

Szkolenie: Microsoft
MS-55610 Planning and implementing Microsoft Sentinel (SIEM & SOAR)



DOSTĘPNE TERMINY

2025-01-15 | 3 dni | Kraków / Wirtualna sala
2025-02-12 | 3 dni | Warszawa / Wirtualna sala
2025-02-26 | 3 dni | Virtual Classroom
2025-03-12 | 3 dni | Kraków / Wirtualna sala
2025-04-09 | 3 dni | Warszawa / Wirtualna sala
2025-05-14 | 3 dni | Kraków / Wirtualna sala
2025-05-14 | 3 dni | Virtual Classroom
2025-06-11 | 3 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Ten 3-dniowy kurs praktyczny pomaga Ci szybko opanować Microsoft Sentinel i zapewnia praktyczne doświadczenie z funkcjami, możliwościami i scenariuszami produktu. Podczas kursu wdrożysz przestrzeń roboczą Microsoft Sentinel i zaimportujesz wcześniej nagrane dane, aby symulować scenariusze, które prezentują różne funkcje Microsoft Sentinel.

Grupa docelowa:

Ten kurs jest przeznaczony dla profesjonalistów IT i administratorów Azure, którzy mają pewne doświadczenie w administracji i konfiguracji Azure, ale chcą zdobyć wgląd w wdrażanie rozwiązania SIEM/SOAR firmy Microsoft, Microsoft Sentinel.

Plan szkolenia:

- Przegląd Microsoft Sentinel
 - Przegląd Microsoft Sentinel
 - Metody pobierania danych
 - Microsoft Sentinel dla MSSP
 - Analiza zachowań użytkowników i podmiotów
 - Fusion
 - Notatniki
 - Narzędzia zarządzania i automatyzacji
 - Logi i koszty
- KQL

- Znaczenie KQL w całym Azure
- Interfejs użytkownika (demo)
- Standardowa struktura KQL
- Powszechne polecenia KQL
- Łączniki danych
 - Zarządzanie treścią w Microsoft Sentinel
 - Łączenie danych z Microsoft Sentinel za pomocą łączników danych
 - Łączenie usług Microsoft z Microsoft Sentinel
 - Łączenie Microsoft 365 Defender z Microsoft Sentinel
 - Łączenie hostów Windows z Microsoft Sentinel
 - Łączenie logów Common Event Format z Microsoft Sentinel
 - Łączenie źródeł danych syslog z Microsoft Sentinel
 - Łączenie wskaźników zagrożeń z Microsoft Sentinel
- Reguły analityczne
 - Wykrywanie zagrożeń z wykorzystaniem analityki Microsoft Sentinel
 - Automatyzacja w Microsoft Sentinel
 - Reagowanie na zagrożenia za pomocą scenariuszy Microsoft Sentinel
- Zarządzanie incydentami
 - Przegląd zarządzania incydentami
 - Analiza zachowań użytkowników i podmiotów
 - Normalizacja danych w Microsoft Sentinel
 - Wyszukiwanie, wizualizacja i monitorowanie danych
- Hunting
 - Koncepcje huntingu na zagrożenia
 - Hunting na zagrożenia z wykorzystaniem Microsoft Sentinel
 - Używanie zadań wyszukiwania w Microsoft Sentinel
 - Hunting na zagrożenia za pomocą notatników
- Listy obserwowanych
 - Priorytetyzacja incydentów
 - Importowanie danych biznesowych
 - Redukowanie zmęczenia alertami
 - Wzbogacanie danych zdarzeń
- Wywiad o zagrożeniach
 - Przegląd wywiadu o zagrożeniach
 - Wywiad o zagrożeniach w Microsoft Sentinel

Wymagania:

- Podstawową wiedzę na temat pojęć Microsoft Azure
- Doświadczenie z urządzeniami Windows 10
- Doświadczenie z Office 365.
- Podstawową wiedzę na temat uwierzytelnienia i upoważnienia
- Podstawową wiedzę na temat sieci komputerowych
- Wiedzę i doświadczenie na temat zarządzania urządzeniami mobilnymi

Poziom trudności



Certyfikaty:

Certyfikat ukończenia autoryzowanego kursu Microsoft.

Prowadzący:

Microsoft Certified Trainer.