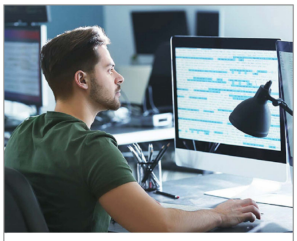
I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

Administracja urządzeniem FortiAnalyzer



Skorzystaj z jednodniowych warsztatów i zdobądź wiedzę jak:

- poprawnie skonfigurować FortiAnalyzera
- monitorować wszystkie Twoje urządzenia Fortinet
- odnaleźć się w gąszczu zdarzeń bezpieczeństwa
- tworzyć użyteczne i czytelne raporty
- wydobyć niestandardowe informacje z bazy danych
- rozwiązywać problemy z urządzeniem

Czas
1 DZIEŃ

Godziny
9:00 - 16:00

Certyfikat
TAK

OPIS SZKOLENIA

Poznasz w jakich trybach może działać FortiAnalyzer, czym jest "Analytics" oraz jak ustawić Log Storage Policy zgodnie z best practice. Nauczysz się tworzyć wzory raportów, które będzie można bezpośrednio przedstawić przełożonym lub zarządowi. Po szkoleniu swobodnie będziesz pisał zapytania do bazy danych FAZ typu SELECT aby wyciągać z nich szczegółowe i najpotrzebniejsze dane, a za pomocą Events Handler konfigurował potrzebne powiadomienia.

CEL SZKOLENIA

Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniem FortiAnalyzer. Poznanie funkcjonalności urządzenia, konfiguracji do współpracy z urządzeniami FortiGate oraz możliwości monitorowania i raportowania. Szkolenie prowadzone jest w oparciu o firmware 6.2.

FORMA SZKOLENIA

Szkolenie prowadzone jest w formie zdalnego wykładu, połączonego z ćwiczeniami warsztatowymi wykonywanymi zdalnie.

WYMAGANIA

Znajomość zagadnień omawianych na szkoleniach z zarządzania urządzeniami FortiGate. Podstawowa wiedza na temat tworzenia zapytań w języku SQL (Structured Query Language).

Administracja urządzeniem FortiAnalyzer

Agenda szkolenia:

Architektura urządzeń FortiAnalyzer

- Rola FortiAnalyzer w infrastrukturze
- Tryby pracy urządzenia i wstępna konfiguracja

Zarządzanie monitorowanymi urządzeniami

- Koncepcja ADOM (Administrative Domains)
- Dodawanie/blokowanie urządzeń
- Bezpieczna komunikacja

Konfiguracja opcji systemowych

- System dashboard
- Zarządzanie logami i archiwizacja
- Agregowanie logów
- Backup i przywracanie po awarii
- Aktualizacja firmware
- Zarządzanie dyskiem

Logowanie i monitorowanie zdarzeń

- Przeglądanie logów i mechanizmy wyszukiwania
- Zabezpieczanie logów
- FortiView
- Log Fetching
- Content Archive
- Indicator of Compromise (IOC)
- Alerty – monitorowanie zdarzeń

NOC–SOC

Wprowadzenie do raportowania

- Projektowanie i przeglądanie raportów
- Dataset – zaawansowane zapytania do bazy danych
- Podstawy SQL

Zaawansowana konfiguracja i rozwiązywanie problemów

TRENERZY

Certyfikowani inżynierowie **FORTINET NETWORK SECURITY EXPERT** posiadający wieloletnie doświadczenie w zakresie wdrażania i wsparcia omawianych rozwiązań.

TADEUSZ SELBIRAK

PAWEŁ PŁACHECKI

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

(22) 427 37 54 / +48 728 540 162