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

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

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

https://www.pass4itsure.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 have an Azure subscription that contains a Microsoft Sentinel workspace named WS1.

You need to ensure that the incidents in WS1 include a list of actions that must be performed. The solution must meet the following requirements:

1.

Ensure that you can build a tailored list of actions for each type of incident.

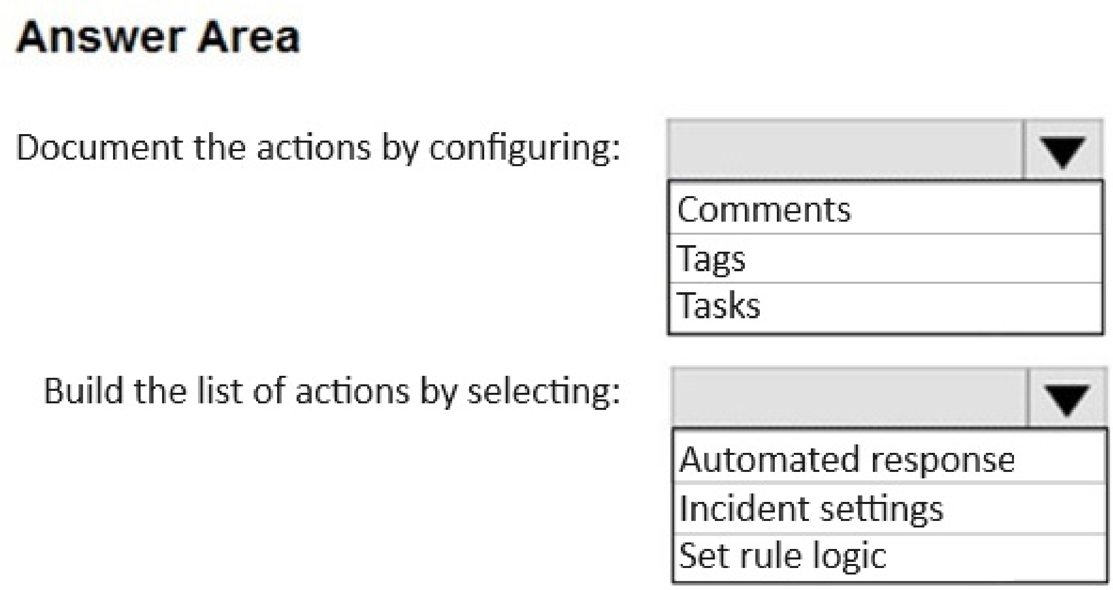
2.

Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

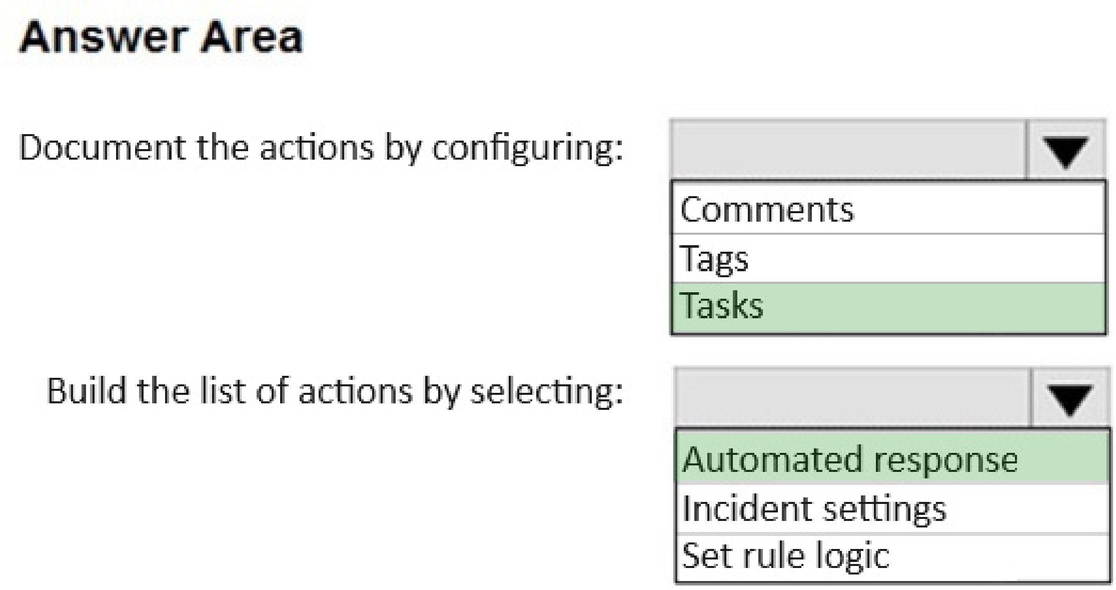
Document the actions by configuring:

