kod szkolenia: SC-200 / PL DL 4d

Microsoft Security Operations Analyst

Autoryzowane szkolenie **Microsoft Security Operations Analyst SC-200** szkolenie w formule Distance Learning. Docelowa grupa odbiorców:

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

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

Przeznaczenie szkolenia

Szkolenie skierowane do osób, które są zainteresowane poznaniem czym jest:

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

Microsoft **Security Operations Analyst** współpracuje z różnymi działami organizacji w celu zabezpieczenia systemów informatycznych. Ich 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 zarządzanie zagrożeniami, monitorowanie i reagowanie przy użyciu różnych rozwiązań zabezpieczających w całym środowisku. Rola przede wszystkim bada, reaguje i poszukuje zagrożeń przy użyciu Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender i produktów zabezpieczających innych firm. Ponieważ Security Operations Analyst używa wyników operacyjnych tych narzędzi, są one również kluczowym interesariuszem w konfiguracji i wdrażaniu tych technologii.

Korzyści wynikające z ukończenia szkolenia

- Wyjaśnij, w jaki sposób program Microsoft Defender for Endpoint może korygować ryzyko w Twoim środowisku
- Utwórz środowisko Microsoft Defender for Endpoint
- Skonfiguruj reguły redukcji powierzchni ataku na urządzeniach z systemem Windows 10
- Wykonuj działania na urządzeniu za pomocą usługi Microsoft Defender for Endpoint
- Zbadaj domeny i adresy IP w Microsoft Defender for Endpoint
- Zbadaj konta użytkowników w Microsoft Defender for Endpoint
- Skonfiguruj ustawienia alertów w Microsoft Defender for Endpoint
- Wyjaśnij, jak ewoluuje krajobraz zagrożeń
- Przeprowadź zaawansowane polowanie w usłudze Microsoft 365 Defender
- Zarządzaj incydentami w usłudze Microsoft 365 Defender
- Wyjaśnij, w jaki sposób program Microsoft Defender for Identity może korygować ryzyko w Twoim środowisku.
- Zbadaj alerty DLP w Microsoft Cloud App Security
- Wyjaśnij rodzaje działań, które możesz podjąć w przypadku zarządzania ryzykiem wewnętrznym.
- Skonfiguruj automatyczne udostępnianie w usłudze Azure Defender
- Napraw alerty w usłudze Azure Defender
- Konstruuj instrukcje KQL
- Filtruj wyszukiwania na podstawie czasu zdarzenia, wagi, domeny i innych istotnych danych za pomocą KQL
- Wyodrębnij dane z nieustrukturyzowanych pól łańcuchowych za pomocą języka KQL
- Zarządzaj obszarem roboczym Azure Sentinel
- Użyj języka KQL, aby uzyskać dostęp do listy obserwowanych na platformie Azure Sentinel
- Zarządzaj wskaźnikami zagrożeń na platformie Azure Sentinel
- Wyjaśnij różnice w łączniku Common Event Format i Syslog w usłudze Azure Sentinel
- Połącz maszyny wirtualne Azure Windows z platformą Azure Sentinel
- Skonfiguruj agenta Log Analytics do zbierania zdarzeń Sysmon
- Utwórz nowe reguły analityczne i zapytania za pomocą kreatora reguł analitycznych
- Utwórz poradnik, aby zautomatyzować reakcję na incydent
- Użyj zapytań do polowania na zagrożenia
- Obserwuj zagrożenia w czasie dzięki transmisji na żywo

Dowiedz się, jak badać zagrożenia, odpowiadać na nie i polować na nie za pomocą platformy Microsoft Azure Sentinel, Azure Defender i Microsoft 365 Defender. Na tym kursie dowiesz się, jak ograniczać cyberzagrożenia za pomocą tych technologii. W szczególności skonfigurujesz i użyjesz Azure Sentinel, a także użyjesz języka Kusto Query Language (KQL) do wykrywania, analizy i raportowania. Kurs został zaprojektowany dla osób, które pracują na stanowisku Security.

Metoda egzaminowania

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

Opis egzaminu

Po kursie SC-200 można przystąpić do certyfikowanego egzaminu: w autoryzowanym centrum egzaminancyjnym, online będąc monitorowanym przez zewnętrznego egzaminatora.Szczegóły na https://docs.microsoft.com/en-us/learn/certifications/exams/sc-200

Oczekiwane przygotowanie słuchaczy

- Podstawowa znajomość platformy Microsoft 365
- Podstawowa wiedza na temat produktów firmy Microsoft związanych z zabezpieczeniami, zgodnością i tożsamością
- Średnio zaawansowana znajomość systemu Windows 10
- Znajomość usług platformy Azure, w szczególności Azure SQL Database i Azure Storage
- Znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych
- Podstawowe rozumienie koncepcji skryptowych
- 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

Język szkolenia

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

Szkolenie obejmuje

* podręcznik w formie elektronicznej dostępny na platformie:
https://learn.microsoft.com/pl-pl/training/
* dostęp do portalu słuchacza Altkom Akademii

