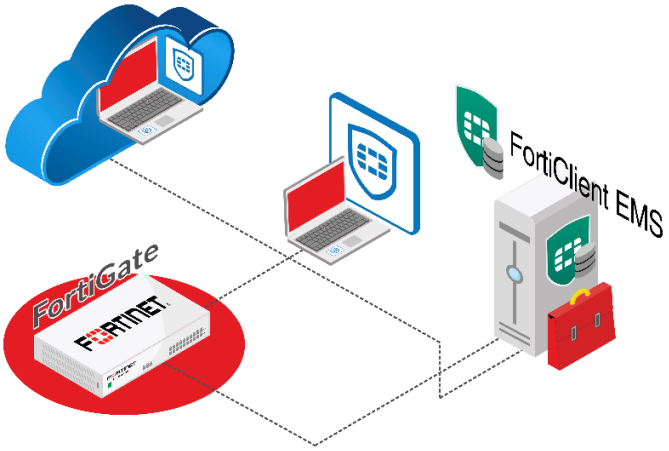

SZKOLENIE

Fortinet bez tajemnic

Cel szkolenia?

Naszym celem jest dostarczenie specjalistom IT i bezpieczeństwa sieciowego solidnej wiedzy na temat wdrożenia podstawowych zabezpieczeń sieci firmowych wykorzystując zaawansowany firewall FortiGate, oraz wiedzy na temat wdrożenia dedykowanego systemu umożliwiającego monitorowanie oraz zarządzanie stacjami roboczymi w ich organizacji - FortiClient EMS. Podczas szkolenia uczestnicy dowiedzą się jak od podstaw skonfigurować funkcje ochronne FortiGate, oraz jak zapewnić bezpieczny dostęp zdalny do ich instytucji. Bez zbędnej teorii, skupiając się na praktycznych wskazówkach trenera skonfigurują własną jednostkę FortiGate, poznają zasady zapory, uwierzytelniania użytkowników, SSL VPN, IPsec-VPN oraz sposoby ochrony sieci przy użyciu profili bezpieczeństwa. Ponadto, każdy z uczestników będzie miał okazję przeprowadzić wdrożenie swojego własnego serwera zarządzającego FortiClient EMS, podczas którego pozna tajniki integracji obu rozwiązań i korzyści z niej płynących. Każdy z uczestników skonfiguruje własne profile zabezpieczeń dla stacji roboczych i przetestuje działanie konfiguracji aplikacji FortiClient w zależności od aktualnego stanu bezpieczeństwa stacji roboczej zarządzanej przez FortiClientEMS.

Dla kogo?

Szkolenie przeznaczone jest dla inżynierów bezpieczeństwa i administratorów systemów zajmujących się zarządzaniem, konfiguracją i monitorowaniem urządzeń FortiGate, którzy jednocześnie stoją przed wyzwaniem zabezpieczenia stacji roboczych w swoich organizacjach, możliwością monitorowania stanu ich bezpieczeństwa podczas gdy znajdują się w sieciach korporacyjnych jak i poza nimi oraz dla administratorów będących świadomymi zagrożeń jakie wynikają ze stale rosnącej ilości sprzętu (często prywatnego), który uzyskuje dostęp do zasobów instytucji.

Jak szkolimy?

Szkolenie realizowane jest w formie mini wykładów oraz ćwiczeń praktycznych. Łączy w sobie fachową wiedzę merytoryczną z praktycznymi przykładami jej wykorzystania w środowisku pracy. W ramach spotkania zapewniamy przerwy kawowe oraz lunch. **Szkolenie zakończone jest certyfikatem.**

Czas trwania?

Szkolimy trzy dni w godzinach od 9:00 do 16:00.

Kto prowadzi szkolenie?

Tomasz Baron

Trener pracujący w Akademii BB, posiadających wieloletnie doświadczenie w branży IT, na co dzień pracujący przy wdrożeniach technologii UTM i rozwiązywaniu problemów sieciowych naszych Klientów. Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (m. in. NSE4, NSE5, NSE7) oraz setki zadowolonych administratorów IT, których Tomek miał okazję przeszkolić.