- Comments
- Tags
- Tasks

Build the list of actions by selecting:

- Automated response
- Incident settings
- Set rule logic

Correct Answer:



Answer Area

Document the actions by configuring:

- Comments
- Tags
- [✓ Tasks]

Build the list of actions by selecting:

- [✓ Automated response]
- Incident settings
- Set rule logic

QUESTION 2

Your company deploys the following services:

1.

Microsoft Defender for Identity

2.

Microsoft Defender for Endpoint

3.

Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle

of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

B. the Active remediation actions role in Microsoft Defender for Endpoint

C. the Security Administrator role in Azure Active Directory (Azure AD)

D. the Security Reader role in Azure Active Directory (Azure AD)

Correct Answer: BD

Reason being that you do not need a Reader Role.

The Active remediation actions role in Microsoft Defender for Endpoint: This role grants the analyst the ability to take active remediation actions, which includes approving and rejecting pending actions in Microsoft Defender for Endpoint.

The Security Administrator role in Azure Active Directory (Azure AD): While not specific to Defender for Endpoint, this role provides broad access to security-related tasks and configuration across Microsoft 365 services, aligning with the

analyst\\'s responsibilities.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

QUESTION 3

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

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. endpoint detection and response (EDR) in block mode

B. custom network indicators

C. web content filtering

D. Live response for servers

Correct Answer: B

Custom network indicators Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

QUESTION 4

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

You need to configure the continuous export of high-severity alerts to enable their retrieval from a third- party security information and event management (SIEM) solution.

To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

D. Azure Data Lake

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal

QUESTION 5

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

Enable and disable advanced features of Microsoft Defender for Cloud.

Apply security recommendations to a resource.

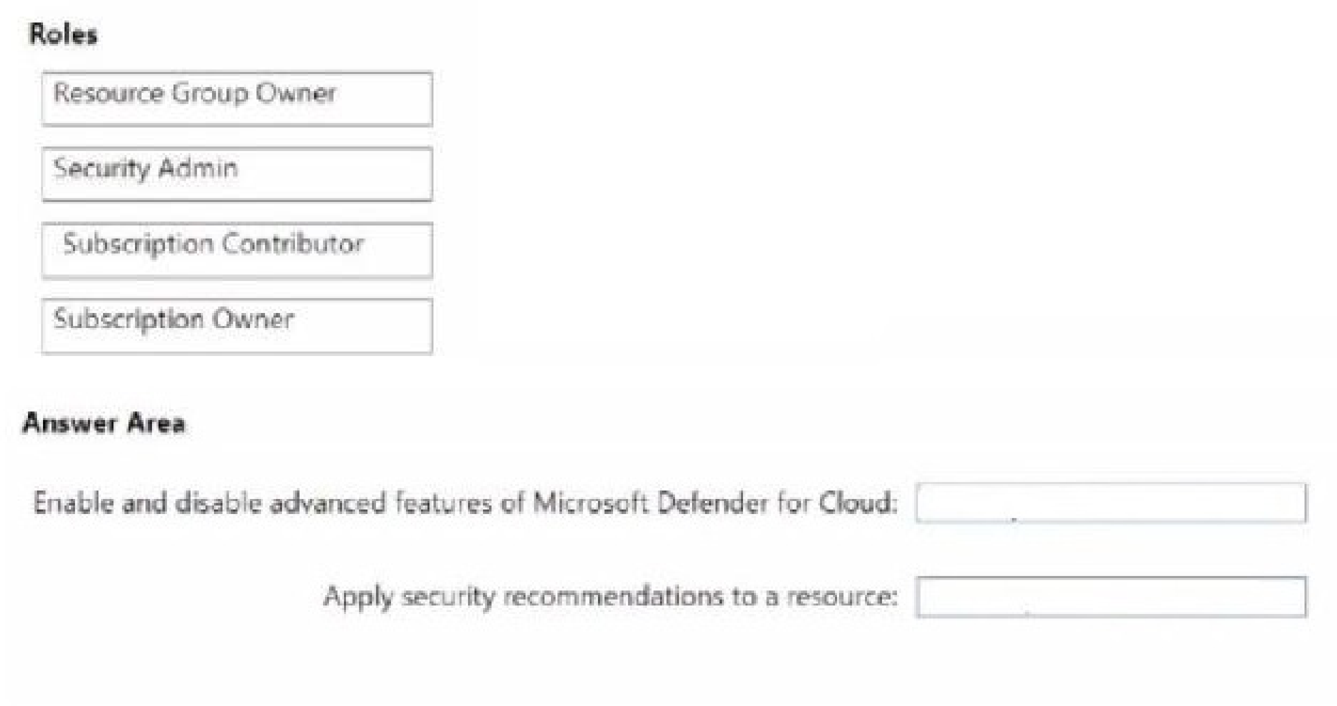
The solution must use the principle of least privilege.

Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote than once, or not at all. You may need to drag the split bar

between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Roles

Resource Group Owner

Security Admin

Subscription Contributor

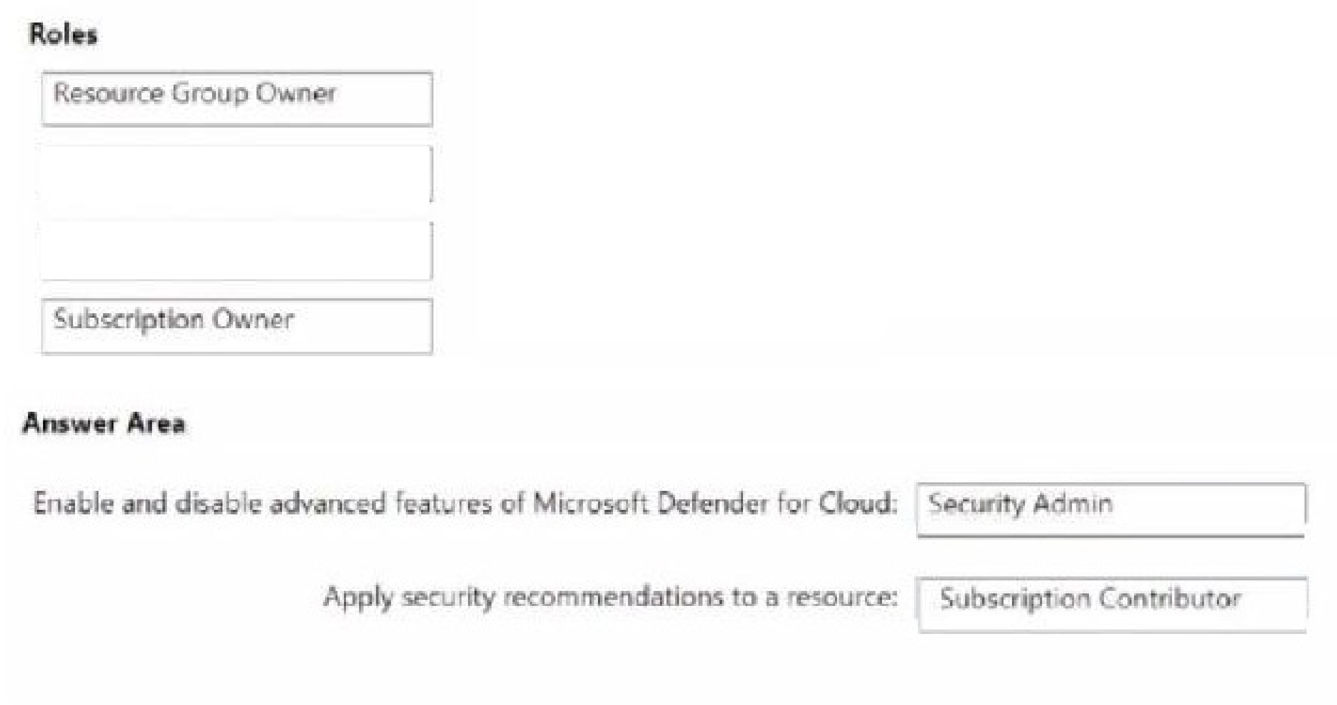
Subscription Owner

Answer Area

Enable and disable advanced features of Microsoft Defender for Cloud:

Apply security recommendations to a resource:

Correct Answer:



Roles

Resource Group Owner

Subscription Owner

Answer Area

Enable and disable advanced features of Microsoft Defender for Cloud: Security Admin

Apply security recommendations to a resource: Subscription Contributor

QUESTION 6

DRAG DROP

You have a Microsoft Sentinel workspace named SW1.

