securitum

WAZUH Expert

Praktyczny kurs z zakresu administrowania narzędziem SIEM

8 3-godzinnych sesji szkoleniowych

- Kompleksowa wiedza: od instalacji po zaawansowaną konfigurację
- Doświadczony trener-praktyk
- Przystępna formuła *online*
- Dostęp do nagrania przez 180 dni od daty szkolenia
- Spełnienie wymogów dyrektywy NIS 2

DLA KOGO

- Administratorzy systemów IT
- Specjaliści bezpieczeństwa IT
- Pracownicy SOC
- Pasjonaci bezpieczeństwa IT

DLACZEGO WAZUH?

- Otwartoźródłowy, darmowy system zarządzania informacjami i zdarzeniami bezpieczeństwa
- Multiplatformowy, wspiera m.in. Windows, Linux i macOS
- Skalowalny, odpowiedni dla małych i dużych infrastruktur
- Integrujący się z głównymi dostawcami rozwiązań chmurowych: AWS, Azure czy Google Cloud
- Oferujący zaawansowane funkcje monitorowania
- Elastyczny, dający możliwość dostosowania do potrzeb organizacji

MODUŁ PODSTAWOWY

- 28.01.2025 r.
- 4, 11, 18, 25.02.2025 r.

899 ZŁ NETTO

MODUŁ ZAAWANSOWANY

- 4, 11 i 18.03.2025 r.

499 ZŁ NETTO

BILET PRO

MODUŁ PODSTAWOWY + ZAAWANSOWANY

1299 ZŁ NETTO

https://sklep.securitum.pl/wazuh-expert

TRENER

Tomasz Turba. Konsultant ds. bezpieczeństwa IT w firmie Securitum. Posiada certyfikaty Cisco, Red Hat, AWS, Microsoft, NSA 4011 oraz ABW. Ma ponadpiętnastoletnie doświadczenie w dziedzinie IT; zaczął już w szkole średniej, realizując zlecenia jako administrator sieci osiedlowej. Współpracował z licznymi instytucjami jako konsultant ds. zabezpieczeń, pentester i inspektor RODO. Ma duże doświadczenie jako szef zespołu CSIRT. Od 2022 r. pełni funkcje researchera i trenera w firmie Securitum. Pasjonat bezpieczeństwa informacji, z zacięciem do przekazywania wiedzy. Prowadzi szkolenia z analizy śledczej, bezpieczeństwa sieci, białego wywiadu OSINT, tematyki związanej z AI, a także wykłady na temat *cyberawareness*. Laureat kilku konkursów na najlepszą publikację o bezpieczeństwie IT. Prelegent na MEGA Sekurak Hacking Party. Redaktor w portalu sekurak.pl oraz książek o bezpieczeństwie IT, wydawanych przez Securitum.

AGENDA

SESJA NR 1: Wazuh – wprowadzenie, instalacja i konfiguracja:

1. **Wprowadzenie do Wazuha:**
   - Co to jest Wazuh i jakie problemy rozwiązuje.
   - Przegląd architektury Wazuha.
2. **Przygotowanie środowiska:**
   - Wymagania systemowe.
   - Przygotowanie maszyny wirtualnej i fizycznej z systemem Linux.
3. **Instalacja Wazuha:**
   - Pobieranie i instalacja serwera Wazuh.
   - Konfiguracja bazowa i instalacja dodatków.
4. **Podstawowa konfiguracja:**
   - Konfiguracja agenta Wazuh na systemach Linux i Windows.
   - Testowanie połączenia, tuning bazowy.
5. **Podsumowanie i sesja Q&A.**

SESJA NR 2: Wazuh – konfiguracja szczegółowa i troubleshooting:

1. **Zaawansowana konfiguracja:**
   - Konfiguracja reguł i polityk bezpieczeństwa.
   - Tworzenie i modyfikacja dekoderów.
2. **Integracja z innymi narzędziami:**
   - Integracja z Elastic Stack (Elasticsearch, Logstash, Kibana).
   - Konfiguracja logowania i monitoringu.
3. **Troubleshooting:**
   - Rozwiązywanie typowych problemów z instalacją i konfiguracją.
   - Analiza logów i błędów.
4. **Podsumowanie i sesja Q&A.**

SESJA NR 3: Wazuh – zarządzanie serwerem i bezpieczeństwo systemu:

