kod szkolenia: SC-5004 / PL DL 1d

Defend against cyberthreats with Microsoft Defender XDR

Szkolenie Defend against cyberthreats with Microsoft Defender XDR przygotowuje do praktycznego wykorzystania Microsoft Defender XDR w pracy związanej z wykrywaniem, analizą i obsługą incydentów bezpieczeństwa. Program koncentruje się na pracy w portalu Microsoft Defender, zarządzaniu incydentami i alertami, konfiguracji Microsoft Defender for Endpoint oraz prowadzeniu dochodzeń na urządzeniach końcowych.

Uczestnicy poznają, jak wdrażać i konfigurować Microsoft Defender for Endpoint, ustawiać alerty i detekcje, wykorzystywać automatyzację reakcji oraz analizować dane telemetryczne i informacje kryminalistyczne. Szkolenie obejmuje również ćwiczenia laboratoryjne z wykrywania i reagowania na zagrożenia z wykorzystaniem Advanced Hunting oraz języka KQL.

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla osób odpowiedzialnych za wykrywanie, analizę, obsługę i ograniczanie skutków incydentów bezpieczeństwa w ekosystemie Microsoft.
W szczególności kurs sprawdzi się dla:
• analityków SOC oraz Security Operations Analyst odpowiedzialnych za obsługę incydentów,
• inżynierów bezpieczeństwa wdrażających i utrzymujących Microsoft Defender for Endpoint oraz Microsoft Defender XDR,
• administratorów bezpieczeństwa odpowiedzialnych za konfigurację alertów, detekcji i automatyzacji reakcji,
• osób przygotowujących się do zadań związanych z reagowaniem na incydenty,
• specjalistów chcących rozwijać umiejętności threat huntingu z wykorzystaniem Advanced Hunting i

KQL w środowisku Microsoft.

Korzyści

1. 1. Obsługa incydentów w Microsoft Defender – poznasz, jak analizować, zarządzać i obsługiwać incydenty oraz alerty w portalu Microsoft Defender.
   2. Wdrożenie Microsoft Defender for Endpoint – nauczysz się przeprowadzać onboarding urządzeń oraz konfigurować podstawowe ustawienia bezpieczeństwa punktów końcowych.
   3. Konfiguracja alertów i detekcji – dowiesz się, jak ustawiać powiadomienia, wskaźniki oraz mechanizmy wykrywania zagrożeń w Microsoft Defender XDR.
   4. Automatyzacja reakcji na zagrożenia – poznasz, jak konfigurować automatyczne reagowanie, działania naprawcze oraz mechanizmy automatyzacji w Microsoft Defender for Endpoint.
   5. Dochodzenia na urządzeniach końcowych – nauczysz się wykorzystywać dane telemetryczne i informacje kryminalistyczne do analizy incydentów na endpointach.
   6. Threat hunting z użyciem KQL – dowiesz się, jak realizować podstawowe scenariusze polowania na zagrożenia z wykorzystaniem Advanced Hunting i korelacji 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)”.

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/jak-dzialamy/o-szkoleniach/?distance-learning

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