

SZKOLENIE WAZUH

PRAKTYCZNY KURS
SIEM/XDR

Cel szkolenia	Forma
Przygotowanie uczestnika do samodzielnej instalacji, konfiguracji i utrzymania Wazuh oraz do analizy alertów i reagowania na incydenty w środowisku organizacji.	Intensywne warsztaty prowadzone stacjonarnie lub online. Ćwiczenia bazują na scenariuszach spotykanych w środowiskach firmowych.

Program

1. Fundamenty bezpieczeństwa i Wazuh

- Rola SIEM/XDR w ochronie infrastruktury
- Architektura i komponenty platformy Wazuh
- Planowanie środowiska laboratoryjnego i produkcyjnego

2. Instalacja i konfiguracja

- Instalacja serwera, indeksera, dashboardu i agentów
- Konfiguracja środowiska oraz pracy w klastrze
- Zarządzanie agentami i bezpieczna komunikacja

3. Detekcja zagrożeń

- Analiza zdarzeń i alertów
- Tworzenie własnych dekodów i reguł
- Scenariusze wykrywania incydentów w systemach Linux i Windows

4. Monitoring i analiza

- Wizualizacja danych i analiza logów
- Monitorowanie integralności plików i konfiguracji
- Identyfikacja anomalii oraz priorytetyzacja alertów

5. Zgodność i audyt

- Monitorowanie zgodności i stanu zabezpieczeń
- Audyt konfiguracji systemów
- Raportowanie wyników i rekomendacji

6. Integracje i automatyzacja

- Integracja z innymi źródłami logów i narzędziami
- Powiadomienia i automatyczne reakcje na incydenty
- Budowa spójnego procesu obsługi zdarzeń

7. Warsztaty praktyczne

- Symulacja wybranych zdarzeń bezpieczeństwa
- Analiza alertu od źródła do decyzji
- Reagowanie i dokumentowanie działań krok po kroku

8. Utrzymanie i rozwój

- Aktualizacje systemu i agentów
- Dobre praktyki administracyjne
- Plan dalszego rozwoju reguł, dashboardów i integracji

Dla kogo

- administratorzy systemów i sieci
- specjaliści cyberbezpieczeństwa i analitycy SOC
- zespoły DevOps/SecOps
- osoby rozwijające kompetencje w obszarze SIEM/XDR

Wymagania wstępne

Podstawowa znajomość systemów Linux i Windows, sieci komputerowych oraz bezpieczeństwa IT.
Doświadczenie administracyjne ułatwi wykonanie ćwiczeń, ale nie jest wymagane na poziomie zaawansowanym.

Efekt po szkoleniu

- samodzielna instalacja i podstawowa administracja Wazuh
- tworzenie i dostosowywanie reguł detekcji
- analiza alertów oraz przygotowanie reakcji na incydenty
- planowanie utrzymania i rozwoju środowiska

**Zapytaj o termin lub szkolenie
dedykowane**

**kontakt@itproconsulting.pl
+48 12 311 02 90**

Aktualny zakres, termin i cena są potwierdzane indywidualnie przed zamówieniem szkolenia.