kod szkolenia: SC-5004 / PL DL 1d

Defend against cyberthreats with Microsoft Defender XDR

Szkolenie przygotowuje do praktycznego wykorzystania Microsoft Defender XDR w pracy analityka operacji bezpieczeństwa. Uczestnicy poznają sposób obsługi incydentów w portalu Microsoft Defender, wdrożą i skonfigurują Microsoft Defender for Endpoint, skonfigurują alerty i detekcje, automatyzację reakcji oraz przeprowadzą dochodzenia na urządzeniach. Zajęcia obejmują również ćwiczenia laboratoryjne z wykrywania i reagowania na zagrożenia z użyciem Advanced Hunting (KQL).

Odbiorcy szkolenia

Szkoleie przeznaoczne dla:

- Analityków SOC / Security Operations Analyst odpowiedzialnych za wykrywanie, analizę i obsługę incydentów.
- Inżynierów i administratorów bezpieczeństwa wdrażających oraz utrzymujących Microsoft Defender for Endpoint i Microsoft Defender XDR.
- Osób przygotowujących się do zadań związanych z reagowaniem na incydenty i threat huntingiem (KQL) w ekosystemie Microsoft.

Korzyści

1. Obsługa incydentów w portalu Microsoft Defender – nauka analizy i zarządzania incydentami oraz alertami w portalu Microsoft Defender.
2. Wdrożenie Microsoft Defender for Endpoint – proces onboardingu urządzeń oraz konfiguracji podstawowych ustawień bezpieczeństwa.
3. Konfiguracja alertów i detekcji – konfiguracja powiadomień, wskaźników (indicators) oraz ustawień związane z wykrywaniem zagrożeń.

4. Automatyzacja reakcji – konfiguracja automatycznego reagowania i działania naprawcze oraz pozostałę mechanizmy automatyzacji w MDE.
5. Dochodzenia na urządzeniach – wykorzystanie danych telemetrycznych i informacji kryminalistycznych (forensics) do analizy incydentów na punktach końcowych (endpoints).
6. Advanced Hunting (KQL) – podstawowe scenariusze polowania na zagrożenia oraz korelacja zdarzeń w Defender XDR.

Program szkolenia

1.Mitygowanie incydentów z użyciem Microsoft Defender.
- Ujednolicony widok incydentów i alertów w portalu Microsoft Defender.
- Podstawy pracy z incydentami, powiązanymi dowodami i działaniami korygującymi.

2.Wdrożenie środowiska Microsoft Defender for Endpoint.
- Onboarding urządzeń i konfiguracja podstawowych ustawień bezpieczeństwa.
- Role i dostęp (RBAC) oraz grupy urządzeń.

3.Konfiguracja alertów i detekcji w Microsoft Defender for Endpoint.
- Powiadomienia, zarządzanie alertami i ich tłumienie.
- Wskaźniki (indicators) jako element procesu detekcji.

4.Automatyzacja i reakcja w Microsoft Defender for Endpoint.
- Ustawienia automatyzacji i automatyczne dochodzenia oraz działania naprawcze.
- Przegląd możliwości automatyzacji i dobrych praktyk.

5.Dochodzenia na urządzeniach w Microsoft Defender for Endpoint.
- Inwentarz urządzeń, analiza zdarzeń i danych telemetrycznych.
- Informacje kryminalistyczne (forensics) i mechanizmy blokowania zachowań.

6.Ćwiczenia laboratoryjne: obrona przed cyberzagrożeniami z użyciem Microsoft Defender XDR.
- Konfiguracja środowiska Defender XDR i wdrożenie Microsoft Defender for Endpoint.
- Symulacja ataku: analiza, mitygacja i reakcja na incydent oraz podstawy Advanced Hunting (KQL).

Oczekiwane przygotowanie uczestnika

- Doświadczenie w korzystaniu z portalu Microsoft Defender.
- Podstawowa znajomość Microsoft Defender for Endpoint oraz podstawowych pojęć SOC (alert, incydent, triage, remediacja).
- Podstawowa znajomość Microsoft Sentinel (zalecane) oraz doświadczenie w użyciu Kusto Query Language (KQL).
- Zalecane ukończenie ścieżki „Introduction to Microsoft Security, Compliance, and Identity (SC-900)”.

Szkolenie obejmuje

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

Produkt zawiera:

- Wykład (60%)
- Warsztaty (10%)
- Ćwiczenia (30%)

Główne narzędzia dydaktyczne obejmują prezentacje PowerPoint, praktyczne środowiska laboratoryjne i zasoby usługi Microsoft Learn https://learn.microsoft.com/pl-pl/training/

Czas trwania

1 dni / 7 godzin

Język

- Wykład: polski
- Materiały: angielski