EDUSUM

#1 Online Certification Guide

MICROSOFT SC-200 STUDY GUIDE PDF

Grab the Microsoft Security Operations Analyst Certification PDF Questions & Answers

Details of the Exam-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:

Get an Overview of the SC-200 Certification:

Who should take the **SC-200 exam**? This is the first question that comes to a candidate's mind when preparing for the Security Operations Analyst certification. The SC-200 certification is suitable for candidates who are keen to earn knowledge on the Microsoft Security Compliance and Identity and grab their Microsoft Certified - Security Operations Analyst Associate certification. When it is about starting the preparation, most candidates get confused regarding the study materials and study approach. But SC-200 study guide PDF is here to solve the problem. SC-200 PDF combines some effective sample questions and offers valuable tips to pass the exam with ease.

Why Should You Earn the Microsoft SC-200 Certification?

There are several reasons why one should grab the SC-200 certification.

- The Security Operations Analyst certification proves to be one of the most recognized certifications.
- The certification badge proves the knowledge of the candidate regarding subject matters and makes his resume presentable to potential employers.
- Thus earning the **Microsoft Certified - Security Operations Analyst Associate** is a powerful qualification for a prosperous career.

What is the Microsoft SC-200 Security Operations Analyst Certification Exam Structure?

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**

Enhance Knowledge with SC-200 Sample Questions:

Question: 1

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: 2

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: 3

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: 4

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: 5

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: 6

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: 7

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

Question: 8

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: 9

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: 10

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

What Study Guide Works Best in Acing the Microsoft SC-200 Security Operations Analyst Certification?

The SC-200 study guide is a combination of some proven study tips and the combination of all valuable study materials like sample questions, syllabus and practice tests in one place.

Explore the Syllabus Topics and Learn from the Core:

If you are determined to earn success in the Security Operations Analyst exam, getting in full touch of the **syllabus** is mandatory. During preparation, you might not like all syllabus sections or topics, but try to get at least the fundamental knowledge from the sections you don't like. The more you possess knowledge on all syllabus sections, the more is the chance to attempt maximum number of questions during the actual exam.

Make Your Schedule:

Studying and completing the syllabus becomes easier, if you work on the syllabus topics after making a schedule. Your study schedule must mention what areas you want to cover and within what time. Once you make a schedule and follow it regularly, syllabus completion becomes easier and preparation becomes smoother.

Get Expert Advice from the Training:

If there is related Microsoft training, don't miss out the chance to join. Training enhances the practical knowledge of a candidate, which helps them to work well in the practical field during projects.

Get Access to the PDF Sample Questions:

If your study material is in a **PDF format** or the materials are mobile-friendly, what could be better than that? Get access to the free sample questions and keep enhancing your knowledge beyond the syllabus.

Avoid Dumps and utilize the Microsoft SC-200 Practice Test:

Why should you rely on practice tests? The reason is simple: you must get familiar with the exam pattern before reaching the exam hall. An aspirant aware of the exam structure and time management during the exam preparation can perform well in the actual exam and attempt the maximum number of questions during the exam.

Many aspirants prefer to read from dumps, but they miss out on the self assessment method. Therefore, SC-200 practice tests always stand out to be the better choice than dumps PDF.

Avail the Proven SC-200 Practice Test for Success!!!

Do you want to pass the SC-200 exam on your first attempt? Stop worrying; EduSum.com is here to provide you the best experience during your Microsoft Security Operations Analyst preparation. Try out our free mock tests to get a glimpse of our quality study materials, and build your confidence with the premium **SC-200 practice tests**. Our expert-designed questions help you to improve performance and pass the exam on your first attempt.