I know IT by softinet

KNOWLEDGE THAT
EMPOWERS BUSINESS

FORTIWEB – zarządzanie ochroną aplikacji webowych

Na tym szkoleniu dowiesz się:

- jak chronić aplikację webową przed atakami za pomocą rozwiązania FortiWeb
- jak kontrolować dostęp do serwerów back-end
- jak zastosować SSL offloading
- jak wykorzystać skaner podatności
- o możliwościach diagnostycznych

Czas	Godziny	Koszt	Certyfikat
2 DNI	9:00 - 16:00	1800 PLN	TAK

OPIS SZKOLENIA

Szkolenie dedykowane administratorom korzystającym z rozwiązania FortiWeb i pragnących zwiększyć bezpieczeństwo aplikacji webowych udostępnianych w swojej organizacji. Prowadzone jest w formie warsztatów, które pozwalają na praktyczne przećwiczenie zdobytych umiejętności.

CEL SZKOLENIA

Zdobycie umiejętności pozwalających na wdrożenie oraz zarządzanie urządzeniami FortiWeb. Podczas szkolenia uczestnicy poznają funkcjonalności urządzenia oraz dowiedzą się jak odpowiednio zabezpieczyć i akcelerować aplikacje webowe. Przedstawione zostaną również kwestie związane z monitorowaniem urządzenia oraz rozwiązywaniem problemów.

FORMA SZKOLENIA

Szkolenie prowadzone jest w formie warsztatów, podczas których uczestnicy będą mieli okazję praktycznego wykorzystania zdobytej wiedzy.

WYMAGANIA

Znajomość podstawowych zagadnień związanych z działaniem aplikacji webowych oraz protokołów http / https.

FORTIWEB – zarządzanie ochroną aplikacji webowych

Agenda szkolenia:

1. **HTTP/HTTPS – wprowadzenie**
2. **Aplikacje web – rodzaje zagrożeń**
3. **Koncepcja Web Application Firewall**
4. **Podstawowa konfiguracja i administracja urządzeniem**
   • Implementacja w strukturze sieciowej
   • Omówienie dostępnych trybów pracy
5. **Zarządzanie ruchem do serwerów back-end**
   • **Wykorzystanie load-balancingu**
6. **SSL/TLS** • Bezpieczeństwo protokołów • SSL offloading • akceleracja aplikacji webowych
7. **Budowanie polityk i profili bezpieczeństwa** • Web Protection Profile • HTTP Content routing • Ochrona przed atakami DoS • Kontrola dostępu
8. **Machine Learning • Anomaly Detection • Botnet Detection**
9. **Dodatkowa kontrola aplikacji webowych** • PCI DSS • OWASP Top 10 • Skanowanie podatności
10. **Monitorowanie urządzenia i rozwiązywanie problemów.**

TRENER – TADEUSZ SEL IRAK

Certyfikowany inżynieFORTINET NETWORK SECURITY EXPERT posiadający wieloletnie doświadczenie w zakresie wdrażania i wsparcia omawianych rozwiązań.

W branży IT od 2005 roku