SC-200$^{\text{Q\&As}}$

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You have an Azure subscription that uses Azure Defender.

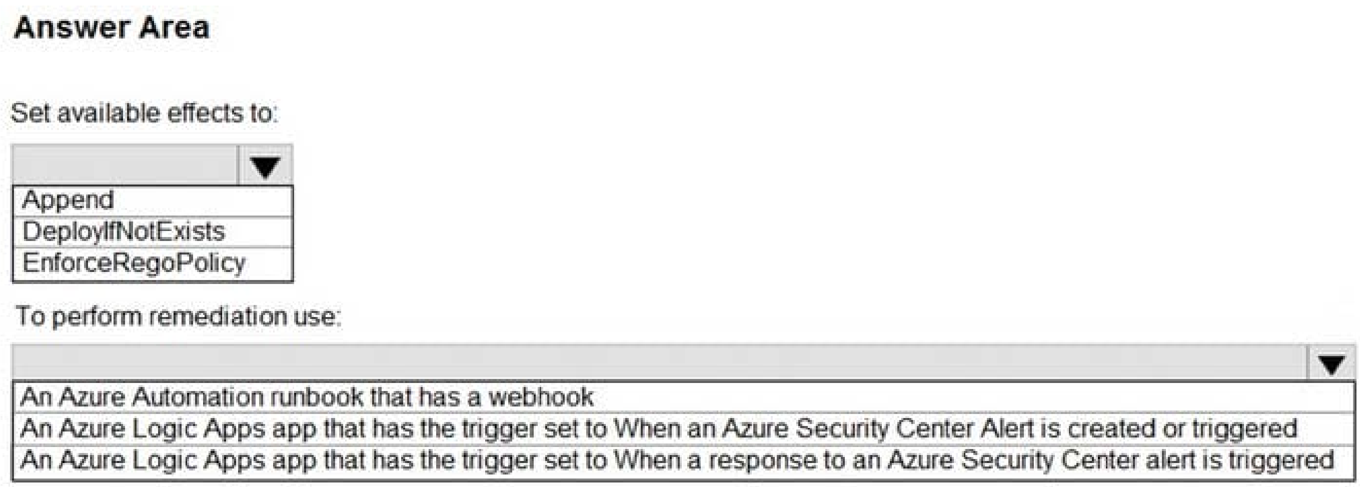
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

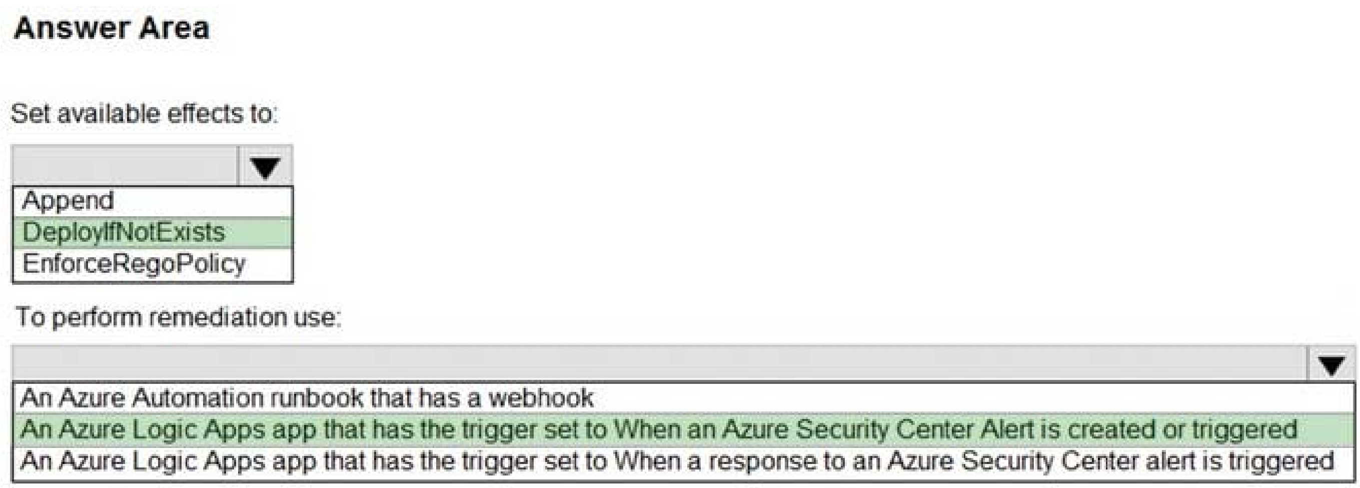
Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Correct Answer:



