Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

441 ocen

Administrator Systemu Informatycznego - kurs praktyczny

Numer usługi 2025/09/10/17164/2998231

zdalna w czasie rzeczywistym

Usługa szkoleniowa

14 h

15.12.2025 do 16.12.2025

3 185,70 PLN brutto

2 590,00 PLN netto

227,55 PLN brutto/h

185,00 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Administracja IT i systemy komputerowe

Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, w tym Pracownicy, właściciele firm MMSP z sektora Telekomunikacja i Cyberbezpieczeństwo, spełniających poniższe wymagania:
	• Podstawowa znajomość systemów operacyjnych Linux/Windows,
	• Umiejętność instalacji oprogramowania, edycji plików konfiguracyjnych, obsługa konsoli,
	• Znajomość zagadnień sieciowych:
	  • znajomość protokołów TCP/UDP
	  • znajomość protokołu IP
	  • zrozumienie zasad routingu i adresacji sieci.
	• Znajomość usług sieciowych: WWW, Poczta, DNS.

Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	08-12-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	14
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 Administratora Systemu Informatycznego - kurs praktyczny. Uczestnik będzie samodzielnie projektował i wdrażał system bezpieczeństwa informacji, budował właściwe i adekwatne zabezpieczenia dla takiego systemu oraz opracowywał skuteczne procedury zarządzania przyjętymi środkami bezpieczeństwa. 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
Zidentyfikować główne zagrożenia dla infrastruktury sieciowej oraz opisać typy ataków i ich skutki – zna podstawowe wektory ataków, rozumie cel tworzenia polityki bezpieczeństwa i potrafi wskazać słabe punkty infrastruktury.	Ćwiczenie: Analiza przykładowych scenariuszy ataku na infrastrukturę IT i wskazanie środków zaradczych – uczestnik rozpoznaje wektory ataku, dobiera odpowiednie działania ochronne i wskazuje możliwe skutki incydentu.	
Zastosować metody zabezpieczania stacji roboczych w środowisku sieciowym – zarządza uprawnieniami użytkowników, wdraża polityki backupu i AV, konfiguruje kontrolę nośników i filtrowanie treści.	Warsztat: Konfiguracja stacji roboczej z politykami bezpieczeństwa (uprawnienia, AV, filtrowanie treści, backup) – uczestnik samodzielnie konfiguruje środowisko pracy zgodnie z dobrymi praktykami.	Obserwacja w warunkach symulowanych
Zaprojektować podstawowe zabezpieczenia dla serwerów i usług sieciowych – stosuje zasady tworzenia DMZ, konfiguruje firewalle, analizuje podatności OWASP Top 10, wdraża IPS/IDS i skanuje serwery pod kątem zagrożeń.	Zadanie: Projekt i implementacja segmentacji sieci (DMZ), konfiguracja firewalla oraz analiza przykładowych podatności serwera – uczestnik przedstawia rozwiązanie problemu zabezpieczenia infrastruktury serwerowej i potrafi je zaimplementować.	

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykrywać i analizować podatności systemowe oraz stosować narzędzia do testowania bezpieczeństwa – wykorzystuje techniki sniffingu, skanowania portów, analizy logów i identyfikacji anomalii. Zidentyfikować zagrożenia wynikające z obecności urządzeń IoT, mobilnych oraz błędów użytkowników – wskazuje ryzyka związane z nieautoryzowanymi urządzeniami, drukarkami, kamerami, aplikacjami mobilnymi i nieuwagą pracowników. Stosować metody monitorowania, logowania zdarzeń i zabezpieczeń fizycznych jako elementy kompleksowego bezpieczeństwa IT – konfiguruje logowanie zdarzeń, ocenia systemy monitorujące oraz wdraża zabezpieczenia fizyczne (dostęp, nadzór, ochrona sprzętu).optymalizowania rozwiązania, stosowania przepisów prawa dotyczących ochrony danych, zapewniania bezpieczeństwa danych oraz rozwiązań w chmurze.	Laboratorium: Użycie narzędzi do sniffingu i wykrywania luk bezpieczeństwa (np. Wireshark, Nmap, Nessus) – uczestnik potrafi wykonać analizę ruchu sieciowego i wykryć nieprawidłowości. Symulacja: Ocena ryzyk związanych z urządzeniami IoT, mobilnymi i błędami ludzkimi – projekt polityki ograniczającej te zagrożenia – uczestnik przygotowuje zestaw zaleceń i opisuje potencjalne zagrożenia z różnych źródeł. Zadanie: Konfiguracja systemu logowania i monitorowania zdarzeń, identyfikacja potencjalnych incydentów – uczestnik przedstawia przykładową konfigurację monitoringu środowiska i reagowania na incydenty.	Obserwacja w warunkach symulowanych
Uczestnik nabędzie kompetencje społeczne, takie jak samokształcenie, rozwiązywanie problemów, kreatywność w działaniu.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny

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

Moduł 1 Co grozi naszej sieci – poznaj swojego wroga by skutecznie z nim walczyć - zajęcia teoretyczne (wykład)

- Typy ataków,
- Polityki bezpieczeństwa

Moduł 2 Bezpieczeństwo stacji roboczych - zajęcia praktyczne (ćwiczenia)

- Zarządzanie uprawnieniami
- Filtrowanie URL
- AV
- Backup
- Kontrola podłączanych nośników

Moduł 3 Ochrona serwerów - zajęcia teoretyczne (wykład)

- DMZ
- Firewall
- WWW
- OWASP Top10

Moduł 4 Szukanie podatności - zajęcia praktyczne (ćwiczenia)

- IPS/IDS
- Poczta
- Serwery pośredniczące
- Skanowanie AV
- Ochrona sieci
- Jak szukać luk w zabezpieczeniach
- Sniffing

Moduł 5 Inne zagrożenia - zajęcia praktyczne (ćwiczenia)

- IoT (Internet of Things)
  - Urządzenia mobilne
  - Monitoring
  - Drukarki

Moduł 6 Błędy użytkowników - - zajęcia teoretyczne (wykład)

- Zabezpieczenia fizyczne
- Logowanie zdarzeń i monitoring środowisk

Godzinowy harmonogram usługi ma charakter orientacyjny - trener, w zależności od potrzeb uczestników, może zmienić długość poszczególnych modułów (przy zachowaniu łącznego wymiaru 14 godz. lekcyjnych). Podczas szkolenia, w zależności od potrzeb uczestników, będą robione krótkie przerwy. Trener ustali z uczestnikami konkretne godziny przerw.

Walidacja

Razem 14 godzin lekcyjnych, (10 godzin i 30 minut zegarowych).

· Walidacja jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba przedmiotów/zajęć: 2

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 2 Administrator Systemu Informatycznego	Adam Jakubiec	15-12-2025	09:00	16:00	07:00
2 z 2 Administrator Systemu Informatycznego	Adam Jakubiec	16-12-2025	09:00	16:00	07:00

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	227,55 PLN
Koszt osobogodziny netto	185,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Adam Jakubiec

"Trener IT w Dagma Szkolenia IT od 2015 roku, prowadzący szkolenia z dziedziny systemów informatycznych, Technologii Microsoft, cyberbezpieczeństwa, infrastruktura klucza publicznego (PKI).
Kierownik działu IT w międzynarodowym przedsiębiorstwie, wykładowca akademicki, trener technologii Microsoft oraz licznych autorskich i autoryzowanych kursów z zakresu bezpieczeństwa infrastruktury teleinformatycznej. Uzyskane certyfikacje: C)TIA: Certified Threat Intelligence Analyst; AZ-900 Microsoft Azure Fundamentals; C)PSH: Certified Powershell Hacker; C)PTE: Certified Penetration Testing Engineer; 70-744 Securing Windows Server 2016; 70-743 Upgrading Your Skills to MCSA: Windows Server 2016; 74-409 Server Virtualization with Windows Server Hyper-V and

System Center; 70-698 Configuring Windows 10; Mictrosoft Certified Trainer, 70-640 Windows Server 2008 Active Directory, Configuration, Wykształcenie: wyższe, Edukacja informatyczno-techniczna, Aplikacje komputerowe (MCA)"

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (e-book, lub dostęp do materiałów autorskich, przygotowanych przez trenera) przesyłane na adres mailowy 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

· Jedna godzina lekcyjna to 45 minut

· W cenę szkolenia nie wchodzą koszta związane z dojazdem, wyżywieniem oraz noclegiem.

· Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT 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 DAGMA Sp. z o.o.

· Podstawa zwolnienia z VAT: dofinansowanie w co najmniej 70% - zgodnie z treścią § 3 ust. 1 pkt 14 Rozporządzenia Ministra Finansów z dnia 20.12.2013r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień (Dz. U. z 2013 r. poz. 1722 ze zm.)"

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 5 czerwca do 6 czerwca)

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: https://szkolenia.dagma.eu/pl/technical-requirements

Kontakt

Wronska Katarzyna

E-mail wronska.k@dagma.pl
Telefon (+48) 32 7931 139