Training: Microsoft
SC-200T00 Microsoft Security Operations Analyst

Gold Microsoft Partner

TRANING TERMS

2026-02-10 | 4 days | Kraków / Virtual Classroom
2026-02-10 | 4 days | Warszawa / Virtual Classroom
2026-03-10 | 4 days | Kraków / Virtual Classroom
2026-03-10 | 4 days | Warszawa / Virtual Classroom
2026-04-14 | 4 days | Kraków / Virtual Classroom
2026-04-14 | 4 days | Warszawa / Virtual Classroom
2026-05-12 | 4 days | Kraków / Virtual Classroom
2026-05-12 | 4 days | Warszawa / Virtual Classroom
2026-06-16 | 4 days | Kraków / Virtual Classroom
2026-06-16 | 4 days | Warszawa / Virtual Classroom

TRAINING GOALS:

Learn how to investigate, respond to, and hunt for threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Azure 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 S.C.-200: Microsoft Security Operations Analyst.

Skills gained:

- Explain how Microsoft Defender for Endpoint can remediate risks in your environment
- Create a Microsoft Defender for Endpoint environment
- Configure Attack Surface Reduction rules on Windows 10 devices
- Perform actions on a device using Microsoft Defender for Endpoint
- Investigate domains and IP addresses in Microsoft Defender for Endpoint
- Investigate user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft Defender for Endpoint
- Explain how the threat landscape is evolving
- Conduct advanced hunting in Microsoft 365 Defender
- Manage incidents in Microsoft 365 Defender
- Explain how Microsoft Defender for Identity can remediate risks in your environment.
- Investigate DLP alerts in Microsoft Cloud App Security

Compendium Education Center Ltd.
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

- Explain the types of actions you can take on an insider risk management case.
- Configure auto-provisioning in Azure Defender
- Remediate alerts in Azure Defender
- Construct KQL statements
- Filter searches based on event time, severity, domain, and other relevant data using KQL
- Extract data from unstructured string fields using KQL
- Manage an Azure Sentinel workspace
- Use KQL to access the watchlist in Azure Sentinel
- Manage threat indicators in Azure Sentinel
- Explain the Common Event Format and Syslog connector differences in Azure Sentinel
- Connect Azure Windows Virtual Machines to Azure Sentinel
- Configure Log Analytics agent to collect Sysmon events
- Create new analytics rules and queries using the analytics rule wizard
- Create a playbook to automate an incident response
- Use queries to hunt for threats
- Observe threats over time with livestream

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 Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

CONSPECT:

- Mitigate threats using Microsoft Defender for Endpoint
  - Protect against threats with Microsoft Defender for Endpoint
  - Deploy the Microsoft Defender for Endpoint environment
  - Implement Windows 10 security enhancements with Microsoft Defender for Endpoint
  - Manage alerts and incidents in Microsoft Defender for Endpoint
  - Perform device investigations in Microsoft Defender for Endpoint
  - Perform actions on a device using Microsoft Defender for Endpoint
  - Perform evidence and entities investigations using Microsoft Defender for Endpoint

Compendium Education Center Ltd.
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

    - Configure and manage automation using Microsoft Defender for Endpoint
    - Configure for alerts and detections in Microsoft Defender for Endpoint
    - Utilize Threat and Vulnerability Management in Microsoft Defender for Endpoint
- Mitigate threats using Microsoft 365 Defender
    - Introduction to threat protection with Microsoft 365
    - Mitigate incidents using Microsoft 365 Defender
    - Protect your identities with Azure AD Identity Protection
    - Remediate risks with Microsoft Defender for Office 365
    - Safeguard your environment with Microsoft Defender for Identity
    - Secure your cloud apps and services with Microsoft Cloud App Security
    - Respond to data loss prevention alerts using Microsoft 365
    - Manage insider risk in Microsoft 365
- Mitigate threats using Azure Defender
    - Plan for cloud workload protections using Azure Defender
    - Explain cloud workload protections in Azure Defender
    - Connect Azure assets to Azure Defender
    - Connect non-Azure resources to Azure Defender
    - Remediate security alerts using Azure Defender
- Create queries for Azure Sentinel using Kusto Query Language (KQL)
    - Construct KQL statements for Azure Sentinel
    - Analyze query results using KQL
    - Build multi-table statements using KQL
    - Work with data in Azure Sentinel using Kusto Query Language
- Configure your Azure Sentinel environment
    - Introduction to Azure Sentinel
    - Create and manage Azure Sentinel workspaces
    - Query logs in Azure Sentinel
    - Use watchlists in Azure Sentinel
    - Utilize threat intelligence in Azure Sentinel
- Connect logs to Azure Sentinel
    - Connect data to Azure Sentinel using data connectors
    - Connect Microsoft services to Azure Sentinel
    - Connect Microsoft 365 Defender to Azure Sentinel
    - Connect Windows hosts to Azure Sentinel
    - Connect Common Event Format logs to Azure Sentinel
    - Connect syslog data sources to Azure Sentinel

Compendium Education Center Ltd.
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

    - Connect threat indicators to Azure Sentinel
- Create detections and perform investigations using Azure Sentinel
    - Threat detection with Azure Sentinel analytics
    - Threat response with Azure Sentinel playbooks
    - Security incident management in Azure Sentinel
    - Use entity behavior analytics in Azure Sentinel
    - Query, visualize, and monitor data in Azure Sentinel
- Perform threat hunting in Azure Sentinel
    - Threat hunting with Azure Sentinel
    - Hunt for threats using notebooks in Azure Sentinel

REQUIREMENTS:

Before attending this course, students must have:

- Basic understanding of Microsoft 365
- Fundamental understanding of Microsoft security, compliance, and identity products
- Intermediate understanding of Windows 10
- Familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking
- Basic understanding of scripting concepts.

Difficulty level

CERTIFICATE:

Certificate of completing an authorized Microsoft training.

TRAINER:

Microsoft Certified Trainer.

Compendium Education Center Ltd.
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