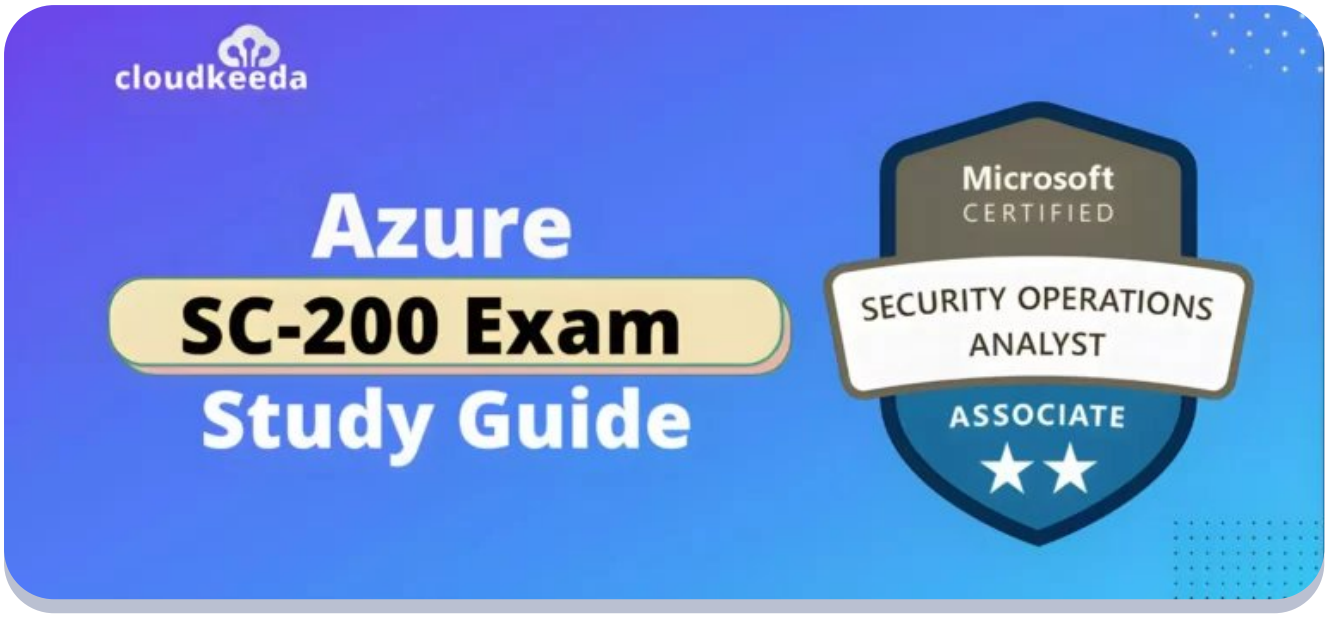


SC-200: Microsoft Azure Security Operations Analyst Exam Study Guide

March 12, 2023 by manish

☆ ☆ ☆ ☆ ☆ Rate this post

The Microsoft SC-200 certification validates a candidate's knowledge and skills in operations security.

These certifications are suitable for cloud administrators, IT professionals, security administrators, Microsoft security administrators, and network administrators who ensure the security of their organization's information technology systems.

Using various security solutions, Microsoft Security Operations Analysts monitor and respond to threats, identify and resolve active attacks, and advise

on threat protection practices.

Obtaining the SC-200 certification can lead to career advancement opportunities, increased earnings, and a deeper understanding of operations security.

SC-200 is a valuable credential for IT professionals who want to demonstrate their expertise in Microsoft operations security.

Table of Contents

SC-200 Certification Overview

The SC-200 is an associate-level certification that covers operations security. Once you pass this Microsoft exam, you'll get the Microsoft Certified Security Operations Analyst Associate certification.

Microsoft Security Operations Analyst (SC-200) tests your ability to defend against threats using Microsoft 365 Defender, Azure Defender, and Azure

Sentinel.

A Microsoft Security Operations Analyst protects the company's IT infrastructure with business partners. They are responsible for ensuring that the organization's information security is maintained.

