Możliwość dofinansowania

"LUGA" AGNIESZKA GLIŃSKA

4,9 / 5

1 274 oceny

Mastering Wazuh - wykrywanie i analiza zarogżeń z wykorzytaniem WAZUH SIEM/XDR

Numer usługi 2026/04/20/7321/3501064

4 305,00 PLN brutto
3 500,00 PLN netto
134,53 PLN brutto/h
109,38 PLN netto/h
261,33 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
32:00 h
08.06.2026 do 11.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Identyfikatory projektów	Kierunek - Rozwój, FELB.06.03-IZ.00-0003/24 ZIPH, Nowy start w Małopolsce z EURESEM, Małopolski Pociąg do kariery, Zachodniopomorskie Bony Szkoleniowe
Grupa docelowa usługi	Szkolenie skierowane jest do administratorów systemów IT, specjalistów ds. bezpieczeństwa, inżynierów sieci oraz osób rozpoczynających pracę w obszarze cyberbezpieczeństwa. Uczestnik powinien posiadać podstawową wiedzę z zakresu systemów operacyjnych Windows i Linux oraz podstaw sieci komputerowych.
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	07-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestnika do samodzielnego wdrażania, konfiguracji oraz zarządzania systemem SIEM Wazuh w środowiskach IT. Uczestnik nabędzie umiejętności w zakresie monitorowania zdarzeń bezpieczeństwa, analizy logów, wykrywania zagrożeń oraz reagowania na incydenty w systemach Windows, Linux oraz środowiskach Active Directory.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Konfiguruje i wdraża system Wazuh	instaluje system Wazuh w architekturze All-in-One oraz klastrowej	Test teoretyczny z wynikiem generowanym automatycznie
	konfiguruje podstawowe komponenty systemu (manager, agent, indexer, dashboard)	Test teoretyczny z wynikiem generowanym automatycznie
	wdraża agentów na systemach Windows i Linux	Test teoretyczny z wynikiem generowanym automatycznie
	organizuje komunikację pomiędzy komponentami systemu	Test teoretyczny z wynikiem generowanym automatycznie
Analizuje zdarzenia i logi bezpieczeństwa	analizuje logi systemowe oraz sieciowe z wykorzystaniem Wazuh	Test teoretyczny z wynikiem generowanym automatycznie
	rozróżnia typy zdarzeń bezpieczeństwa i identyfikuje potencjalne zagrożenia	Test teoretyczny z wynikiem generowanym automatycznie
	interpretuje alerty generowane przez system Wazuh	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje dashboard do monitorowania i analizy zdarzeń	Test teoretyczny z wynikiem generowanym automatycznie
Tworzy i dostosowuje reguły detekcji	tworzy i modyfikuje reguły detekcji oraz dekodery	Test teoretyczny z wynikiem generowanym automatycznie
	dostosowuje zestaw reguł do specyfiki środowiska IT	Test teoretyczny z wynikiem generowanym automatycznie
		Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje listy CDB do rozszerzania mechanizmów detekcji	Test teoretyczny z wynikiem generowanym automatycznie
	aktualizuje i zarządza zestawem reguł Wazuh	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wykrywa zagrożenia i reaguje na incydenty	monitoruje integralność plików z wykorzystaniem mechanizmu FIM	Test teoretyczny z wynikiem generowanym automatycznie
	wykrywa rootkity oraz anomalie systemowe	Test teoretyczny z wynikiem generowanym automatycznie
	konfiguruje mechanizmy Active Response	Test teoretyczny z wynikiem generowanym automatycznie
	wdraża automatyczne reakcje na incydenty (np. blokowanie adresów IP)	Test teoretyczny z wynikiem generowanym automatycznie
Integruje Wazuh z innymi systemami	integruje Wazuh z systemami zewnętrznymi (np. Active Directory, Microsoft 365, IDS/IPS)	Test teoretyczny z wynikiem generowanym automatycznie
	konfiguruje przekazywanie danych do systemów zewnętrznych	Test teoretyczny z wynikiem generowanym automatycznie
	wykorzystuje API Wazuh do pobierania i analizy danych	Test teoretyczny z wynikiem generowanym automatycznie
	organizuje przepływ danych pomiędzy systemami bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie
Ocenia poziom bezpieczeństwa systemu IT	stosuje polityki SCA do oceny konfiguracji systemów	Test teoretyczny z wynikiem generowanym automatycznie
	analizuje podatności na podstawie danych inwentaryzacyjnych	Test teoretyczny z wynikiem generowanym automatycznie
	mapuje zdarzenia do frameworka MITRE ATT&CK	Test teoretyczny z wynikiem generowanym automatycznie
	ocenia skuteczność wdrożonych mechanizmów bezpieczeństwa	Test teoretyczny z wynikiem generowanym automatycznie

