

kod szkolenia: SC-200 / PL DL 4d

Microsoft Security Operations Analyst

Autoryzowane szkolenie Microsoft Security Operations Analyst SC-200 szkolenie w formule Distance Learning.

Zainwestuj w swoją przyszłość:

<https://www.altkomakademia.pl/zainwestuj-w-swoja-przyszlosc-my-dorzucimy-cos-ekstra/>

Docelowa grupa odbiorców:

- Administrator
- Specjalista IT
- Specjalista ds. bezpieczeństwa
- Inżynier ds. bezpieczeństwa

[Dyrektywa NIS2](#)

Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi.

[Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2](#)

Zobacz film: <https://youtu.be/KwL-ywrykeA>

Wywiad: 15 minut z ekspertem z tematyki Microsoft Azure:

Zobacz film: <https://youtu.be/sXfpx7KEqQ8>

Wywiad: 15 minut z ekspertem z tematyki bezpieczeństwa usług chmurowych Microsoft 365:

Zobacz film: <https://youtu.be/8p5ioOu4WX8>



Odbiorcy szkolenia

Microsoft Security Operations Analyst współpracuje z różnymi działami organizacji w celu zabezpieczenia systemów informatycznych. Jego celem jest zmniejszenie ryzyka organizacyjnego poprzez:

- szybkie korygowanie aktywnych ataków w środowisku,
- doradzanie w zakresie doskonalenia praktyk ochrony przed zagrożeniami
- kierowanie naruszeń polityk organizacyjnych do odpowiednich interesariuszy.

Obowiązki obejmują monitorowanie, analizę i reagowanie na zagrożenia przy użyciu różnych rozwiązań zabezpieczających w całym środowisku. Osoba na takim stanowisku przede wszystkim bada, reaguje i poszukuje zagrożeń przy użyciu Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender i produktów zabezpieczających innych firm. Security Operations Analyst używa wyników operacyjnych tych narzędzi.

Szkolenie skierowane do administratorów bezpieczeństwa, administratorów chmury oraz osób, które są zainteresowane poznaniem, czym jest:

- Zarządzanie Microsoft Azure Sentinel
- Zarządzanie Azure Defender
- Zarządzanie Microsoft 365 Defender
- Korzystanie z Kusto Query Language



Korzyści

Podczas szkolenia uczestnik dowie się, jak badać i reagować na zagrożenia oraz jak polować na nie za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Na tym kursie można się dowiedzieć, jak ograniczać cyberzagrożenia za pomocą tych rozwiązań. W szczególności można zdobyć wiedzę i praktyczne doświadczenie w zakresie konfiguracji i użycia Microsoft 365 Defender XDR oraz Azure Sentinel, a także korzystania z języka Kusto Query Language (KQL) do

wykrywania, analizy i raportowania. Kurs został zaprojektowany dla osób, które pracują na stanowisku Security.

Szkolenie pomaga uczestnikom przygotować się do egzaminu SC-200.

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf



Program szkolenia

1: Ograniczanie zagrożeń za pomocą Microsoft Defender XDR

- Wprowadzenie do ochrony przed zagrożeniami za pomocą Microsoft Defender XDR

- Ograniczanie incydentów za pomocą Microsoft Defender XDR

- Korygowanie ryzyka za pomocą Defender for Office 365 w programie Microsoft Defender XDR

- Microsoft Defender for Identity w Microsoft Defender XDR

- Chroń swoje tożsamości za pomocą Entra ID Protection

- Defender for Cloud Apps w programie Microsoft Defender XDR

2: Ograniczanie zagrożeń za pomocą Microsoft Copilot for Security

- Podstawy generatywnej sztucznej inteligencji

- Opis Microsoft Copilot for Security

- Opis podstawowych funkcji Microsoft Copilot for Security

- Opis wbudowanych rozwiązań Microsoft Copilot for Security

3: Ograniczanie zagrożeń za pomocą programu Microsoft Purview

- Rozwiązania zgodności programu Microsoft Purview

- Badanie i korygowanie naruszeń zidentyfikowanych przez zasady zapobiegania utracie danych (DLP) programu Microsoft Purview

- Badanie i korygowanie zagrożeń wewnętrznych zidentyfikowanych przez zasady Microsoft Purview

- Badanie zagrożeń za pomocą wyszukiwania zawartości w Microsoft Purview

- Badanie zagrożeń przy użyciu Microsoft Purview Audit (Standard)

- Badanie zagrożeń przy użyciu Microsoft Purview Audit (Premium)