Are you new to Azure Cloud? Do check out our blog post on the Microsoft Azure Certification Path 2023 and choose the best certification for you.

Who Is Microsoft Security Operations Analyst?

Microsoft security operations analysts collaborate with organizational stakeholders to ensure the security of information technology systems.

As part of their responsibility, they rapidly resolve active attacks and advise on the improvement of threat protection practices. And refer violations of organizational policies to relevant stakeholders.

They use a variety of security solutions across their environment to manage threats, monitor and respond.

In this role, they investigate, respond to, and hunt for threats using Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender, and third-party security products.

Who Is This Certification For?

The certification is for:

- Cloud Administrator
- IT Professional
- IT Security Professional
- Microsoft Security Administrators
- Network Administrators

Why SC-200 Certification

There are many benefits to earning Microsoft certifications, which is why their popularity has grown dramatically recently:

- With this certification, threats are managed, tracked, and responded to within their environment.
- This certification gives an in-depth understanding of operations security.
- The SC-200 certification improves your understanding of Microsoft Azure Sentinel and Azure Defender.
- This credential validates your security knowledge.
- Additionally, it shows a commitment to lifelong learning.
- Your career will advance and your salary will rise.
- For organizations searching for operations security, it adds value.
- You will gain an understanding of Microsoft 365 Defender, Azure Defender, and Azure Sentinel.
- It opens doors since security is a top priority in business.
- In the job market, it keeps you ahead of the competition.

Microsoft Security Operations Analyst Responsibilities

- Microsoft Security Operations Analysts are responsible for delivering secure information technology systems to an organization. It is important that they work with organizational stakeholders to accomplish this goal.

- They identify violations of organizational policies and, by reporting them, decrease risk by promptly identifying and correcting active attacks in the environment.

- Providing advice on how to enhance threat protection activities is one of their responsibilities.

- Microsoft Security Operations Analysts are also responsible for monitoring, threat management, and response by utilizing various security solutions.

- They conduct threat hunting with Microsoft 365 Defender, Azure Security Centre, Azure Defender, Azure Sentinel, and third-party products.

Check Out: Top 10 Microsoft Azure Security Best Practices

SC-200 Exam Details

Exam Name SC-200: Microsoft Security Operations Analyst	**Passing Marks** 700
Exam Fee $165	**Exam Duration** 120 Minutes
Exam Validity 1 Year	**Exam Languages** English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Chinese (Traditional), Italian

Total Questions	Exam Type
40-60 Questions	Multiple-choice and Multiple response questions

SC-200 Exam Skills Measured

Mitigate threats using Microsoft 365 Defender	**25-30%**
Mitigate threats using Microsoft Defender for Cloud	**20-25%**
Mitigate threats using Microsoft Sentinel	**50-55%**

How to Register for SC 200 Certification Exam

You can register for the Microsoft Certified Cybersecurity Architect Expert Exam (SC-100) by going to the Official Microsoft Page.

Prerequisite for SC-200 Certification

SC-200 certification prerequisites include:

- The basics of Microsoft 365 Defender
- Understanding of Microsoft security, compliance, and identification

products.

- A working understanding of Windows 10/11
- Understanding of Azure services, including Azure SQL
- The ability to create, deploy and manage virtual machines on Azure.
- Knowledge of scripting concepts.

SC-200 Study Guide

Mitigate threats using Microsoft 365 Defender (25–30%)

Mitigate threats to the productivity environment by using Microsoft 365 Defender

- Investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive
  - Threat Explorer and Real-time detections
  - Threat investigation and response
  - Microsoft uses threat intelligence to protect, detect, and respond to threats
  - Remediate malicious email delivered in Office 365
- Investigate, respond, and remediate threats to email by using Microsoft Defender for Office 365
  - Threat Explorer and Real-time detections
  - How automated investigation and response works in Microsoft Defender for Office 365
  - Automated investigation and response (AIR) in Microsoft Defender for Office 365
  - Remediation actions in Microsoft Defender for Office 365
- Investigate and respond to alerts generated from Data Loss Prevention policies
  - Configure and view alerts for data loss prevention polices
- Investigate and respond to alerts generated from insider risk policies
  - Get started with insider risk management

