SC-200 – Microsoft Security Operations Analyst

Microsoft Official Course (MOC)

Course

Course SC-200T00-A: Microsoft Security Operations Analyst

(4 days)

About this Course:

- 4 Days
- Instructor-led training
- Intermediate
- English

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 SC-200: Microsoft Security Operations Analyst.

Course Goals/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
- 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:

- 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.

Course Format:

Присъствен (Classroom) Курс в Учебната ни зала или В Офис на Клиент	**Онлайн (Online/Virtual) Курс във виртуална зала с инструктор**

Course Language Option

Български (Bulgarian)	**Английски (English)**

You can choose the language in which the training will be conducted – Bulgarian or English. All our instructors are fluent in English.

Student Guides:

The training materials are available in electronic format. They can be used online / offline on any device. Lifetime access.

Lab Environment:

Each student has their own lab environment where the exercises are conducted, part of the course. You do not need to install software on a computer or special hardware requirements.
Participants in a face-to-face format in our Training Center have an individual computer during the training.

At Course Completion:

Lifetime Access - Video Archive 24/7	**Certificate of Course Completion**

Lifetime access to a video archive with recording of each individual lecture.
Official internationally recognized certificate for completed training course.

Course Duration:

- 4 working days (09:00 – 17:00)
  or
- 32 hours training (theory and practice) in non-working hours lasting 4 weeks
  Saturday and Sunday 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
  Monday and Wednesday 19:00 – 23:00
  Tuesday and Thursday 19:00 – 23:00

Payments:

An application for an invoice is accepted at the time of enrollment in the respective course.

An invoice is issued within 7 days of confirming the payment.

Upcoming Courses

■ Notice
There are no upcoming events.
For more information, use the contact form.

We will contact you to confirm the dates.

Prerequisites:

- 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.

The course prepares for the following certification levels

- **SC-200: Microsoft Security Operations Analyst**
  You can be certified in our test center with a voucher with a discount on the price of the exam.
- Може да се сертифицирате в нашия тест център с ваучер с отстъпка от цената на изпит.