SC-200^Q&As^

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

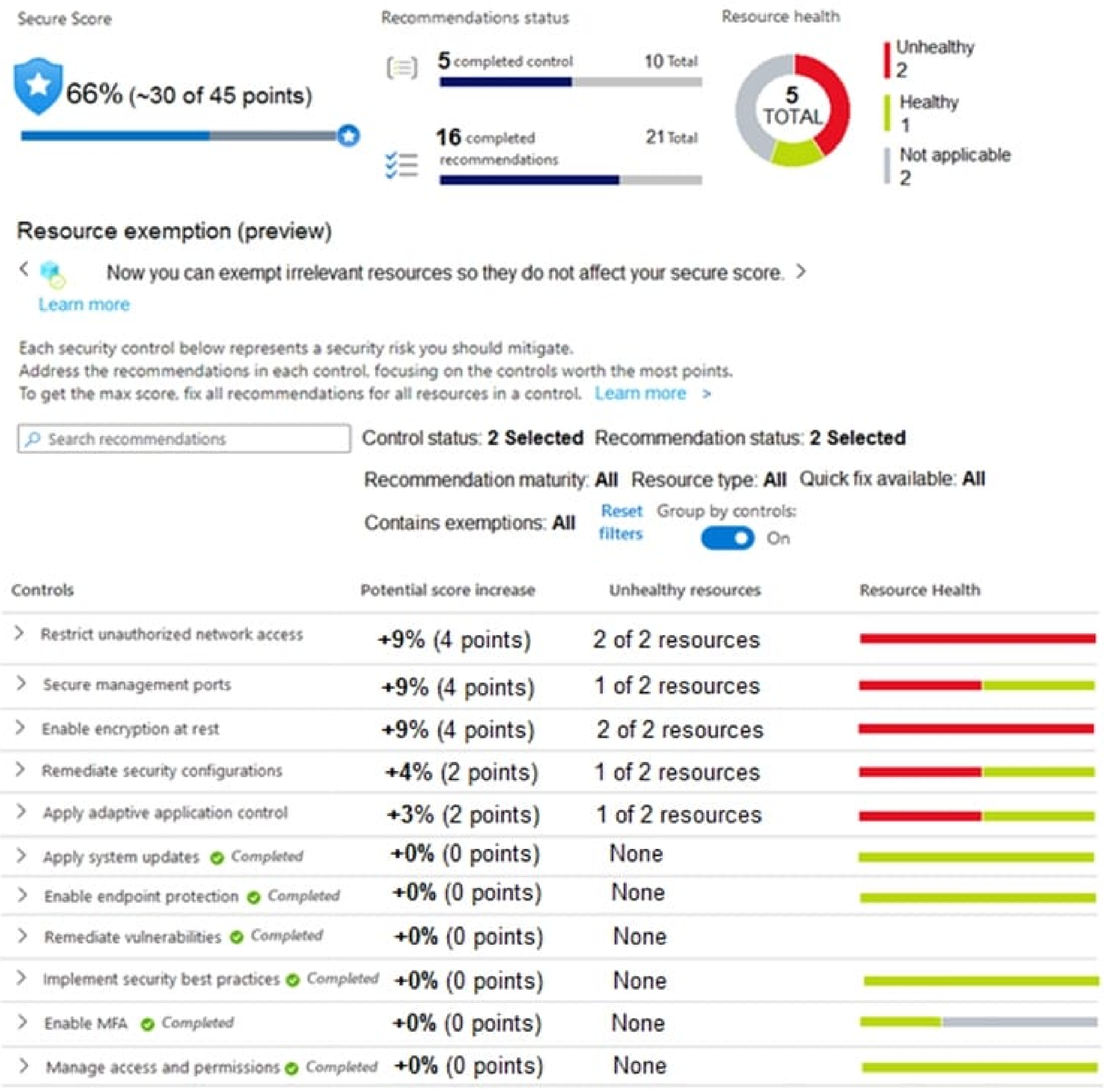
Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

HOTSPOT

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Secure Score

66% (~30 of 45 points)

Recommendations status

5 completed control 10 Total

16 completed recommendations 21 Total

Resource health

5 TOTAL

Unhealthy 2

Healthy 1

Not applicable 2

Resource exemption (preview)

Now you can exempt irrelevant resources so they do not affect your secure score.

