

Szkolenie: Fortinet
FortiAnalyzer AnalystPremier Authorized
Training Center

DOSTĘPNE TERMINY

2026-05-07 | 2 dni | Virtual
2026-06-08 | 2 dni | Virtual Classroom
2026-06-08 | 2 dni | Warszawa / Wirtualna sala
2026-06-18 | 2 dni | DE - München
2026-06-18 | 2 dni | Virtual - Alternative zu DE Onsite Termin

Cel szkolenia:

W tym szkoleniu zdobędziesz praktyczne umiejętności analityka SOC z wykorzystaniem FortiAnalyzera do scentralizowanego logowania i analityki. Nauczysz się analizować i zarządzać zdarzeniami oraz automatyzować reakcję na zagrożenia przy użyciu **event handlerów** i **playbooków**. Poznasz także metody identyfikowania aktualnych i potencjalnych zagrożeń poprzez analizę incydentów oraz raporty o ogniskach zagrożeń (outbreak reports). Na końcu nauczysz się włączać **FortiAI** oraz generować raporty bezpieczeństwa.

Cele

Po ukończeniu kursu uczestnik będzie potrafił:

- SOC & Security Fabric:
 - Opisać cele, odpowiedzialności i role SOC
 - Wyjaśnić rolę FortiAnalyzera w SOC
 - Opisać integrację Security Fabric z FortiAnalyzerem
 - Wyjaśnić, jak działa logowanie w Security Fabric
- FortiAnalyzer – działanie i przetwarzanie logów
 - Opisać typy wdrożeń FortiAnalyzera
 - Opisać tryby pracy FortiAnalyzera
 - Wyjaśnić sposób parsowania i normalizacji logów
 - Walidować parsery logów
 - Wyszukiwać logi używając pól znormalizowanych
 - Przeglądać logi w log view
 - Tworzyć zapisane filtry i dashboardy

- Przeglądać dane podsumowujące w FortiView
- Pracować z dashboardami i widgetami
- Zdarzenia, incydenty, wskaźniki
 - Konfigurować event handlers
 - Zarządzać zdarzeniami
 - Konfigurować wskaźniki (indicators)
 - Tworzyć incydenty
 - Analizować incydenty
 - Konfigurować ustawienia incydentów
- FortiAI i Threat Hunting
 - Opisać działanie i przypadki użycia FortiAI
 - Wyjaśnić koncepcje threat huntingu
 - Korzystać z wykresu zliczania logów (log count chart)
 - Korzystać z tabeli analitycznej SIEM
- Raportowanie
 - Opisać alerty outbreak
 - Zbierać statystyki wolumenu logów
 - Konfigurować automation stitch
 - Tworzyć event handler z włączonym automation stitch
 - Uruchamiać i dostrajać predefiniowane raporty
 - Tworzyć raporty niestandardowe wykorzystując makra, wykresy i zestawy danych
 - Konfigurować zewnętrzną pamięć dla raportów
 - Grupować raporty
 - Importować i eksportować raporty oraz wykresy
 - Załączać raporty do incydentów
 - Zarządzać raportami i rozwiązywać problemy
- Playbooki
 - Tworzyć nowe playbooki
 - Używać zmiennych w zadaniach
 - Monitorować działanie playbooków
 - Eksportować i importować playbooki

Grupa docelowa

Szkolenie przeznaczone jest dla specjalistów ds. bezpieczeństwa odpowiedzialnych za analitykę Fortinet Security Fabric oraz automatyzację zadań związanych z wykrywaniem i reagowaniem na

cyberataki z wykorzystaniem FortiAnalyzeera.

Plan szkolenia:

- Koncepcje SOC i Security Fabric
- Przepływ danych logów i nawigacja
- Zdarzenia, wskaźniki i incydenty
- FortiAI, threat hunting i rozwiązywanie problemów
- Raporty
- Playbooki

Wymagania:

Uczestnik powinien znać zagadnienia omawiane w następujących szkoleniach lub posiadać równoważne doświadczenie:

- *FortiOS Administrator/FortiGate Administrator*
- *FortiAnalyzer Administrator*

Zalecana jest również znajomość:

- składni zapytań SQL SELECT

Poziom trudności



Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez Fortinet (ukończenie szkolenia).

Szkolenie przygotowuje do egzaminu *NSE5 - FortiAnalyzer Analyst*, który jest częścią ścieżki certyfikacyjnej [FCP Security Operations](#)

Prowadzący:

Fortinet Certified Trainer (FCT)

Informacje dodatkowe:

Realizacja tego szkolenia uprawnia do zdobycia kredytów CPE (Continuing Professional Education) ISC2

- CPE training hours: 6
- CPE lab hours: 5
- CISSP domains: Security Operations