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

Usługa realizowana jest w formie szkolenia online (rozmowa na żywo) w czasie rzeczywistym. Program dostosowany jest do potrzeb uczestników z obszaru administracji IT i cyberbezpieczeństwa oraz ukierunkowany na zdobycie praktycznych umiejętności wdrażania i obsługi systemu Wazuh.

Szkolenie trwa **4 dni (32 godziny dydaktyczne)**.

1 godzina dydaktyczna = 45 minut.

Przerwy nie są wliczone w czas trwania usługi.

Podział zajęć:

- zajęcia teoretyczne: ok. 30%
- zajęcia praktyczne: ok. 70%

Każdy uczestnik pracuje na **indywidualnym środowisku laboratoryjnym w chmurze**, obejmującym systemy Windows, Linux oraz Active Directory.

Zakres tematyczny szkolenia:

Dzień 1:

- Wprowadzenie do Wazuh
- Architektura i bezpieczna komunikacja
- Projektowanie architektury
- Instalacja Wazuh (All-in-One, klaster)

Dzień 2:

- Wdrażanie i zarządzanie agentami (Linux/Windows, GPO)
- Centralna konfiguracja agentów
- Analiza logów i przepływ danych
- Monitorowanie syslog

Dzień 3:

- Wazuh Indexer i Dashboard
- Reguły i dekodery
- Listy CDB i ich zastosowanie
- Monitorowanie integralności plików (FIM)
- Wykrywanie rootkitów

Dzień 4:

- Inwentaryzacja i wykrywanie podatności
- Wykrywanie ataków (Active Directory)
- Integracje (Microsoft 365, IDS/IPS, API)

- Active Response
- SCA i ocena bezpieczeństwa
- MITRE ATT&CK

Warunki organizacyjne:

- szkolenie realizowane w trybie online (na żywo)
- grupa szkoleniowa: do 10 osób
- każdy uczestnik posiada dostęp do indywidualnego środowiska laboratoryjnego
- wymagany komputer z dostępem do Internetu

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Wprowadzenie do Wazuh, architektura systemu – rozmowa na żywo	Rafał Decyk	08-06-2026	09:00	10:30	01:30
2 z 16 Projektowanie architektury, komunikacja – rozmowa na żywo	Rafał Decyk	08-06-2026	10:45	12:15	01:30
3 z 16 Instalacja Wazuh (All-in-One) – rozmowa na żywo + ćwiczenia praktyczne	Rafał Decyk	08-06-2026	12:30	14:00	01:30
4 z 16 Instalacja klastra Wazuh – rozmowa na żywo + ćwiczenia praktyczne	Rafał Decyk	08-06-2026	14:15	15:45	01:30
5 z 16 Wdrażanie agentów (Linux/Windows) – rozmowa na żywo + ćwiczenia	Rafał Decyk	09-06-2026	09:00	10:30	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
6 z 16 Wdrażanie agentów GPO, aktualizacje – rozmowa na żywo	Rafał Decyk	09-06-2026	10:45	12:15	01:30
7 z 16 Centralna konfiguracja agentów – rozmowa na żywo + ćwiczenia	Rafał Decyk	09-06-2026	12:30	14:00	01:30
8 z 16 Analiza logów i przepływ danych – rozmowa na żywo + ćwiczenia	Rafał Decyk	09-06-2026	14:15	15:45	01:30
9 z 16 Wazuh Indexer i Dashboard – rozmowa na żywo	Rafał Decyk	10-06-2026	09:00	10:30	01:30
10 z 16 Reguły i dekodery – rozmowa na żywo + ćwiczenia	Rafał Decyk	10-06-2026	10:45	12:15	01:30
11 z 16 Listy CDB – rozmowa na żywo + ćwiczenia	Rafał Decyk	10-06-2026	12:30	14:00	01:30
12 z 16 FIM i wykrywanie rootkitów – rozmowa na żywo + ćwiczenia	Rafał Decyk	10-06-2026	14:15	15:45	01:30
13 z 16 Inwentaryzacja i podatności – rozmowa na żywo	Rafał Decyk	11-06-2026	09:00	10:30	01:30
14 z 16 Wykrywanie ataków (Active Directory) – rozmowa na żywo + ćwiczenia	Rafał Decyk	11-06-2026	10:45	12:15	01:30