In SW1, you enable User and Entity Behavior Analytics (UEBA).

You need to use KQL to perform the following tasks:

1.

View the entity data that has fields for each type of entity.

2.

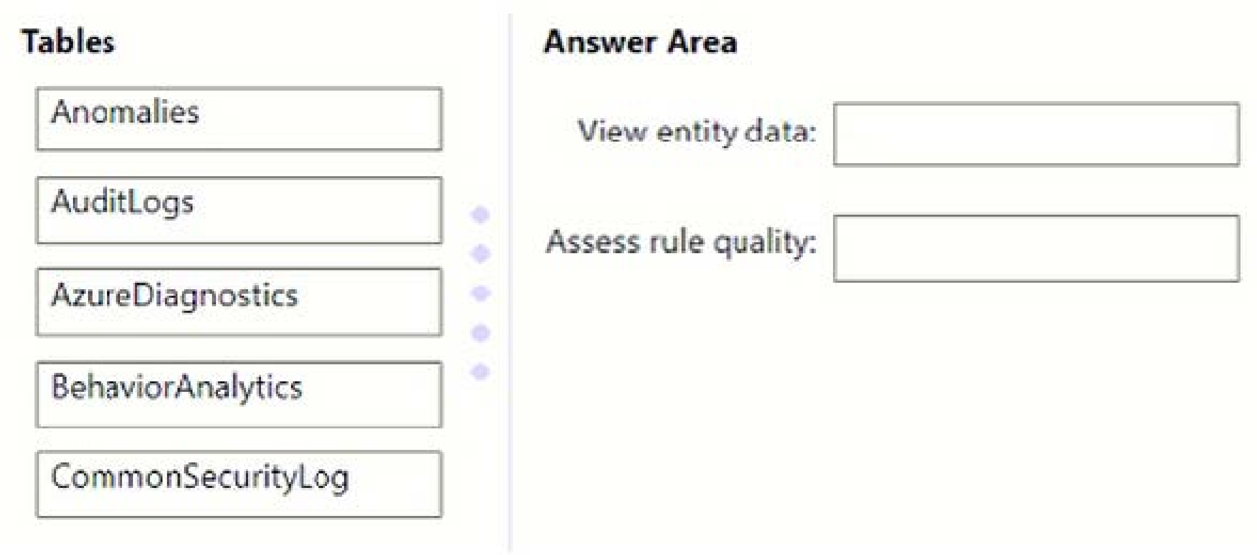
Assess the quality of rules by analyzing how well a rule performs.

Which table should you use in KQL for each task? To answer, drag the appropriate tables to the correct tasks. Each table 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.

NOTE: Each correct selection is worth one point.

Select and Place:



