



Free Questions for SC-200 by certscare

Shared by Barrett on 18-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

for the Azure virtual

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Image not found or type unknown



Answer:

Explanation:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

Question 2

Question Type: MultipleChoice

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution. create a KQL query that will i create a KQL query that will i

NOTE: Each correct selection is worth one point.

Options:

- A) Create custom rule based on the Office 365 connector templates.
- B) Create a Microsoft incident creation rule based on Azure Security Center.
- C) Create a Microsoft Cloud App Security connector.
- D) Create an Azure AD Identity Protection connector.

Answer:

A, D

Explanation:

To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:

Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.

Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference:<https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules>

Question 3

Question Type: DragDrop

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>

Question 4

Question Type: MultipleChoice

You need to correlate data from the SecurityEvent Log Analytics table to meet the Microsoft Sentinel requirements for using UEBA. Which Log Analytics table should you use?

Options:

- A) SentwlAuoNt
- B) AADRiskyUsers
- C) IdentityOirectoryEvents
- D) Identityinfo

Answer:

C

Question 5

Question Type: Hotspot

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

What should you recommend for each threat? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Image not found or type unknown



Answer:

Explanation:

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault>

Question 6

Question Type: Hotspot

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Image not found or type unknown



Answer:

Explanation:

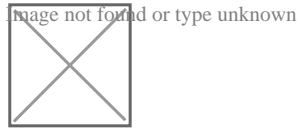
<https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run>

Question 7

Question Type: OrderList

You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

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.



Answer:

In the Azure portal, create a custom analytics rule that uses a scheduled query

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom>

Question 8

Question Type: MultipleChoice

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

Options:

- A) Create custom rule based on the Office 365 connector templates.
- B) Create a Microsoft incident creation rule based on Azure Security Center.
- C) Create a Microsoft Cloud App Security connector.
- D) Create an Azure AD Identity Protection connector.

Answer:

A, D

Explanation:

To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:

Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.

Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription. Reference:<https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules>

Question 9

Question Type: MultipleChoice

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to filter the security alerts view to show the following alerts:

- * Unusual user accessed a key vault
- * Log on from an unusual location
- * Impossible travel activity

Which severity should you use?

Options:

A) Informational

B) Low

C) Medium

D) High

Answer:

C

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>

