Możliwość dofinansowania

Cyberbezpieczeństwo - narzędzia i strategie umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami. Szkolenie i konsultacje. Certyfikowane szkolenie

1 709,70 PLN brutto
1 390,00 PLN netto
142,48 PLN brutto/h
115,83 PLN netto/h

Centrum Organizacji Szkoleń i Konferencji SEMPER Magdalena Wolniewicz-Kesaria

★★★★½

Numer usługi 2024/04/12/8282/2122602

zdalna w czasie rzeczywistym
Usługa szkoleniowa
12 h
08.08.2024 do 09.08.2024

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	1. Pracownicy działów IT i informatycy odpowiedzialni za bezpieczeństwo systemów informatycznych. 2. Specjaliści ds. bezpieczeństwa informacji i cyberbezpieczeństwa. 3. Kierownictwo i kadra zarządzająca, odpowiedzialna za podejmowanie decyzji dotyczących bezpieczeństwa cybernetycznego. 4. Specjaliści zainteresowani rozwojem zawodowym w dziedzinie cyberbezpieczeństwa. 5. Wszystkie osoby zainteresowane omawianą podczas szkolenia tematyką.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	01-08-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	12
Podstawa uzyskania wpisu do BUR	Znak Jakości TGLS Quality Alliance

Cel

Cel edukacyjny

Zwiększenie świadomości na temat cyberbezpieczeństwa wśród uczestników.
Zdobycie wiedzy teoretycznej i praktycznych umiejętności z zakresu cyberbezpieczeństwa.
Wyposażenie uczestników w narzędzia i strategie umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami cybernetycznymi.
Promowanie postaw odpowiedzialnego korzystania z technologii i przeciwdziałanie cyberprzestępczości.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Kompetencje społeczne: - ocenia jak odpowiednio reagować w różnych sytuacjach związanych z wykonywanym zawodem - identyfikuje własny styl uczenia się i wybiera sposoby dalszego kształcenia, - określa znaczenie komunikacji interpersonalnej oraz potrafi prawidłowo identyfikować i rozstrzygać dylematy związane z wykonywaniem zawodu.	- Umiejętność dostosowania reakcji do różnorodnych kontekstów zawodowych - Wybór adekwatnych metod do dalszego kształcenia.	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Otrzymane zaświadczenie po ukończonym szkoleniu zawiera szczegółowe informacje dotyczące osiągniętych efektów edukacyjnych przez uczestnika.

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

Nabyta wiedza poddawana jest ocenie poprzez kończącą zajęcia dyskusję trenera z uczestnikami, bazującą na ściśle określonych kryteriach weryfikacji.

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

Świadectwo potwierdza, że proces walidacji jest niezależny od etapu szkolenia, a obiektywność trenerów przeprowadzających walidację jest zagwarantowana.

Program

Moduł 1: Podstawy cyberbezpieczeństwa

1. Wprowadzenie do cyberbezpieczeństwa: definicja, znaczenie i aktualne zagrożenia.
2. Rodzaje ataków cybernetycznych: malware, phishing, ransomware, ataki DDoS itp.
3. Podstawowe pojęcia związane z cyberbezpieczeństwem: poufność, integralność, dostępność, poufność, niezaprzeczalność.
4. Regulatory i standardy związane z cyberbezpieczeństwem: GDPR, ISO 27001.

Moduł 2: Bezpieczeństwo sieci

1. Zagrożenia związane z sieciami komputerowymi.
2. Architektura sieciowa i zasady projektowania bezpiecznej sieci.
3. Firewalle: rodzaje, konfiguracja i zarządzanie nimi.
4. Zabezpieczanie sieci bezprzewodowych: uwierzytelnianie, szyfrowanie, filtrowanie adresów MAC.
5. Zarządzanie hasłami i autoryzacją: zasady tworzenia silnych haseł, zarządzanie kontami użytkowników.

Moduł 3: Bezpieczeństwo systemów operacyjnych

1. Aktualizacje systemów operacyjnych i aplikacji: znaczenie i procedury.
2. Antywirusy i antimalware: instalacja, konfiguracja i skanowanie systemu.
3. Bezpieczne korzystanie z systemu: zasady tworzenia kont użytkowników, zarządzanie uprawnieniami.
4. Monitorowanie systemu: logi, analiza zdarzeń bezpieczeństwa, wykrywanie nieprawidłowości.

Moduł 4: Bezpieczeństwo aplikacji

1. Testowanie penetracyjne: zasady, narzędzia i techniki.
2. Ochrona przed atakami typu SQL injection i cross-site scripting.
3. Bezpieczeństwo aplikacji webowych: filtrowanie wejścia, zabezpieczanie sesji, walidacja danych.
4. Bezpieczeństwo aplikacji mobilnych: uwierzytelnianie, szyfrowanie danych, zarządzanie uprawnieniami.

Moduł 5: Zarządzanie incydentami i reagowanie na ataki

1. Planowanie reakcji na incydenty: tworzenie procedur, zespoły odpowiedzialne za reagowanie.
2. Analiza zdarzeń bezpieczeństwa: narzędzia i techniki identyfikacji i analizy ataków.
3. Reagowanie na incydenty: odizolowanie systemów, odzyskiwanie danych, przywracanie działania.
4. Audyt bezpieczeństwa: przegląd systemów, ocena zgodności z zasadami bezpieczeństwa.

