EDUSUM

#1 Online Certification Guide

# MICROSOFT SC-200

**Microsoft Security Operations Analyst Certification Questions & Answers**

Exam Summary – Syllabus –Questions

**SC-200**

**Microsoft Certified - Security Operations Analyst Associate**

**40-60 Questions Exam – 700 / 1000 Cut Score – Duration of 120 minutes**

# Table of Contents:

# Know Your SC-200 Certification Well:

The SC-200 is best suitable for candidates who want to gain knowledge in the Microsoft Security Compliance and Identity. Before you start your SC-200 preparation you may struggle to get all the crucial Security Operations Analyst materials like SC-200 syllabus, sample questions, study guide.

But don't worry the SC-200 PDF is here to help you prepare in a stress free manner.
The PDF is a combination of all your queries like-

- What is in the SC-200 syllabus?
- How many questions are there in the SC-200 exam?
- Which Practice test would help me to pass the SC-200 exam at the first attempt?

Passing the SC-200 exam makes you Microsoft Certified - Security Operations Analyst Associate. Having the Security Operations Analyst certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

# Microsoft SC-200 Security Operations Analyst Certification Details:

| | |
|---|---|
| Exam Name | Microsoft Certified - Security Operations Analyst Associate |
| Exam Code | SC-200 |
| Exam Price | $165 (USD) |
| Duration | 120 mins |
| Number of Questions | 40-60 |
| Passing Score | 700 / 1000 |
| Books / Training | **Course SC-200T00: Microsoft Security Operations Analyst** |
| Schedule Exam | **Pearson VUE** |
| Sample Questions | **Microsoft Security Operations Analyst Sample Questions** |
| Practice Exam | **Microsoft SC-200 Certification Practice Exam** |

# SC-200 Syllabus:

| Topic | Details |
|---|---|
| **Mitigate threats using Microsoft 365 Defender (25-30%)** | |
| Detect, investigate, respond, and remediate threats to the productivity environment by using Microsoft Defender for Office 365 | - detect, investigate, respond, and remediate threats to Microsoft Teams, SharePoint, and OneDrive<br>- detect, investigate, respond, remediate threats to email by using Defender for Office 365<br>- manage data loss prevention policy alerts<br>- assess and recommend sensitivity labels<br>- assess and recommend insider risk policies |
| Detect, investigate, respond, and remediate endpoint threats by using Microsoft Defender for Endpoint | - manage data retention, alert notification, and advanced features<br>- configure device attack surface reduction rules<br>- configure and manage custom detections and alerts<br>- respond to incidents and alerts<br>- manage automated investigations and remediations<br>- assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution.<br>- manage Microsoft Defender for Endpoint threat indicators<br>- analyze Microsoft Defender for Endpoint threat analytics |
| Detect, investigate, respond, and remediate identity threats | - identify and remediate security risks related to sign-in risk policies<br>- identify and remediate security risks related to Conditional Access events<br>- identify and remediate security risks related to Azure Active Directory<br>- identify and remediate security risks using Secure Score<br>- identify, investigate, and remediate security risks related to privileged identities<br>- configure detection alerts in Azure AD Identity Protection<br>- identify and remediate security risks related to Active |

| Topic | Details |
|---|---|
| | Directory Domain Services using Microsoft Defender for Identity |
| Detect, investigate, respond, and remediate application threats | - identify, investigate, and remediate security risks by using Microsoft Cloud Application Security (MCAS)<br>- configure MCAS to generate alerts and reports to detect threats |
| Manage cross-domain investigations in Microsoft 365 Defender portal | - manage incidents across Microsoft 365 Defender products<br>- manage actions pending approval across products<br>- perform advanced threat hunting |
| **Mitigate threats using Microsoft Defender for Cloud (25-30%)** | |
| Design and configure a Microsoft Defender for Cloud implementation | - plan and configure Microsoft Defender for Cloud settings, including selecting target subscriptions and workspace<br>- configure Microsoft Defender for Cloud roles<br>- configure data retention policies<br>- assess and recommend cloud workload protection |
| 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<br>- configure automated onboarding for Azure resources<br>- connect on-premises computers<br>- connect AWS cloud resources<br>- connect GCP cloud resources<br>- configure data collection |
| Manage Microsoft Defender for Cloud alert rules | - validate alert configuration<br>- setup email notifications<br>- create and manage alert suppression rules |
| Configure automation and remediation | - configure automated responses in Microsoft Defender for Cloud<br>- design and configure workflow automation in Microsoft Defender for Cloud<br>- remediate incidents by using Microsoft Defender for Cloud recommendations |

| Topic | Details |
|---|---|
| | - create an automatic response using an Azure Resource Manager template |
| Investigate Microsoft Defender for Cloud alerts and incidents | - describe alert types for Azure workloads<br>- manage security alerts<br>- manage security incidents<br>- analyze Microsoft Defender for Cloud threat intelligence<br>- respond to Microsoft Defender Cloud for Key Vault alerts<br>- manage user data discovered during an investigation |
| **Mitigate threats using Microsoft Sentinel (40-45%)** | |
| Design and configure a Microsoft Sentinel workspace | - plan a Microsoft Sentinel workspace<br>- configure Microsoft Sentinel roles<br>- design Microsoft Sentinel data storage<br>- configure security settings and access for Microsoft Sentinel |
| Plan and Implement the use of data connectors for ingestion of data sources in Microsoft Sentinel | - identify data sources to be ingested for Microsoft Sentinel<br>- identify the prerequisites for a data connector<br>- configure and use Microsoft Sentinel data connectors<br>- configure data connectors by using Azure Policy<br>- design and configure Syslog and CEF event collections<br>- design and Configure Windows Security events collections<br>- configure custom threat intelligence connectors<br>- create custom logs in Azure Log Analytics to store custom data |
| Manage Microsoft Sentinel analytics rules | - design and configure analytics rules<br>- create custom analytics rules to detect threats<br>- activate Microsoft security analytics rules<br>- configure connector provided scheduled queries<br>- configure custom scheduled queries<br>- define incident creation logic |
| Configure Security Orchestration Automation and Response (SOAR) in Microsoft Sentinel | - create Microsoft Sentinel playbooks<br>- configure rules and incidents to trigger playbooks<br>- use playbooks to remediate threats<br>- use playbooks to manage incidents<br>- use playbooks across Microsoft Defender solutions |

