Cel szkolenia?

Celem szkolenia FORTINET THREE – COMPLETE jest kompleksowe przygotowanie uczestników do skutecznego zarządzania infrastrukturą sieciową oraz bezpieczeństwem IT przy wykorzystaniu zaawansowanych technologii Fortinet. Podczas szkolenia uczestnicy zdobędą praktyczne umiejętności w zakresie konfiguracji, monitorowania i integracji rozwiązań FortiGate, FortiAuthenticator, FortiSwitch oraz FortiAP. Program obejmuje kluczowe aspekty związane z ochroną sieci, zarządzaniem tożsamością użytkowników oraz segmentacją ruchu. Szkolenie pozwoli specjalistom IT na efektywne wdrażanie polityk bezpieczeństwa, automatyzację procesów oraz zwiększenie kontroli nad infrastrukturą, co przełoży się na wyższy poziom ochrony organizacji przed cyberzagrożeniami.

Dla kogo?

Szkolenie jest dedykowane inżynierom bezpieczeństwa, administratorom systemów oraz specjalistom IT, którzy zarządzają infrastrukturą sieciową i chcą poszerzyć swoją wiedzę na temat zaawansowanych technologii Fortinet. Jest to idealna propozycja dla osób odpowiedzialnych za konfigurację, monitorowanie i zabezpieczanie sieci, które chcą nauczyć się skutecznie integrować rozwiązania FortiGate, FortiAuthenticator, FortiSwitch oraz FortiAP. Szkolenie jest szczególnie wartościowe dla specjalistów pragnących zwiększyć poziom ochrony swojej organizacji poprzez optymalizację dostępu, segmentację ruchu oraz automatyzację polityk bezpieczeństwa.

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.**

Kto prowadzi szkolenie?

Jacek Baron

Ekspert w dziedzinie rozwiązań bezpieczeństwa systemów i sieci teleinformatycznych. Szkoleniowiec i wdrożeniowiec z ponad 20 letnim doświadczeniem. Specjalizuje się w projektowaniu i wdrażaniu kompleksowej architektury bezpieczeństwa, obejmującej zarówno aspekty technologiczne jak i organizacyjne. Potwierdzeniem jego fachowej wiedzy i praktycznych umiejętności są liczne certyfikaty i autoryzowane certyfikaty Producentów takich jak: Fortinet, Cisco, VMware, Veeam, Eset, Sophos, WitchSecure, Qnap.

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.	Omówienie podstawowej konfiguracji sieciowej a) Pojęcia. b) Zasady działania.
II.	FORTIGATE
3.	Zadania a) Konfiguracja Adresacji. b) Konfiguracja Fortilink. c) Ustawienia Tras Statycznych. d) Konfiguracja SD-WAN. e) Polityki Bezpieczeństwa. f) Weryfikacja logów.
III.	FORTIAUTHENTICATOR
4.	Integracja urządzeń w środowisku a) Podłączenie FortiAuthenticator do Fortigate. b) Podłączenie FortiAuthenticator do AD.
5.	Zadania a) Tworzenie grup. b) Synchronizacja i import użytkowników. c) Klienci RADIUS. d) Polityki RADIUS. e) Automatyzacja na FG. f) Konfiguracja polityk.

	g) Konfiguracja atrybutów RADIUS. h) DEBUG i weryfikacja logów.
IV.	FORTISWITCH
6.	Integracja z FortiGate a) Adresacja urządzeń. b) Autoryzacja urządzeń. c) Ustawienia profili zarządzania.
7.	Zadania a) Konfgiruacja vlan. b) Segmentacja sieci. c) Autoryzacja dostępu do sieci 802.1x.
V.	FORTIAP
8.	Integracja z FortiGate.
9.	Zadania z konfiguracji SSID: a) Wpa2 personal - 1 klucz dostępu. b) Wpa2 personal - wiele kluczy dostępu wraz z przydziałem vlan. c) Wpa2 enterprise - lokalne uwierzytelnienie. d) Wpa2 enterprise - zewnętrzny serwer radius + dynamiczne przydzielanie vlanów.
VI.	ZAKOŃCZENIE
10.	Zakończenie i testy wiedzy

Dlaczego warto?

Po szkoleniu uczestnicy będą potrafili:

- Skutecznie konfigurować i zarządzać urządzeniami FortiGate, FortiAuthenticator, FortiSwitch oraz FortiAP.
- Monitorować i analizować ruch sieciowy w celu wykrywania i neutralizowania zagrożeń.
- Optymalizować zabezpieczenia sieciowe poprzez wdrażanie polityk bezpieczeństwa i automatyzację procesów.
- Zarządzać tożsamością użytkowników i kontrolować dostęp do zasobów organizacji.
- Segmentować ruch sieciowy w celu zwiększenia wydajności i bezpieczeństwa infrastruktury.
- Integrować rozwiązania Fortinet w celu stworzenia spójnej i skutecznej strategii ochrony IT.
- Reagować na incydenty bezpieczeństwa i minimalizować ryzyko cyberzagrożeń.

B&B Prosta Spółka Akcyjna

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

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