Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

441 ocen

BLUE TEAM - Poziom 2 - Zawansowane bezpieczeństwo infrastruktury. Active Directory. Systemy zabezpieczeń sieciowych

Numer usługi 2026/01/12/17164/3252888

zdalna w czasie rzeczywistym

Usługa szkoleniowa

7 h

13.02.2026 do 13.02.2026

2 201,70 PLN brutto

1 790,00 PLN netto

314,53 PLN brutto/h

255,71 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**To trzecie szkolenie z cyklu Blue Team, skupiające się na zaawansowanych aspektach bezpieczeństwa infrastruktury IT oraz Active Directory.** Współczesne sieci korporacyjne są nieustannie narażone na ataki – od prób włamania i eksfiltracji danych po lateral movement i przejęcia kont uprzywilejowanych. Szkolenie to wyposaży uczestników w wiedzę i umiejętności niezbędne do skutecznej ochrony infrastruktury IT, wykrywania zagrożeń oraz reagowania na incydenty. Uczestnicy dowiedzą się, jak dbać o bezpieczeństwo Active Directory, skutecznie konfigurować firewalle, IDS/IPS oraz WAF, a także jak zabezpieczać krytyczne tożsamości (IAM, PAM) oraz dane przed wyciekiem (DLP, backup).
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	09-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	7
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

Praktyczne laboratoria oparte na realnych zagrożeniach – uczestnicy przeanalizują rzeczywiste przypadki ataków i incydentów bezpieczeństwa, wykorzystując narzędzia na co dzień używane przez specjalistów. Dzięki temu nauczą się stosować skuteczne metody ochrony systemów IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Zrozumiesz, jak działa Active Directory i jakie są kluczowe zagrożenia	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Nauczysz się skutecznie bronić AD przed atakami	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Opanujesz zaawansowaną konfigurację firewalli, IDS/IPS oraz WAF	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Zdobędziesz umiejętności w zakresie zarządzania tożsamościami i dostępem (IAM, PAM)	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Poznasz strategie ochrony danych przed wyciekiem i backupu odpornego na ransomware	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Będziesz potrafił monitorować incydenty i wykrywać zagrożenia w sieci	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?

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: Bezpieczeństwo Active Directory

Active Directory jest kluczowym elementem infrastruktury IT, ale także jednym z najczęstszych celów ataków. W tym module uczestnicy poznają mechanizmy działania AD, metody uwierzytelniania (Kerberos, NTLM) oraz popularne techniki ataków, takie jak Pass-the-Hash, Kerberoasting inne. Nauczą się również wdrażać najlepsze praktyki zabezpieczeń, w tym hardening GPO, zarządzać uprawnieniami oraz monitorować logi AD.

- Struktura i mechanizmy AD (LDAP, Kerberos, NTLM)
- Ataki na AD (Pass-the-Hash, Kerberoasting, i inne)
- Obrona i hardening Active Directory (GPO, LAPS, monitorowanie logów)
- LAB

Moduł 2: Firewall, IDS/IPS, WAF & UTM

Skuteczna ochrona sieci wymaga znajomości narzędzi takich jak firewalle, systemy IDS/IPS oraz WAF do ochrony aplikacji webowych. Uczestnicy dowiedzą się, jak analizować ruch sieciowy, tworzyć skuteczne reguły blokowania zagrożeń, a także jak optymalnie konfigurować rozwiązania UTM do wielowarstwowej ochrony organizacji.

- Konfiguracja firewalli
- IDS/IPS – analiza ruchu i tworzenie oraz tuning reguł
- WAF – zabezpieczenie aplikacji webowych
- UTM – ochrona wielowarstwowa i zarządzanie zagrożeniami
- LAB

Moduł 3: IAM, PAM, DLP & Backup

Tożsamości i dane to jedne z najcenniejszych zasobów organizacji – dlatego wymagają zaawansowanej ochrony. W tym module zaprezentowane zostanie zarządzanie tożsamościami i dostępem (IAM), uprzywilejowanymi kontami (PAM) oraz strategie kontroli dostępu do krytycznych systemów. Uczestnicy nauczą się także zabezpieczać dane przed wyciekiem za pomocą DLP oraz wdrażać skuteczne mechanizmy backupu odporne na ransomware.

- IAM – zarządzanie tożsamościami i dostępem
- PAM – ochrona kont uprzywilejowanych
- DLP – zabezpieczenie przed wyciekiem danych
- Backup i odzyskiwanie danych po ataku ransomware
- DEMO

Harmonogram

Liczba przedmiotów/zajęć: 4

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 4 Moduł 1: Bezpieczeństwo Active Directory	Paweł Kryński	13-02-2026	09:00	15:45	06:45
2 z 4 Moduł 2: Firewall, IDS/IPS, WAF & UTM	Paweł Kryński	13-02-2026	09:00	15:45	06:45

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
3 z 4 Moduł 3: IAM, PAM, DLP & Backup	Paweł Kryński	13-02-2026	09:00	15:45	06:45
4 z 4 walidacja	-	13-02-2026	15:45	16:00	00:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 201,70 PLN
Koszt przypadający na 1 uczestnika netto	1 790,00 PLN
Koszt osobogodziny brutto	314,53 PLN
Koszt osobogodziny netto	255,71 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Kryński

Trener IT, prowadzący szkolenia w Dagma Szkolenia IT z zakresu cyberbezpieczeństwa. Specjalista z dziedziny rozwiązań ESET, prowadzący kursy z tematyki BlueTeam. Certyfikaty: Certified Ethical Hacker, Azure Fundamentals, Junior Penetration Tester, Certified ESET Inspect Optimization Specialist i wiele innych. Wykształcenie wyższe.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja, do której dostęp zostanie udostępniony na adres e-mail uczestnika)

Warunki uczestnictwa

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

Warunki techniczne

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

- **ZOOM 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 aktualnym systemem operacyjnym Microsoft Windows lub macOS; aktualna wersja przeglądarki internetowej, zgodnej z HTML5 (Google Chrome, Mozilla Firefox, Edge); mikrofon. Opcjonalnie: minimalna rozdzielczość ekranu 1920 x 1080, kamera, drugi monitor lub inne urządzenie, na którym będziesz mógł przeglądać materiały

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.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

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

Kontakt

Michalina Krzyszkowska

E-mail krzyszkowska.m@dagma.pl
Telefon (+48) 327 931 015