
## Cel szkolenia?

**Celem szkolenia FORTINET ONE – FortiGate + FortiAnalyzer** jest przekazanie uczestnikom kompleksowej wiedzy oraz praktycznych umiejętności w zakresie zarządzania, konfiguracji i monitorowania urządzeń FortiGate oraz efektywnego wykorzystania FortiAnalyzer do analizy i optymalizacji bezpieczeństwa sieci.

Uczestnicy nauczą się, jak skutecznie identyfikować i reagować na zagrożenia, analizować ruch sieciowy oraz wdrażać najlepsze praktyki w zakresie cyberbezpieczeństwa. Szkolenie pozwoli na lepsze zrozumienie mechanizmów zabezpieczeń Fortinet i ich zastosowania w codziennej pracy, co przełoży się na zwiększenie ochrony infrastruktury IT organizacji.

## Dla kogo?

**Szkolenie dedykowane** jest inżynierom bezpieczeństwa oraz administratorom systemów, którzy na co dzień zarządzają, konfigurują i monitorują urządzenia FortiGate. Program został opracowany z myślą o specjalistach świadomych wyzwań związanych z dynamicznie rosnącą liczbą urządzeń w infrastrukturze sieciowej oraz potrzebą skutecznej analizy zachowań w sieci. Uczestnicy zdobędą praktyczne umiejętności wykorzystania technologii FortiAnalyzer do precyzyjnego monitorowania i optymalizacji bezpieczeństwa swojej organizacji.

## Jak szkolimy?

Nasze szkolenie to dynamiczne połączenie merytorycznej wiedzy z praktycznymi ćwiczeniami, które pozwalają natychmiast zastosować zdobyte umiejętności w codziennej pracy. Dzięki interaktywnej formule – łączącej inspirujące mini wykłady z angażującymi warsztatami – uczestnicy nie tylko zdobywają cenną wiedzę, ale także uczą się, jak skutecznie wdrażać ją w swoim środowisku zawodowym.

Podczas szkolenia dbamy o komfort uczestników, zapewniając przerwy kawowe oraz lunch.

**Na zakończenie każdy uczestnik otrzymuje certyfikat potwierdzający ukończenie specjalistycznego szkolenia.**

## Czas trwania?

Szkolimy w godzinach **od 9:00 do 14:00.**

## Kto prowadzi szkolenie?

### Adrian Kamizela

Inżynier pracujący w Akademii BB, wyspecjalizowany w zakresie szeroko pojętej technologii IT, w tym sieci komputerowych i bezpieczeństwa systemów komputerowych oraz komputerowych systemach zarządzania i sterowania.
Na co dzień pracuje przy wdrożeniach technologii UTM i rozwiązywaniu problemów sieciowych naszych Klientów, a także realizuje audyty bezpieczeństwa danych w systemach informatycznych i sieci ICT oraz KRI i KSC.
Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (FCF Fortinet Certified Fundamentals, FCA Fortinet Certified Associate, FCP Fortinet Certified Professional Network Security, FCSS Fortinet Certified Solution Network Security)

### Jakub Szablewski

Inżynier pracujący w Akademii BB, posiadający kilkuletnie doświadczenie w administrowaniu systemami teleinformatycznymi. Na co dzień pracuje przy wdrożeniach technologii UTM i pomaga naszym Klientom chronić ich sieci i dane przed zagrożeniami
Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności dot. urządzeń Fortinet są liczne certyfikaty (FCF Fortinet Certified Fundamentals, FCA Fortinet Certified Associate, FCP Fortinet Certified Professional Network Security, FCSS Fortinet Certified Solution Network Security).

## Agenda szkolenia:

I. Wstęp

1. Powitanie i wprowadzenie do szkolenia
   a) Oficjalne powitanie uczestników oraz przedstawienie planu szkolenia.
   b) Krótkie omówienie struktury i harmonogramu zajęć.
   c) Zapoznanie uczestników z celami szkolenia oraz oczekiwanymi rezultatami.
2. Prezentacja Rozwiązań Fortinet
   a) Przegląd ekosystemu Fortinet oraz jego roli w ochronie sieci.
   b) Omówienie kluczowych funkcji FortiGate i FortiAnalyzer.
   c) Wskazanie korzyści wynikających z integracji tych technologii.

