Course Title: SC-200T00-A Microsoft Security Operations Analyst [Cloud Slice Provided]	**Course Duration**: 4.0 Days
Exam: Not Included	**Exam Type**: Proctored Exam
Qualification: SC-200 Completion Certificate	

Course Syllabus

1 - Introduction to Microsoft 365 threat protection

- Explore Extended Detection & Response (XDR) response use cases
- Understand Microsoft Defender XDR in a Security Operations Center (SOC)
- Explore Microsoft Security Graph
- Investigate security incidents in Microsoft Defender XDR

2 - Mitigate incidents using Microsoft 365 Defender

- Use the Microsoft Defender portal
- Manage incidents
- Investigate incidents
- Manage and investigate alerts
- Manage automated investigations
- Use the action center
- Explore advanced hunting
- Investigate Microsoft Entra sign-in logs
- Understand Microsoft Secure Score
- Analyze threat analytics
- Analyze reports
- Configure the Microsoft Defender portal

3 - Protect your identities with Microsoft Entra ID Protection

- Microsoft Entra ID Protection overview
- Detect risks with Microsoft Entra ID Protection policies
- Investigate and remediate risks detected by Microsoft Entra ID Protection

4 - Remediate risks with Microsoft Defender for Office 365

- Automate, investigate, and remediate
- Configure, protect, and detect
- Simulate attacks

5 - Safeguard your environment with Microsoft Defender for Identity

- Configure Microsoft Defender for Identity sensors
- Review compromised accounts or data

- Integrate with other Microsoft tools

6 - Secure your cloud apps and services with Microsoft Defender for Cloud Apps

- Understand the Defender for Cloud Apps Framework
- Explore your cloud apps with Cloud Discovery
- Protect your data and apps with Conditional Access App Control
- Walk through discovery and access control with Microsoft Defender for Cloud Apps
- Classify and protect sensitive information
- Detect Threats

7 - Respond to data loss prevention alerts using Microsoft 365

- Describe data loss prevention alerts
- Investigate data loss prevention alerts in Microsoft Purview
- Investigate data loss prevention alerts in Microsoft Defender for Cloud Apps

8 - Manage insider risk in Microsoft Purview

- Insider risk management overview
- Create and manage insider risk policies
- Investigate insider risk alerts
- Take action on insider risk alerts through cases
- Manage insider risk management forensic evidence
- Create insider risk management notice templates

9 - Investigate threats by using audit features in Microsoft Defender XDR and Microsoft Purview Standard

- Explore Microsoft Purview Audit solutions
- Implement Microsoft Purview Audit (Standard)
- Start recording activity in the Unified Audit Log
- Search the Unified Audit Log (UAL)
- Export, configure, and view audit log records
- Use audit log searching to investigate common support issues

10 - Investigate threats using audit in Microsoft Defender XDR and Microsoft Purview (Premium)

- Explore Microsoft Purview Audit (Premium)
- Implement Microsoft Purview Audit (Premium)
- Manage audit log retention policies
- Investigate compromised email accounts using Purview Audit (Premium)

11 - Investigate threats with Content search in Microsoft Purview

- Explore Microsoft Purview eDiscovery solutions
- Create a content search
- View the search results and statistics
- Export the search results and search report
- Configure search permissions filtering
- Search for and delete email messages

12 - Protect against threats with Microsoft Defender for Endpoint

- Practice security administration

- Hunt threats within your network

13 - Deploy the Microsoft Defender for Endpoint environment

- Create your environment
- Understand operating systems compatibility and features
- Onboard devices
- Manage access
- Create and manage roles for role-based access control
- Configure device groups
- Configure environment advanced features

14 - Implement Windows security enhancements with Microsoft Defender for Endpoint

- Understand attack surface reduction
- Enable attack surface reduction rules

15 - Perform device investigations in Microsoft Defender for Endpoint

- Use the device inventory list
- Investigate the device
- Use behavioral blocking
- Detect devices with device discovery

16 - Perform actions on a device using Microsoft Defender for Endpoint

- Explain device actions
- Run Microsoft Defender antivirus scan on devices
- Collect investigation package from devices
- Initiate live response session

17 - Perform evidence and entities investigations using Microsoft Defender for Endpoint

- Investigate a file
- Investigate a user account
- Investigate an IP address
- Investigate a domain