Moduł 6: Polityka bezpieczeństwa i świadomość użytkowników

1. Tworzenie polityki bezpieczeństwa: cele, zasady i procedury.
2. Szkolenia dla pracowników: edukacja w zakresie bezpiecznego korzystania z technologii.
3. Zarządzanie ryzykiem: ocena ryzyka, zarządzanie incydentami, planowanie ciągłości działania.
4. Bezpieczeństwo w chmurze: zagrożenia i najlepsze praktyki związane z usługami chmurowymi.

Program szkolenia będzie obejmował zarówno wykłady teoretyczne, jak i praktyczne warsztaty, w których uczestnicy będą mieli okazję zastosować zdobytą wiedzę w praktyce. Podczas szkolenia będą używane różne narzędzia i symulacje, aby umożliwić uczestnikom eksplorację rzeczywistych scenariuszy i sytuacji związanych z cyberbezpieczeństwem.

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 Cyberbezpieczeństwo - narzędzia i strategie umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami. Szkolenie i konsultacje.	Ewa Krzykowska	08-08-2024	09:00	15:00	06:00
2 z 2 Cyberbezpieczeństwo - narzędzia i strategie umożliwiające skuteczną ochronę danych i systemów przed zagrożeniami. Szkolenie i konsultacje.	Ewa Krzykowska	09-08-2024	09:00	15:00	06:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 709,70 PLN
Koszt przypadający na 1 uczestnika netto	1 390,00 PLN
Koszt osobogodziny brutto	142,48 PLN
Koszt osobogodziny netto	115,83 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Ewa Krzykowska

Specjalista i praktyk w zakresie pozyskiwania i obsługi funduszy oraz projektów unijnych, opracowywania strategii rozwoju firm, miast i gmin, biznes planów, analiz, raportów i ekspertyz. Absolwentka SGH. Autorka i współautorka wielu strategii rozwoju miast i gmin. Trener z wieloletnim doświadczeniem w realizacji i obsłudze szkoleń o tematyce unijnej, w tym na zlecenie MRR i PARP.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- materiały szkoleniowe w wersji elektronicznej
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu
- otrzymujesz indywidualną kartę rabatową upoważniającą do 10% zniżki na wszystkie kolejne szkolenia stacjonarne i online organizowane przez Centrum Organizacji Szkoleń i Konferencji SEMPER

Warunki uczestnictwa

ZGŁOSZENIE NA USŁUGĘ

- Rezerwacji miejsca szkoleniowego można dokonać za pośrednictwem BUR.

Inwestycja: 1390.00zł netto (+23% VAT)

- Dla jednostek budżetowych finansujących udział w szkoleniu w minimum 70% lub w całości ze środków publicznych stawka podatku VAT = zw.

Informacje dodatkowe

- wygodna forma szkolenia - wystarczy dostęp do urządzenia z Internetem (komputer, tablet, telefon), słuchawki lub głośniki i ulubiony fotel
- szkolenie realizowane jest w nowoczesnej formie w wirtualnym pokoju konferencyjnym i kameralnej grupie uczestników
- bierzesz udział w pełnowartościowym szkoleniu - Trener prowadzi zajęcia "na żywo" - widzisz go i słyszysz
- pokaz prezentacji, ankiet i ćwiczeń widzisz na ekranie swojego komputera w czasie rzeczywistym.
- podczas szkolenia Trener aktywizuje uczestników zadając pytania, na które można odpowiedzieć w czasie rzeczywistym
- otrzymujesz certyfikat wydany przez jedną z wiodących firm szkoleniowych w Polsce
- masz dostęp do konsultacji poszkoleniowych w formie e-mail do 4 tygodni po zrealizowanym szkoleniu
- otrzymujesz indywidualną kartę rabatową upoważniającą do 10% zniżki na wszystkie kolejne szkolenia stacjonarne i online organizowane przez Centrum Organizacji Szkoleń i Konferencji SEMPER

Warunki techniczne

Wymagania techniczne:

- Platforma /rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa - Platforma Zoom (https://zoom-video.pl/)

Wymagania sprzętowe:

- Minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji - komputer, laptop lub inne urządzenie z dostępem do internetu
- Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik - minimalna prędkość łącza: 512 KB/sek
- Niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów - komputer, laptop lub inne urządzenie z dostępem do internetu. Nie ma potrzeby instalowania specjalnego oprogramowania.
- Okres ważności linku umożliwiającego uczestnictwo w spotkaniu on-line - od momentu rozpoczęcia szkolenia do momentu zakończenia szkolenia

- Potrzebna jest zainstalowana najbardziej aktualna oficjalna wersja jednej z przeglądarek: Google Chrome, Mozilla Firefox, Safari, Edge lub Opera. Procesor dwurdzeniowy 2GHz lub lepszy (zalecany czterordzeniowy); 2GB pamięci RAM (zalecane 4GB lub więcej); System operacyjny taki jak Windows 8 (zalecany Windows 10), Mac OS wersja 10.13 (zalecana najnowsza wersja), Linux, Chrome OS. Łącze internetowe o minimalnej przepustowości do zapewnienia transmisji dźwięku 512Kb/s, zalecane

Kontakt

Angelika Poznańska

E-mail info@szkolenia-semper.pl
Telefon (+48) 570 590 060