| Topic | Details |
|---|---|
| Manage Microsoft Sentinel Incidents | - investigate incidents in Microsoft Sentinel<br>- triage incidents in Microsoft Sentinel<br>- respond to incidents in Microsoft Sentinel<br>- investigate multi-workspace incidents<br>- identify advanced threats with User and Entity Behavior Analytics (UEBA) |
| Use Microsoft Sentinel workbooks to analyze and interpret data | - activate and customize Microsoft Sentinel workbook templates<br>- create custom workbooks<br>- configure advanced visualizations<br>- view and analyze Microsoft Sentinel data using workbooks<br>- track incident metrics using the security operations efficiency workbook |
| Hunt for threats using Microsoft Sentinel | - create custom hunting queries<br>- run hunting queries manually<br>- monitor hunting queries by using Livestream<br>- perform advanced hunting with notebooks<br>- track query results with bookmarks<br>- use hunting bookmarks for data investigations<br>- convert a hunting query to an analytical |

# Microsoft SC-200 Sample Questions:

Question: 1

Your company has a single office in Istanbul and a Microsoft 365 subscription. The company plans to use conditional access policies to enforce multi-factor authentication (MFA). You need to enforce MFA for all users who work remotely.

What should you include in the solution?

a) a fraud alert
b) a user risk policy
c) a sign-in user policy
d) a named location

**Answer: d**

Question: 2

You are responsible for responding to Azure Defender for Key Vault alerts. During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node. What should you configure to mitigate the threat?

a) Key Vault firewalls and virtual networks
b) Azure Active Directory (Azure AD) permissions
c) role-based access control (RBAC) for the key vault
d) the access policy settings of the key vault

**Answer: a**

Question: 3

You are currently using Azure Sentinel for the collection of Windows security events. You want to use Azure Sentinel to identify Remote Desktop Protocol (RDP) activity that is unusual for your environment.

You need to enable the Anomalous RDP Login Detection rule. What two prerequisites do you need to ensure are in place before you can enable this rule?

Each correct answer presents part of the solution.

a) Let the machine learning algorithm collect 30 days' worth of Windows Security events data.
b) Collect Security events or Windows Security Events with Event ID 4720.
c) Collect Security events or Windows Security Events with Event ID 4624.
d) Select an event set other than None.

**Answer: c, d**

Question: 4

Reference Scenario: **click here**

Which rule setting should you configure to meet the Azure Sentinel requirements?

a) From Set rule logic, turn off suppression.
b) From Analytics rule details, configure the tactics.
c) From Set rule logic, map the entities.
d) From Analytics rule details, configure the severity.

**Answer: c**

## Question: 5

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks. The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center. You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

a) the severity level of email notifications
b) a cloud connector
c) the Azure Defender plans
d) the integration settings for Threat detection

**Answer: a**

## Question: 6

You implement Safe Attachments policies in Microsoft Defender for Office 365. Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

a) Dynamic Delivery
b) Replace
c) Block and Enable redirect
d) Monitor and Enable redirect

**Answer: a**

## Question: 7

You receive a security bulletin about a potential attack that uses an image file. You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack. Which indicator type should you use?

a) a URL/domain indicator that has Action set to Alert only
b) a URL/domain indicator that has Action set to Alert and block
c) a file hash indicator that has Action set to Alert and block
d) a certificate indicator that has Action set to Alert and block

**Answer: c**

## Question: 8

You are using the Microsoft 365 Defender portal to conduct an investigation into a multi-stage incident related to a suspected malicious document. After reviewing all the details, you have determined that the alert tied to this potentially malicious document is also related to another incident in your environment.
However, the alert is not currently listed as a part of that second incident. Your investigation into the alert is ongoing, as is your investigation into the two related incidents. You need to appropriately categorize the alert and ensure that it is associated with the second incident.
What two actions should you take in the Manage alert pane to fulfill this part of the investigation?
Each correct answer presents a part of the solution.

a) Enter the Incident ID of the related incident in the Comment section.
b) Set status to In progress.
c) Set classification to True alert.
d) Set status to New.
e) Select the Link alert to another incident option.

**Answer: b, e**

## Question: 9

You receive an alert from Azure Defender for Key Vault. You discover that the alert is generated from multiple suspicious IP addresses. You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

a) Modify the access control settings for the key vault.
b) Enable the Key Vault firewall.
c) Create an application security group.
d) Modify the access policy for the key vault.

**Answer: b**

## Question: 10

Reference Scenario: **click here**
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

a) executive
b) sales
c) marketing
d) security

**Answer: b**

# Study Guide to Crack Microsoft Security Operations Analyst SC-200 Exam:

- Getting details of the SC-200 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the SC-200 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the Microsoft provided training for SC-200 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the SC-200 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on SC-200 practice tests is must. Continuous practice will make you an expert in all syllabus areas.