altkom akademia

training code: SC-200 / ENG DL 4d / EN

Microsoft Security Operations Analyst

Authorized Microsoft Security Operations Analyst SC-200 Distance Learning training.

Target audience:

- Administrator
- IT specialist
- Security specialist
- Security engineer

Training recipients

The Microsoft Security Operations Analysts work with various departments in an organization to secure IT systems. Their goal is to reduce organizational risk by:
• Rapidly remediating active attacks in the environment,
• Advising on improving threat protection practices,
• Referring violations of organizational policies to appropriate stakeholders.

Responsibilities include monitoring, analyzing, and responding to threats using a variety of security solutions across the environment. The Security Operations Analysts role primarily investigates, responds, and searches for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. The Security Operations Analyst uses the operational results of these tools.

This course is intended for security administrators, cloud administrators, IT specialists and individuals who are interested in learning about:

- Managing Microsoft Azure Sentinel
- Managing Azure Defender
- Managing Microsoft 365 Defender
- Using Kusto Query Language

Benefits

During the training, the participant will learn how to investigate, respond to, and hunt threats using Microsoft Azure Sentinel, Azure Defender, and Microsoft 365 Defender. This course will teach you how to mitigate cyber threats using these solutions. In particular, you will gain knowledge and practical experience in configuring and using Microsoft 365 Defender XDR and Azure Sentinel, as well as using Kusto Query Language (KQL) for detection, analysis, and reporting. The course is designed for people who work in a Security position.
The training helps participants prepare for the SC-200 exam.

Training program

1: Mitigate threats using Microsoft Defender XDR
Introduction to threat protection with Microsoft Defender XDR
Mitigate incidents using Microsoft Defender XDR
Remediate risks with Defender for Office 365 in Microsoft Defender XDR
Microsoft Defender for Identity in Microsoft Defender XDR
Protect your identities with Entra ID Protection
Defender for Cloud Apps in Microsoft Defender XDR
2: Mitigate threats using Microsoft Copilot for Security
Fundamentals of Generative AI
Describe Microsoft Copilot for Security
Describe the core features of Microsoft Copilot for Security
Describe the embedded experiences of Microsoft Copilot for Security
3: Mitigate threats using Microsoft Purview
Microsoft Purview Compliance Solutions
Investigate and remediate compromised entities identified by Microsoft Purview data loss prevention (DLP) policies
Investigate and remediate insider risk threats identified by Microsoft Purview policies

Investigate threats using Content search in Microsoft Purview
Investigate threats using Microsoft Purview Audit (Standard)
Investigate threats using Microsoft Purview Audit (Premium)

4: Mitigate threats using Microsoft Defender for Endpoint
Protect against threats with Microsoft Defender for Endpoint
Deploy the Microsoft Defender for Endpoint environment
Implement Windows security enhancements
Perform device investigations
Perform actions on a device
Perform evidence and entities investigations
Configure and manage automation
Configure for alerts and detections
Utilize Threat and Vulnerability Management

5: Mitigate threats using Microsoft Defender for Cloud
Plan for cloud workload protections using Microsoft Defender for Cloud
Connect Azure assets to Microsoft Defender for Cloud
Connect non-Azure assets to Microsoft Defender for Cloud
Manage your cloud security posture management
Workload protections in Microsoft Defender for Cloud
Remediate security alerts using Microsoft Defender for Cloud

6: Create queries for Microsoft Sentinel using Kusto Query Language (KQL)
Construct KQL statements for Microsoft Sentinel
Analyze query results using KQL
Build multi-table statements using KQL
Work with string data in using KQL statements

7: Configure your Microsoft Sentinel environment
Introduction to Microsoft Sentinel
Create and manage Microsoft Sentinel workspaces
Query logs in Microsoft Sentinel
Use watchlists in Microsoft Sentinel
Utilize threat intelligence in Microsoft Sentinel

8: Connect logs to Microsoft Sentinel
Manage content in Microsoft Sentinel
Connect data to Microsoft Sentinel using data connectors
Connect Microsoft services to Microsoft Sentinel
Connect Microsoft Defender XDR to Microsoft Sentinel
Connect Windows hosts to Microsoft Sentinel
Connect Common Event Format logs to Microsoft Sentinel
Connect syslog data sources to Microsoft Sentinel
Connect threat indicators to Microsoft Sentinel

9: Create detections and perform investigations using Microsoft Sentinel

Threat detection with Microsoft Sentinel analytics

Automation in Microsoft Sentinel

Threat response with Microsoft Sentinel playbooks

Security incident management in Microsoft Sentinel

Entity behavioral analytics in Microsoft Sentinel

Data normalization in Microsoft Sentinel

Query, visualize, and monitor data in Microsoft Sentinel

10: Perform threat hunting in Microsoft Sentinel

Explain threat hunting concepts in Microsoft Sentinel

Threat hunting with Microsoft Sentinel

Use Search jobs in Microsoft Sentinel

Optional – Hunt for threats using notebooks in Microsoft Sentinel

Expected preparation of the participant

- Knowledge of Microsoft 365
- Knowledge of Microsoft security and compliance technologies.
- Knowledge of information protection concepts.
- Understanding of cloud computing concepts.
- Intermediate knowledge of Windows 10/11
- Knowledge of Azure services
- Basic understanding of scripting concepts
- Ability to use English-language materials
- Pre-training: AZ-900, MS-900, SC-900, SC-300, SC-400
- An ability to use English language materials

To make work more convenient and training more effective we suggest using additional screen. Lack of extra screen does not make it impossible to participate in the training, but significantly influences the convenience of work during classes

Information and requirements conerning participation in distance learning trainings is available at: https://www.altkomakademia.pl/distance-learning/#FAQ

Training Includes

* electronic handbook available at:

https://learn.microsoft.com/pl-pl/training/

- access to the Altkom Akademia student portal
- training conducted in the form of a presentation

- trainer demonstrations
- practical exercises (laboratories)

Training method:

- Distance Learning formula

Language

- **Training**: English
- **Materials**: English

Examination method

The exam is on-line. You can enroll at: https://home.pearsonvue.com/Clients/Microsoft.aspx

Duration

4 days / 28 hours

Examination description

After the SC-200 course, you can take Microsoft certification exams:an Authorized Test Center,online being monitored by an offsite proctor. Details on the website: https://docs.microsoft.com/en-us/learn/certifications/exams/sc-200