



Free Questions for SC-200 by [braindumpscollection](#)

Shared by [Melendez](#) on [24-05-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

You have a Microsoft Sentinel workspace that contains a custom workbook named Workbook1.

You need to create a visual based on the SecurityEvent table. The solution must meet the following requirements:

- * Identify the number of security events ingested during the past week.
- * Display the count of events by day in a timechart

What should you add to Workbook1?

Options:

- A- a query
- B- a metric
- C- a group
- D- links or tabs

Answer:

A

Question 2

Question Type: MultipleChoice

Your on-premises network contains an Active Directory Domain Services (AD DS) forest.

You have a Microsoft Entra tenant that uses Microsoft Defender for Identity. The AD DS forest syncs with the tenant

You need to create a hunting query that will identify LDAP simple binds to the AD DS domain controllers.

Which table should you query?

Options:

A- AADServicePrincipalRiskEventi

B- IdentityLOgonEvents

C- AADDomainServicesAccountLogon

D- Signinlogs

Answer:

B

Question 3

Question Type: MultipleChoice

You have an Azure subscription that has the enhanced security features in Microsoft Defender for Cloud enabled and contains a user named User1.

You need to ensure that User1 can export alert data from Defender for Cloud. The solution must use the principle of least privilege.

Which role should you assign to User1?

Options:

- A- Contributor
- B- User Access Administrator
- C- Owner
- D- Reader

Answer:

C

Question 4

Question Type: OrderList

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Configure workflow automation.

Create an Azure logic app that includes the Defender for Cloud regulatory compliance assessment trigger.

Configure a trigger condition.

Create an Azure logic app that includes the Defender for Cloud alert trigger.

Create an Azure logic app that includes a Defender for Cloud recommendation trigger.



Answer Area

Answer:

Create an Azure Logic App that includes the Defender for Cloud alert trigger.

Question 5

Question Type: MultipleChoice

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

Options:

- A- Azure Synapse Analytics
- B- Azure Databricks
- C- Azure Machine Learning
- D- Log Analytics

Answer:

D

Question 6

Question Type: Hotspot

You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Answer Area

Answer:

Group1:

- Contributor
- Owner
- Security Admin**
- Security Assessment Contributor

Group2:

- Contributor**
- Owner
- Security Admin
- Security Assessment Contributor

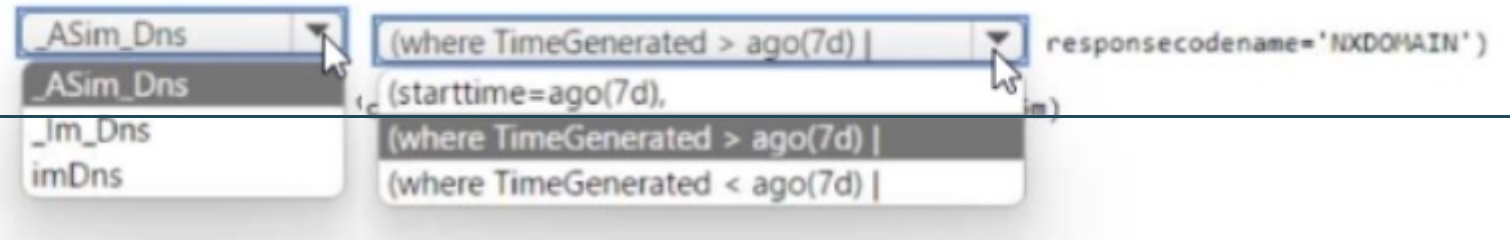
Question 7

Question Type: Hotspot

You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area

Answer:



Question 8

Question Type: MultipleChoice

You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

Options:

- A- Create an AWS user for Defender for Cloud.
- B- Create an Access control (IAM) role for Defender for Cloud.
- C- Configure AWS Security Hub.
- D- Deploy the AWS Systems Manager (SSM) agent

Answer:

D

Question 9

Question Type: Hotspot

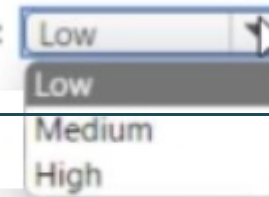
You need to meet the Microsoft Defender for Cloud Apps requirements

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Set the sensitivity level of the impossible travel alert policies to:



A screenshot of a dropdown menu with the text "Set the sensitivity level of the impossible travel alert policies to:" to its left. The dropdown menu is open, showing four options: "Low", "Medium", and "High". The "Low" option is currently selected and highlighted.

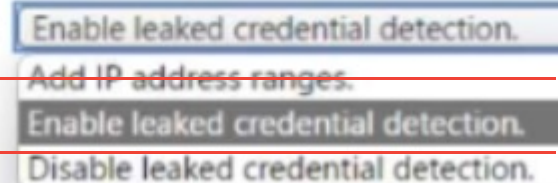
Answer:

Question 10

Question Type: MultipleChoice

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

To reduce the amount of false positive alerts:



A screenshot of a multiple-choice question. The text "To reduce the amount of false positive alerts:" is to the left of a list of four options. The options are: "Enable leaked credential detection.", "Add IP address ranges.", "Enable leaked credential detection.", and "Disable leaked credential detection.". The second option, "Add IP address ranges.", is highlighted.

Options:

- A- the status update time
- B- the alert status
- C- the certainty of the source computer
- D- the resolution method of the source computer

Answer:

B

Question 11

Question Type: MultipleChoice

You use Microsoft Sentinel.

You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point

Options:

- A- Create a bookmark.
- B- Create an analytics rule.
- C- Create a livestream.
- D- Create a hunting query.
- E- Add a data connector.

Answer:

D, E

To Get Premium Files for SC-200 Visit

<https://www.p2pexams.com/products/sc-200>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/sc-200>

