Możliwość dofinansowania

Monitorowanie infrastruktury z użyciem systemu SIEM Wazuh: od surowych logów do wykrycia incydentu

Numer usługi 2026/07/06/17164/3672255

3 185,70 PLN brutto
2 590,00 PLN netto
227,55 PLN brutto/h
185,00 PLN netto/h
261,33 PLN cena rynkowa

Dagma sp. z o.o.

4,5 / 5

467 ocen

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
14:00 h
01.12.2026 do 02.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób pracujących w sektorze IT, spełniających poniższe wymagania: • Podstawowa znajomość systemów Linux i Windows na poziomie administracyjnym • Podstawowa wiedza dotycząca zagadnień związanych z cyberbezpieczeństwem • Doświadczenie z narzędziami monitorującymi logi • Doświadczenie z urządzeniami sieciowymi
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	23-11-2026
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

Szkolenie skupia się na praktycznym wdrożeniu i eksploatacji Wazuh jako zaawansowanego systemu SIEM do monitorowania bezpieczeństwa infrastruktury IT.

Uczestnicy nauczą się instalować platformę, konfigurować agentów oraz analizować zdarzenia w czasie rzeczywistym, z naciskiem na wykrywanie zagrożeń i automatyzację reakcji. Po dwudniowym programie każdy będzie w stanie samodzielnie optymalizować Wazuh pod kątem firmowych potrzeb, w tym integracji z istniejącymi środowiskami serwerowymi i chmurow

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Efekty dotyczące wiedzy: uczestnik obsługuje konsolę Safetica Maintanance	Kategoryzuje aplikacje oraz strony internetowe, dezaktywuje moduły klienta Safetica	Obserwacja w warunkach symulowanych
Efekty dotyczące kompetencji społecznych: uczestnik buduje relacje społeczne.	Projektuje działania w oparciu o zasady empatii, budowania zaufania i efektywnej komunikacji	Wywiad swobodny
Efekty dotyczące umiejętności: uczestnik zarządza Safetica Discovery	Uruchomienia moduły Discovery, analizuje potencjalnych wycieków danych, dostosowuje konsole do filtrowania danych.	Obserwacja w warunkach symulowanych

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

Instalacja i podstawy konfiguracji Wazuh

- Wprowadzenie do Wazuh: funkcje, zastosowania i miejsce SIEM w bezpieczeństwie IT.
- Szczegółowa architektura: rola serwera, agentów, indexera oraz interfejsu graficznego.

- Pobranie i instalacja serwera Wazuh w środowisku Linux
- Konfiguracja agentów na systemach Windows i Linux; w tym tryb agentless na urządzeniach sieciowych (Syslog).
- Testowanie komunikacji między agentami i serwerem, podstawowy tuning ustawień.
- Wprowadzenie do zarządzania dashboardem Wazuh i monitorowanie pierwszych zdarzeń.

Zaawansowana konfiguracja i monitorowanie

- Tworzenie i modyfikacja reguł detekcji, pisanie własnych dekoderów do logów niestandardowych.
- Ustawienia monitorowania integralności plików (FIM) oraz detekcja rootkitów.
- Przegląd i rozszerzenie polityk bezpieczeństwa, konfiguracja alertów i powiadomień.
- Automatyzacja reakcji na incydenty (Active Response) i integracja z narzędziami IDS/IPS.
- Analiza logów oraz optymalizacja wydajności systemu poprzez tuning indeksów i konfiguracji indexera.
- Tworzenie i dostosowywanie dashboardów zgodnie z potrzebami codziennego monitoringu i raportowania.

Harmonogram

Liczba pozycji harmonogramu: 18

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 18 Wprowadzenie do Wazuh: funkcje, zastosowania i miejsce SIEM w bezpieczeństwie IT.	Zajęcia	Adam Jakubiec	01-12-2026	09:00	09:30	00:30
2 z 18 Szczegółowa architektura: rola serwera, agentów, indexera oraz interfejsu graficznego.	Zajęcia	Adam Jakubiec	01-12-2026	09:30	10:15	00:45
3 z 18 Pobranie i instalacja serwera Wazuh w środowisku Linux	Zajęcia	Adam Jakubiec	01-12-2026	10:15	11:15	01:00
4 z 18 -	Przerwa	-	01-12-2026	11:15	11:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 18 Konfiguracja agentów na systemach Windows i Linux; w tym tryb agentless na urządzeniach sieciowych (Syslog).	Zajęcia	Adam Jakubiec	01-12-2026	11:45	13:00	01:15
6 z 18 -	Przerwa	-	01-12-2026	13:00	13:30	00:30
7 z 18 Testowanie komunikacji między agentami i serwerem, podstawowy tuning ustawień.	Zajęcia	Adam Jakubiec	01-12-2026	13:30	14:30	01:00
8 z 18 Wprowadzenie do zarządzania dashboardem Wazuh i monitorowanie pierwszych zdarzeń.	Zajęcia	Adam Jakubiec	01-12-2026	14:30	16:00	01:30
9 z 18 Tworzenie i modyfikacja reguł detekcji, pisanie własnych dekoderów do logów niestandardowych.	Zajęcia	Adam Jakubiec	02-12-2026	09:00	10:30	01:30
10 z 18 Ustawienia monitorowania integralności plików (FIM) oraz detekcja rootkitów.	Zajęcia	Adam Jakubiec	02-12-2026	10:30	11:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 18 -	Przerwa	-	02-12-2026	11:30	11:45	00:15
12 z 18 Przegląd i rozszerzenie polityk bezpieczeństwa, konfiguracja alertów i powiadomień.	Zajęcia	Adam Jakubiec	02-12-2026	11:45	13:00	01:15
13 z 18 -	Przerwa	-	02-12-2026	13:00	13:30	00:30
14 z 18 Automatyzacja reakcji na incydenty (Active Response) i integracja z narzędziami IDS/IPS.	Zajęcia	Adam Jakubiec	02-12-2026	13:30	14:15	00:45
15 z 18 Analiza logów oraz optymalizacja wydajności systemu poprzez tuning indeksów i konfiguracji indexera.	Zajęcia	Adam Jakubiec	02-12-2026	14:15	14:45	00:30
16 z 18 Tworzenie i dostosowywanie dashboardów zgodnie z potrzebami codziennego monitoringu i raportowania.	Zajęcia	Adam Jakubiec	02-12-2026	14:45	15:30	00:45
17 z 18 -	Przerwa	-	02-12-2026	15:30	15:45	00:15
18 z 18 -	Walidacja	-	02-12-2026	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	3 185,70 PLN
Koszt przypadający na 1 uczestnika netto	2 590,00 PLN
Koszt osobogodziny brutto	227,55 PLN
Koszt osobogodziny netto	185,00 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 (dostęp do materiałów autorskich, przygotowanych przez trenera, przesłany na adres mailowy uczestnika)
- dostęp do przygotowanego środowiska wirtualnego na czas szkolenia

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

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

Kontakt

Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 327 931 093