kod szkolenia: SC-200 / PL AA 4d

Defend against cyberthreats with Microsoft's security operations platform

Autoryzowane szkolenie Microsoft Defend against cyberthreats with Microsoft's security operations platform SC-200 szkolenie w formule stacjonarnej.
Szkolenie kierowane jest do specjalistów IT i administratorów, którzy chcą skutecznie wykrywać, analizować i reagować na cyberzagrożenia z wykorzystaniem platformy bezpieczeństwa Microsoft.

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 Defend against cyberthreats with Microsoft's security operations platform 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.

Szkolenie skierowane jest do:

- administratorów bezpieczeństwa oraz administratorów chmury, odpowiedzialnych za ochronę systemów informatycznych w organizacji,
- specjalistów IT i analityków bezpieczeństwa zainteresowanych monitorowaniem, analizą i reagowaniem na zagrożenia w środowisku Microsoft,
- osób chcących zdobyć praktyczne umiejętności w zakresie wykrywania i reagowania na cyberzagrożenia z wykorzystaniem narzędzi Microsoft oraz innych rozwiązań zabezpieczających,
- profesjonalistów, którzy chcą poznać i praktycznie stosować:
  - Microsoft Azure Sentinel – zarządzanie i monitorowanie bezpieczeństwa,
  - Azure Defender – ochrona zasobów chmurowych,
  - Microsoft 365 Defender – zabezpieczanie środowiska Microsoft 365,
  - Kusto Query Language (KQL) – analiza danych i zagrożeń w środowisku Microsoft.

Korzyści

- Umiejętność badania, wykrywania i reagowania na zagrożenia w środowisku Microsoft.
- Praktyczne poznanie metod „threat hunting” z wykorzystaniem platformy Microsoft Azure Sentinel, Azure Defender oraz Microsoft 365 Defender.
- Zdolność skutecznego ograniczania cyberzagrożeń przy użyciu rozwiązań Microsoft Security.
- Zdobycie wiedzy i doświadczenia w zakresie konfiguracji oraz wykorzystania Microsoft 365 Defender XDR i Azure Sentinel.
- Umiejętność stosowania języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania incydentów bezpieczeństwa.
- Przygotowanie merytoryczne do przystąpienia do egzaminu certyfikacyjnego **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. 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
6. 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
7. 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
8. 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
9. 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-104, AZ-900, SC-900, SC-300, SC-401
- 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