Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

441 ocen

BLUE TEAM - Poziom 1 - Analiza Logów i ruchu sieciowego. IT Monitoring & Hardening

Numer usługi 2026/01/12/17164/3252633

zdalna w czasie rzeczywistym

Usługa szkoleniowa

7 h

15.05.2026 do 15.05.2026

1 832,70 PLN brutto

1 490,00 PLN netto

261,81 PLN brutto/h

212,86 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie **Blue Team Poziom 1** to drugie szkolenie z cyklu defensywnego cyberbezpieczeństwa, prowadzone przez doświadczonych inżynierów Dagma Blue Team. Program skupia się na praktycznych aspektach monitorowania i analizy bezpieczeństwa systemów IT. Uczestnicy poznają mechanizmy rejestrowania zdarzeń oraz analizę logów w systemach Windows i Linux, ucząc się identyfikować aktywności użytkowników i procesów mogące wskazywać na zagrożenia. Istotnym elementem szkolenia jest analiza ruchu sieciowego – omówione zostaną wzorce prawidłowej komunikacji, anomalie oraz metody wykrywania prób nieautoryzowanego dostępu. Szkolenie obejmuje również podstawy hardeningu systemów i usług, a także wprowadzenie do pracy z rozwiązaniami AV i EDR oraz ich wykorzystania w reagowaniu na incydenty. Całość uzupełniają laboratoria praktyczne, pozwalające zastosować zdobytą wiedzę w realnych scenariuszach i skutecznie wspierać zespoły bezpieczeństwa IT.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	11-05-2026
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
Praktyczne umiejętności – analiza logów, monitorowania systemów i wykrywania zagrożeń w rzeczywistych scenariuszach.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Wiedza o monitorowaniu ruchu sieciowego – identyfikacja anomalii w sieci i rozróżnianie normalnego oraz podejrzanego ruchu.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Podstawy hardeningu – nauka zabezpieczania systemów operacyjnych i usług przed atakami.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Świadomość zagrożeń i ataków – lepsze zrozumienie metod wykorzystywanych przez cyberprzestępców i sposoby ich neutralizacji.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Praca z narzędziami wykorzystywanymi przez Blue Team – praktyczne ćwiczenia z wykorzystaniem narzędzi do monitorowania i analizy bezpieczeństwa.	Samodzielna praca w środowisku wirtualnym	Obserwacja w warunkach rzeczywistych
Praca z AV i EDR – nauka interpretacji zdarzeń rejestrowanych przez oprogramowanie antywirusowe oraz identyfikacji potencjalnych zagrożeń.	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: Wprowadzenie

- Znaczenie monitorowania systemów informatycznych
- Logi w kontekście cyberbezpieczeństwa
- Wykrywanie nieautoryzowanego dostępu
- Monitorowanie aplikacji
- Reakcje na zdarzenia

Moduł 2: Windows – Monitorowanie i analiza logów

- Wprowadzenie do systemu Windows w kontekście bezpieczeństwa
- Monitorowanie aktywności użytkowników i aplikacji w systemie Windows
- Analiza logów w Windows Event Viewer: Security Logs, Application Logs
- Podstawowe komendy systemowe, cmd & powershell
- Analiza zdarzeń związanych z bezpieczeństwem
- Lab

Moduł 3: Linux – Monitorowanie i analiza logów

- Wprowadzenie do systemu Linux z perspektywy bezpieczeństwa
- Analiza podstawowych logów systemowych: /var/log/auth.log, /var/log/syslog
- Monitorowanie działań użytkowników w systemie Linux
- Podstawowe komendy systemowe i narzędzia analityczne w Linuxie
- Lab

Moduł 4: Hardening systemów

- Wprowadzenie do hardeningu systemów Windows i Linux
- Zasady zabezpieczania systemów operacyjnych i usług
- Podstawowe komendy sieciowe (ping, tracert, nslookup, netstat, tcpdump i inne).
- Analiza ruchu sieciowego - Wireshark
- Najlepsze praktyki w zakresie zabezpieczania systemów przed atakami
- Lab

Moduł 5: AV/EDR – Analiza logów i wykrywanie zagrożeń

- Wprowadzenie do ESET Inspect jako narzędzia EDR (Endpoint Detection and Response)
- Analiza logów z ESET Inspect: wykrywanie podejrzanych działań
- Interpretacja zdarzeń bezpieczeństwa w logach antywirusowych
- Praktyczne ćwiczenia w analizie logów ESET i identyfikacji zagrożeń
- Demo

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	1 832,70 PLN
Koszt przypadający na 1 uczestnika netto	1 490,00 PLN
Koszt osobogodziny brutto	261,81 PLN
Koszt osobogodziny netto	212,86 PLN

Prowadzący

Liczba prowadzących: 0

Brak wyników.

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