SC-200 Q&As

Microsoft Security Operations Analyst

QUESTION 1

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

A. the Microsoft Monitoring Agent

B. the Azure Monitor agent

C. the Azure Arc agent

D. the Azure Pipelines agent

Correct Answer: B

Connect your non-Azure machines to Microsoft Defender for Cloud

Defender for Cloud can monitor the security posture of your non-Azure computers, but first you need to connect them to Azure.

You can connect your non-Azure computers in any of the following ways:

Using Azure Arc-enabled servers (recommended)

From Defender for Cloud\\'s pages in the Azure portal (Getting started and Inventory)

Add non-Azure machines with Azure Arc

The preferred way of adding your non-Azure machines to Microsoft Defender for Cloud is with Azure Arc-enabled servers.

A machine with Azure Arc-enabled servers becomes an Azure resource and - when you\\'ve installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.

Note: The Log Analytics agent is on a deprecation path and won\\'t be supported after August 31, 2024. If you use the Log Analytics agent to ingest data to Azure Monitor, migrate to the new Azure Monitor agent prior to that date.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

QUESTION 2

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security operator

B. Security Admin

C. Owner

D. Contributor

Correct Answer: B

Security Admin

View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.

Incorrect:

*

Security Reader

View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes.

* owner - too much permissions

*

Contributor (too much permissions)

Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Reference:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

QUESTION 3

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

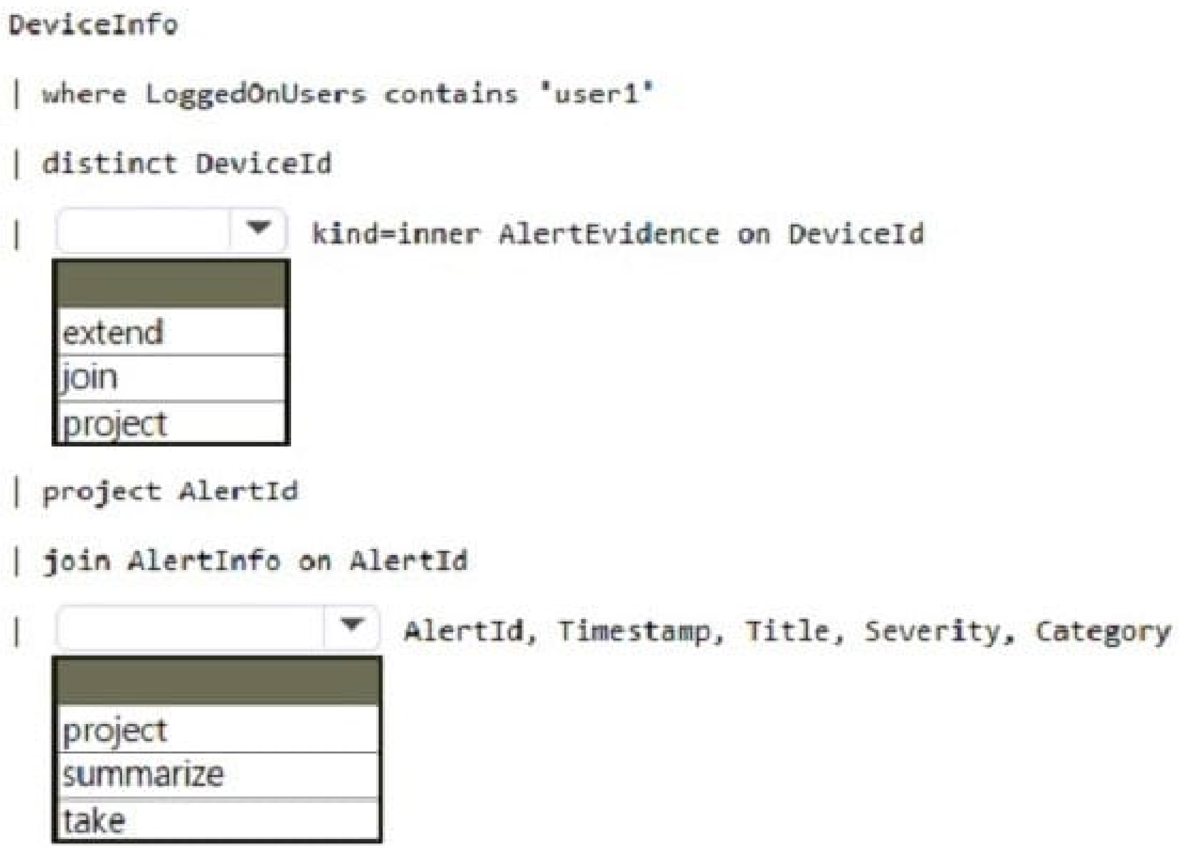
You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

How should you complete the query? To answer, select the appropriate options in the answer area.

