

## Szkolenie

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

[Strona szkolenia](#) | [Terminy szkolenia](#) | [Rejestracja na szkolenie](#) | [Promocje](#)

## Opis szkolenia

**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 chmurowymi.

### 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

## Harmonogram szkolenia

### Instalacja i podstawy konfiguracji Wazuh

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | [szkolenia@dagma.pl](mailto:szkolenia@dagma.pl)  
[szkolenia.dagma.eu](http://szkolenia.dagma.eu)

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15  
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy  
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł  
Numer NIP 634-012-60-68, numer REGON: 008173852  
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy  
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym  
opóźnieniom w transakcjach handlowych.

- 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 dekodów 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.

## Tagi:

Adres korespondencyjny:

**DAGMA Szkolenia IT** | ul. Bażantów 6a/3 | Katowice (40-668)  
tel. 32 793 11 80 | szkolenia@dagma.pl  
[szkolenia.dagma.eu](mailto:szkolenia.dagma.eu)

D3

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15  
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy  
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł  
Numer NIP 634-012-60-68, numer REGON: 008173852  
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy  
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym  
opóźnieniom w transakcjach handlowych.