Training: Microsoft

SC-5004: Defend against cyberthreats with Microsoft Defender XDR

Microsoft Partner

TRAINING GOALS:

Implement the Microsoft Defender for Endpoint environment to manage devices, perform investigations on endpoints, manage incidents in Defender XDR, and use Advanced Hunting with Kusto Query Language (KQL) to detect unique threats.

Audience Profile:
The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders.

Skills earned upon completion:
- Defend against cyberthreats with Microsoft Defender XDR

CONSPECT:

- Defend against cyberthreats with Microsoft Defender XDR
  - Module 1: Mitigate incidents using Microsoft Defender
  - Module 2: Deploy the Microsoft Defender for Endpoint environment
  - Module 3: Configure for alerts and detections in Microsoft Defender for Endpoint
  - Module 4: Configure and manage automation using Microsoft Defender for Endpoint
  - Module 5: Perform device investigations in Microsoft Defender for Endpoint
  - Module 6: Defend against Cyberthreats with Microsoft Defender XDR lab exercises

REQUIREMENTS:

- Experience using the Microsoft Defender portal
- Basic understanding of Microsoft Defender for Endpoint
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in 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.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Microsoft (course completion). This course is not directly mapped to a Microsoft certification exam.

TRAINER:

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.
EUR: PL 79 1600 1462 1853 6451 3000 0006
USD: PL 52 1600 1462 1853 6451 3000 0007