18 - Configure and manage automation using Microsoft Defender for Endpoint

- Configure advanced features
- Manage automation upload and folder settings
- Configure automated investigation and remediation capabilities
- Block at risk devices

19 - Configure for alerts and detections in Microsoft Defender for Endpoint

- Configure advanced features
- Configure alert notifications
- Manage alert suppression
- Manage indicators

20 - Utilize Vulnerability Management in Microsoft Defender for Endpoint

- Understand vulnerability management

- Explore vulnerabilities on your devices
- Manage remediation

21 - Plan for cloud workload protections using Microsoft Defender for Cloud

- Explain Microsoft Defender for Cloud
- Describe Microsoft Defender for Cloud workload protections
- Enable Microsoft Defender for Cloud

22 - Connect Azure assets to Microsoft Defender for Cloud

- Explore and manage your resources with asset inventory
- Configure auto provisioning
- Manual log analytics agent provisioning

23 - Connect non-Azure resources to Microsoft Defender for Cloud

- Protect non-Azure resources
- Connect non-Azure machines
- Connect your AWS accounts
- Connect your GCP accounts

24 - Manage your cloud security posture management

- Explore Secure Score
- Explore Recommendations
- Measure and enforce regulatory compliance
- Understand Workbooks

25 - Explain cloud workload protections in Microsoft Defender for Cloud

- Understand Microsoft Defender for servers
- Understand Microsoft Defender for App Service
- Understand Microsoft Defender for Storage
- Understand Microsoft Defender for SQL
- Understand Microsoft Defender for open-source databases
- Understand Microsoft Defender for Key Vault
- Understand Microsoft Defender for Resource Manager
- Understand Microsoft Defender for DNS
- Understand Microsoft Defender for Containers
- Understand Microsoft Defender additional protections

26 - Remediate security alerts using Microsoft Defender for Cloud

- Understand security alerts
- Remediate alerts and automate responses
- Suppress alerts from Defender for Cloud
- Generate threat intelligence reports
- Respond to alerts from Azure resources

27 - Construct KQL statements for Microsoft Sentinel

- Understand the Kusto Query Language statement structure
- Use the search operator

- Use the where operator
- Use the let statement
- Use the extend operator
- Use the order by operator
- Use the project operators

28 - Analyze query results using KQL

- Use the summarize operator
- Use the summarize operator to filter results
- Use the summarize operator to prepare data
- Use the render operator to create visualizations

29 - Build multi-table statements using KQL

- Use the union operator
- Use the join operator

30 - Work with data in Microsoft Sentinel using Kusto Query Language

- Extract data from unstructured string fields
- Extract data from structured string data
- Integrate external data
- Create parsers with functions

31 - Introduction to Microsoft Sentinel

- What is Microsoft Sentinel
- How Microsoft Sentinel works
- When to use Microsoft Sentinel

32 - Create and manage Microsoft Sentinel workspaces

- Plan for the Microsoft Sentinel workspace
- Create a Microsoft Sentinel workspace
- Manage workspaces across tenants using Azure Lighthouse
- Understand Microsoft Sentinel permissions and roles
- Manage Microsoft Sentinel settings
- Configure logs

33 - Query logs in Microsoft Sentinel

- Query logs in the logs page
- Understand Microsoft Sentinel tables
- Understand common tables
- Understand Microsoft Defender XDR tables

34 - Use watchlists in Microsoft Sentinel

- Plan for watchlists
- Create a watchlist
- Manage watchlists

35 - Utilize threat intelligence in Microsoft Sentinel

- Define threat intelligence
- Manage your threat indicators
- View your threat indicators with KQL

36 - Connect data to Microsoft Sentinel using data connectors

- Ingest log data with data connectors
- Understand data connector providers
- View connected hosts

37 - Connect Microsoft services to Microsoft Sentinel

- Plan for Microsoft services connectors
- Connect the Microsoft Office 365 connector
- Connect the Microsoft Entra connector
- Connect the Microsoft Entra ID Protection connector
- Connect the Azure Activity connector

38 - Connect Microsoft Defender XDR to Microsoft Sentinel

- Plan for Microsoft Defender XDR connectors
- Connect the Microsoft Defender XDR connector
- Connect Microsoft Defender for Cloud connector
- Connect Microsoft Defender for IoT
- Connect Microsoft Defender legacy connectors

39 - Connect Windows hosts to Microsoft Sentinel

- Plan for Windows hosts security events connector
- Connect using the Windows Security Events via AMA Connector
- Connect using the Security Events via Legacy Agent Connector
- Collect Sysmon event logs