Tables

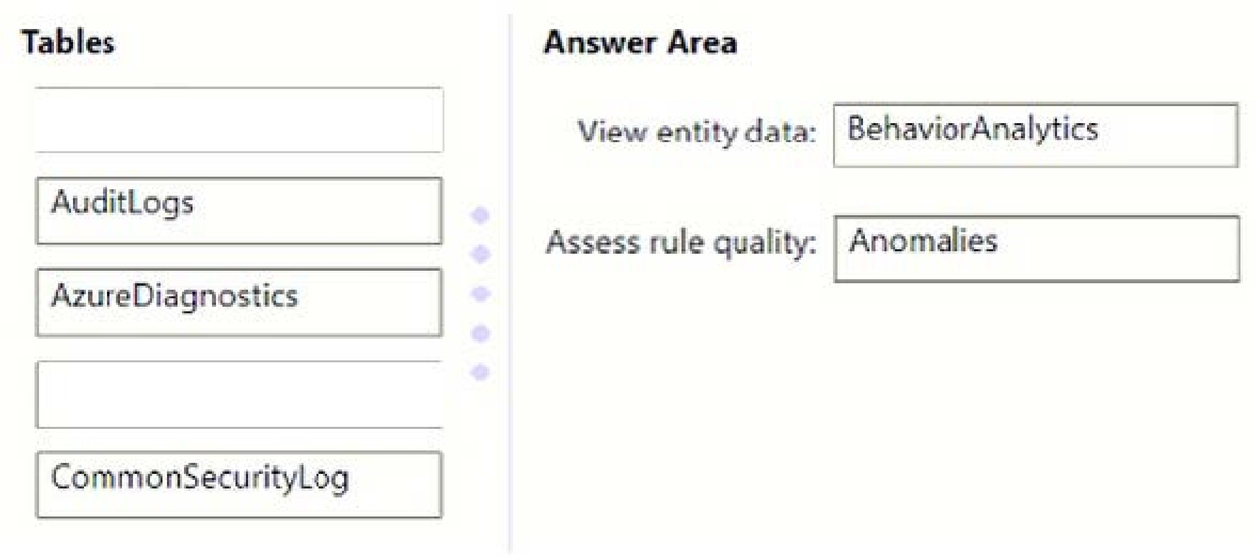
- Anomalies
- AuditLogs
- AzureDiagnostics
- BehaviorAnalytics
- CommonSecurityLog

Answer Area

View entity data:

Assess rule quality:

Correct Answer:



Tables

- AuditLogs
- AzureDiagnostics
- CommonSecurityLog

Answer Area

View entity data: BehaviorAnalytics

Assess rule quality: Anomalies

QUESTION 7

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device1.

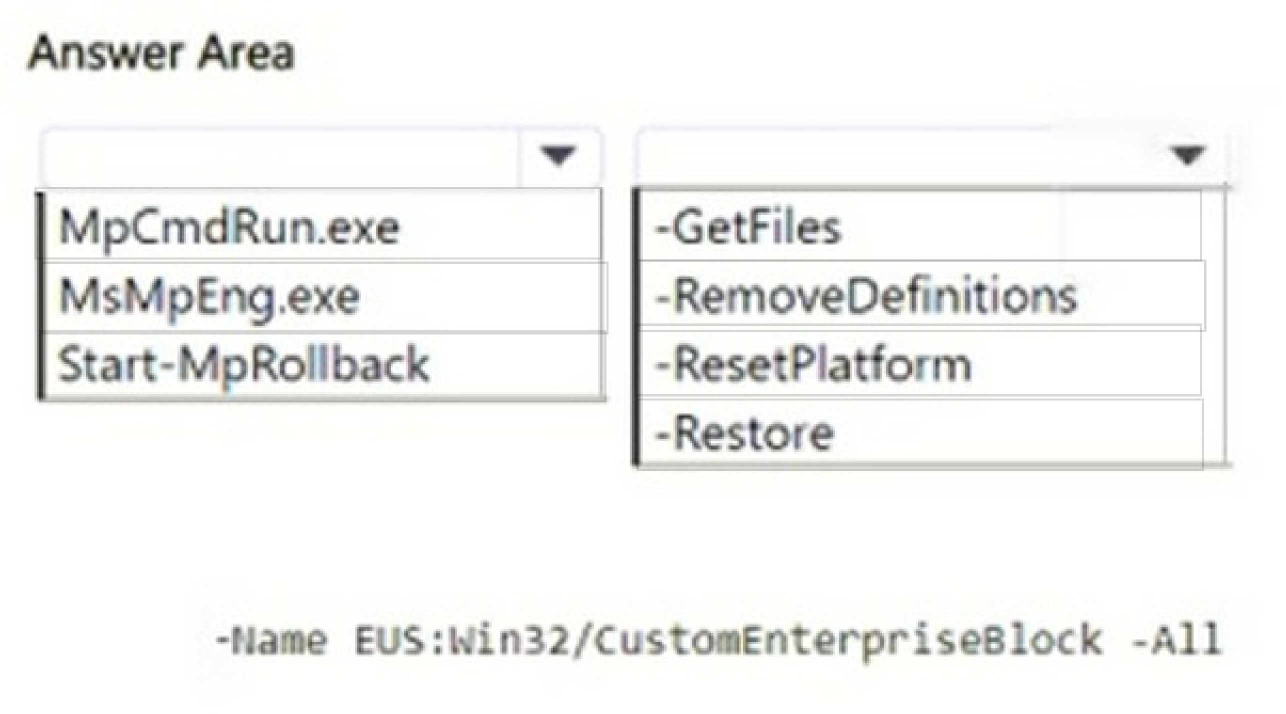
Twenty files on Device1 are quarantined by custom indicators as part of an investigation.

