SC-200T00 Microsoft Security Operations Analyst

Czas trwania: 4 dni

Dla kogo:
Szkolenie skierowane do specjalistów IT odpowiedzialnych za bezpieczeństwo informacji, ograniczanie zagrożeń, przeprowadzanie dochodzeń oraz wykrywanie, analizę i raportowanie przy wykorzystaniu platformy Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender.

Wymagania wstępne:
- podstawowa wiedza o usłudze Microsoft 365
- podstawowe rozumienie zabezpieczeń, zgodności i tożsamości produktów firmy Microsoft
- znajomość systemu Windows 10
- znajomość usług platformy Azure, w szczególności usługi Azure SQL Database i usługi Azure Storage
- znajomość maszyn wirtualnych platformy Azure i sieci wirtualnych
- podstawowa wiedza na temat pojęć skryptów.

Zakres tematyczny:

1. Ograniczanie zagrożeń przy użyciu usługi Microsoft 365 Defender
    - wprowadzenie do ochrony przed zagrożeniami dzięki usłudze Microsoft 365
    - ograniczanie zdarzeń przy użyciu usługi Microsoft 365 Defender
    - eliminowanie ryzyka z programem Microsoft Defender dla usługi Office 365
    - ochrona tożsamości za pomocą usługi Azure AD Identity Protection
    - ochrona tożsamości za pomocą usługi Azure AD Identity Protection
    - zabezpieczanie aplikacji i usług w chmurze za pomocą Microsoft Defender
    - reagowanie na alerty dotyczące zapobiegania utracie danych przy użyciu Microsoft 365
    - zarządzanie ryzykiem wewnętrznym w Microsoft 365
2. Ograniczanie zagrożeń przy użyciu usługi Microsoft Defender for Endpoint
    - ochrona przed zagrożeniami za pomocą programu Microsoft Defender for Endpoint
    - wdrażanie środowiska usługi Microsoft Defender for Endpoint
    - wdrażanie ulepszeń zabezpieczeń systemu Windows 10
    - zarządzanie alertami i zdarzeniami w usłudze Microsoft Defender for Endpoint
    - wykonywanie dochodzeń dotyczących urządzeń w usłudze Microsoft Defender for Endpoint
    - wykonywanie akcji na urządzeniu przy użyciu usługi Microsoft Defender for Endpoint
    - wykonywanie dochodzeń w sprawie dowodów i jednostek przy użyciu usługi Microsoft Defender for Endpoint
    - konfigurowanie automatyzacji i zarządzanie nią przy użyciu usługi Microsoft Defender for Endpoint
    - konfigurowanie alertów i wykrywanie w usłudze Microsoft Defender for Endpoint
    - korzystanie z zarządzania zagrożeniami i lukami w zabezpieczeniach w programie Microsoft Defender for Endpoint
3. Ograniczanie zagrożeń przy użyciu usługi Microsoft Sentinel for Cloud
    - planowanie zabezpieczeń obciążeń przy użyciu usługi Microsoft Sentinel for Cloud
    - wyjaśnianie zabezpieczenia obciążeń w chmurze w usłudze Microsoft Sentinel
    - łączenie zasobów platformy Azure z usługą Microsoft Sentinel for Cloud
    - łączenie zasobów innych niż platforma Azure z usługą Microsoft Sentinel for Cloud
    - korygowanie alertów zabezpieczeń przy użyciu usługi Microsoft Sentinel for Cloud
4. Tworzenie zapytań dla usługi Microsoft Sentinel przy użyciu języka KQL (Kusto Query Language)
    - konstruowanie instrukcji KQL dla usługi Microsoft Sentinel
    - analizowanie wyników kwerend przy użyciu funkcji KQL

- tworzenie instrukcji wielospajowych przy użyciu funkcji KQL
- praca z danymi w usłudze Azure Sentinel przy użyciu języka zapytań Kusto

5. Konfigurowanie środowiska Microsoft Sentinel
   - wprowadzenie do usługi Microsoft Sentinel
   - tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
   - dzienniki zapytań w usłudze Microsoft Sentinel
   - używanie list obserwowanych w usłudze Microsoft Sentinel
   - korzystanie z analizy zagrożeń w usłudze Microsoft Sentinel
6. Łączenie dzienników z usługą Microsoft Sentinel
   - łączenie danych z usługą Microsoft Sentinel przy użyciu łączników danych
   - łączenie usług Microsoft z usługą Microsoft Sentinel
   - łączenie usługi Microsoft 365 Defender z usługą Microsoft Sentinel
   - łączenie hostów systemu Windows z usługą Microsoft Sentinel
   - łączenie dzienników wspólnego formatu zdarzeń z usługą Microsoft Sentinel
   - łączenie źródeł danych syslogu z usługą Microsoft Sentinel
   - łączenie wskaźników zagrożeń z usługą Microsoft Sentinel
7. Tworzenie wykrywania i przeprowadzanie dochodzeń przy użyciu usługi Microsoft Sentinel
   - wykrywanie zagrożeń za pomocą analizy Microsoft Sentinel
   - zarządzanie zdarzeniami zabezpieczeń w usłudze Microsoft Sentinel
   - reagowanie na zagrożenia za pomocą podręczników Microsoft Sentinel
   - analiza zachowań użytkowników i podmiotów w Microsoft Sentinel
   - wysyłanie zapytań, wizualizacja i monitorowanie danych w usłudze Microsoft Sentinel
8. Neutralizacja zagrożeń w usłudze Microsoft Sentinel
   - koncepcja polowania na zagrożenia za pomocą usługi Microsoft Sentinel
   - polowanie na zagrożenia za pomocą usługi Microsoft Sentinel
   - polowanie na zagrożenia przy użyciu notesów w usłudze Microsoft Sentinel