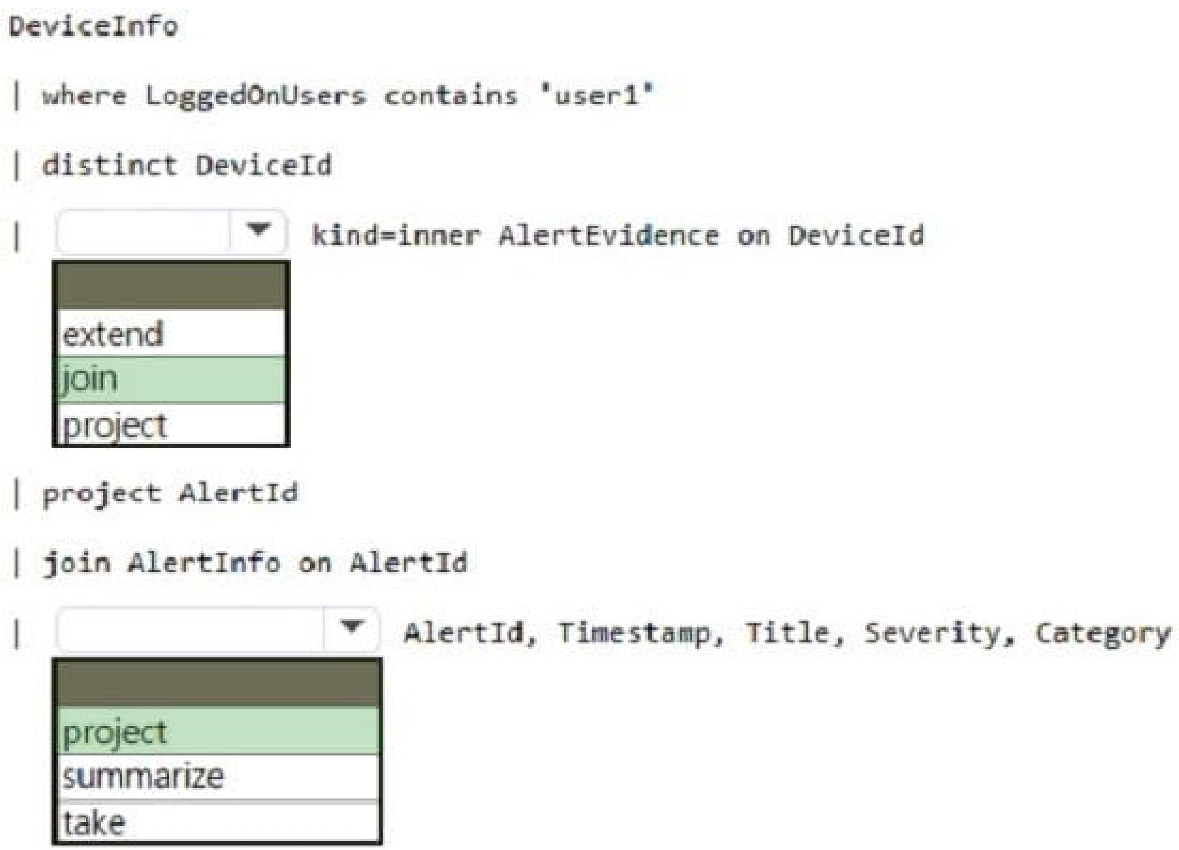
NOTE: Each correct selection is worth one point.

Hot Area:



```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
| [ ▼ ] kind=inner AlertEvidence on DeviceId
| project AlertId
| join AlertInfo on AlertId
| [ ▼ ] AlertId, Timestamp, Title, Severity, Category
```

Correct Answer:



```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
| [ ▼ ] kind=inner AlertEvidence on DeviceId
| project AlertId
| join AlertInfo on AlertId
| [ ▼ ] AlertId, Timestamp, Title, Severity, Category
```

Box 1: join An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user () has logged on to any devices and then lists the alerts that have been triggered on those devices. DeviceInfo //Query for devices that the potentially compromised account has logged onto | where LoggedOnUsers contains \\'\\' | distinct DeviceId //Crosscheck devices against alert records in AlertEvidence and AlertInfo tables | join kind=inner AlertEvidence on DeviceId | project AlertId //List all alerts on devices that user has logged on to | join AlertInfo on AlertId | project AlertId, Timestamp, Title, Severity, Category DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"

Box 2: project

QUESTION 4

You have a Microsoft Sentinel workspace.

