Training: Microsoft
Azure Security Bootcamp

Microsoft Partner

TRAINING GOALS:

This course is a combination of the **SC-900T00: Introduction to Microsoft Security, Compliance, and Identity** and **SC-200T00: Defend against cyberthreats with Microsoft's security operations platform courses**.

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft Sentinel as well as utilize Kusto Query Language (KQL) to perform detection, analysis, and reporting. The course was designed for people who work in a Security Operations job role and helps learners prepare for the exam SC-200: Microsoft Security Operations Analyst.

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. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud, and third-party security products.

Skills earned upon completion:

- Manage threat mitigation using Microsoft Defender XDR
- Manage threat mitigation using Microsoft Purview
- Manage threat mitigation using Microsoft Defender for Endpoint
- Manage threat mitigation using Microsoft Defender for Cloud
- Create KQL queries for Microsoft Sentinel
- Configure your environment in Microsoft Sentinel
- Manage log connection 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

- Detect and remediate threats using Microsoft Sentinel
- Manage threat hunting in Microsoft Sentinel

CONSPECT:

- Introduction to security, compliance, and identity concepts
  - Module 1: Describe security and compliance concepts
  - Module 2: Describe identity concepts
- Introduction to Microsoft Entra
  - Module 1: Describe the function and identity types of Microsoft Entra ID
  - Module 2: Describe the authentication capabilities of Microsoft Entra ID
  - Module 3: Describe access management capabilities of Microsoft Entra
  - Module 4: Describe the identity protection and governance capabilities of Microsoft Entra
- Introduction to Microsoft security solutions
  - Module 1: Describe Microsoft Security Copilot
  - Module 2: Describe core infrastructure security services in Azure
  - Module 3: Describe the security management capabilities in Azure
  - Module 4: Describe security capabilities of Microsoft Sentinel
  - Module 5: Describe threat protection with Microsoft Defender XDR
- Introduction to Microsoft Purview and Microsoft's privacy principles
  - Module 1: Describe Microsoft's Service Trust portal and privacy principles
  - Module 2: Describe the data security solutions of Microsoft Purview
  - Module 3: Describe the data compliance solutions of Microsoft Purview
  - Module 4: Describe the data governance solutions of Microsoft Purview
- Mitigate threats using Microsoft Defender XDR
  - Module 1: Introduction to Microsoft Defender XDR threat protection
  - Module 2: Mitigate incidents using Microsoft Defender
  - Module 3: Remediate threats using Microsoft Defender
  - Module 4: Manage Microsoft Entra Identity Protection
  - Module 5: Secure your cloud apps and services with Microsoft Defender for Cloud Apps
  - Module 6: Manage Microsoft Defender for Office 365
- Mitigate threats using Microsoft Security Copilot
  - Module 1: Introduction to generative AI and agents
  - Module 2: Describe Microsoft Security Copilot
  - Module 3: Describe the core features of Microsoft Security Copilot

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 4: Describe the embedded experiences of Microsoft Security Copilot
- Module 5: Experience Security Copilot through guided simulations

- Mitigate threats using Microsoft Purview
  - Module 1: Investigate and respond to Microsoft Purview Data Loss Prevention alerts
  - Module 2: Investigate insider risk alerts and related activity
  - Module 3: Search and investigate with Microsoft Purview Audit
  - Module 4: Search for content with Microsoft Purview eDiscovery
- Mitigate threats using Microsoft Defender for Endpoint
  - Module 1: Protect against threats with Microsoft Defender for Endpoint
  - Module 2: Deploy the Microsoft Defender for Endpoint environment
  - Module 3: Implement Windows security enhancements with Microsoft Defender for Endpoint
  - Module 4: Perform device investigations in Microsoft Defender for Endpoint
  - Module 5: Perform actions on a device using Microsoft Defender for Endpoint
  - Module 6: Perform evidence and entities investigations using Microsoft Defender for Endpoint
  - Module 7: Configure and manage automation using Microsoft Defender for Endpoint
  - Module 8: Configure for alerts and detections in Microsoft Defender for Endpoint
  - Module 9: Utilize Vulnerability Management in Microsoft Defender for Endpoint
- Mitigate threats using Microsoft Defender for Cloud
  - Module 1: Plan for cloud workload protections using Microsoft Defender for Cloud
  - Module 2: Connect Azure assets to Microsoft Defender for Cloud
  - Module 3: Connect non-Azure resources to Microsoft Defender for Cloud
  - Module 4: Manage your cloud security posture management
  - Module 5: Explain cloud workload protections in Microsoft Defender for Cloud
  - Module 6: Remediate security alerts using Microsoft Defender for Cloud
- Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
  - Module 1: Construct KQL statements for Microsoft Sentinel
  - Module 2: Analyze query results using KQL
  - Module 3: Build multi-table statements using KQL
  - Module 4: Work with data in Microsoft Sentinel using Kusto Query Language
- Configure your Microsoft Sentinel environment
  - Module 1: Introduction to Microsoft Sentinel
  - Module 2: Create and manage Microsoft Sentinel workspaces
  - Module 3: Query logs in Microsoft Sentinel
  - Module 4: Use watchlists in Microsoft Sentinel
  - Module 5: Utilize threat intelligence 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: Integrate Microsoft Defender XDR with Microsoft Sentinel

- Connect logs to Microsoft Sentinel
  - Module 1: Connect data to Microsoft Sentinel using data connectors
  - Module 2: Connect Microsoft services to Microsoft Sentinel
  - Module 3: Connect Microsoft Defender XDR to Microsoft Sentinel
  - Module 4: Connect Windows hosts to Microsoft Sentinel
  - Module 5: Connect Common Event Format logs to Microsoft Sentinel
  - Module 6: Connect syslog data sources to Microsoft Sentinel
  - Module 7: Connect threat indicators to Microsoft Sentinel
- Create detections and perform investigations using Microsoft Sentinel
  - Module 1: Threat detection with Microsoft Sentinel analytics
  - Module 2: Automation in Microsoft Sentinel
  - Module 3: Threat response with Microsoft Sentinel playbooks
  - Module 4: Security incident management in Microsoft Sentinel
  - Module 5: Identify threats with Behavioral Analytics
  - Module 6: Data normalization in Microsoft Sentinel
  - Module 7: Query, visualize, and monitor data in Microsoft Sentinel
  - Module 8: Manage content in Microsoft Sentinel
- Perform threat hunting in Microsoft Sentinel
  - Module 1: Explain threat hunting concepts in Microsoft Sentinel
  - Module 2: Threat hunting with Microsoft Sentinel
  - Module 3: Use Search jobs in Microsoft Sentinel
  - Module 4: Hunt for threats using notebooks in Microsoft Sentinel

REQUIREMENTS:

- Fundamental understanding of Microsoft security, compliance, and identity products
- Basic understanding of Microsoft Defender XDR
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage (for LP5)
- Familiarity with Azure virtual machines and virtual networking (for LP5)
- Foundational knowledge of computer networking
- Understanding of KQL usage in Microsoft Sentinel

Difficulty level



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

CERTIFICATE:

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

This course will help prepare you for the **Microsoft Certified: Security, Compliance, and Identity Fundamentals** certification exam (Exam SC-900), which is available through the Pearson VUE test centers and help prepare you for the **Microsoft Certified: Security Operations Analyst Associate** certification exam (Exam SC-200), which is available through the Pearson VUE test centers.

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