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

Purpose of the training

The training is intended for:

- Configuring Microsoft Azure Sentinel
- Managing Azure Defender
- Managing Microsoft 365 Defender
- The use of Kusto Query Language

Microsoft Security Operations Analyst cooperates with different corporate departments to secure IT systems. They aim to diminish the organisational risk by Troubleshooting active attacks in environment, consulting in the area of mastering the practice of securing against threats and addressing organisational policies’ violations to appropriate stakeholders. The responsibilities include managing threats, monitoring and reacting with the use of different protective solutions in the whole environment. First of all, the role aims to study, react and search threats with the use of Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender and products securing other companies. Since Security Operations Analyst uses operational results of these tools, they are also the key stakeholder in configuring and implementing these technologies.

Benefits of completing the training

- Explain how Microsoft Defender for Endpoint application may troubleshoot the risk in your environment
- Create Microsoft Defender for Endpoint environment
- Configure the rules of reducing the area of the attack on devices with Windows 10 system
- Perform actions on device using Microsoft Defender for Endpoint
- Study domains and IP addresses in Microsoft Defender for Endpoint
- Study user accounts in Microsoft Defender for Endpoint
- Configure alert settings in Microsoft Defender for Endpoint
- Explain how the view of threats is evolving
- Perform an advanced hunt in Microsoft 365 Defender service
- Manage incidents in Microsoft 365 Defender service
- Explain how Microsoft Defender for Identity application might troubleshoot the risk in your environment.
- Study DLP alerts in Microsoft Cloud App Security
- Explain the types of actions which you may undertake in case of managing internal risk.
- Configure automatic sharing in automatyczne Azure Defender service
- Fix alerts in Azure Defender service
- Write KQL instructions
- Filter the search based on time of event, significance, domain and other important data with the use of KQL
- Distinguish data from unstructured chain fields with the use of KQL language
- Manage Azure Sentinel working area
- Use KQL language to gain access to the observed list on Azure Sentinel platform
- Manage threat indicators on Azure Sentinel platform
- Explain differences in Common Event Format connector and Syslog in Azure Sentinel service
- Combine Azure Windows virtual machines with Azure Sentinel platform
- Configure Log Analytics agent to collect Sysmon events
- Create new analytical rules and queries with the use of analytical rules creator
- Write a guide to automate reaction to incident
- Use queries to hunt for threats
- Observe threats in time thanks to live transmission

Find out how to study threats, reply to them and hunt them with the use Microsoft Azure Sentinel, Azure Defender and Microsoft 365 Defender platforms. During the course you will learn how to limit cyberthreats using these technologies. Especially you will configure and use Azure Sentinel, and also apply Kusto Query Language (KQL) to detect, analyse and report. The course has been designed for the people who work on Security position.

Examination method

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

Exam 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

Expected Listener Preparation

- Basic knowledge of Microsoft 365 platform
- Basic knowledge about Microsoft products related to securities, compatibility and identity
- Intermediate knowledge about Windows 10 system
- Knowledge of Azure platform services, especially Azure SQL Database and Azure Storage
- Knowledge of Azure platform virtual machines and virtual networks
- Basic understanding of script concepts
- 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 Language

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

Training Includes

* electronic handbook available at:

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

* access to Altkom Akademia student portal

Training method:

- theory
- demos
- individual laboratories
- 50% theory
- 50% practice

Duration

4 days / 28 hours

Training agenda

1: Limting threats with the use of Microsoft Defender for Endpoint service

- Protect yourself against threats thanks to Microsoft Defender for Endpoint service
- Deploy Microsoft Defender for Endpoint environment
- Implement enhancements to Windows 10 system with the use of Microsoft Defender for Endpoint service
- Manage alerts and incidents in Microsoft Defender for Endpoint application
- Conduct a research of devices in Microsoft Defender for Endpoint application
- Perform actions on device using Microsoft Defender for Endpoint service
- Conduct research of evidence and subjects with the use of Microsoft Defender for Endpoint application
- Configure automation and manage it with the use of Microsoft Defender for Endpoint service
- Configure alerts and detections in Microsoft Defender for Endpoint application
- Make use of threats and gaps in Microsoft Defender for Endpoint application

2: Limiting threats with the use of Microsoft 365 Defender

- Introduction to security against threats thanks to Microsoft 365 platform
- Limit incidents with the use of Microsoft 365 Defender service
- Protect your identities thanks to Azure AD Identity Protection service
- Diminish the risk thanks to Microsoft Defender dla usługi Office 365 service
- Protect your environment thanks to Microsoft Defender for Identity
- Secure your applications and services in cloud thanks to Microsoft Cloud App Security
- Reply to alerts related to data loss prevention, by using Microsoft 365 platform

- Manage internal risk on Microsoft 365 platform

3: Threat mitigation with Azure Defender

- Plan sceruing overloads in cloud with the use of Azure Defender service
- Explain securities of cloud overloads in Azure Defender service
- Combine Azure platform resources with Azure Defender service
- Combine non-Azure platform resources with Azure Defender service
- Troubleshoot security alerts with the use of Azure Defender service

4: Creating queries for Azure Sentinel with the ues of Kusto Query Language (KQL)

- Write KQL instructions for Azure Sentinel service
- Analyse results of queries with the use of KQL
- Write multi-table instructions with the use of KQL
- Work with data on Azure Sentinel platform with the use of Kusto Query Language

5: Configure Azure Sentinel environment

- Introduction to Azure Sentinel
- Create Azure Sentinel working areas and manage them
- Query logs on Azure Sentinel platform
- Use observed lists on Azure Sentinel platform
- Use threat analysis in Azure Sentinel service

6: Combine logs from Azure Sentinel

- Combine data with Azure Sentinel platform using data connectors
- Combine Microsoft services with Azure Sentinel service
- Combine Microsoft 365 Defender service with Azure Sentinel service
- Combine Windows system hosts with Azure Sentinel platform
- Combine Common Event Format logs with Azure Sentinel service
- Combine syslog data sources with Azure Sentinel service
- Combine threat indicators with Azure Sentinel service

7: Create detection and run investigations using Azure Sentinel service

- Detecting threats thanks to Azure Sentinel Analytics service
- Reacting to threat using Azure Sentinel handbooks
- Managing security events on Azure Sentinel platform
- Use analysis of individuals’ behaviour on Azure Sentinel platform
- Performing queries and monitoring data in Azure Sentinel service

8: Hunt for threats in Azure Sentinel

- Hunting for threats with Azure Sentinel
- Hunt for threats with the use of notebooks in Azure Sentinel service