You need to identify which rules are used to detect advanced multistage attacks that comprise two or more alerts or activities. The solution must minimize administrative effort.

Which rule type should you query?

A. Fusion

B. Microsoft Security

C. ML Behavior Analytics

D. Scheduled

Correct Answer: A

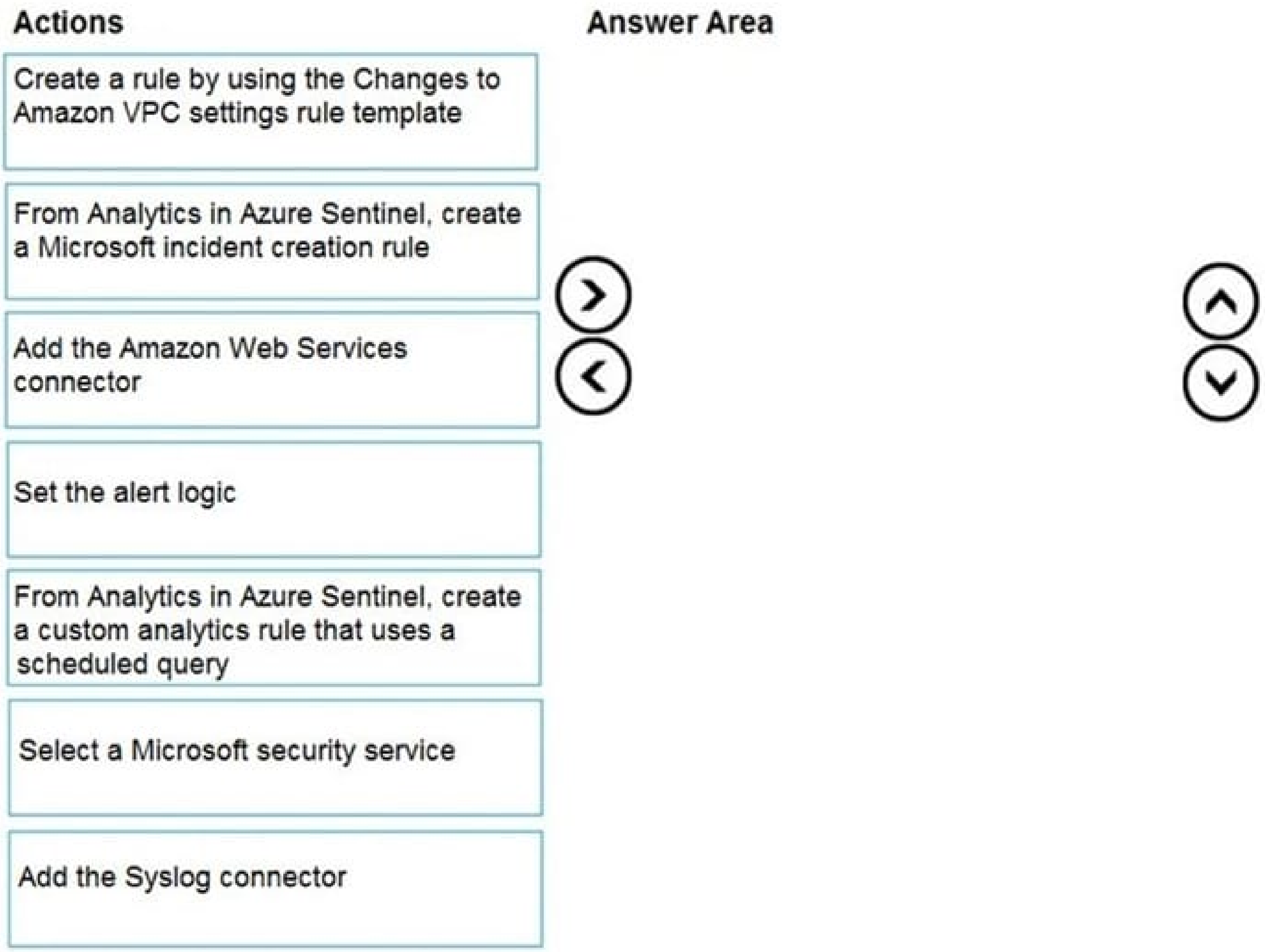
QUESTION 5

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:

