Szkolenie: Fortinet
FortiAnalyzer Analyst

FORTINET Premier Authorized Training Center

DOSTĘPNE TERMINY

2026-06-18 | 2 dni | DE - München
2026-06-18 | 2 dni | Virtual - Alternative zu DE Onsite Termin
2026-06-23 | 2 dni | Kraków / Wirtualna sala *(Termin gwarantowany)*
2026-07-06 | 2 dni | Virtual Classroom
2026-08-20 | 2 dni | Warszawa / Wirtualna sala
2026-08-31 | 2 dni | Virtual Classroom
2026-09-07 | 2 dni | Virtual Classroom
2026-09-17 | 2 dni | Kraków / Wirtualna sala
2026-09-30 | 2 dni | Virtual Classroom
2026-10-08 | 2 dni | Warszawa / Wirtualna sala
2026-10-12 | 2 dni | Virtual Classroom
2026-11-19 | 2 dni | Kraków / Wirtualna sala
2026-11-23 | 2 dni | Virtual Classroom
2026-12-10 | 2 dni | Virtual Classroom
2026-12-17 | 2 dni | Warszawa / Wirtualna sala

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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- 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 handlery
  - 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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- 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 FortiAnalyzera.

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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

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

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001