

Wazuh – SIEM w praktyce (kod: LX-WAZUH)

Opis i cel szkolenia

Wazuh to darmowy system klasy SIEM, który coraz częściej pojawia się w firmach i instytucjach, także w projektach realizowanych pod NIS2. Na szkoleniu uczestnicy instalują serwer Wazuh, podłączają agentów na Windowsie i Linuksie oraz urządzenia sieciowe przez Syslog, a potem uczą system rozpoznawać to, co ważne: piszą własne reguły i dekodery, włączają monitorowanie integralności plików, konfigurują alerty i automatyczną reakcję na incydenty.

Po tych dwóch dniach:

- zainstalujesz Wazuh i zrozumiesz rolę serwera, agentów, indexera i dashboardu,
- podłączysz stacje, serwery i urządzenia sieciowe do centralnej analizy logów,
- napiszesz własną regułę detekcji i dekodery dla nietypowych logów,
- skonfigurujesz monitorowanie integralności plików, wykrywanie rootkitów i powiadomienia,
- ustawisz automatyczną reakcję na wybrane incydenty i połączysz Wazuh z systemem IDS/IPS,
- przygotujesz dashboardy i raporty do codziennego monitoringu bezpieczeństwa.

Asystenci AI przydadzą się tu głównie przy pisaniu i sprawdzaniu reguł oraz dekoderek – pokazujemy, jak z nich korzystać i jak weryfikować wynik.

To szkolenie skupia się na samym narzędziu – jak Wazuh wdrożyć, skonfigurować i utrzymać. Jeśli bardziej interesuje Cię praca analityka na takim systemie – wykrywanie ataków, ocena alertów i obsługa incydentu od pierwszego sygnału do raportu – wybierz trzydniowe szkolenie Analityk SOC – monitoring, detekcja, reagowanie, które również opiera się na Wazuh.

Skorzystają z niego administratorzy systemów i sieci, inżynierowie bezpieczeństwa odpowiedzialni za utrzymanie SIEM, informatycy działów IT i OT, a także osoby odpowiedzialne za wdrożenie i odbiór systemu SIEM od wykonawcy.

Czas trwania

2 dni

Program

1. Wazuh i SIEM – wprowadzenie
 - Co robi SIEM i gdzie jest jego miejsce w bezpieczeństwie IT
 - Funkcje i typowe zastosowania Wazuh
2. Architektura
 - Serwer, agenci, indexer i dashboard – rola i współpraca komponentów
 - Wdrożenie jednowęzłowe i rozproszone – kiedy które
3. Instalacja i pierwsze uruchomienie
 - Pobranie i instalacja serwera Wazuh na Linuksie
 - Agenci na Windowsie i Linuksie: instalacja, rejestracja, grupy
 - Tryb bezagentowy: logi z urządzeń sieciowych przez Syslog
 - Sprawdzenie komunikacji i podstawowy tuning
 - Dashboard: nawigacja i pierwsze zdarzenia
4. Reguły i dekodery
 - Jak Wazuh przetwarza logi: dekodowanie, reguły, poziomy alertów

Zapytaj o szczegóły

tel. 22 63 64 164

akademia@alx.pl

- Modyfikacja reguł wbudowanych
- Własne reguły detekcji
- Własne dekodery dla niestandardowych logów
- 5. Monitorowanie hostów
 - Monitorowanie integralności plików (FIM)
 - Wykrywanie rootkitów
 - Ocena konfiguracji i polityki bezpieczeństwa – przegląd i rozszerzanie
- 6. Alerty i reakcja na incydenty
 - Konfiguracja alertów i powiadomień
 - Active Response – automatyczna reakcja na zdarzenia
 - Integracja z systemami IDS/IPS
- 7. Analiza i wydajność
 - Analiza logów i wyszukiwanie zdarzeń
 - Tuning indeksów i konfiguracji indexera
- 8. Dashboardy i raporty
 - Własne dashboardy do codziennego monitoringu
 - Raporty dla zespołu i kierownictwa

Zapytaj o szczegóły

tel. 22 63 64 164

akademia@alx.pl

Dla grup na zamówienie możemy rozszerzyć szkolenie o klaster Wazuh, wykrywanie podatności, integracje z narzędziami do obsługi incydentów albo przygotować przykłady pod infrastrukturę zamawiającego.

Przeznaczenie i wymagania

Szkolenie jest przeznaczone przede wszystkim dla:

- administratorów systemów Windows i Linux oraz administratorów sieci,
- inżynierów bezpieczeństwa, którzy wdrażają lub utrzymują SIEM,
- informatyków działów IT i OT w firmach i instytucjach,
- osób wdrażających Wazuh lub przejmujących go po wykonawcy.

Od uczestników oczekujemy:

- podstawowej znajomości pracy w wierszu poleceń Linuksa,
- ogólnej orientacji w sieciach i w tym, czym są logi systemowe,
- podstawowej znajomości administracji systemem Windows lub Linux.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

- Warszawa – ul. Jasna 14/16A
- Zdalnie – zajęcia realizowane poprzez platformę Zoom
- Kraków – ul. św. Filipa 23
- Warsaw (English) – Jasna 14/16A
- Online (English) – your home, office or wherever you want
- na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

1990 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

- autorskie materiały szkoleniowe,
- indywidualne stanowisko komputerowe do pracy podczas zajęć,
- certyfikaty ukończenia szkolenia,

- drobny poczęstunek oraz ciepłe i zimne napoje,
- możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły

tel. 22 63 64 164

akademia@alx.pl