Learn more

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

Search recommendations

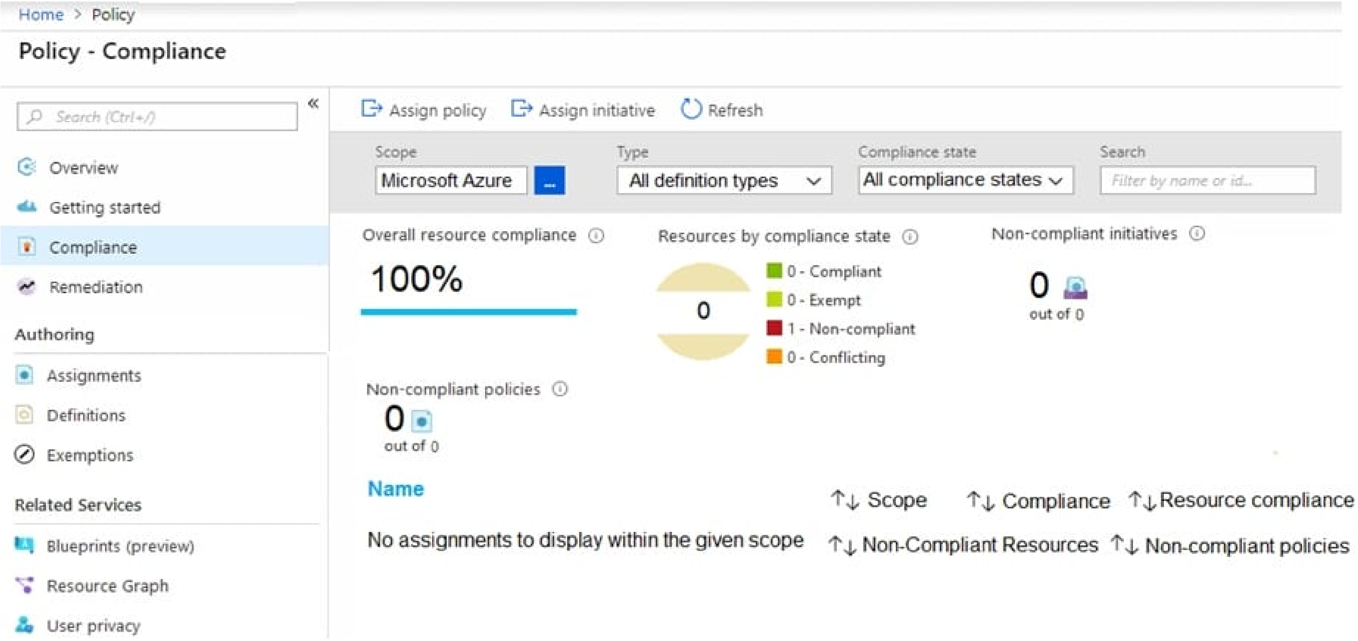
Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** Reset filters Group by controls: On

Controls	Potential score increase	Unhealthy resources	Resource Health
Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	🟥🟥
Secure management ports	+9% (4 points)	1 of 2 resources	🟥🟩
Enable encryption at rest	+9% (4 points)	2 of 2 resources	🟥🟥
Remediate security configurations	+4% (2 points)	1 of 2 resources	🟥🟩
Apply adaptive application control	+3% (2 points)	1 of 2 resources	🟥🟩
Apply system updates ✓ Completed	+0% (0 points)	None	🟩🟩
Enable endpoint protection ✓ Completed	+0% (0 points)	None	🟩🟩
Remediate vulnerabilities ✓ Completed	+0% (0 points)	None	
Implement security best practices ✓ Completed	+0% (0 points)	None	🟩🟩
Enable MFA ✓ Completed	+0% (0 points)	None	🟩⬜
Manage access and permissions ✓ Completed	+0% (0 points)	None	🟩🟩

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



Policy - Compliance

Scope: Microsoft Azure

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or id...

