Training: Microsoft

SC-5001: Configure SIEM security operations using Microsoft Sentinel

Microsoft Partner

TRAINING GOALS:

Get started with Microsoft Sentinel security operations by configuring the Microsoft Sentinel workspace, connecting Microsoft services and Windows security events to Microsoft Sentinel, configuring Microsoft Sentinel analytics rules, and responding to threats with automated responses. After completing this course, students will be able to:

- Create and configure a Microsoft Sentinel workspace
- Deploy a Microsoft Sentinel content hub solution
- Connect Windows hosts to Microsoft Sentinel
- Configure analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel

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:
- Configure SIEM operations with Microsoft Sentinel

CONSPECT:

- Configure SIEM security operations using Microsoft Sentinel
  - Module 1: Create and manage Microsoft Sentinel workspaces
  - Module 2: Connect Microsoft services to Microsoft Sentinel
  - Module 3: Connect Windows hosts to Microsoft Sentinel
  - Module 4: Threat detection with Microsoft Sentinel analytics
  - Module 5: Automation 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

- Module 6: Configure SIEM security operations using Microsoft Sentinel

REQUIREMENTS:

- Fundamental understanding of Microsoft Azure
- Basic understanding of Microsoft Sentinel
- Experience using Kusto Query Language (KQL) in Microsoft Sentinel

Difficulty level



CERTIFICATE:

The participants will obtain certificates signed by Microsoft (course completion).

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