Możliwość dofinansowania

Cyberbezpieczeństwo – podstawy

Numer usługi 2024/06/24/10940/2196379

4 305,00 PLN brutto
3 500,00 PLN netto
172,20 PLN brutto/h
140,00 PLN netto/h

Ernst & Young spółka z ograniczoną odpowiedzialnością Academy of Business sp. k.

★★★★½

zdalna w czasie rzeczywistym
Usługa szkoleniowa
25 h
27.11.2024 do 29.11.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
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	3
Maksymalna liczba uczestników	18
Data zakończenia rekrutacji	25-11-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	25

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 metody ochrony danych cyfrowych * definiuje złożone hasła dostępu do danych stosując uwierzytelnienie wieloskładnikowe * omawia rolę cyberbezpieczeństwa w audycie	Wywiad swobodny
		Obserwacja w warunkach symulowanych
Uczestnik wykorzystuje techniki i sposoby walki z cyberzagrożeniem	* tworzy i nadzoruje system szyfrowania plików * monitoruje działania złośliwego oprogramowania * przeprowadza ocenę poziomu zagrożenia własnych zabezpieczeń * projektuje rozwiązania dot. ochrony stacji komputerowych oraz pracy na przenośnych nośnikach pamięci * charakteryzuje się umiejętnością podejmowania decyzji pod wpływem stresu	Wywiad swobodny
		Obserwacja w warunkach symulowanych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się.

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

Dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji.

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

Dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji.

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 złośliwego oprogramowania

- Przepełnienie 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 tchniczne:

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.

Czas trwania szkolenia:

Szkolenie trwa **25 godziny dydaktyczne** (tj. 45 minut).

Podana ilość godzin szkolenia nie zawiera czasu przerw.

Walidacja:

W trakcie szkolenia przeprowadzana będzie walidacja w formie wywiadu swobodnego oraz obserwacji w warunkach symulowanych.

Osoba walidująca, waliduje usługę w formie zdalnej, po jej zakończeniu, w oparciu o checklistę od trenera prowadzącego usługę, a następnie potwierdza osiągnięcie efektów kształcenia swoim podpisem na zaświadczeniu o zakończeniu udziału w usłudze rozwojowej.

W harmonogramie szkolenia, został wskazany przybliżony czas przeprowadzenia walidacji usługi rozwojowej.

Harmonogram

Liczba przedmiotów/zajęć: 27

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 27 Zrozumienie podstawowych zasad bezpieczeństwa- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	09:00	10:00	01:00
2 z 27 Zrozumienie struktur, procesów i audytów cyberbezpieczeństwa w firmie lub organizacji- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	10:00	11:00	01:00
3 z 27 Przerwa	Marcin Nowicki	27-11-2024	11:00	11:15	00:15
4 z 27 Zrozumienie bezpieczeństwa fizycznego- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	11:15	12:00	00:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 27 Zrozumienie bezpieczeństwa w Internecie- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	12:00	13:00	01:00
6 z 27 Przerwa	Marcin Nowicki	27-11-2024	13:00	14:00	01:00
7 z 27 Zrozumienie bezpieczeństwa sieci bezprzewodowej- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	14:00	15:00	01:00
8 z 27 Przerwa	Marcin Nowicki	27-11-2024	15:00	15:15	00:15
9 z 27 Zrozumienie bezpieczeństwa komputerów- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	27-11-2024	15:15	16:30	01:15
10 z 27 Zrozumienie uprawnień- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	09:00	10:00	01:00
11 z 27 Zrozumienie zasad dotyczących haseł- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	10:00	11:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 27 Przerwa	Marcin Nowicki	28-11-2024	11:00	11:15	00:15
13 z 27 Zrozumienie zasad protokołowania- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	11:15	12:00	00:45
14 z 27 Zrozumienie szyfrowania- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	12:00	13:00	01:00
15 z 27 Przerwa	Marcin Nowicki	28-11-2024	13:00	14:00	01:00
16 z 27 Zrozumienie złośliwego oprogramowania- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	14:00	15:00	01:00
17 z 27 Przerwa	Marcin Nowicki	28-11-2024	15:00	15:15	00:15
18 z 27 Zrozumienie dedykowanych zapór ogniowych- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	28-11-2024	15:15	16:30	01:15
19 z 27 Zrozumienie izolacji sieci- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	29-11-2024	09:00	10:00	01:00

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
20 z 27 Zrozumienie zabezpieczenia protokołów- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	29-11-2024	10:00	11:00	01:00
21 z 27 Przerwa	Marcin Nowicki	29-11-2024	11:00	11:15	00:15
22 z 27 Zrozumienie ochrony stacji klienckich- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	29-11-2024	11:15	13:00	01:45
23 z 27 Przerwa	Marcin Nowicki	29-11-2024	13:00	14:00	01:00
24 z 27 Zrozumienie ochrony poczty elektronicznej- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	29-11-2024	14:00	15:00	01:00
25 z 27 Przerwa	Marcin Nowicki	29-11-2024	15:00	15:15	00:15
26 z 27 Zrozumienie ochrony serwera- ćwiczenia, rozmowa na żywo, chat, współdzielenie ekranu	Marcin Nowicki	29-11-2024	15:15	16:30	01:15
27 z 27 Walidacja usługi	-	29-11-2024	16:30	17:15	00:45

Cennik

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	172,20 PLN
Koszt osobogodziny netto	140,00 PLN

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 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: Dwurdzeniowy 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

Mateusz Banasiak

E-mail mateusz.banasiak@pl.ey.com
Telefon (+48) 453 712 759