1. **Zarządzanie użytkownikami:**
   - Tworzenie kont użytkowników i zarządzanie nimi w Wazuhu.
   - Konfiguracja ról i uprawnień użytkowników.
   - Implementacja polityk bezpieczeństwa dla użytkowników.
   - Audyt i monitorowanie działań użytkowników.
2. **Bezpieczeństwo systemu:**
   - Zabezpieczenie komunikacji między komponentami Wazuha (SSL/TLS).
   - Konfiguracja i zarządzanie zaporami sieciowymi.
   - Implementacja polityk bezpieczeństwa systemu operacyjnego.
   - Monitorowanie i reakcja na próby naruszenia bezpieczeństwa.
3. **Backup i przywracanie danych:**
   - Strategie tworzenia kopii zapasowych dla Wazuha.
   - Konfiguracja automatycznego backupu.
   - Procedury przywracania danych w przypadku awarii.
4. **Analiza i raportowanie:**
   - Tworzenie niestandardowych raportów bezpieczeństwa.
   - Konfiguracja powiadomień i alertów dotyczących naruszeń bezpieczeństwa.
   - Analiza logów pod kątem wykrywania potencjalnych zagrożeń.
5. **Podsumowanie i sesja Q&A.**

SESJA NR 4: Wazuh – reagowanie na incydenty:

1. **Wprowadzenie do podstawowych pojęć i zagrożeń.**
2. **Wykrywanie i reagowanie na incydenty:**
   - Tworzenie reguł detekcji i zarządzanie nimi.
   - Analiza i reagowanie na alerty.
3. **Symulacja ataku i analiza jego skutków za pomocą Wazuha.**
4. **Przykłady realnych incydentów i reagowania na nie.**
5. **Podsumowanie i sesja Q&A.**

SESJA NR 5: Wazuh – konfiguracja klastra:

1. **Wprowadzenie do instalacji klastrowej:**
   - Korzyści z użycia klastra.
   - Przegląd architektury klastrowej.
2. **Instalacja klastra:**
   - Konfiguracja węzłów klastra.
   - Load balancing i redundancja.
3. **Skalowanie i optymalizacja:**
   - Monitorowanie wydajności.
   - Optymalizacja konfiguracji pod kątem wydajności.
4. **Podsumowanie i sesja Q&A.**

SESJA NR 6: Wazuh – konfiguracje zaawansowane:

1. **Integracja z usługami zewnętrznymi:**
   - Wykrywanie zagrożeń w środowisku Office 365.
   - Wykrywanie sygnatur za pomocą YARA.
   - Wzbogacanie komunikatów za pomocą ChatGPT.
   - Automatyzacja za pomocą Ansible.
   - Integracja innych rozwiązań za pomocą API.
2. **Monitorowanie zdarzeń w kontenerach.**
3. **Monitorowanie infrastruktury chmurowej.**
4. **Aktualizacja agentów przez polityki GPO.**
5. **Podsumowanie i sesja Q&A.**

SESJA NR 7: Wazuh – optymalizacje zaawansowane:

1. **Odnajdywanie wąskich gardeł za pomocą Prometheus i Grafana.**
2. **Monitorowanie wydajności indeksowań i zapytań.**
3. **Implementacja Cross-Cluster Search.**
4. **Automatyzacja audytów zgodności i raportowania za pomocą Global Compliance Dashboard.**
5. **Zarządzanie automatyzacją reakcji na incydenty za pomocą Jira.**
6. **Optymalizacja retencji danych i zarządzanie logami.**
7. **Sesja Q&A.**

SESJA NR 8: Wazuh – integracje eksperta:

1. **Integracja z MISP.**
2. **Integracja z Suricata.**
3. **Integracja z Zeek.**
4. **Integracja z Zabbix.**
5. **Integracja z OpenVAS.**
6. **Integracja z Git.**
7. **Integracja z Graylog.**
8. **Integracja z OTRS.**
9. **Integracja z nmap i ChatGPT.**
10. **Integracja z OSSIM AlienVault.**
11. **Integracja z Atlassian Jira.**
12. **Integracja z Sysmon.**
13. **Sesja Q&A.**

Do każdej z sesji zostanie dołączone praktyczne ćwiczenie – laboratorium do samodzielnej realizacji.

ZAPISY I SZCZEGÓŁY

https://sklep.securitum.pl/wazuh-expert

Dodatkowe pytania: Aneta Jandziś
aneta.jandzis@securitum.pl
tel. +48 (12) 352 33 82
+48 516 824 029