Overall resource compliance: 100%

Resources by compliance state: 0

- 🟩 0 - Compliant
- 🟩 0 - Exempt
- 🟥 1 - Non-compliant
- 🟧 0 - Conflicting

Non-compliant initiatives: 0 out of 0

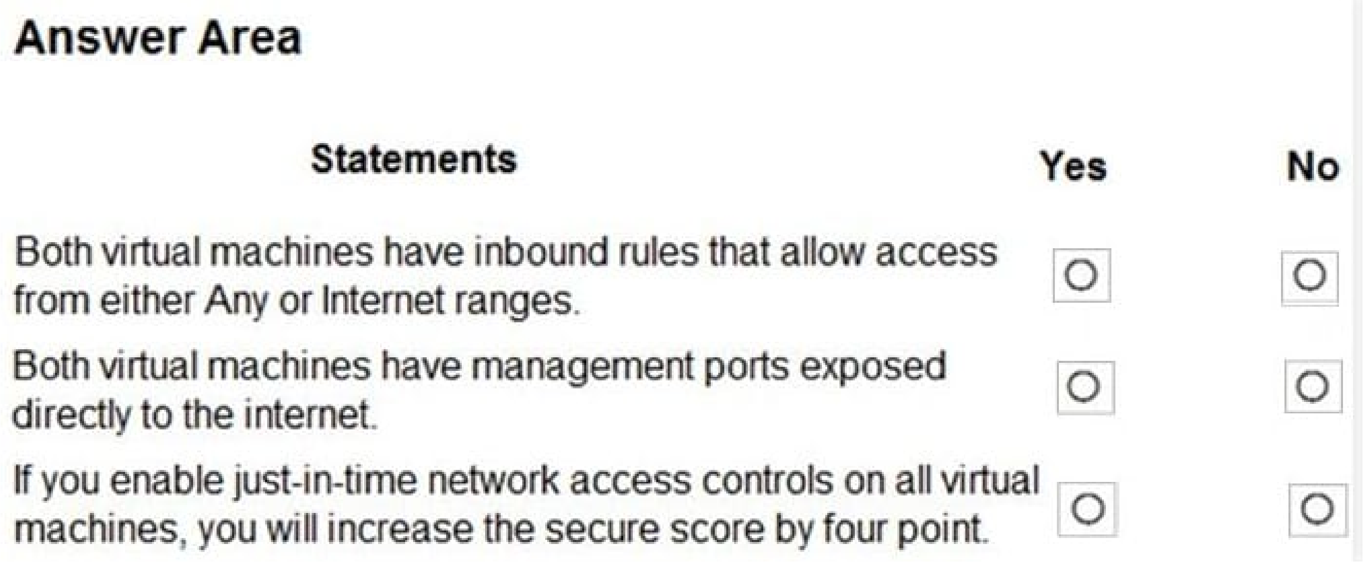
Non-compliant policies: 0 out of 0

Name	↑↓ Scope	↑↓ Compliance	↑↓ Resource compliance	↑↓ Non-Compliant Resources	↑↓ Non-compliant policies
No assignments to display within the given scope					

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

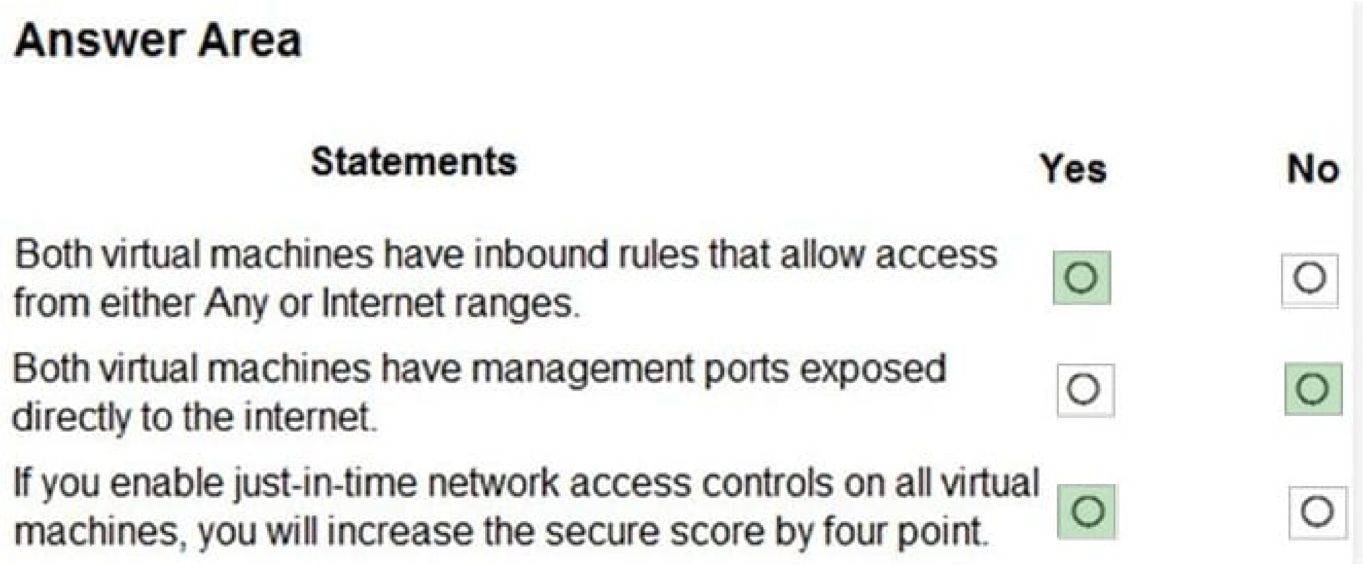
Hot Area:



Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	[✓ ○]	○
Both virtual machines have management ports exposed directly to the internet.	○	[✓ ○]
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	[✓ ○]	○

Reference: https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833 https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

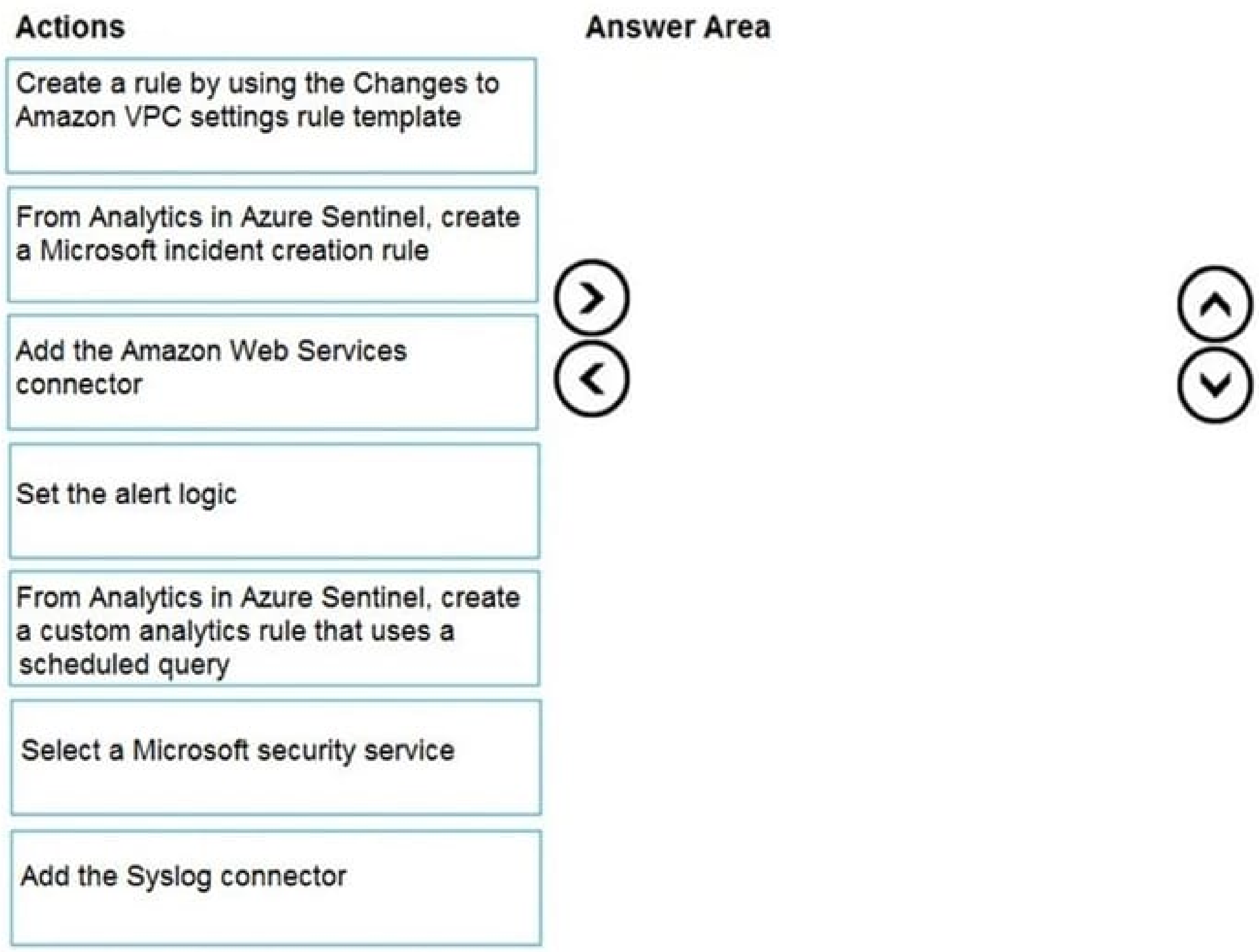
QUESTION 2

DRAG DROP

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.

