kod szkolenia: SC-5001 / PL DL 1d

Configure SIEM security operations using Microsoft Sentinel

Szkolenie podstawowe przygotowujące do pracy z usługą Microsoft Sentinel. Zakres szkolenia obejmuje konfigurację obszaru roboczego usługi Microsoft Sentinel, poznanie konektorów, podłączenie źródeł zdarzeń, przygotowanie reguł analitycznych oraz wdrożenie automatycznego reagowania na zagrożenia

Odbiorcy szkolenia

Szkolenie jest przeznaczone dla:

- Analityków ds. zabezpieczeń, którzy zajmują się zarządzaniem, monitorowaniem i reagowaniem na zagrożenia,
- Specjalistów IT, którzy potrzebują wdrożyć system typu SMIE/SOAR w swojej organizacji.

W przypadku osób przygotowujących się do Microsoft Certified: Security Operations Analyst Associate (SC-200), może stanowić jeden z elementów przygotowujących do tej certyfikacji

Korzyści

1. Tworzenie i konfigurowanie obszaru roboczego usługi Microsoft Sentinel – Dowiesz się o rodzajach obszarów roboczych, zarządzaniu oraz kosztach.
2. Wdrażanie rozwiązania centrum zawartości usługi Microsoft Sentinel – Poznasz możliwości konfiguracyjnych konektorów dla źródeł zdarzeń.
3. Łączenie hostów systemu Windows z usługą Microsoft Sentinel – Podłączysz pierwsze źródła zdarzeń.
4. Konfigurowanie reguł analizy w usłudze Microsoft Sentinel – Nauczysz się konstruować reguły analityczne w celu wykrywania zagrożeń.

5. Konfigurowanie automatyzacji w usłudze Microsoft Sentinel – Będziesz tworzyć reguły automatyzacji w usłudze Microsoft Sentinel.
6. Może stanowić jeden z elementów procesu przygotowania do egzaminu SC-200, zapewniając omówienie praktycznych zagadnień i kompetencji wymaganych w roli analityka operacji bezpieczeństwa.

Program szkolenia

1.Tworzenie i zarządzanie obszarów roboczych usługi Microsoft Sentinel.
- Planowanie obszaru roboczego usługi Microsoft Sentinel.
- Tworzenie obszaru roboczego usługi Microsoft Sentinel.
- Zarządzanie obszarami roboczymi między dzierżawami przy użyciu usługi Azure Lighthouse.
- Omówienie uprawnień i ról usługi Microsoft Sentinel.

2.Łączenie usług firmy Microsoft z usługą Microsoft Sentinel.
- Planowanie konektorów usługi firmy Microsoft.
- Łączenie konektora platformy Microsoft 365.
- Łączenie konektora Microsoft Entra.
- Łączenie konektora aktywności platformy Azure.

3.Łączenie hostów systemu Windows z usługą Microsoft Sentinel.
- Planowanie łącznika zdarzeń zabezpieczeń hostów systemu Windows.
- Łączenie przy użyciu Zdarzeń zabezpieczeń Windows za pośrednictwem łącznika AMA.

4.Wykrywanie zagrożeń za pomocą analizy usługi Microsoft Sentinel.
- Co to jest analiza usługi Microsoft Sentinel?
- Typy reguł analizy.
- Tworzenie reguły analizy na podstawie szablonów.
- Tworzenie reguły analizy z poziomu kreatora.
- Zarządzanie regułami analizy.

5.Automatyzacja w usłudze Microsoft Sentinel.
- Omówienie opcji automatyzacji.
- Tworzenie reguł automatyzacji.

Oczekiwane przygotowanie uczestnika

- Podstawowa wiedza na temat platformy Microsoft Azure – na poziomie kursu „Microsoft Azure Fundamentals, AZ-900”.
- Znajomość zagadnień związanych z zarządzaniem incydentami – alerty, incydenty, zamykanie, hunting.

- Doświadczenie w korzystaniu z języka Kusto Query Language (KQL).
- Ukończenie ścieżki szkoleniowej "Introduction to Microsoft Security, Compliance, and Identity, SC-900" (zalecane).

Szkolenie obejmuje

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

Czas trwania

1 dni / 7 godzin

Język

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