Szkolenie: Microsoft

SC-5001: Configure SIEM security operations using Microsoft Sentinel

Microsoft Partner

Cel szkolenia:

Rozpocznij pracę z operacjami zabezpieczeń usługi Microsoft Sentinel, konfigurując obszar roboczy usługi Microsoft Sentinel, łącząc usługi firmy Microsoft i zdarzenia zabezpieczeń systemu Windows z usługą Microsoft Sentinel, konfigurując reguły analizy usługi Microsoft Sentinel i reagując na zagrożenia za pomocą automatycznych odpowiedzi. Po ukończeniu tego kursu uczniowie będą mogli wykonywać następujące czynności:

- Tworzenie i konfigurowanie obszaru roboczego usługi Microsoft Sentinel
- Wdrażanie rozwiązania centrum zawartości usługi Microsoft Sentinel
- Łączenie hostów systemu Windows z usługą Microsoft Sentinel
- Konfigurowanie reguł analizy w usłudze Microsoft Sentinel
- Konfigurowanie automatyzacji w usłudze Microsoft Sentinel

Profil odbiorców:
Analityk ds. zabezpieczeń firmy Microsoft współpracuje z uczestnikami projektu w organizacji w celu zabezpieczenia systemów informatycznych dla organizacji. Ich celem jest zmniejszenie ryzyka organizacyjnego poprzez szybkie korygowanie aktywnych ataków w środowisku, doradzanie w zakresie ulepszeń praktyk ochrony przed zagrożeniami i odwoływania się do naruszeń zasad organizacyjnych odpowiednim uczestnikom projektu.

Umiejętności zdobyte po ukończeniu:
- Konfigurowanie operacji zabezpieczeń SIEM przy użyciu usługi Microsoft Sentinel

Plan szkolenia:

- Konfigurowanie operacji zabezpieczeń rozwiązania SIEM przy użyciu usługi Microsoft Sentinel
  - Moduł 1: Tworzenie obszarów roboczych usługi Microsoft Sentinel i zarządzanie nimi
  - Moduł 2: Łączenie usług firmy Microsoft z usługą Microsoft Sentinel
  - Moduł 3: Łączenie hostów z systemem Windows z usługą Microsoft Sentinel
  - Moduł 4: Wykrywanie zagrożeń za pomocą analizy w usłudze Microsoft Sentinel
  - Moduł 5: Automatyzacja w usłudze Microsoft Sentinel

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Moduł 6: Konfigurowanie operacji zabezpieczeń rozwiązania SIEM przy użyciu usługi Microsoft Sentinel

Wymagania:

- Podstawowa wiedza na temat platformy Microsoft Azure
- Podstawowa wiedza o usłudze Microsoft Sentinel
- Doświadczenie w korzystaniu z języka Kusto Query Language (KQL) w usłudze Microsoft Sentinel

Poziom trudności

Certyfikaty:

Uczestnicy otrzymają certyfikaty podpisane przez Microsoft (ukończenie kursu).

Prowadzący:

Microsoft Certified Trainer (MCT)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Postępu 18B, 02-676 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001