- Identify, investigate, and remediate security risks by using Microsoft Defender for Cloud Apps
  - Investigate cloud app risks and suspicious activity
- Configure Microsoft Defender for Cloud Apps to generate alerts and reports to detect threats
  - Manage alerts

Mitigate endpoint threats by using Microsoft Defender for Endpoint

- Manage data retention, alert notification, and advanced features
  - Data Retention
    - What is Microsoft's data retention policy?
    - Configure general Defender for Endpoint settings
  - Alert notifications
    - Manage Microsoft Defender for Endpoint alerts
  - Advanced features
    - Configure advanced features in Defender for Endpoint
- Recommend security baselines for devices
  - Security baselines
- Respond to incidents and alerts
  - Incident response with Microsoft 365 Defender
- Manage automated investigations and remediations
  - Overview of automated investigations
  - Configure automated investigation and remediation capabilities in Microsoft Defender for Endpoint
- Assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution
  - Microsoft's Threat & Vulnerability Management
  - What is Microsoft Defender Vulnerability Management
  - Remediate vulnerabilities
- Manage endpoint threat indicators
  - Create indicators

- Manage indicators

Mitigate identity threats

- Identify and remediate security risks related to events for Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
  - Remediate risks and unblock users
- Identify and remediate security risks related to Azure AD Identity Protection events
  - Configure Conditional Access in Microsoft Defender for Endpoint
- Identify and remediate security risks related to Azure AD Conditional Access events
  - Configure Conditional Access in Microsoft Defender for Endpoint
- Identify and remediate security risks related to Active Directory Domain Services using Microsoft Defender for Identity
  - Investigate a domain
  - Microsoft Defender for Identity frequently asked questions

Manage extended detection and response (XDR) in Microsoft 365 Defender

- Manage incidents across Microsoft 365 Defender products
  - Manage incidents in Microsoft 365 Defender
- Manage investigation and remediation actions in the Action Center
  - View and manage actions in the Action center
- Perform threat hunting
  - Proactively hunt for threats with advanced hunting in Microsoft 365 Defender
- Identify and remediate security risks using Microsoft Secure Score
  - Security posture for Microsoft Defender for Cloud
  - Microsoft Secure Score
- Analyze threat analytics
  - Threat analytics in Microsoft 365 Defender

- Configure and manage custom detections and alerts
  - Create and manage custom detections rules

Mitigate threats using Microsoft Defender for Cloud (20–25%)

Implement and maintain cloud security posture management and workload protection

- Plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspaces
  - Enable enhanced security features
- Configure Microsoft Defender for Cloud roles
  - User roles and permissions
- Assess and recommend cloud workload protection
  - What is Microsoft Defender for Cloud?
- Identify and remediate security risks using the Microsoft Defender for Cloud Secure Score
  - Remediate security risks in Microsoft Defender for Cloud
  - Security posture for Microsoft Defender for Cloud
  - Microsoft Secure Score
- Manage policies for regulatory compliance
  - What is Azure Policy?
  - Get compliance data of Azure resources
- Review and remediate security recommendations
  - Implement security recommendations in Microsoft Defender for Cloud

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Defender for Cloud

- Identify data sources to be ingested for Microsoft Defender for Cloud
  - Microsoft Sentinel data connectors
- Configure automated onboarding for Azure resources

    - Automate onboarding
    - Automate onboarding of Microsoft Defender for Cloud using PowerShell
- Connect multi-cloud and on-premises resources
    - Azure Arc overview
- Configure data collections
    - How does Defender for Cloud collect data?

