Możliwość dofinansowania

Dagma sp. z o.o.

4,5 / 5

441 ocen

ESET - XDR Administrator

Numer usługi 2026/01/14/17164/3258173

zdalna w czasie rzeczywistym

Usługa szkoleniowa

7 h

12.03.2026 do 12.03.2026

2 447,70 PLN brutto

1 990,00 PLN netto

349,67 PLN brutto/h

284,29 PLN netto/h

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Szkolenie wprowadza uczestników w świat Threat Huntingu i praktycznego wykorzystania platformy ESET Inspect.** **Wymagania:** podstawowa znajomość konfiguracji sieci komputerowych, podstawowa znajomość zagadnień związanych z TCP/IP, podstawowa znajomość działania procesów i składników w systemie operacyjnym Microsoft Windows, ukończenie szkolenia ESET Client & Network Security Administrator (wersja 13.0 lub nowsza) lub szkolenia ESET Protect Advanced - poziom podstawowy. **Szkolenie i materiały w języku polskim.**
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	05-03-2026
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

Celem szkolenia jest wykształcenie umiejętności praktycznego wykorzystania platformy XDR (Extended Detection and Response) w zakresie wykrywania, analizy oraz reagowania na zagrożenia IT, poprzez konfigurację i obsługę narzędzi ESET Inspect, tworzenie playbooków, analizowanie incydentów oraz raportowanie wyników w środowisku firmowym.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik potrafi skonfigurować i zarządzać platformą ESET XDR oraz integrować ją z innymi systemami bezpieczeństwa.	Poprawna konfiguracja środowiska XDR i integracja z co najmniej jednym systemem monitoringu lub SIEM.	Obserwacja w warunkach rzeczywistych
Uczestnik umie monitorować i analizować zdarzenia bezpieczeństwa w konsoli ESET Inspect.	Prawidłowa identyfikacja i klasyfikacja symulowanych incydentów w systemie XDR.	Obserwacja w warunkach rzeczywistych
Uczestnik potrafi tworzyć i wdrażać playbooki reagowania na incydenty w środowisku XDR.	Utworzenie i poprawne uruchomienie playbooku w środowisku testowym.	Obserwacja w warunkach rzeczywistych
Uczestnik zna metody raportowania i analizowania danych o zagrożeniach w celu podejmowania decyzji bezpieczeństwa.	Przygotowanie raportu zawierającego analizę incydentów i rekomendacje działań.	Obserwacja w warunkach rzeczywistych
Uczestnik potrafi reagować na zagrożenia i podejmować działania naprawcze zgodnie z procedurami bezpieczeństwa.	Skuteczne wykonanie działań reagowania na przykładowy incydent (np. izolacja endpointu, usunięcie zagrożenia).	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

1. Omówienie podstawowych pojęć związanych z Threat Huntingiem.
2. Przygotowanie playbook'a.
3. Wdrożenie serwera ESET Inspect on-prem – ćwiczenie.
4. Wdrożenie i konfiguracja ESET Inspect Connector – ćwiczenie.
5. Omówienie konsoli ESET Inspect oraz jakie dane zbiera XDR.
6. Podstawowe detekcje i reagowanie.
7. Uruchomienie podstawowej detekcji – ćwiczenie.
8. Weryfikacja incydentu.
9. Wykluczenia i ich tworzenie – ćwiczenie.
10. Przeprowadzenie analizy powłamaniowej – ćwiczenie.
11. Raportowanie i powiadomienia – ćwiczenie.

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	2 447,70 PLN
Koszt przypadający na 1 uczestnika netto	1 990,00 PLN
Koszt osobogodziny brutto	349,67 PLN
Koszt osobogodziny netto	284,29 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Michał Janik

Trener IT, specjalista, a następnie inżynier systemowy, prowadzący szkolenia w Dagma Szkolenia IT od 2016 roku z dziedziny cyberbezpieczeństwa, w tym CEH i produktów ESET. Obszar specjalizacji: Aplikacje typu Antywirus, szyfrowanie, DLP, MDM, Antyspam dla serwera pocztowego, CEH. Wykształcenie: wyższe, magister inżynier Informatyki.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- materiały dydaktyczne w formie elektronicznej (prezentacja przygotowana przez trenera, wysyłana na adres mailowy uczestnika)
- dostęp do 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.
- Szkolenie nie zawiera egzaminu.
- 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.

Warunki techniczne

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

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

Kontakt

Michalina Krzyszkowska

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