Answer Area

Set available effects to:

- Append
- [✓ DeployIfNotExists]
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- [✓ An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered]
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Reference: https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

QUESTION 2

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.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

QUESTION 3

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.

You need to create a query that will be used to display a bar graph.

What should you include in the query?

A. extend

B. bin

C. count

D. workspace

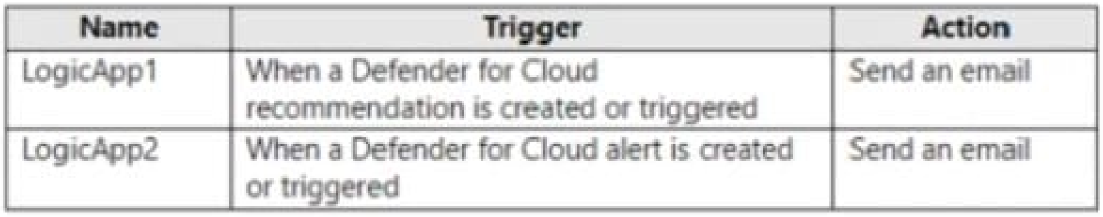
Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

QUESTION 4

DRAG DROP

You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

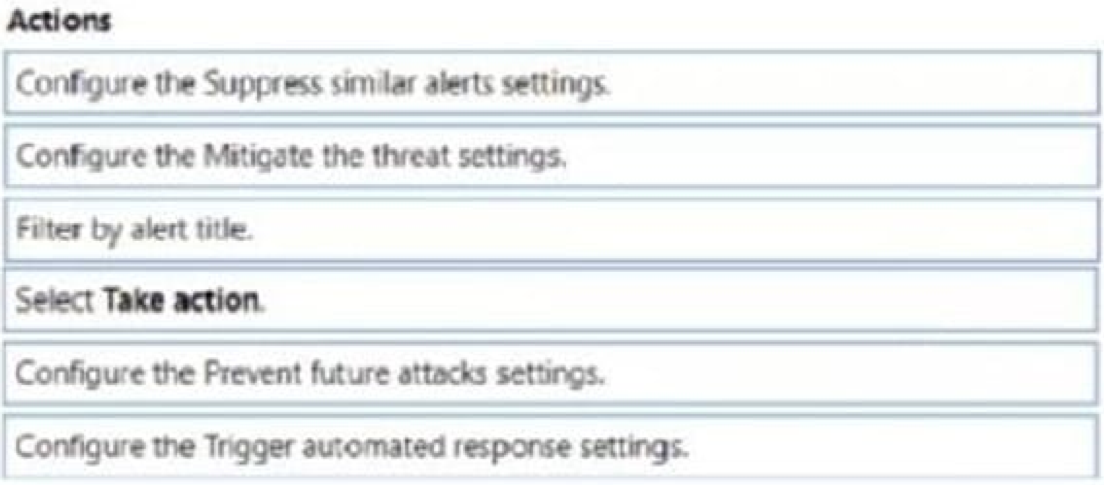


Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.

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.

Select and Place:



Actions

Configure the Suppress similar alerts settings.

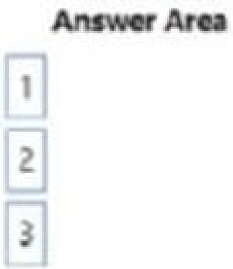
Configure the Mitigate the threat settings.

Filter by alert title.

Select **Take action**.

Configure the Prevent future attacks settings.

Configure the Trigger automated response settings.