Agenda szkolenia:

I. PODSTAWY ZARZĄDZANIA UTM

1. KONFIGURACJA SIECIOWA
   a) konfiguracja urządzeń z poziomu CLI - poruszanie się; komendy SHOW / GET
   b) adresacja IP; rodzaje interfejsów
   c) dns; serwer usługi dns
   d) routing statyczny
2. BACKUP USTAWIEŃ
   a) backup ręczny / GUI / USB
   b) backup automatyczny

II. FIREWALL

1. POLITYKI FIREWALLA
   a) tworzenie obiektów / adresów / serwisów / przedziałów czasowych
   b) zasady działania polityk firewalla / przykłady reguł
2. POLITYKI OCHRONY DOS
   a) zasady działania / tworzenie ochrony
3. ZARZĄDZANIE PASMEM
   a) tworzenie polityk
   b) tworzenie profili

III. PROFILE UTM

1. ANTIVIRUS
   a) tworzenie profili / metody skanowania (proxy / flow)
   b) skanowanie portów; ograniczenia
   c) blokowanie; sprawdzanie logów
2. WEB FILTER
   a) tworzenie profili / metody skanowania (proxy / flow)
   b) blokowanie stron po kategoriach producenta / własnych / wyjątki
   c) blokowanie statyczne URL
3. DNS FILTER
   a) zasady działania / tworzenie profili
   b) kontrola zapytań wg. wzorców producenta
   c) ręczna kontrola zapytań
4. APPLICATION CONTROL
   a) zasady działania / tworzenie profili
   b) kontrola aplikacji / grup
   c) tworzenie wyjątków
5. INTRUSION PREVENTION
   a) zasady działania / tworzenie profili
   b) kontrola ochrony na podstawie sygnatur
   c) tworzenie wyjątków

IV. VPN

1. SSL-VPN
   a) zasady działania / konfiguracja dostępu
   b) dostęp do portalu web / możliwości auto-konfiguracji
   c) tryb pełnego tunelowania / zasady dostępu
2. IPSEC DIALUP

a) zasady działania / konfiguracja dostępu
b) **tworzenie polityk i kontrola ruchu**

3. IPSEC SITE-TO-SITE
   a) konfiguracja tuneli między dwoma FG
   b) polityki dostępu / logowanie ruch

V. PORADY DOŚWIADCZONEGO ADMINA

1. DOBRE PRAKTYKI
   a) wdrożenie ochrony antywirusowej - Integracja z FortiSandbox Cloud
   b) podwójne uwierzytelnienie - wdrożenie tokenów 2FA
2. LOGOWANIE / alertowanie / debugowanie
   a) przeglądanie logów
   b) konfiguracja powiadomień
   c) debug ruchu / rozwiązywanie problemów

VI. FORTI CLIENT EMS

1. WPROWADZENIE DO FORTI CLIENT EMS
   a) Wprowadzenie do FortiClient oraz FortiClient EMS
   b) Omówienie możliwości aplikacji FortiClient
   c) Omówienie możliwości aplikacji FortiClient EMS
   d) Przedstawienie możliwości wdrożenia FortiClient EMS
2. LICENCJONOWANIE
   a) omówienie licencjonowania
   a) przedstawienie różnic licencjonowania w zależności od typu wdrożenia
3. WDROŻENIE SERWERA FORTI CLIENT EMS
   a) omówienie wymaganych komponentów
   b) instalacja aplikacji na serwerze Windows Server 2022
4. KONFIGURACJA SERWERA ZARZĄDZAJĄCEGO FORTI CLIENT EMS
   a) konfiguracja ustawień sieciowych serwera
   b) konfiguracja ustawień telemetrii
   c) konfiguracja klucza zabezpieczeń telemetrii
   d) konfiguracja alertów o zdarzeniach w systemie EMS
   e) integracja z Active Directory
   f) integracja z FortiGate
5. KONFIGURACJA FORTI CLIENT ZA POMOCĄ FORTI CLIENT EMS
   a) konfiguracja Endpoint Policy
   b) konfiguracja Endpoint Profile
   c) utworzenie instalatora FortiClient
   d) konfiguracja instalatora FortiClient dla odpowiednich grup
   e) wdrożenie FortiClient na stacjach roboczych
6. ZTNA
   a) omówienie zasady działania
   b) konfiguracja FortiGate dla ZTNA
   c) przykładowe wdrożenie ZTNA za pomocą FortiClient EMS + FortiGate