II. FORTIGATE

3. Konfiguracja Podstawowych Ustawień Sieciowych
   a) Adresacja IP i przypisywanie interfejsów.
   b) Konfiguracja routingu oraz serwerów DNS.
   c) Optymalizacja ustawień wydajności i bezpieczeństwa.
4. Tworzenie polityk firewalla
   a) Definicja obiektów, adresów, serwisów i przedziałów czasowych.
   b) Konfiguracja obiektów, adresów i serwisów w kontekście ochrony przed DOS.
   c) Zasady i przykłady implementacji reguł firewalla.
   d) Polityki ochrony przed DOS.
5. Profile ochronne
   a) Antywirus
      - *Tworzenie i zarządzanie profilami ochrony antywirusowej, metody skanowania (proxy/flow).*
      - *Blokowanie wykrytych zagrożeń i analiza logów.*
   b) Filtrowanie treści WWW

- *Konfiguracja profili filtrujących oraz metod skanowania (proxy/flow).*
- *Blokowanie niepożądanych treści i sprawdzanie logów.*

c) Filtrowanie DNS
- *Tworzenie polityk i profili filtrujących DNS.*
- *Kontrola zapytań zgodnie z wzorcami dostarczonymi przez producenta.*

d) Kontrola aplikacji
- *Tworzenie polityk i profili kontrolujących aplikacje.*
- *Tworzenie wyjątków dla aplikacji i usług.*

III. FORTIANALYZER

6. Integracja z FortiAnalyzer
   a) Wprowadzenie do FortiAnalyzer.
   b) Przesyłanie logów i analiza danych.
   c) Integracja z FortiGate: konfiguracja i synchronizacja.
   d) Raportowanie i alertowanie.
7. Zarządzanie alarmami i powiadomieniami
   a) Konfiguracja alarmów i powiadomień w FortiAnalyzer.
   b) Automatyczne akcje w przypadku wykrycia zagrożenia.
   c) Analiza przykładowych logów.

IV. ZAKOŃCZENIE

8. Podsumowanie i Sesja Q&A
   a) Omówienie kluczowych zagadnień poruszonych podczas szkolenia.
   b) Otwarta sesja pytań i odpowiedzi dla uczestników.
9. Zakończenie i Testy Wiedzy

## Dlaczego warto?

**Po szkoleniu uczestnicy będą potrafili:**

- Skutecznie zarządzać i konfigurować urządzenia FortiGate – poznają kluczowe funkcje i mechanizmy działania zapór sieciowych Fortinet.
- Monitorować ruch sieciowy oraz wykrywać zagrożenia – nauczą się analizować logi i zdarzenia oraz szybko identyfikować potencjalne ataki.
- Wykorzystywać FortiAnalyzer do analizy i raportowania – zdobędą umiejętności efektywnego przetwarzania danych, generowania raportów i optymalizacji polityki bezpieczeństwa.
- Wdrażać najlepsze praktyki w zakresie cyberbezpieczeństwa – dowiedzą się, jak skutecznie zabezpieczać infrastrukturę IT swojej organizacji przed zagrożeniami.
- Optymalizować polityki bezpieczeństwa – będą potrafili dostosować konfigurację systemów Fortinet do specyficznych potrzeb organizacji.
- Reagować na incydenty bezpieczeństwa – nauczą się analizować zagrożenia w czasie rzeczywistym oraz podejmować właściwe działania zapobiegawcze i naprawcze.
- Dzięki zdobytej wiedzy i praktycznym umiejętnościom uczestnicy będą mogli efektywnie zarządzać bezpieczeństwem sieci oraz zwiększyć poziom ochrony swojej organizacji!

**B&B Prosta Spółka Akcyjna**

ul. Walentego Roździeńskiego 2A | 41-946 Piekary Śląskie

www.b-and-b.pl | biuro@b-and-b.pl