PROFESSIONAL COURSE OUTLINE

Security Operations Analyst Associate

Microsoft

SC-200

Learn how to investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender XDR and Microsoft Defender for Cloud. In this course you will learn how to mitigate cyberthreats using these technologies. Specifically, you will configure and use Microsoft 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.

Security | Intermediate | Azure

PROGRAM CODE	DELIVERY	DURATION	CERTIFICATION
SC-200	Virtual, On-site, or Hybrid	4 days	Microsoft Certified: Security Operations Analyst Associate

AUDIENCE PROFILE

Who This Program Is For

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 Sentinel, Microsoft Defender XDR, Microsoft Defender for Cloud, 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.

PROGRAM SUMMARY

What This Course Covers

As a candidate for this certification, you're a security operations analyst who reduces organizational risk by performing triage, responding to incidents, hunting for threats, and engineering detections.

TAILORED DELIVERY

Adapt the program around your team.

This outline can be adapted for virtual, on-site, or hybrid delivery, with emphasis adjusted for yourteam's platform priorities, role mix, and implementation goals.

Enterprise-ready delivery format

VNode ITeS can align labs, examples, delivery pace, and assessment checkpoints to the required audience profile while preserving the official program sequence where applicable.

COMPLETE MODULE SEQUENCE

Module Flow and Topic Coverage

The structure below presents the current delivery flow for this program, including the associated topics covered under each module.

1

MODULE 1

Mitigate threats using Microsoft Defender XDR

Mitigate threats using Microsoft Defender XDR

- Introduction to Microsoft Defender XDR threat protection
- Mitigate incidents using Microsoft Defender
- Remediate threats using Microsoft Defender
- Manage Microsoft Entra Identity Protection
- Safeguard your environment with Microsoft Defender for Identity
- Secure your cloud apps and services with Microsoft Defender for Cloud Apps

2

MODULE 2

Mitigate threats using Microsoft Security Copilot

Mitigate threats using Microsoft Security Copilot

- Introduction to generative AI and agents
- Describe Microsoft Security Copilot
- Describe the core features of Microsoft Security Copilot
- Describe the embedded experiences of Microsoft Security Copilot
- Explore use cases of Microsoft Security Copilot

3

MODULE 3

Mitigate threats using Microsoft Purview

Use Microsoft Purview to discover, classify, and protect sensitive data in your organization. This learning path aligns with exam SC-200: Microsoft Security Operations Analyst.

- Investigate and respond to Microsoft Purview Data Loss Prevention alerts
- Investigate insider risk alerts and related activity
- Search and investigate with Microsoft Purview Audit
- Search for content with Microsoft Purview eDiscovery

4

MODULE 4

Mitigate threats using Microsoft Defender for Endpoint

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 with 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
- Configure and manage automation using Microsoft Defender for Endpoint
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Utilize Vulnerability Management in Microsoft Defender for Endpoint

5

MODULE 5

Mitigate threats using Microsoft Defender for Cloud

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 resources to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Explain cloud workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

6

MODULE 6

Create queries for Microsoft Sentinel using Kusto Query Language (KQL)

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 data in Microsoft Sentinel using Kusto Query Language

7

MODULE 7

Configure your Microsoft Sentinel environment

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
- Integrate Microsoft Defender XDR with Microsoft Sentinel

8

MODULE 8

Connect logs to Microsoft Sentinel

Connect logs to 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

MODULE 9

Create detections and perform investigations using Microsoft Sentinel

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
- Identify threats with Behavioral Analytics
- Data normalization in Microsoft Sentinel
- Query, visualize, and monitor data in Microsoft Sentinel
- Manage content in Microsoft Sentinel

10

MODULE 10

Perform threat hunting in Microsoft Sentinel

Perform threat hunting in Microsoft Sentinel

- Explain threat hunting concepts in Microsoft Sentinel
- Threat hunting with Microsoft Sentinel
- Use Search jobs in Microsoft Sentinel
- Hunt for threats using notebooks in Microsoft Sentinel