40 - Connect Common Event Format logs to Microsoft Sentinel

- Plan for Common Event Format connector
- Connect your external solution using the Common Event Format connector

41 - Connect syslog data sources to Microsoft Sentinel

- Plan for syslog data collection
- Collect data from Linux-based sources using syslog
- Configure the Data Collection Rule for Syslog Data Sources
- Parse syslog data with KQL

42 - Connect threat indicators to Microsoft Sentinel

- Plan for threat intelligence connectors
- Connect the threat intelligence TAXII connector
- Connect the threat intelligence platforms connector
- View your threat indicators with KQL

43 - Threat detection with Microsoft Sentinel analytics

- What is Microsoft Sentinel Analytics

- Types of analytics rules
- Create an analytics rule from templates
- Create an analytics rule from wizard
- Manage analytics rules

44 - Automation in Microsoft Sentinel

- Understand automation options
- Create automation rules

45 - Threat response with Microsoft Sentinel playbooks

- What are Microsoft Sentinel playbooks
- Trigger a playbook in real-time
- Run playbooks on demand

46 - Security incident management in Microsoft Sentinel

- Understand incidents
- Incident evidence and entities
- Incident management

47 - Identify threats with Behavioral Analytics

- Understand behavioral analytics
- Explore entities
- Display entity behavior information
- Use Anomaly detection analytical rule templates

48 - Data normalization in Microsoft Sentinel

- Understand data normalization
- Use ASIM Parsers
- Understand parameterized KQL functions
- Create an ASIM Parser
- Configure Azure Monitor Data Collection Rules

49 - Query, visualize, and monitor data in Microsoft Sentinel

- Monitor and visualize data
- Query data using Kusto Query Language
- Use default Microsoft Sentinel Workbooks
- Create a new Microsoft Sentinel Workbook

50 - Manage content in Microsoft Sentinel

- Use solutions from the content hub
- Use repositories for deployment

51 - Explain threat hunting concepts in Microsoft Sentinel

- Understand cybersecurity threat hunts
- Develop a hypothesis
- Explore MITRE ATT&CK

52 - Threat hunting with Microsoft Sentinel

- Explore creation and management of threat-hunting queries
- Save key findings with bookmarks
- Observe threats over time with livestream

53 - Use Search jobs in Microsoft Sentinel

- Hunt with a Search Job
- Restore historical data

54 - Hunt for threats using notebooks in Microsoft Sentinel

- Access Azure Sentinel data with external tools
- Hunt with notebooks
- Create a notebook
- Explore notebook code

Course Overview

This course equips IT security professionals to detect, investigate, and respond to threats using Microsoft security tools. It covers Microsoft 365 Defender, Azure Defender, Azure Sentinel, threat intelligence, and incident response processes. Cloud Slice labs provide hands-on experience simulating real-world security operations and incident handling.

Course Learning Outcomes

By the end of this course, learners will be able to configure and manage security solutions in Microsoft 365 and Azure environments, monitor security alerts, investigate potential threats, respond to incidents, implement automation and orchestration in security operations, analyze threat intelligence data, and apply best practices for ongoing security monitoring and compliance. Learners gain the skills to operate as a security operations analyst in enterprise Microsoft environments.

Audience

Security analysts, SOC team members, IT professionals responsible for threat detection and response, and anyone preparing for the SC-200 certification

Entry-Level Requirements

Understanding of Microsoft 365 and Azure fundamentals recommended (SC-900 level), knowledge of security concepts and networking beneficial

Recommended Reading

Microsoft Learn SC-200 learning path, Microsoft 365 Defender and Azure Sentinel documentation, Exam Ref SC-200 Security Operations Analyst

What's Included

Instructor-led training, hands-on labs, course materials, exam preparation guide

Exam Information

This course prepares learners for the SC-200: Microsoft Security Operations Analyst certification exam. The exam measures the ability to monitor, detect, investigate, and respond to security threats using Microsoft security tools. It includes scenario-based, multiple-choice, and case-study questions reflecting real-world SOC operations. Successful candidates earn the Microsoft Certified: Security Operations Analyst Associate credential.

What's Next

After completing SC-200, learners can progress to SC-300 (Identity and Access Administrator), SC-400 (Information Protection Administrator), or advanced Azure security roles such as AZ-500 (Azure Security Engineer).

Additional Information

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.