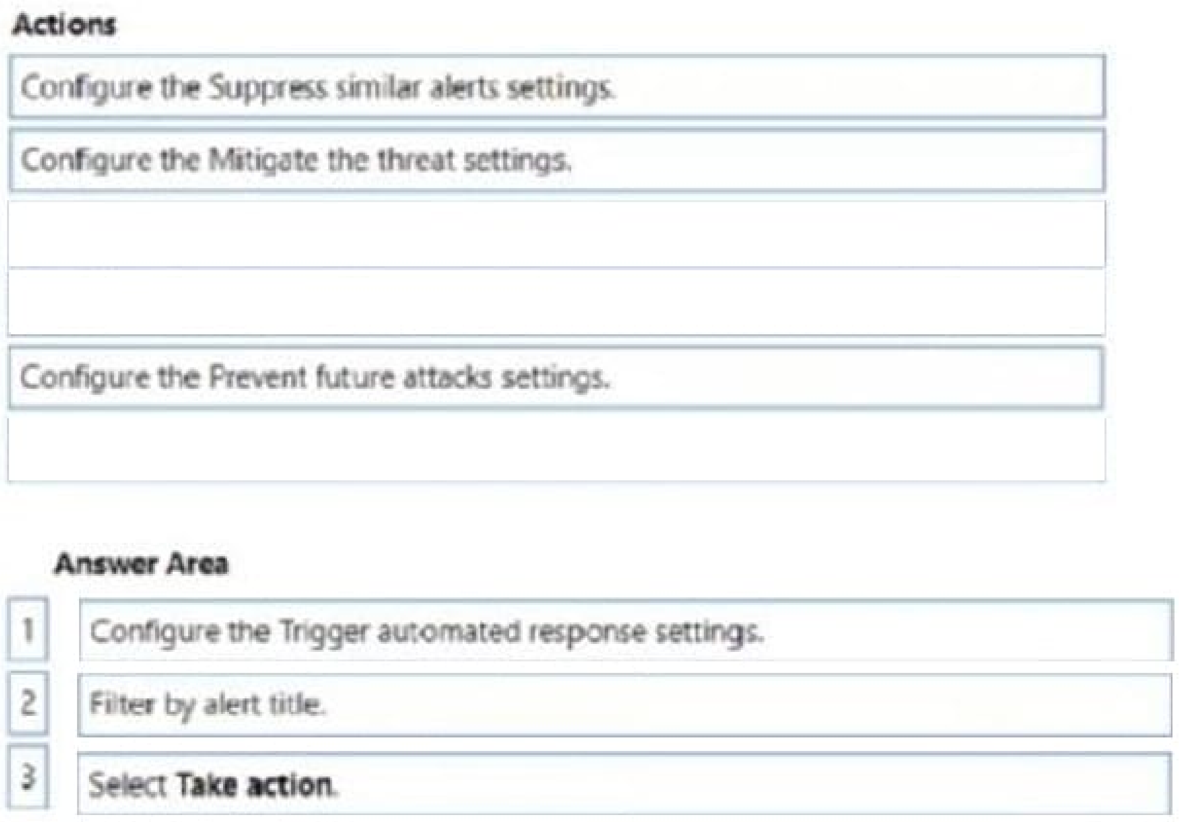
Answer Area

1

2

3

Correct Answer:



Actions

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

Configure the Prevent future attacks settings.

Answer Area

1 Configure the Trigger automated response settings.

2 Filter by alert title.

3 Select **Take action**.

QUESTION 5

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

A. Create an Azure Policy assignment.

B. Modify the Workload protections settings in Defender for Cloud.

C. Create an alert rule in Azure Monitor.

D. Modify the alert settings in Defender for Cloud.

Correct Answer: D

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud. Note: To create a rule directly in the Azure portal:

1.

From Defender for Cloud\\'s security alerts page:

Select the specific alert you don\\'t want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

2.

In the new suppression rule pane, enter the details of your new rule. Your rule can dismiss the alert on all resources so you don\\'t get any alerts like this one in the future. Your rule can dismiss the alert on specific criteria - when it relates to

a specific IP address, process name, user account, Azure resource, or location.

3.

Enter details of the rule.

4.

Save the rule.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules