



Dagma sp. z o.o.

**ELEMENTY SYSTEMU ZABEZPIECZEŃ
INFRASTRUKTURY
TELEINFORMATYCZNEJ**

Numer usługi 2025/05/19/17164/2756131

zdalna w czasie rzeczywistym

Usługa szkoleniowa

16 h

11.08.2025 do 12.08.2025

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	04-08-2025
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
Identyfikować zagrożenia bezpieczeństwa IT w infrastrukturze organizacji oraz analizować ryzyko – stosuje modele analizy ryzyka, w tym STRIDE, potrafi wskazać słabe punkty systemów i procesów oraz dobrać adekwatne zabezpieczenia. Projektować polityki bezpieczeństwa dla zasobów IT (kont, danych, usług sieciowych, zarządzania siecią) – tworzy polityki blokowania kont, zarządzania hasłami, dostępu do danych, zasobów oraz zarządzania środowiskiem IT. Implementować mechanizmy kryptograficzne do zabezpieczania danych i komunikacji – zna i stosuje metody szyfrowania (BitLocker, EFS), zabezpieczania transmisji (SSL/TLS, IPSec) oraz korzystania z uwierzytelniania opartego na certyfikatach (PKI). Zarządzać infrastrukturą klucza publicznego (PKI) i certyfikatami cyfrowymi w środowisku organizacyjnym – wdraża rozwiązania oparte o certyfikaty, konfiguruje ich dystrybucję, integruje z systemami logowania i transmisji danych. Zabezpieczać usługi katalogowe (Active Directory) oraz DNS w środowiskach Windows – zna zagrożenia tych usług, stosuje funkcjonalności takie jak Credential Guard, DNSSEC, RADIUS/WPA2-Enterprise. Reagować na incydenty bezpieczeństwa i wspierać działania w ramach śledztw IT – potrafi identyfikować oznaki naruszenia bezpieczeństwa, wdrażać procedury reakcji i dokumentować zdarzenia zgodnie z dobrymi praktykami.	Zadanie: Analiza scenariusza zagrożenia – identyfikacja luk i zaprojektowanie odpowiednich zabezpieczeń (wg modelu STRIDE) – uczestnik przeprowadza analizę ryzyka dla wybranego zasobu, opisuje zagrożenia i dobiera odpowiednie mechanizmy ochronne. Warsztat: Tworzenie polityki bezpieczeństwa kont użytkowników (hasła, blokady, MFA) – uczestnik konfiguruje politykę hasel i blokady kont, wdraża zalecenia dobrej praktyki uwierzytelniania. Laboratorium: Konfiguracja BitLocker, EFS, DNSSEC oraz uwierzytelniania RADIUS w środowisku testowym – uczestnik samodzielnie wdraża i testuje zabezpieczenia dla danych, systemów i sieci. Ćwiczenie: Projekt i wdrożenie infrastruktury PKI oraz dystrybucji certyfikatów cyfrowych dla pracowników organizacji – uczestnik tworzy strukturę certyfikatów, konfiguruje uwierzytelnianie i podpis cyfrowy. Zadanie: Opracowanie planu reakcji na incydent (IRP) oraz analiza przykładowego włamania – uczestnik przedstawia kroki identyfikacji, reakcji i dokumentacji incydentu oraz omawia rolę zespołu bezpieczeństwa. Egzamin końcowy (opcjonalny): Test wiedzy weryfikujący znajomość zagrożeń, zabezpieczeń oraz metod ich wdrażania w praktyce.	Obserwacja w warunkach symulowanych Obserwacja w warunkach symulowanych

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
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, 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?

Tak, dokument stanowi potwierdzenie, 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?

Tak, dokument potwierdza, że zostały zastosowane rozwiązania zapewniające rozdzielenie procesów kształcenia i szkolenia od walidacji.

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.

Walidacja

Razem 16 godzin lekcyjnych, (12 godzin 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 Moduł od 1 do 6	Adam Jakubiec	11-08-2025	09:00	17:00	08:00
2 z 2 Moduł od 7 do 12	Adam Jakubiec	12-08-2025	09:00	17:00	08:00

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	199,11 PLN
Koszt osobogodziny netto	161,88 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Adam Jakubiec

Technologie Microsoft, cyberbezpieczeństwo, 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. Prowadzi szkolenia z tematyki ADMINISTRATOR SYSTEMU INFORMATYCZNEGO - KURS PRAKTYCZNY w DAGMA Szkolenia IT od 2015 r. Zna teoretyczne aspekty zagadnień i posiada minimum trzyletnie doświadczenie dydaktyczne oraz praktyczne w dziedzinie.

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 wchodzi koszt związany 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 4 marca do 5 marca)

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

Kontakt



Agnieszka Palenga

E-mail palenga.a@dagma.pl

Telefon (+48) 32 7931 139