I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

FORTISIEM - monitorowanie infrastruktury IT

Skorzystaj tego zaawansowanego szkolenia i poznaj wszystkie funkcje rozwiązania FortiSiem. Po jego ukończeniu będziesz mógł samodzielnie:

- wdrożyć i skonfigurować rozwiązanie
- dodać wszystkie systemy, które chcesz monitorować
- poprawnie skonfigurować reguły i reakcje na incydenty
- korzystać z funkcji monitorowania i raportowania

Czas
3 DNI

Godziny
9:00 - 16:00

Certyfikat
TAK

OPIS SZKOLENIA

Szkolenie dedykowane jest wszystkim tym, którzy administrują lub planują wdrożenie rozwiązania FortiSiem. Porusza wszystkie aspekty konieczne do przeprowadzenia konfiguracji i nadzorowania pracy systemu. Uczestnicy mogą przećwiczyć zdobytą wiedzę podczas ćwiczeń praktycznych.

CEL SZKOLENIA

Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji rozwiązaniem FortiSIEM. Poznanie funkcjonalności rozwiązania oraz metod integracji z infrastrukturą IT.

FORMA SZKOLENIA

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

WYMAGANIA

Znajomość podstawowych zagadnień dotyczących administracji infrastrukturą sieciową, Active Directory, serwerami Windows/Unix/Linux. Znajomość podstawowych protokołów sieciowych.

FORTISIEM - monitorowanie infrastruktury IT

Agenda szkolenia:

Wprowadzenie do systemów SIEM

- Co to jest i do czego służy SIEM

Architektura FortiSIEM

- Omówienie składników FortiSIEM
- Metody przechowywania danych
- Indicators of Compromise (IOC)

Wstępna konfiguracja rozwiązania

Monitorowanie zdarzeń (SIEM)

- Które logi są istotne
- Metody zasilania logami
- Proces normalizacji i wzbogacania
- RAW vs. Structured
- Klasyfikacja - typy i atrybuty

Monitorowanie wydajności i dostępności urządzeń (PAM)

Wykrywanie i dodawanie urządzeń

- Auto-log discovery
- GUI discovery

Agent dla systemów Windows/Linux

Wyszukiwanie i analiza danych

- Simple Search
- Structured Search

CMDB

- Co to jest CMDB
- Wykorzystywanie CMDB w wyszukiwaniu danych
- Watchlists

Agregacja i grupowanie danych

Reguły

Incydenty i powiadomienia

Raporty i panele użytkownika

TRENER - TADEUSZ SELBIRAK

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

W branży IT od 2005 roku

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

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