Możliwość dofinansowania

Administrator Systemu Informatycznego - kurs praktyczny

Numer usługi 2026/07/14/17164/3688265

3 308,70 PLN brutto
2 690,00 PLN netto
236,34 PLN brutto/h
192,14 PLN netto/h
332,00 PLN cena rynkowa

Dagma sp. z o.o.

4,5 / 5

465 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
14:00 h
10.12.2026 do 11.12.2026

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	02-12-2026
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

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 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

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

· Walidacja jest wliczona w czas trwania szkolenia.

· Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 11

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 11 Moduł 1 Co grozi naszej sieci – poznaj swojego wroga by skutecznie z nim walczyć - zajęcia teoretyczne (wykład)	Zajęcia	Adam Jakubiec	10-12-2026	09:00	11:15	02:15
2 z 11 -	Przerwa	-	10-12-2026	11:15	11:45	00:30
3 z 11 Moduł 2 Bezpieczeństwo stacji roboczych - zajęcia praktyczne (ćwiczenia)	Zajęcia	Adam Jakubiec	10-12-2026	11:45	13:30	01:45
4 z 11 -	Przerwa	-	10-12-2026	13:30	14:00	00:30
5 z 11 Moduł 3 Ochrona serwerów - zajęcia teoretyczne (wykład)	Zajęcia	Adam Jakubiec	10-12-2026	14:00	16:00	02:00
6 z 11 Moduł 4 Szukanie podatności - zajęcia praktyczne (ćwiczenia)	Zajęcia	Adam Jakubiec	11-12-2026	09:00	10:45	01:45
7 z 11 -	Przerwa	-	11-12-2026	10:45	11:15	00:30
8 z 11 Moduł 5 Inne zagrożenia - zajęcia praktyczne (ćwiczenia)	Zajęcia	Adam Jakubiec	11-12-2026	11:15	13:30	02:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 11 -	Przerwa	-	11-12-2026	13:30	14:00	00:30
10 z 11 Moduł 6 Błędy użytkowników - - zajęcia teoretyczne (wykład)	Zajęcia	Adam Jakubiec	11-12-2026	14:00	15:45	01:45
11 z 11 -	Walidacja	-	11-12-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	14:00
w tym suma godzin zajęć	11:45
w tym suma godzin walidacji	00:15
w tym suma przerw	02:00
Suma godzin dydaktycznych bez przerw	16:00

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	3 308,70 PLN
Koszt przypadający na 1 uczestnika netto	2 690,00 PLN
Koszt osobogodziny brutto	236,34 PLN

Koszt osobogodziny netto	192,14 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	14:00

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

- W cenę szkolenia nie wchodzą koszty związane z dojazdem, wyżywieniem oraz noclegiem.
- Szkolenie nie zawiera egzaminu.
- Harmonogram ma charakter ramowy i trener może na potrzeby grupy szkoleniowej zmienić długość poszczególnych modułów, przy zachowaniu niezmienionej łącznej liczby godzin usługi szkoleniowej.
- 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 SZKOLENIA IT.
- Organizator szkolenia zastrzega sobie prawo do zmiany trenera prowadzącego/walidującego jeśli z przyczyn niezależnych od Organizatora (np. zdarzenie losowe) wyznaczony trener nie będzie mógł przeprowadzić szkolenia. Przy czym Organizator zobowiązuje się do zapewnienia w zastępstwie trenera o takich samych/zbliżonych kompetencjach.

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

Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 32 7931 180