Metoda szkolenia:

- teoria
- dema
- labolatoria indywidualne
- 50% teoria
- 50% praktyka

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

Ścieżka szkoleniowa 01: Ogranicz zagrożenia za pomocą usługi Microsoft 365 Defender

- Wprowadzenie do ochrony przed zagrożeniami na platformie Microsoft 365
- Ogranicz incydenty za pomocą usługi Microsoft 365 Defender
- Eliminuj zagrożenia za pomocą usługi Microsoft Defender dla usługi Office 365
- Microsoft Defender dla tożsamości
- Chroń swoje tożsamości za pomocą usługi Azure AD Identity Protection
- Microsoft Defender dla aplikacji w chmurze
- Reaguj na alerty zapobiegania utracie danych przy użyciu Microsoft 365
- Zarządzaj ryzykiem wewnętrznym na platformie Microsoft 365

Ścieżka szkoleniowa 02: Ogranicz zagrożenia za pomocą usługi Microsoft Defender dla punktów końcowych

- Chroń się przed zagrożeniami za pomocą usługi Microsoft Defender dla punktów końcowych
- Wdróż środowisko usługi Microsoft Defender dla punktów końcowych
- Implementuj ulepszenia zabezpieczeń systemu Windows
- Wykonaj badania urządzeń
- Wykonaj czynności na urządzeniu
- Przeprowadzaj dochodzenia w sprawie dowodów i podmiotów
- Konfiguruj i zarządzaj automatyzacją

- Skonfiguruj alerty i wykrycia
- Wykorzystaj zarządzanie zagrożeniami i lukami w zabezpieczeniach

Ścieżka szkoleniowa 03 — ograniczaj zagrożenia za pomocą usługi Microsoft Defender for Cloud

- Zaplanuj ochronę obciążeń w chmurze przy użyciu usługi Microsoft Defender for Cloud
- Połącz zasoby platformy Azure z usługą Microsoft Defender for Cloud
- Połącz zasoby spoza platformy Azure z usługą Microsoft Defender for Cloud
- Zarządzaj stanem bezpieczeństwa w chmurze
- Zabezpieczenia obciążeń w usłudze Microsoft Defender for Cloud
- Koryguj alerty zabezpieczeń za pomocą usługi Microsoft Defender for Cloud

Ścieżka szkoleniowa 04 — Tworzenie zapytań dla Microsoft Sentinel przy użyciu języka Kusto Query Language

- Skonstruuj instrukcje KQL dla Microsoft Sentinel
- Analizuj wyniki zapytań za pomocą KQL
- Twórz wielotabelowe zestawienia przy użyciu języka KQL
- Praca z danymi łańcuchowymi przy użyciu instrukcji KQL

Ścieżka szkoleniowa 05 — Skonfiguruj swoje środowisko Microsoft Sentinel

- Wprowadzenie do Microsoft Sentinel
- Twórz i zarządzaj obszarami roboczymi Microsoft Sentinel
- Dzienniki zapytań w Microsoft Sentinel
- Użyj list obserwacyjnych w Microsoft Sentinel
- Wykorzystaj analizę zagrożeń w Microsoft Sentinel

Ścieżka szkoleniowa 06 — Połącz dzienniki z Microsoft Sentinel

- Połącz dane z Microsoft Sentinel za pomocą łączników danych
- Połącz usługi Microsoft z Microsoft Sentinel
- Połącz Microsoft 365 Defender z Microsoft Sentinel
- Połącz hosty Windows z Microsoft Sentinel
- Połącz dzienniki Common Event Format z Microsoft Sentinel
- Połącz źródła danych syslog z Microsoft Sentinel
- Połącz wskaźniki zagrożeń z Microsoft Sentinel

Ścieżka szkoleniowa 07 — Twórz wykrywanie i prowadź dochodzenia przy użyciu programu Microsoft Sentinel

- Wykrywanie zagrożeń za pomocą analiz Microsoft Sentinel
- Automatyzacja w Microsoft Sentinel
- Reaguj na zagrożenia za pomocą podręczników Microsoft Sentinel
- Zarządzanie incydentami bezpieczeństwa w Microsoft Sentinel
- Analityka behawioralna jednostek w Microsoft Sentinel
- Normalizacja danych w Microsoft Sentinel
- Wykonuj zapytania, wizualizuj i monitoruj dane w Microsoft Sentinel
- Zarządzaj zawartością w Microsoft Sentinel

Ścieżka szkoleniowa 08 — Polowanie na zagrożenia w Microsoft Sentinel

- Wyjaśnij koncepcje wykrywania zagrożeń w programie Microsoft Sentinel
- Polowanie na zagrożenia z Microsoft Sentinel
- Użyj funkcji wyszukiwania ofert pracy w programie Microsoft Sentinel

- Poluj na zagrożenia za pomocą notatników w Microsoft Sentinel