kod szkolenia: SC-5001 / PL DL 1d

Configure SIEM security operations using Microsoft Sentinel

Dyrektywa NIS2 Unijne przepisy rozszerzają zakres przepisów dotyczących cyberbezpieczeństwa. Przedsiębiorcy objęci regulacją NIS2, wynikającą z ustawy o krajowym systemie bezpieczeństwa, będą objęci obowiązkiem stosowania produktów, usług bądź procesów, objętych tymi schematami certyfikacyjnymi. Sprawdź, czy Twoja firma będzie objęta dyrektywą NIS2

Przeznaczenie szkolenia

Szkolenie dedykowane dla specjalistów pełniących rolę analityka ds. operacji bezpieczeństwa firmy Microsoft, którzy współpracują z innymi specjalistami w celu zabezpieczenia systemów technologii informatycznych w organizacji. Zadaniem analityka ds. operacji bezpieczeństwa jest ograniczenie ryzyka organizacyjnego poprzez szybkie reagowanie na aktywne ataki w środowisku, doradzanie w zakresie ulepszeń praktyk ochrony przed zagrożeniami oraz zgłaszanie naruszeń polityk organizacyjnych odpowiednim interesariuszom. Obowiązki obejmują zarządzanie zagrożeniami, monitorowanie i reagowanie przy użyciu różnych rozwiązań bezpieczeństwa w całym środowisku. Ta rola polega przede wszystkim na badaniu zagrożeń, reagowaniu na nie i wykrywaniu ich przy użyciu programów Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft Defender XDR i produktów zabezpieczających innych firm. Ponieważ analityk ds. operacji bezpieczeństwa korzysta z wyników operacyjnych tych narzędzi, jest on także kluczową stroną zainteresowaną konfiguracją i wdrażaniem tych technologii.

Korzyści wynikające z ukończenia szkolenia

Zdobycie wiedzy i umiejętności w zakresie obsługi Microsoft Sentinel:

- Tworzenie i konfiguracja obszaru roboczego Microsoft Sentinel.
- Wdrożenie rozwiązań w centrum treści Microsoft Sentinel
- Połączenie hostów Windows z Microsoft Sentinel
- Konfiguracja reguł analitycznych w Microsoft Sentinel
- Konfiguracja automatyzacji w Microsoft Sentinel.

Oczekiwane przygotowanie słuchaczy

Podstawowa znajomość produktów Microsoft związanych z bezpieczeństwem, zgodnością i tożsamością. Średnio zaawansowana znajomość systemu Microsoft Windows. Znajomość usług Azure, w szczególności Azure Virtual Machines. Znajomość maszyn wirtualnych Azure i sieci wirtualnych. Podstawowa znajomość pojęć związanych ze skryptami.

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

Czas trwania

1 dni / 7 godzin

Agenda szkolenia

1. Tworzenie i zarządzanie obszarem roboczym Microsoft Sentinel.
   - Planowanie obszaru roboczego Microsoft Sentinel.
   - Utworzenie obszaru roboczego Microsoft Sentinel.
   - Zarządzanie obszarami roboczymi wśród dzierżawców przy użyciu usługi Azure Lighthouse.
   - Zapoznanie się z uprawnieniami i rolami Microsoft Sentinel.
   - Zarządzanie ustawieniami Microsoft Sentinel
   - Konfiguracja logów.
2. Połączenie usług Microsoft z Microsoft Sentinel.
   - Zaplanowanie łączników usług Microsoft.
   - Podłączenie łącza do Microsoft Office 365.
   - Podłączenie łącza do Microsoft Entra.
   - Podłączenie łącza do Microsoft Entra ID Protection.
   - Podłączenie łącza do aktywności platformy Azure.
3. Połączenie hostów Windows z Microsoft Sentinel.
   - Planowania łącznika zdarzeń związanych z bezpieczeństwem hostów systemu Windows.
   - Połączenie za pośrednictwem złącza AMA do dziennika zdarzeń zabezpieczeń systemu Windows .
   - Połączenie za pośrednictwem starszego oprogramowania sprzęgającego do dziennika zdarzeń zabezpieczeń.
   - Połączenie do dziennika zdarzeń Sysmon.
4. Wykrywanie zagrożeń za pomocą analiz Microsoft Sentinel.
   - Co to jest Microsoft Sentinel Analytics?
   - Rodzaje reguł analitycznych.
   - Tworzenie reguł analitycznych na podstawie szablonów.
   - Tworzenie reguł analitycznych za pomocą kreatora.
   - Zarządzanie regułami analitycznymi.
5. Automatyzacja w Microsoft Sentinel.
   - Poznanie opcji automatyzacji.
   - Tworzenie reguły automatyzacji.