I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

FortiMail - kompleksowe bezpieczeństwo poczty elektronicznej

Weź udział w szkoleniu i poznaj wszystkie funkcje rozwiązania FortiMail. Podczas praktycznych warsztatów dowiesz się jak:

- wybrać optymalny tryb pracy urządzenia
- działają moduły ochronne rozwiązania
- poprawnie skonfigurować polityki bezpieczeństwa
- korzystać z logów i raportowania
- diagnozować i rozwiązywać problemy

Czas
2 DNI

Godziny
9:00 - 16:00

Certyfikat
TAK

OPIS SZKOLENIA

Celem szkolenia jest zdobycie praktycznych umiejętności przydatnych w budowaniu ochrony przed zagrożeniami pochodzącymi z poczty elektronicznej. Zapoznanie z protokołem SMTP umożliwi Ci swobodniejszą analizę maili oraz wybór odpowiedniej techniki ochrony na przykładzie rozwiązania FortiMail.

Uczestnicząc w warsztatach zwiększysz pewność swoich działań oraz poznasz istotne funkcje jakimi FortiMail dysponuje. W miłej atmosferze będziesz mógł sprawdzić i wymienić doświadczenia z naszymi inżynierami.

CEL SZKOLENIA

Zdobycie umiejętności praktycznych potrzebnych do samodzielnej administracji urządzeniami FortiMail. Poznanie najczęściej spotykanych zagrożeń związanych z pocztą elektroniczną oraz sposobów ich zwalczania przy użyciu urządzeń FortiMail.

FORMA SZKOLENIA

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

WYMAGANIA

Podstawowa znajomość TCP/IP oraz zagadnień bezpieczeństwa sieci komputerowych. Znajomość zasad działania protokołów poczty elektronicznej.

FortiMail - kompleksowe bezpieczeństwo poczty elektronicznej

Agenda szkolenia:

Przegląd modeli oraz podstawowe tryby pracy urządzeń FortiMail

Protokół SMTP i zagrożenia sieciowe z nim związane

Podstawowa konfiguracja urządzenia

- Konfiguracja trybu pracy
- Ustawienia sieciowe
- Administracja domeną pocztową
- Listy dostępowe
- Ustawienia logowania i raportowania

Mechanizmy zabezpieczające wykorzystywane przez urządzenie

- Etapy analizy wiadomości
- Zastosowanie profili
- Polityki bezpieczeństwa
- Opcje uwierzytelniania

Zaawansowana konfiguracja profili

- Metody blokowania niechcianych wiadomości
- Konfiguracja uwierzytelniania (SMTP, IMAP, POP3, RADIUS)
- Synchronizacja z bazą LDAP
- Filtrowanie zawartości
- Wykorzystanie profili TLS

Administrowanie kwarantanną

Wykorzystanie sieciowych pamięci masowych

Archiwizacja wiadomości

Analiza logów i raportów

Budowa klastra HA, omówienie możliwych konfiguracji

Zaawansowana konfiguracja i rozwiązywanie problemów

- Wykorzystanie CLI
- Podnoszenie wersji firmware
- Eksport konfiguracji

Omówienie problemów poruszonych przez uczestników szkolenia

TRENER – PAWEŁ PŁACHECKI

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

Doświadczenie w obszarze cybersecurity zdobywa od ponad dekady.

www.iknowit.com.pl

AL. JEROZOLIMSKIE 142B, 02-305 WARSZAWA

szkolenia@ iknowit.com.pl

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