Configure and respond to alerts and incidents in Microsoft Defender for Cloud

- Validate alert configuration
    - Validating Microsoft Defender for DNS Alerts
    - Alert validation in Microsoft Defender for Cloud
- Set up email notifications
    - Configure email notifications for security alerts
- Create and manage alert suppression rules
    - Suppress alerts from Microsoft Defender for Cloud
    - Manage suppression rules
- Design and configure workflow automation in Microsoft Defender for Cloud
    - Automate responses to Microsoft Defender for Cloud triggers
- Remediate alerts and incidents by using Microsoft Defender for Cloud recommendations
    - Security alerts and incidents
- Manage security alerts and incidents
    - Manage and respond to security alerts in Microsoft Defender for Cloud
- Analyze Microsoft Defender for Cloud threat intelligence reports
    - Microsoft Defender for Cloud threat intelligence report
- Manage user data discovered during an investigation
    - How Azure Security Center helps analyze attacks using Investigation and Log Search

Mitigate threats using Microsoft Sentinel (50–55%)

Design and configure a Microsoft Sentinel workspace

- Plan a Microsoft Sentinel workspace
  - Create and manage Microsoft Sentinel workspaces
- Configure Microsoft Sentinel roles
  - Roles and permissions in Microsoft Sentinel
- Design and configure Microsoft Sentinel data storage
  - Design your Microsoft Sentinel workspace architecture
- Implement and use Content hub, repositories, and community resources
  - Community hub and GitHub

Plan and implement the use of data connectors for ingestion of data sources in Microsoft Sentine

- Identify data sources to be ingested for Microsoft Sentinel
  - Microsoft Sentinel data connectors
- Identify the prerequisites for a Microsoft Sentinel data connector
  - Microsoft Sentinel data connectors
- Configure and use Microsoft Sentinel data connectors
  - Microsoft Sentinel data connectors
- Configure Microsoft Sentinel data connectors by using Azure Policy
- Configure Microsoft Sentinel connectors for Microsoft 365 Defender and Microsoft Defender for Cloud
  - Connect data from Microsoft 365 Defender to Microsoft Sentinel
- Design and configure Syslog and CEF event collections
  - Collect data from Linux-based sources using Syslog
  - Get CEF-formatted logs from your device or appliance into Microsoft Sentinel
  - Best Practices for Common Event Format (CEF) collection in Azure Sentinel

- Design and configure Windows Security event collections
  - Windows Security Events via AMA
- Configure custom threat intelligence connectors
  - Connect your threat intelligence platform to Microsoft Sentinel

Manage Microsoft Sentinel analytics rules

- Design and configure analytics rules
  - Define the rule query logic and configure settings
- Activate Microsoft security analytics rules
  - Using Microsoft Security incident creation analytics rules
- Configure built-in scheduled queries
  - Detect threats out-of-the-box
- Configure custom scheduled queries
  - Create a custom analytics rule with a scheduled query
- Define incident creation logic
  - Configure the incident creation settings
- Manage and use watchlists
  - Use watchlists in Microsoft Sentinel
- Manage and use threat indicators
  - Create indicators
  - Manage indicators

Perform data classification and normalization

- Classify and analyze data by using entities
  - Classify and analyze data using entities in Microsoft Sentinel
- Create custom logs in Azure Log Analytics to store custom data
  - Collect text logs with the Log Analytics agent in Azure Monitor
- Query Microsoft Sentinel data by using Advanced SIEM Information Model (ASIM) parsers
  - Using the Advanced Security Information Model (ASIM) (Public preview)

- Develop and manage ASIM parsers
  - Using the Advanced Security Information Model (ASIM) (Public preview)

Configure Security Orchestration, Automation, and Response (SOAR) in Microsoft Sentinel

- Configure automation rules
  - Create and use Microsoft Sentinel automation rules to manage response
- Create and configure Microsoft Sentinel playbooks
  - Automate threat response with playbooks in Microsoft Sentinel
  - Create and use Microsoft Sentinel automation rules to manage response
- Configure alerts and incidents to trigger automation
  - Use playbooks with automation rules in Microsoft Sentinel
- Use automation to remediate threats
  - Configure automated investigation and remediation capabilities in Microsoft Defender for Endpoint
- Use automation to manage incidents
  - Configure automated investigation and response capabilities in Microsoft 365 Defender

Manage Microsoft Sentinel incidents

- Triage incidents in Microsoft Sentinel
  - Triage security alerts
- Investigate incidents in Microsoft Sentinel
  - Investigate incidents with Microsoft Sentinel
- Respond to incidents in Microsoft Sentinel
  - Investigate incidents with Microsoft Sentinel
- Investigate multi-workspace incidents
  - Work with incidents in many workspaces at once

