Możliwość dofinansowania

Dagma sp. z o.o.

★★★★½

ELEMENTY SYSTEMU ZABEZPIECZEŃ INFRASTRUKTURY TELEINFORMATYCZNEJ

Numer usługi 2024/07/04/17164/2208931

zdalna w czasie rzeczywistym
Usługa szkoleniowa
16 h
09.09.2024 do 10.09.2024

3 185,70 PLN brutto
2 590,00 PLN netto
199,11 PLN brutto/h
161,88 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Sposób dofinansowania	wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: • bardzo dobra znajomość zagadnień z zakresu administracji systemami komputerowymi.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	02-09-2024
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	16
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 dostarczenie kompetencji z zakresu ELEMENTÓW SYSTEMU ZABEZPIECZEŃ INFRASTRUKTURY TELEINFORMATYCZNEJ, dzięki którym uczestnik będzie posiadał praktyczną wiedzę z ogólnego obszaru, jakim jest infrastruktura teleinformatyczna.

Uczestnik po ukończonym szkoleniu nabędzie kompetencje społeczne takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik wie, jak PRZEWIDYWAĆ ZAGROŻENIA BEZPIECZEŃSTWA, Potrafi WYZNACZAĆ ZAGROŻENIA I ANALIZOWAĆ RYZYKA.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

Uczestnik wie, jak PRZEWIDYWAĆ ZAGROŻENIA BEZPIECZEŃSTWA NA PODSTAWIE MODELU STRIDE;
WYZNACZAĆ ZAGROŻENIA I ANALIZOWAĆ RYZYKA DLA KONT W ORGANIZACJI;
Uczestnik nabędzie umiejętności: DYSTRYBUCJI I ZARZĄDZANIA CERTYFIKATAMI. TWORZENIA STRUKTUR PKI.

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

MODUŁ 1 ZAPOZNANIE Z ELEMENTAMI PODATNYMI NA NIEBEZPIECZEŃSTWO ORAZ METODAMI ICH WYKORZYSTYWANIA PRZEZ INTRUZA - zajęcia teoretyczne (wykład)

PRZEWIDYWANIE ZAGROŻEŃ BEZPIECZEŃSTWA NA PODSTAWIE MODELU STRIDE.

- tworzenie planu zarządzania ryzykiem
- projektowanie zabezpieczeń dla zasobów fizycznych
- wyznaczenie zagrożeń i analiza ryzyka w sieci

MODUŁ 2 WYZNACZENIE ZAGROŻEŃ I ANALIZA RYZYKA DLA KONT W ORGANIZACJI - zajęcia praktyczne (ćwiczenia)

- projektowanie zabezpieczeń kont – polityki blokowania konta, granularne zasady haseł
- wyznaczenie zagrożeń i analiza ryzyka dla procesu uwierzytelniania

WYZNACZENIE ZAGROŻEŃ, PROJEKTOWANIE ZABEZPIECZEŃ I ANALIZA RYZYKA DLA DANYCH

- Encrypted File System, Bitlocker i Bitlocker To Go
- Implementacja Dynamic Access Control

WYZNACZENIE ZAGROŻEŃ, PROJEKTOWANIE ZABEZPIECZEŃ I ANALIZA RYZYKA DLA TRANSMISJI DANYCH.

MODUŁ 3 PROJEKTOWANIE POLIS INSPEKCJI - zajęcia teoretyczne (wykład)

ANALIZA RYZYKA TWORZONEGO PRZEZ UŻYTKOWNIKÓW SIECI, PROJEKTOWANIE POLITYKI BEZPIECZNEGO UŻYWANIA KOMPUTERA.

ANALIZA RYZYKA ZARZĄDZANIA SIECI, PROJEKTOWANIE POLITYKI BEZPIECZEŃSTWA DLA ZARZĄDZANIA SIECIĄ.

MODUŁ 4 ELEMENTY KRYPTOGRAFII - zajęcia teoretyczne (wykład)

- sposoby wykorzystania kryptografii do zabezpieczania informacji
- metody szyfrowania
- zabezpieczanie informacji w organizacji przy użyciu uwierzytelniania oraz kontroli dostępu

MODUŁ 5 DYSTRYBUCJA I ZARZĄDZANIE CERTYFIKATAMI. TWORZENIE STRUKTURY PKI - zajęcia praktyczne (ćwiczenia)

- zabezpieczanie transmisji danych
- implementacja zabezpieczeń dla typowych metod transmisji danych (IPSec), zdalnego dostępu i sieci bezprzewodowych (RADIUS)
- zabezpieczanie wiadomości e-mail i przed typowymi zagrożeniami
- dystrybucja kart inteligentnych w środowisku Windows
- ochrona własności intelektualnych dokumentów w formacie MS Office (AD RMS)

ZABEZPIECZANIE ŚRODOWISKA WEB PRZEZ IMPLEMENTACJĘ ZABEZPIECZEŃ SSL ORAZ OPARTE O CERTYFIKATY UWIERZYTELNIANIE DLA APLIKACJI SIECIOWYCH.

MODUŁ 6 TYPOWE ZAGROŻENIA USŁUG KATALOGOWYCH I DNS ORAZ ZASTOSOWANIE METOD ZABEZPIECZAJĄCYCH TE USŁUGI - zajęcia praktyczne (ćwiczenia)

NIEZAWODNOŚĆ TO TEŻ BEZPIECZEŃSTWO - IMPLEMENTACJA BEZPIECZNEJ STRATEGII ODZYSKIWANIA SPRAWNOŚCI PO AWARII, MINIMALIZACJI ZAGROŻEŃ W KOMUNIKACJI ORAZ TWORZENIA BEZPIECZNYCH KOPII BEZPIECZEŃSTWA I ICH ODTWARZANIA.

IDENTYFIKACJA, ODPOWIEDŹ NA INCYDENTY ORAZ ASYSTOWANIE PRZY FORMALNYM ŚLEDZTWIE W PRZYPADKU WŁAMANIA.

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 16 godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	3 185,70 PLN

Koszt przypadający na 1 uczestnika netto	2 590,00 PLN
Koszt osobogodziny brutto	199,11 PLN
Koszt osobogodziny netto	161,88 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-book, przesyłany na adres e-mail uczestnika)
- dostęp do przygotowanego środowiska wirtualnego

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową **https://szkolenia.dagma.eu/pl** w celu rezerwacji miejsca.

Informacje dodatkowe

Informacje organizacyjne:

- Jedna godzina lekcyjna to 45 minut
- W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Uczestnik otrzyma zaświadczenie ACS o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez Autoryzowane Centrum Szkoleniowe DAGMA.

Warunki techniczne

WARUNKITECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM i/lub MS Teams**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi (czyt. od 4 marca do 5 marca)

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie:
https://www.acsdagma.com/pl/szkolenia-online

Kontakt

Agnieszka Palenga

E-mail palenga.a@dagma.pl
Telefon (+48) 32 7931 139