacji ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	26-08-2026	10:00	11:00	01:00
3 z 26 -	Przerwa	-	26-08-2026	11:00	11:15	00:15
4 z 26 Zrozumienie bezpieczeństwa fizycznego ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	26-08-2026	11:15	13:00	01:45
5 z 26 -	Przerwa	-	26-08-2026	13:00	13:45	00:45
6 z 26 Zrozumienie bezpieczeństwa w Internecie ćwiczenia, rozmowa na żywo, chat, współdzielenie ekran	Zajęcia	Marcin Nowicki	26-08-2026	13:45	15:00	01:15
7 z 26 -	Przerwa	-	26-08-2026	15:00	15:15	00:15
8 z 26 Zrozumienie bezpieczeństwa sieci bezprzewodowej ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	26-08-2026	15:15	16:30	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 26 Zrozumienie bezpieczeństwa komputerów ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	27-08-2026	09:00	11:00	02:00
10 z 26 -	Przerwa	-	27-08-2026	11:00	11:15	00:15
11 z 26 Zrozumienie uprawnień ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	27-08-2026	11:15	13:00	01:45
12 z 26 -	Przerwa	-	27-08-2026	13:00	13:45	00:45
13 z 26 Zrozumienie zasad dotyczących haseł- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekran	Zajęcia	Marcin Nowicki	27-08-2026	13:45	15:00	01:15
14 z 26 -	Przerwa	-	27-08-2026	15:00	15:15	00:15
15 z 26 Zrozumienie zasad protokołowania ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	27-08-2026	15:15	16:30	01:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
16 z 26 Zrozumienie szyfrowania ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	09:00	10:00	01:00
17 z 26 Zrozumienie złośliwego oprogramowania ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	10:00	11:00	01:00
18 z 26 -	Przerwa	-	28-08-2026	11:00	11:15	00:15
19 z 26 Zrozumienie dedykowanych zapór ogniowych ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	11:15	12:00	00:45
20 z 26 Zrozumienie izolacji sieci ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	12:00	13:00	01:00
21 z 26 -	Przerwa	-	28-08-2026	13:00	13:45	00:45
22 z 26 Zrozumienie zabezpieczeń a protokołów ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	13:45	15:00	01:15
23 z 26 -	Przerwa	-	28-08-2026	15:00	15:15	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
24 z 26 Zrozumienie ochrony stacji klienckich. Zrozumienie ochrony poczty elektronicznej ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	15:15	16:00	00:45
25 z 26 Zrozumienie ochrony serwera ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Zajęcia	Marcin Nowicki	28-08-2026	16:00	16:30	00:30
26 z 26 -	Walidacja	-	28-08-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	23:00
w tym suma godzin zajęć	18:45
w tym suma godzin walidacji	00:30
w tym suma przerw	03:45
Suma godzin dydaktycznych bez przerw	25:30

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	4 305,00 PLN
Koszt przypadający na 1 uczestnika netto	3 500,00 PLN
Koszt osobogodziny brutto	187,17 PLN
Koszt osobogodziny netto	152,17 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	23:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Marcin Nowicki

Marcin jest absolwentem Technical University of Darmstadt, na kierunku Informatyka. Od ponad 20 lat z powodzeniem pracuje jako wykładowca, programista i usługodawca w dziedzinie IT dla firm różnej wielkości i z różnych branż w Niemczech, Polsce i wielu innych krajach na całym świecie. Posiada kompetencje w zakresie tworzenia złożonych baz danych, aplikacji i struktur Microsoft 365 oraz doradztwa, m.in. w zakresie cyberbezpieczeństwa. Dzięki współorganizacji kilku tysięcy konferencji IT w Niemczech, Holandii, Polsce, Serbii i USA, jest moderatorem wielu wydarzeń. Prowadzi również audycję radiową o tematyce informacyjno-naukowej w Radiu Darmstadt. Marcin realizował projekty szkoleniowe dla takich klientów jak: Microsoft, DHL, Lufthansa, EY, Organizacja Narodów Zjednoczonych (ONZ), Credit Agricole, Deutsche Bank, ministerstwa i organizacje rządowe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy z uczestników otrzyma komplet materiałów szkoleniowych w formie skryptu.

Warunki uczestnictwa

Ogólne warunki świadczenia usług poprzez Ernst & Young spółka z ograniczoną odpowiedzialnością Academy of Business sp. k. dostępne są na stronie: <https://www.academyofbusiness.pl/ogolne-warunki-swiadczenia-uslug-osobom-prawnym/>

Informacje dodatkowe

- Harmonogram godzinowy szkolenia każdorazowo dostosowywany jest do grupy szkoleniowej.
- Godziny realizacji poszczególnych modułów szkolenia mogą ulec zmianie.

Warunki techniczne

Do realizacji szkoleń online korzystamy z platformy Zoom. Każdy uczestnik otrzymuje przed szkoleniem link do platformy internetowej (na wskazany adres mailowy), na której znajdować się będzie transmisja online. Uczestnictwo w streamingu nie wymaga żadnych, specjalnych oprogramowań: wystarczy, że komputer jest podłączony do Internetu (należy korzystać z przeglądarek: Google Chrome, Mozilla Firefox lub Safari). Uczestnicy oglądają i słuchają na żywo tego, co dzieje się w sali szkoleniowej oraz śledzą treści wyświetlane na komputerze prowadzącego. Dodatkowo, wszyscy mogą zadawać pytania za pośrednictwem chatu online. W przypadku mniejszych szkoleń uczestnicy mogą przez mikrofon komunikować się z trenerem i innymi uczestnikami kursu. Link do szkolenia online generowany jest przed szkoleniem i ważny jest przez cały czas trwania szkolenia (uczestnik może połączyć się w dowolnym momencie).

Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji: Dwuurdzeniowy procesor Intel Core i5 2,5 GHz i wyższy

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik: pobieranie: 10 Mb/s, wysyłanie: 5 Mb/s

Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów: Nie trzeba pobierać oprogramowania. Aby wziąć udział w szkoleniu online potrzebny jest komputer, laptop, telefon lub tablet ze stabilnym internetem i bez blokad firmowych

Podczas szkoleń online wykorzystujemy następujące funkcjonalności:

1) Praca w grupach (breakout rooms)

- trener może podzielić uczestników automatycznie lub manualnie
- trener ustala czas trwania pracy w grupach
- pojawia się krótki komunikat na ekranie uczestnika, który informuje, że gospodarz zaprasza do podpokoju
- prowadzący może wysłać wiadomość do wszystkich pokoi jednocześnie, np. z opisem zadania do wykonania.

2) Narzędzia dostępne podczas sesji w breakout rooms:

- tablica, możliwość pisania mają wszyscy uczestnicy, efekt pracy można zapisać i pokazać w pokoju szkoleniowym, wszystkim uczestnikom szkolenia
- pokazywanie ekranu, każdy uczestnik może udostępnić swój ekran
- czat
- użytkownik pracujący w pokoju, może w dowolnym momencie zaprosić prowadzącego do pokoju grupowego

Usługa jest nagrywana na potrzeby ewentualnej kontroli.

W związku z tym, prosimy o włączenie kamery na czas udziału w szkoleniu. Dziękujemy.

Kontakt



Dominika Machul

E-mail dominika.machul@pl.ey.com

Telefon (+48) 502 782 693