4: Ograniczanie zagrożeń przy użyciu Microsoft Defender for Endpoint

- Ochrona przed zagrożeniami przy użyciu Microsoft Defender for Endpoint

- Wdrażanie środowiska Microsoft Defender for Endpoint

- Implementacja ulepszeń zabezpieczeń systemu Windows

- Przeprowadzanie dochodzeń dotyczących urządzeń

- Wykonywanie działań na urządzeniach końcowych

- Przeprowadzanie dochodzeń dotyczących dowodów i jednostek

- Konfigurowanie i zarządzanie automatyzacją

- Konfigurowanie alertów i wykryć

- Korzystanie z funkcji Threat and Vulnerability Management

5: Ograniczanie zagrożeń przy użyciu Microsoft Defender for Cloud

- Planowanie ochrony obciążeń w chmurze przy użyciu Microsoft Defender for Cloud
- Łączenie zasobów platformy Azure z usługą Microsoft Defender for Cloud
- Łączenie zasobów spoza platformy Azure z usługą Microsoft Defender for Cloud
- Zarządzanie postawą bezpieczeństwa w chmurze
- Ochrona obciążeń w usłudze Microsoft Defender for Cloud
- Reagowanie i naprawianie w oparciu o alerty zabezpieczeń przy użyciu usługi Microsoft Defender for Cloud

6: Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka zapytań Kusto (KQL)

- Konstruowanie instrukcji języka KQL dla Microsoft Sentinel
- Analiza wyników zapytań za pomocą KQL
- Konstruowanie instrukcji wielotabelowych za pomocą KQL
- Praca z danymi ciągu za pomocą instrukcji KQL

7: Konfiguracja środowiska Microsoft Sentinel

- Wprowadzenie do Microsoft Sentinel
- Tworzenie i zarządzanie obszarami roboczymi Microsoft Sentinel
- Dzienniki zapytań w Microsoft Sentinel
- Użycie list obserwacyjnych w Microsoft Sentinel
- Wykorzystywanie informacji o zagrożeniach w Microsoft Sentinel

8: Łączenie dzienników z Microsoft Sentinel

- Zarządzanie treścią w Microsoft Sentinel
- Łączenie danych z Microsoft Sentinel za pomocą łączników danych
- Łączenie usług Microsoft z Microsoft Sentinel
- Łączenie Microsoft Defender XDR z Microsoft Sentinel
- Łączenie hostów Windows z Microsoft Sentinel
- Łączenie dzienników Common Event Format z Microsoft Sentinel
- Łączenie źródeł danych syslog z Microsoft Sentinel
- Łączenie wskaźników zagrożeń z Microsoft Sentinel

9: Tworzenie wykryć i przeprowadzanie dochodzeń za pomocą Microsoft Sentinel

- Wykrywanie zagrożeń za pomocą Microsoft Sentinel Analytics
- Automatyzacja w Microsoft Sentinel
- Reagowanie na zagrożenia za pomocą podręczników Microsoft Sentinel
- Bezpieczeństwo zarządzania incydentami w Microsoft Sentinel
- Analityka behawioralna w Microsoft Sentinel
- Normalizacja danych w Microsoft Sentinel
- Zapytania, wizualizacja i monitorowanie danych w Microsoft Sentinel

10: Przeprowadzanie polowania na zagrożenia w Microsoft Sentinel

- Wyjaśnienie koncepcji polowania na zagrożenia w Microsoft Sentinel
- Polowanie na zagrożenia za pomocą Microsoft Sentinel
- Korzystanie z funkcji wyszukiwania zadań w Microsoft Sentinel
- Opcjonalnie – Polowanie na zagrożenia za pomocą notatników w Microsoft Sentinel



Oczekiwane przygotowanie uczestnika

- Znajomość platformy Microsoft 365
- Znajomość technologii zabezpieczeń i zgodności firmy Microsoft.
- Znajomość pojęć związanych z ochroną informacji.
- Zrozumienie koncepcji przetwarzania w chmurze.
- Średniozaawansowana znajomość systemu Windows 10/11
- Znajomość usług platformy Azure
- Podstawowe rozumienie koncepcji skryptowych
- Umiejętność korzystania z anglojęzycznych materiałów
- Szkolenia poprzedzające: AZ-900, MS-900, SC-900, SC-300, SC-400
- Umiejętność korzystania z anglojęzycznych materiałów

Dla zwiększenia komfortu pracy oraz efektywności szkolenia zalecamy skorzystanie z dodatkowego ekranu. Brak dodatkowego ekranu nie jest przeciwwskazaniem do udziału w szkoleniu, ale w znaczący sposób wpływa na komfort pracy podczas zajęć.

Informacje oraz wymagania dotyczące uczestniczenia w szkoleniach w formule zdalnej dostępne na:

<https://www.altkomakademia.pl/distance-learning/#FAQ>



Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie:

<https://learn.microsoft.com/pl-pl/training/>

* dostęp do portalu słuchacza AltKom Akademii

- szkolenie prowadzone w formie prezentacji
- demonstracje trenera
- ćwiczenia praktyczne w formie laboratoriów

Metoda szkolenia:

- formuła stacjonarna / formuła Distance Learning



Język

- **Szkolenie:** polski
- **Materiały:** angielski

Metoda egzaminacyjna

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf

Egzamin w formie on-line. Zapis na stronie <https://home.pearsonvue.com/Clients/Microsoft.aspx>

Czas trwania

4 dni / 28 godzin

Opis egzaminu

Microsoft Certified: Security Operations Analyst Associate

Exam URL: <https://docs.microsoft.com/en-us/learn/certifications/exams/SC-200>

Become Microsoft Certified: https://arch-center.azureedge.net/Credentials/Certification-Poster_en-us.pdf