Microsoft Security Operations Analyst

Trainer Preparation Guide

Purpose

This document is for Microsoft Certified Trainers preparing to teach the SC-200 Microsoft Security Operations Analyst course.

Security Operation Analyst Role Definition

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.

Certification Exam

Certification exams measure your ability to accomplish certain technical tasks for a job role. Each study area has a percentage indicating the relative weight of the area on the exam. The higher the percentage, the more questions you are likely to see in that area.

Study Area	Percentage
Mitigate threats using Microsoft 365 Defender	25-30%
Mitigate threats using Azure Defender	25-30%
Mitigate threats using Azure Sentinel	40-45%

✔ For more information, on the skills measured in the exam, please visit the SC-200 Microsoft Security Operations Analyst certification page.

Preparing to Teach

In the next sections we will cover the main course components and how they can used in class. There is a lot of flexibility in how you use this content to create the best learning experience for your students.

Content

The content for your course is organized into Modules, Lessons, and Topics. There are four modules corresponding to the four testing domain areas.

Module 01 – Mitigate threats using Microsoft Defender for Endpoint
Module 02 – Mitigate threats using Microsoft 365 Defender
Module 03 – Mitigate threats using Azure Defender
Module 04 – Create queries for Azure Sentinel using Kusto Query Language (KQL)
Module 05 – Configure your Azure Sentinel environment
Module 06 – Connect logs to Azure Sentinel
Module 07 – Create detections and perform investigations using Azure Sentinel
Module 08 – Perform threat hunting in Azure Sentinel

✔ This is a suggested order. Always ensure you are covering the content most applicable to your audience. There is a Change Log that provides more detailed information on how this course has changed from the previous version.

PowerPoint Slides

Each module has a PowerPoint deck. Each course topic has a PowerPoint slide. Instructor Notes are provided below each slide to identity the Documentation page and provide discussion points.

✔ The Module 00 PowerPoint provides a course overview. Adjust this module to your needs.

Guided Demonstrations

This course includes numerous guided demonstrations which are intended for the learners to perform as interactions between the course labs. Some of these interactive guides are only listed in the notes section of the PPT and are considered optional. We have also provided advice about demonstrations you should perform as an instructor if you see fit.

Videos

For numerous topics within the course there are links to related videos for that topic in the notes section of the PPT. These videos are entirely supplemental to be used at your discretion.

Labs

The labs for this course require both a Microsoft 365 E5 licensed tenant as well as an Azure subscription.

- You can request Microsoft Learning Azure Passes for yourself and your students.
- Ensure that you request these passes at least two weeks before the class starts. After receiving the passes each student will need to activate their pass.
- The Azure pass effectively functions in the same way as the publicly available Microsoft Azure Trial Subscription. This means there are limitations on what you can do with the pass.
- The lab instructions are in the SC-200 Microsoft Learning GitHub repository.

Classroom Schedule

Day 1	Day 2	Day 3	Day 4
Microsoft 365 Defender and Defender for Endpoint	Azure Defender and KQL queries	Azure Sentinel – setup and connecting data	Azure Sentinel – detections, investigations, and hunting

Each day of this course you should be able to get through about two modules with the learners.

In module 2 there are lots of guided demonstrations whereas the lab for that module is exploratory. Our intention was to give the learners a sense of the product capabilities with the guided demonstrations. However, since the guided demonstrations are non-tenant-based interactions, the lab was designed to enable the learners to explore the parts of the Microsoft 365 tenant that most interests them. We requisitioned a Microsoft 365 E5 tenant with 25 users for this course to allow for maximum security and compliance feature licensing. You might consider having the learners perform tasks they learned during the guided demonstrations in the lab exploration.

In module 3, you will cover Azure Defender and need to use the Azure pass for the first time during the labs. The labs for this course were tested multiple times and never incurred more than $3USD of Azure service usage. If learners don't have access to an Azure pass, they can sign-up for a trial subscription in a number of ways presented in the Azure console. Labs for module 3, 5-8 require an Azure subscription.

In module 4, you will discuss and demonstrate Kusto querying. This module is more like a transact-SQL module than a typical Azure or Microsoft 365 module. You should practice running the scripts against the demo data. KQL is critical to threat investigation and hunting so this foundational module on KQL was placed before the Azure Sentinel content in the course.

In module 6 you will connect data sources to Azure Sentinel. The lab for this module involves connecting two Linux VMs to Azure Sentinel. These VMs are not provided by Microsoft but should be available from an authorized lab hoster. Signal from these VMs is not used in later labs.

Whereas the first six modules are mostly about setup, configuration, and building a foundation, modules 7 and 8 are composed of the day-to-day tasks for the SecOps Analyst. The labs for module 7 are longer than usual. During testing it took two to three hours to complete these labs. You might consider having the module 7 labs

span a lunch period to accommodate for the variance students might require completing this lab.

This diagram is included to give you a general sense of how we anticipate the 4-day course to be covered.

	Day 1	Day 2	Day 3	Day 4
AM	Module 1	Module 3	Module 5	Module 7
	Module 1	Module 3	Lab mod 5	Labs mod 7
	Labs	Labs	Module 6	Labs mod 7
PM	Module 2	Module 4	Module 6	Labs mod 7
	Module 2	Module 4	Labs mod 6	Module 8
	Labs	Labs	Module 7	Lab 8

Module Knowledge Check Questions

Knowledge checks are provided at the end of each module. These are multiple choice questions. You can use these review questions in several ways:

- Have the student's pre-test before the lesson starts and then at the end to see what they have learned.
- As a group, review the questions before moving on to another section.
- Sprinkle the questions into the content as you cover the appropriate material.

✔ These questions are not at the level of the certification exam. You may wish to supplement with questions of your own choosing. The applicable Learn modules may also have Check Your Knowledge questions you can use.

References

There are a lot of resources to help you and the student learn about Security Operations. We recommend you bookmark these pages. The list is included in the Welcome section of the student materials.

- Microsoft Learn. Provides searchable learning paths and modules for a variety of roles and levels.
- Microsoft Azure Blog. Keep current on what's happening in Azure, including what's now in preview, generally available, news & updates, and more.
- Azure forums. The Azure forums are very active. You can search the threads for a specific area of interest. You can also browse categories like Azure Storage, Pricing and Billing, Azure Virtual Machines, and Azure Migrate.
- Azure Tuesdays with Corey. Corey Sanders answers your questions about Microsoft Azure - Virtual Machines, Web Sites, Mobile Services, Dev/Test etc.
- Azure Fridays. Join Scott Hanselman as he engages one-on-one with the engineers who build the services that power Microsoft Azure, as they demo capabilities, answer Scott's questions, and share their insights.
- Microsoft Learning Community Blog. Get the latest information about the certification tests and exam study groups.
- Azure Documentation. Stay informed on the latest products, tools, and features. Get information on pricing, partners, support, solutions, and more.

Connect with Others

- MCT Central. Your one stop for all things MCT. Stay up to date with the latest MCT news, learn about upcoming events, find job opportunities, or connect with other MCTs around the world. You can also ask questions and discuss a variety of topics including courseware and certification with Microsoft and other MCTs through the MCT Central Forums.
- MOC Courseware Support. If there are problems with a course or you need to log a support ticket, contact the Official Support channel for MOC courses. This channel is monitored by support agents and is the quickest way to log your course support issue.

Feedback

In this course we have provided a framework for you to work with. Take time to prepare and think about the value that only an instructor can bring to training. We

hope to partner with you to provide an exceptional student experience and we welcome your feedback.

Happy learning!
Microsoft Security Operations Analyst course development team