Training: Microsoft

MS-55610 Planning and implementing Microsoft Sentinel (SIEM & SOAR)

Microsoft Partner

TRAINING GOALS:

This 3 day hands on course helps you get ramped up with Microsoft Sentinel and provide hands-on practical experience for product features, capabilities, and scenarios.

During the course you will deploy a Microsoft Sentinel workspace and ingest pre-recorded data to simulate scenarios that showcase various Microsoft Sentinel features.

This course is aimed at IT professionals and Azure administrators that have some experience administering and configuring Azure, but want to gain an insight into implementing Microsoft's SIEM/SOAR solution, Microsoft Sentinel.

CONSPECT:

- Microsoft Sentinel Overview
  - Microsoft Sentinel Overview
  - Data ingestion methods
  - Microsoft Sentinel for MSSPs
  - User and entity behavior analysis
  - Fusion
  - Notebooks
  - Management and automation tools
  - Logs and costs
- KQL
  - The importance of KQL across Azure
  - User interface (demo)
  - Standard KQL structure
  - Common KQL commands
- Data connectors
  - Managing content in Microsoft Sentinel
  - Connecting data to Microsoft Sentinel using data connectors
  - Connecting Microsoft services to Microsoft Sentinel
  - Connecting Microsoft 365 Defender to 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

- Connecting Windows hosts to Microsoft Sentinel
- Connecting Common Event Format logs to Microsoft Sentinel
- Connecting syslog data sources to Microsoft Sentinel
- Connecting threat indicators to Microsoft Sentinel

- Analytic rules
  - Detecting threats using Microsoft Sentinel analytics
  - Automation in Microsoft Sentinel
  - Responding to threats using Microsoft Sentinel playbooks
- Incident management
  - Incident management overview
  - User and entity behavior analysis
  - Data normalization in Microsoft Sentinel
  - Searching, visualizing, and monitoring data
- Hunting
  - Threat hunting concepts
  - Threat hunting using Microsoft Sentinel
  - Using hunting queries in Microsoft Sentinel
  - Threat hunting using notebooks
- Watchlists
  - Prioritizing incidents
  - Importing business data
  - Reducing alert fatigue
  - Enriching event data
- Threat intelligence
  - Threat intelligence overview
  - Threat intelligence in Microsoft Sentinel

REQUIREMENTS:

- Basic conceptual understanding of Microsoft Azure.
- Experience with Windows 10 devices.
- Experience with Office 365.
- Basic understanding of authorization and authentication.
- Basic understanding of computer networks.
- Working knowledge of managing mobile devices.

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:

Certificate of completing an authorized Microsoft training.

TRAINER:

Microsoft Certified Trainer.

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