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
15 z 16 Integracje (M365, IDS/IPS, API) – rozmowa na żywo	Rafał Decyk	11-06-2026	12:30	14:00	01:30
16 z 16 Active Response, SCA, MITRE ATT&CK + podsumowanie – rozmowa na żywo + ćwiczenia	Rafał Decyk	11-06-2026	14:15	15:45	01:30

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	4 305,00 PLN
Koszt przypadający na 1 uczestnika netto	3 500,00 PLN
Koszt osobogodziny brutto	134,53 PLN
Koszt osobogodziny netto	109,38 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Rafał Decyk

Szkolenie prowadzone jest przez doświadczonego Trenera – Architekta/Konsultanta Cyberbezpieczeństwa, posiadającego minimum 5-letnie doświadczenie zawodowe w zakresie administracji systemami IT oraz bezpieczeństwa informacji.
Trener posiada praktyczne doświadczenie w:
• wdrażaniu i utrzymaniu systemów SIEM (w tym Wazuh),
• analizie zdarzeń bezpieczeństwa oraz reagowaniu na incydenty,
• pracy z systemami Windows, Linux oraz środowiskami Active Directory,
• integracji systemów bezpieczeństwa (SIEM, IDS/IPS, rozwiązania chmurowe).
Posiada aktualne kwalifikacje oraz certyfikaty branżowe, potwierdzające kompetencje w zakresie

prowadzenia szkoleń oraz technologii IT, m.in.:
• certyfikaty Microsoft (np. MCSE / równoważne),
• certyfikat trenerski (MCT lub równoważny),
• inne certyfikaty z obszaru cyberbezpieczeństwa i administracji systemami.
Osoba prowadząca posiada doświadczenie w realizacji szkoleń dla osób dorosłych oraz prowadzeniu zajęć w formie zdalnej (online, w czasie rzeczywistym).

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

skrypty pdf

Warunki uczestnictwa

Uczestnik powinien:

- posiadać podstawową wiedzę z zakresu administracji systemami operacyjnymi Windows i Linux,
- znać podstawy sieci komputerowych oraz zagadnień bezpieczeństwa IT,
- posiadać komputer z dostępem do Internetu oraz przeglądarką internetową,
- mieć możliwość pracy w środowisku szkoleniowym udostępnionym przez organizatora (laboratorium w chmurze).

Warunki techniczne

Warunki techniczne – usługa zdalna

Zajęcia realizowane są w formie zdalnej, synchronicznej (rozmowa na żywo) z wykorzystaniem platformy ClickMeeting, umożliwiającej bezpośrednią komunikację audio-wideo (face to face), współdzielenie ekranu oraz bieżącą interakcję z uczestnikami.

W trakcie szkolenia stosowane są następujące metody realizacji zajęć:

- wykład (rozmowa na żywo),
- ćwiczenia praktyczne realizowane w środowisku laboratoryjnym,
- prezentacja,
- czat umożliwiający zadawanie pytań i konsultacje,
- współdzielenie ekranu przez trenera i uczestników.

Wymagania techniczne:

Uczestnik powinien dysponować:

- komputerem lub laptopem z dostępem do Internetu (stabilne łącze),
- procesorem min. dwurdzeniowym 2 GHz (zalecany czterordzeniowy),
- min. 4 GB pamięci RAM (zalecane 8 GB),
- systemem operacyjnym: Windows 10/11, macOS, Linux lub ChromeOS,
- aktualną przeglądarką internetową (Chrome, Firefox, Edge, Safari),
- sprawnie działającym mikrofonem, głośnikami oraz kamerą,

Dodatkowo uczestnik otrzymuje dostęp do środowiska laboratoryjnego w chmurze, niezbędnego do realizacji ćwiczeń praktycznych.

Kontakt

Agnieszka Glińska

E-mail info@luga.pl

Telefon (+48) 663 770 804