- Identify advanced threats with User and Entity Behavior Analytics (UEBA)
  - Identify advanced threats with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel

Use Microsoft Sentinel workbooks to analyze and interpret data

- Activate and customize Microsoft Sentinel workbook templates
  - Use Azure Monitor workbooks to visualize and monitor your data
- Create custom workbooks
  - Create new workbooks
- Configure advanced visualizations
  - Query and visualize data with Microsoft Sentinel Workbooks
- View and analyze Microsoft Sentinel data using workbooks
  - Use Azure Monitor workbooks to visualize and monitor your data
- Track incident metrics using the security operations efficiency workbook
  - Manage your SOC better with incident metrics

Hunt for threats using Microsoft Sentinel

- Create custom hunting queries
  - Create custom queries to refine threat hunting
- Run hunting queries manually
  - Hunt for threats by using Microsoft Sentinel
- Monitor hunting queries by using Livestream
  - Manage hunting and livestream queries in Microsoft Sentinel using REST API
- Configure and use MSTICPy in notebooks
  - Get started with Jupyter notebooks and MSTICPy in Microsoft Sentinel
- Perform hunting by using notebooks
  - Use Jupyter notebooks to hunt for security threats

- Track query results with bookmarks
  - Add a bookmark
- Use hunting bookmarks for data investigations
  - Exploring bookmarks in the investigation graph
- Convert a hunting query to an analytical rule
  - Threat hunting vs Analytics rule?

SC-200 Exam Retake Policy

- If the candidate does not achieve the passing score, he/she must wait 24 hours before reapplying.
- A candidate can reschedule their exam from their certificate dashboard.
- A candidate can reappear for the examination only five times.
- A candidate will have another chance after 14 days if it fails the second time.
- The fourth and fifth attempts will also require 14 days of waiting.

Conclusion

Microsoft SC-200 certification is a valuable credential for security administrators, network administrators, and IT professionals. This certification validates your security knowledge and helps you better understand Microsoft 365 Defender, Azure Defender, and Azure Sentinel.

Earning the SC-200 certification can help you advance your career, earn more money, and demonstrate your commitment to learning.

In addition to monitoring, managing, and responding to threats using a variety of security tools, Microsoft Security Operations Analysts play an essential role in the security of their organization's IT infrastructure.

Adding value to operations security with SC-200 certification will keep you

ahead of the competition in the job market.

FAQs

Q1. Who should take SC-200?

Cloud administrators, IT Professionals, IT Security Professionals, Microsoft Security Administrators, and Network Administrators should take SC-200.

Q2. How long is SC 200 valid?

SC- 200 certifications will remain valid for two years.

Q3. How many questions are on the SC 200 exam?

The Microsoft SC-200 exam has 40-60 questions. Questions include mark reviews, multiple-choice, build lists, case studies, and more.

Q4. Is it easy to pass SC-200?

You may not pass the SC-200 certification exam if you only prepare half-heartedly. Preparing for the SC-200 begins with a commitment to study.

Related Articles

- SC-100: Microsoft Certified Cybersecurity Architect Expert Exam Study Guide
- AZ-220: Microsoft Azure IoT Developer Exam Study Guide
- AZ-140: Microsoft Azure Virtual Desktop Specialty Exam Study Guide
- AI-102: Microsoft Azure AI Engineer Associate Exam Study Guide
- AZ-305: Microsoft Azure Solutions Architect Expert Exam Study Guide
- AZ-400: Microsoft Azure DevOps Engineer Expert Exam Study Guide

Leave a Comment

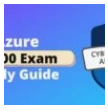
Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Post Comment

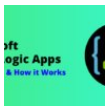
Recent Posts



SC-100: Microsoft Azure Certified Cybersecurity Architect Expert Exam Study Guide

Microsoft Azure Certification Path in 2023 | Azure Certification Roadmap for Beginners

Azure Storage Explorer: Download, Install, and Setup Overview



What are Azure Logic Apps: Components, Advantages and How it Works

Microsoft Azure Application Insights: A Complete Beginners Guide