MICROSOFT SC-200

Microsoft Security Operations Analyst Certification Questions & Answers

Get Instant Access to Vital Exam Acing Materials | Study Guide | Sample Questions | Practice Test

SC-200

Microsoft Certified - Security Operations Analyst Associate

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

Table of Contents:

Discover More about the SC-200 Certification

Are you interested in passing the Microsoft SC-200 exam? First discover, who benefits from the SC-200 certification. The SC-200 is suitable for a candidate if he wants to learn about Microsoft Security Compliance and Identity. Passing the SC-200 exam earns you the Microsoft Certified - Security Operations Analyst Associate title.

While preparing for the SC-200 exam, many candidates struggle to get the necessary materials. But do not worry; your struggling days are over. The SC-200 PDF contains some of the most valuable preparation tips and the details and instant access to useful **SC-200 study materials just at one click**.

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 - detect, investigate, respond, remediate threats to email by using Defender for Office 365 - manage data loss prevention policy alerts - assess and recommend sensitivity labels - 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 - configure device attack surface reduction rules - configure and manage custom detections and alerts - respond to incidents and alerts - manage automated investigations and remediations - assess and recommend endpoint configurations to reduce and remediate vulnerabilities by using the Microsoft's threat and vulnerability management solution. - manage Microsoft Defender for Endpoint threat indicators - 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 - identify and remediate security risks related to Conditional Access events - identify and remediate security risks related to Azure Active Directory - identify and remediate security risks using Secure Score - identify, investigate, and remediate security risks related to privileged identities - configure detection alerts in Azure AD Identity Protection - 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 Defender for Cloud Apps - configure Microsoft Defender for Cloud Apps to generate alerts and reports to detect threats
Manage cross-domain investigations in Microsoft 365 Defender portal	- manage incidents across Microsoft 365 Defender products - manage actions pending approval across products - 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 - configure Microsoft Defender for Cloud roles - configure data retention policies - 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 - configure automated onboarding for Azure resources - connect on-premises computers - connect AWS cloud resources - connect GCP cloud resources - configure data collection
Manage Microsoft Defender for Cloud alert rules	- validate alert configuration - setup email notifications - create and manage alert suppression rules
Configure automation and remediation	- configure automated responses in Microsoft Defender for Cloud - design and configure workflow automation in Microsoft Defender for Cloud - 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 - manage security alerts - manage security incidents - analyze Microsoft Defender for Cloud threat intelligence - respond to Microsoft Defender Cloud for Key Vault alerts - 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 - configure Microsoft Sentinel roles - design Microsoft Sentinel data storage - 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 - identify the prerequisites for a data connector - configure and use Microsoft Sentinel data connectors - configure data connectors by using Azure Policy - design and configure Syslog and CEF event collections - design and Configure Windows Security events collections - configure custom threat intelligence connectors - create custom logs in Azure Log Analytics to store custom data
Manage Microsoft Sentinel analytics rules	- design and configure analytics rules - create custom analytics rules to detect threats - activate Microsoft security analytics rules - configure connector provided scheduled queries - configure custom scheduled queries - define incident creation logic
Configure Security Orchestration Automation and Response (SOAR) in Microsoft Sentinel	- create Microsoft Sentinel playbooks - configure rules and incidents to trigger playbooks - use playbooks to remediate threats - use playbooks to manage incidents - use playbooks across Microsoft Defender solutions

Topic	Details
Manage Microsoft Sentinel Incidents	- investigate incidents in Microsoft Sentinel - triage incidents in Microsoft Sentinel - respond to incidents in Microsoft Sentinel - investigate multi-workspace incidents - 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 - create custom workbooks - configure advanced visualizations - view and analyze Microsoft Sentinel data using workbooks - track incident metrics using the security operations efficiency workbook
Hunt for threats using Microsoft Sentinel	- create custom hunting queries - run hunting queries manually - monitor hunting queries by using Livestream - perform advanced hunting with notebooks - track query results with bookmarks - use hunting bookmarks for data investigations - convert a hunting query to an analytical

Broaden Your Knowledge with Microsoft SC-200 Sample Questions:

Question: 1

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: 2

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: 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

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: 6

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: 7

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: 8

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: 9

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: 10

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

Avail the Study Guide to Pass Microsoft SC-200 Security Operations Analyst Exam:

- Find out about the SC-200 syllabus topics. Visiting the official site offers an idea about the exam structure and other important study resources. Going through the syllabus topics help to plan the exam in an organized manner.
- Once you are done exploring the **SC-200 syllabus**, it is time to plan for studying and covering the syllabus topics from the core. Chalk out the best plan for yourself to cover each part of the syllabus in a hassle-free manner.
- A study schedule helps you to stay calm throughout your exam preparation. It should contain your materials and thoughts like study hours, number of topics for daily studying mentioned on it. The best bet to clear the exam is to follow your schedule rigorously.
- The candidate should not miss out on the scope to learn from the SC-200 training. Joining the Microsoft provided training for SC-200 exam helps a candidate to strengthen his practical knowledge base from the certification.
- Learning about the probable questions and gaining knowledge regarding the exam structure helps a lot. Go through the **SC-200 sample questions** and boost your knowledge
- Make yourself a pro through online practicing the syllabus topics. SC-200 practice tests would guide you on your strengths and weaknesses regarding the syllabus topics. Through rigorous practicing, you can improve the weaker sections too. Learn well about time management during exam and become confident gradually with practice tests.

Career Benefits:

- Passing the SC-200 exam, helps a candidate to prosper highly in his career. Having the certification on the resume adds to the candidate's benefit and helps to get the best opportunities.

Here Is the Trusted Practice Test for the SC-200 Certification

EduSum.Com is here with all the necessary details regarding the SC-200 exam. We provide authentic practice tests for the SC-200 exam. What do you gain from these practice tests? You get to experience the real exam-like questions made by industry experts and get a scope to improve your performance in the actual exam. Rely on EduSum.Com for rigorous, unlimited two-month attempts on the **SC-200 practice tests**, and gradually build your confidence. Rigorous practice made many aspirants successful and made their journey easy towards grabbing the Microsoft Certified - Security Operations Analyst Associate.

Start Online Practice of SC-200 Exam by visiting URL
https://www.edusum.com/microsoft/sc-200-microsoft-security-operations-analyst