VII. PODSTAWY PRACY Z FORTIANALYZER

1. OPIS LICENCJONOWANIA / WYMAGANIA SYSTEMOWE
   a) wybór licencji; utworzenie konta forticloud; pobranie oprogramowania
   b) przygotowanie zasobów VMware / Hyper-V; instalacja i konfiguracja maszyny
2. KONFIGURACJA URZĄDZENIA
   a) konfiguracja urządzenia do pracy w sieci
   b) konta administracyjne / ustawienia
3. INTEGRACJA Z FORTIGATE
   a) podłączenie FG z FAZ
   b) tryby pracy / zarządzanie ADOM
   c) odczyt logów / możliwości personalizacji widoku
4. ZARZĄDZANIE PRZECHOWYWANIEM DANYCH
   a) polityki logowania / analiza; archiwum
   b) forwardowanie; rolowanie; backup / logów

VIII. LOGOWANIE I ALERTOWANIE

1. EFEKTYWNOŚĆ LOGOWANIA
   a) jak logować / jak odczytywać logi
   b) filtrowanie logów / szukanie zdarzeń
   c) logi w czasie rzeczywistym
2. ALERTY I FORTISOC

	b) konfiguracja i wykrywanie zdarzeń c) automatyzacja powiadomień d) analiza incydentów
IX. RAPORTY	
1. TWORZENIE RAPORTÓW	a) konfiguracja zakresów / szablonów / makr raportów b) personalizacja / spolszczenie wyglądu
2. AUTOMATYZACJA	a) harmonogram raportów b) dostarczenie na życzenie

Dlaczego warto?

Po szkoleniu uczestnicy będą potrafili:

- Administrować serwerem zarządzającym FortiClient EMS.
- Identyfikować oraz wdrażać konkretne wersje FortiClient.
- Stworzyć oraz wdrożyć własną konfigurację FortiClient za pomocą FortiClient EMS.
- Skonfigurować i wdrożyć FortiClient ZTNA.
- Zablokować dostęp do stron w sieci za pomocą kilku metod.
- Stworzyć obiekty i grupy dla reguł firewall.
- Wdrożyć moduł antywirusowy w celu zabezpieczenia sieci przed szkodliwym oprogramowaniem.
- Skonfigurować moduł IPS i monitorować próby nieautoryzowanego dostępu.
- Sprawnie zarządzać dostępem do poszczególnych aplikacji (lokalnych, chmurowych oraz webowych).
- Skonfigurować połączenia SSL-VPN oraz IPsec-VPN dla bezpieczeństwa połączeń sieciowych.
- Wdrożyć uwierzytelnianie dwuetapowe dla użytkowników końcowych z wykorzystaniem FortiToken Mobile lub kodów wysyłanych na adres email.
- Zestawić tunel IPsec między 2 lokalizacjami/ urządzeniami dla bezpiecznej integracji sieci LAN do LAN (site to site).
- Wdrożyć FortiAnalyzer w swojej sieci lokalnej.
- Skonfigurować Fortianalyzer do wykrywania podatności oraz analizy logów.
- Skonfigurować domeny Administracyjne (ADOM) oraz zarządzać nimi.
- Wygenerować raport zdarzeń sieciowych z poszczególnych segmentów sieci.
- Stworzyć harmonogram raportów sieciowych w celu zachowania ciągłości informacji na temat zdarzeń w sieci.
- Skonfigurować moduł FortiSoc w celu analizy podatności sieci na ataki.
- Analizować zdarzenia wykryte przez moduł FortiSoC i umiejętnie na nie reagować.
- Przywrócić logi oraz ustawienia gdy urządzenie ulegnie awarii.

Jesteś zainteresowany ofertą?

Jeśli masz dodatkowe pytania lub chcesz zapoznać się z naszą ofertą handlową zapraszamy do kontaktu z opiekunami handlowymi.

B&B Jacek Baron

Ul. Walentego Roździeńskiego 2a | 41-946 Piekary Śląskie