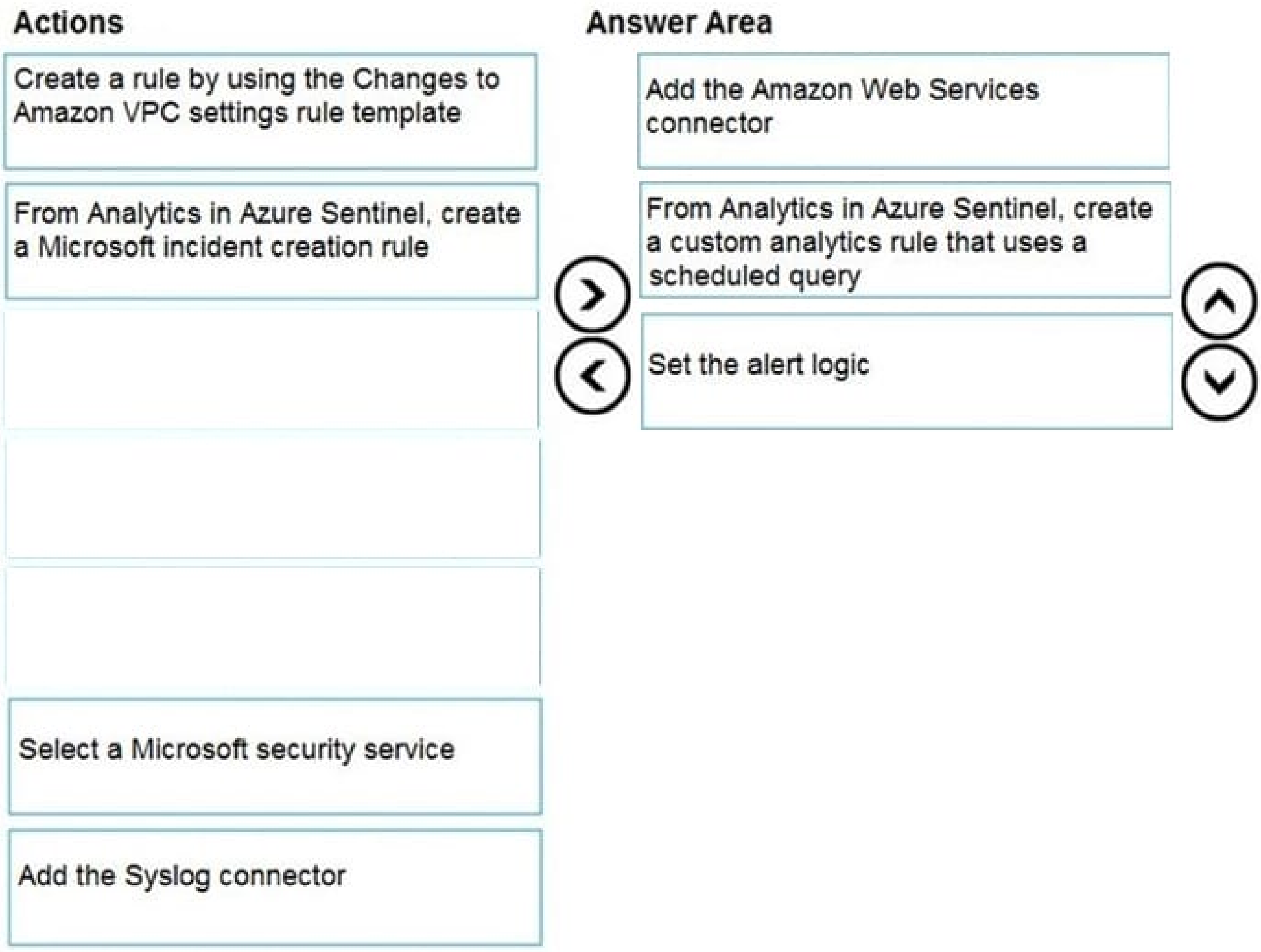


Actions

- 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

SC-200 VCE Dumps SC-200 Practice Test SC-200 Exam Questions