Select and Place:

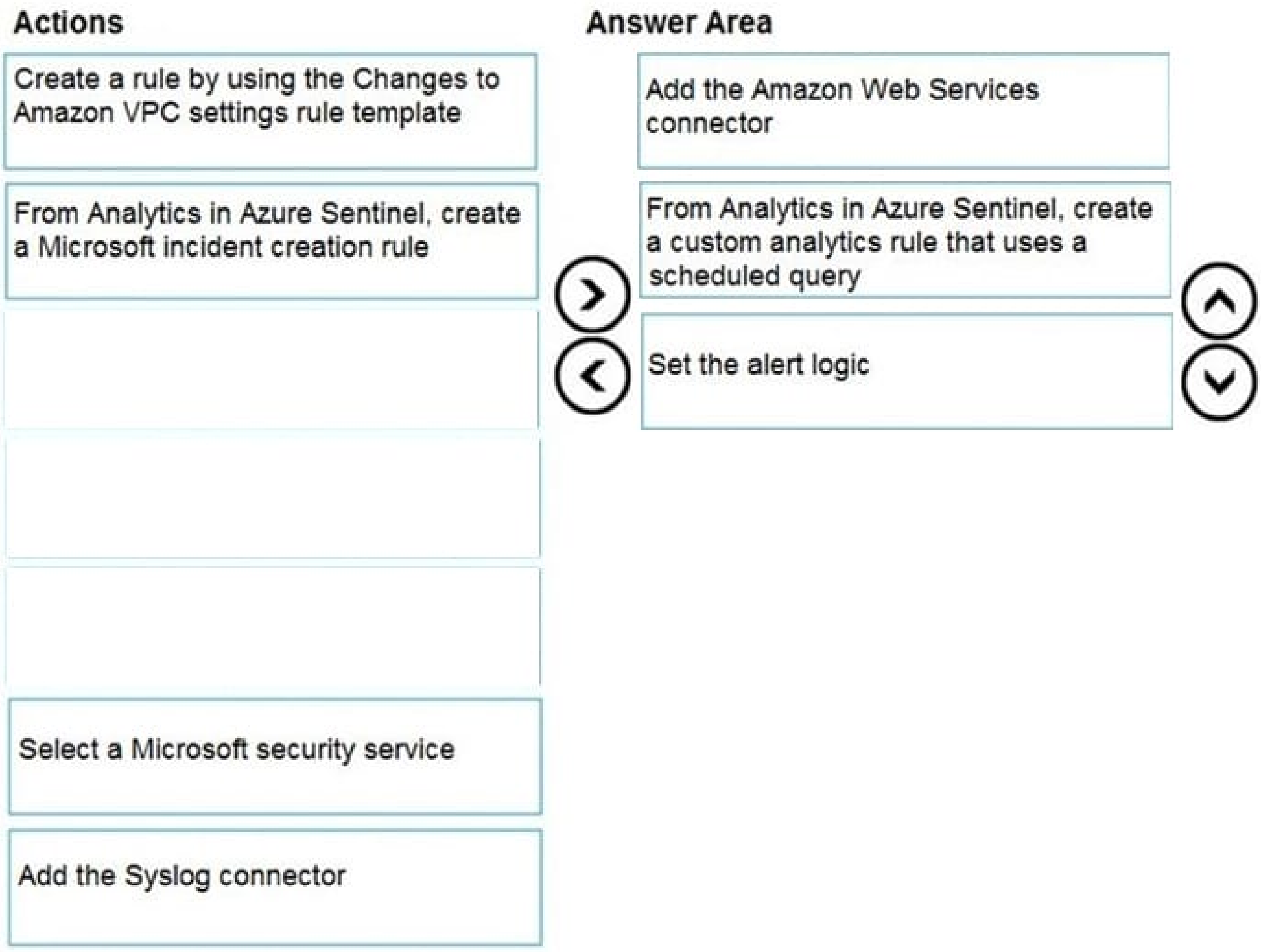


Actions

- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
- Select a Microsoft security service
- Add the Syslog connector

Answer Area

Correct Answer:



Actions

Create a rule by using the Changes to Amazon VPC settings rule template

From Analytics in Azure Sentinel, create a Microsoft incident creation rule

Select a Microsoft security service

Add the Syslog connector

Answer Area

Add the Amazon Web Services connector

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Set the alert logic

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

QUESTION 3

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.

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

NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

B. Create an Azure logic app that has a manual trigger.

C. Create an Azure logic app that has an Azure Security Center alert trigger.

D. Create an Azure logic app that has an HTTP trigger.

E. From Azure Active Directory (Azure AD), add an app registration.

Correct Answer: AC

Reference: https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

QUESTION 4

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a livestream from a query.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

QUESTION 5

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment.

C. Add Azure Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Latest SC-200 Dumps SC-200 Practice Test SC-200 Braindumps