You need to release the 20 files from quarantine.

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

NOTE: Each correct selection is worth one point.

Hot Area:



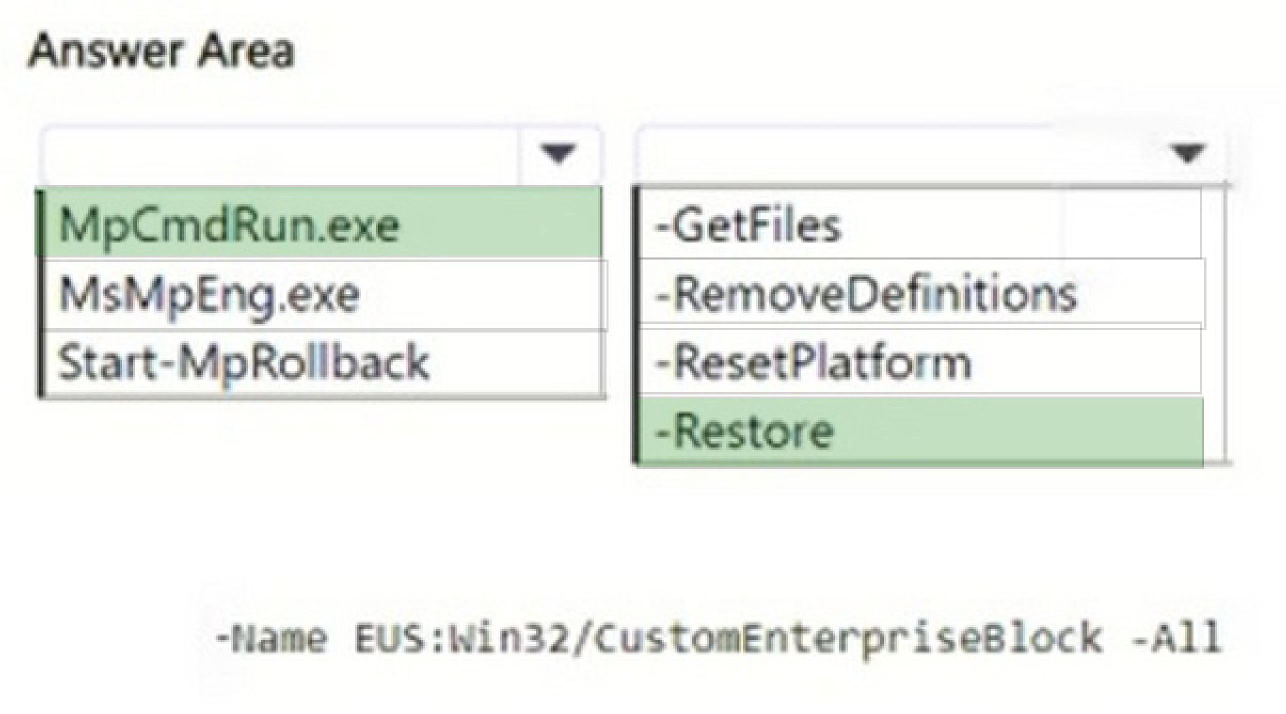
Answer Area

- MpCmdRun.exe
- MsMpEng.exe
- Start-MpRollback

- -GetFiles
- -RemoveDefinitions
- -ResetPlatform
- -Restore

```
-Name EUS:Win32/CustomEnterpriseBlock -All
```

Correct Answer:



Answer Area

- [✓ MpCmdRun.exe]
- MsMpEng.exe
- Start-MpRollback

- -GetFiles
- -RemoveDefinitions
- -ResetPlatform
- [✓ -Restore]

```
-Name EUS:Win32/CustomEnterpriseBlock -All
```

QUESTION 8

You have 50 Microsoft Sentinel workspaces.

You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.

Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents

B. Microsoft Sentinel - Workbooks

C. Microsoft Sentinel

D. Log Analytics workspaces

Correct Answer: A

When you open Microsoft Sentinel, you are presented with a list of all the workspaces to which you have access rights, across all selected tenants and subscriptions. To the left of each workspace name is a checkbox. Selecting the name of a single workspace will bring you into that workspace. To choose multiple workspaces, select all the corresponding checkboxes, and then select the View incidents button at the top of the page.

https://learn.microsoft.com/en-us/azure/sentinel/multiple-workspace-view

QUESTION 9

HOTSPOT

You have an Azure subscription that contains the following resources:

1.

A virtual machine named VM1 that runs Windows Server

2.

A Microsoft Sentinel workspace named Sentinel1 that has User and Entity Behavior Analytics (UEBA) enabled

You have a scheduled query rule named Rule1 that tracks sign-in attempts to VM1.

You need to update Rule1 to detect when a user from outside the IT department of your company signs in to VM1. The solution must meet the following requirements:

1.

Utilize UEBA results.

2.

Maximize query performance.

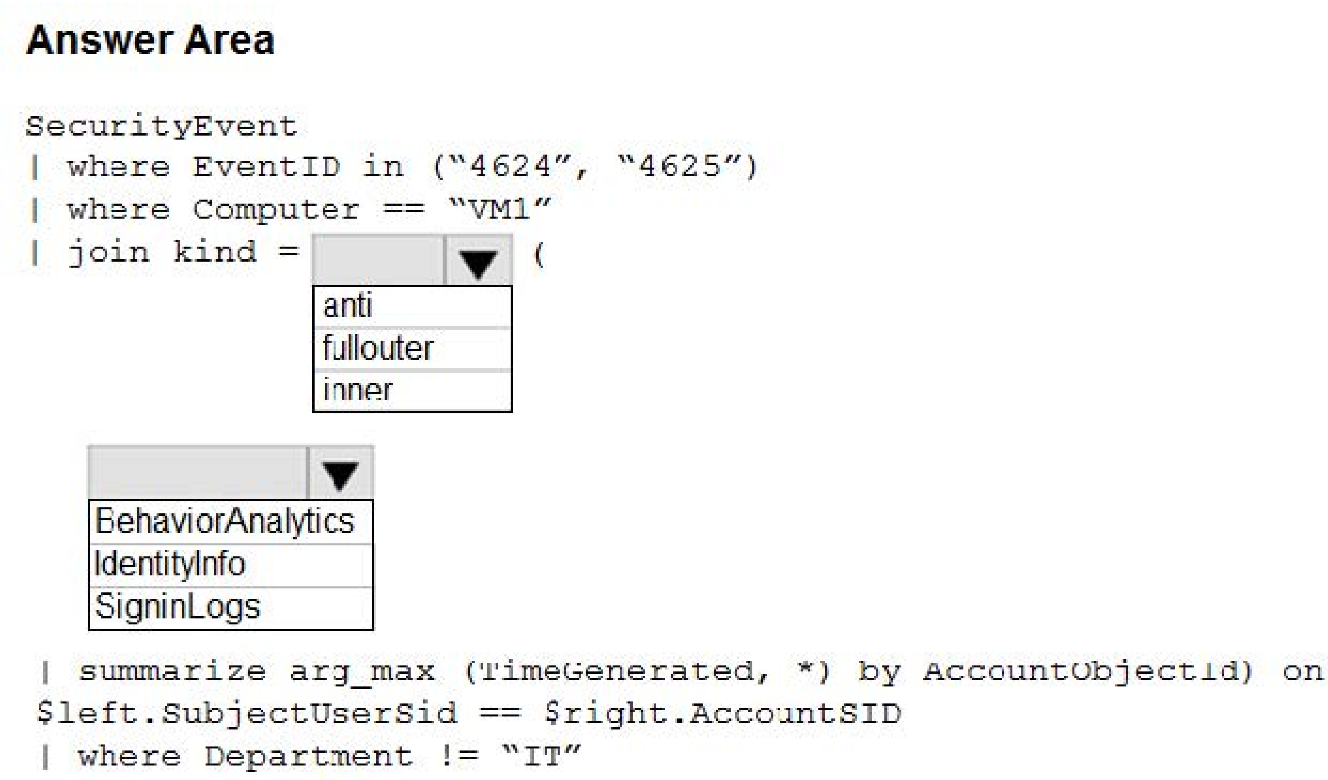
3.

Minimize the number of false positives.

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

NOTE: Each correct selection is worth one point.

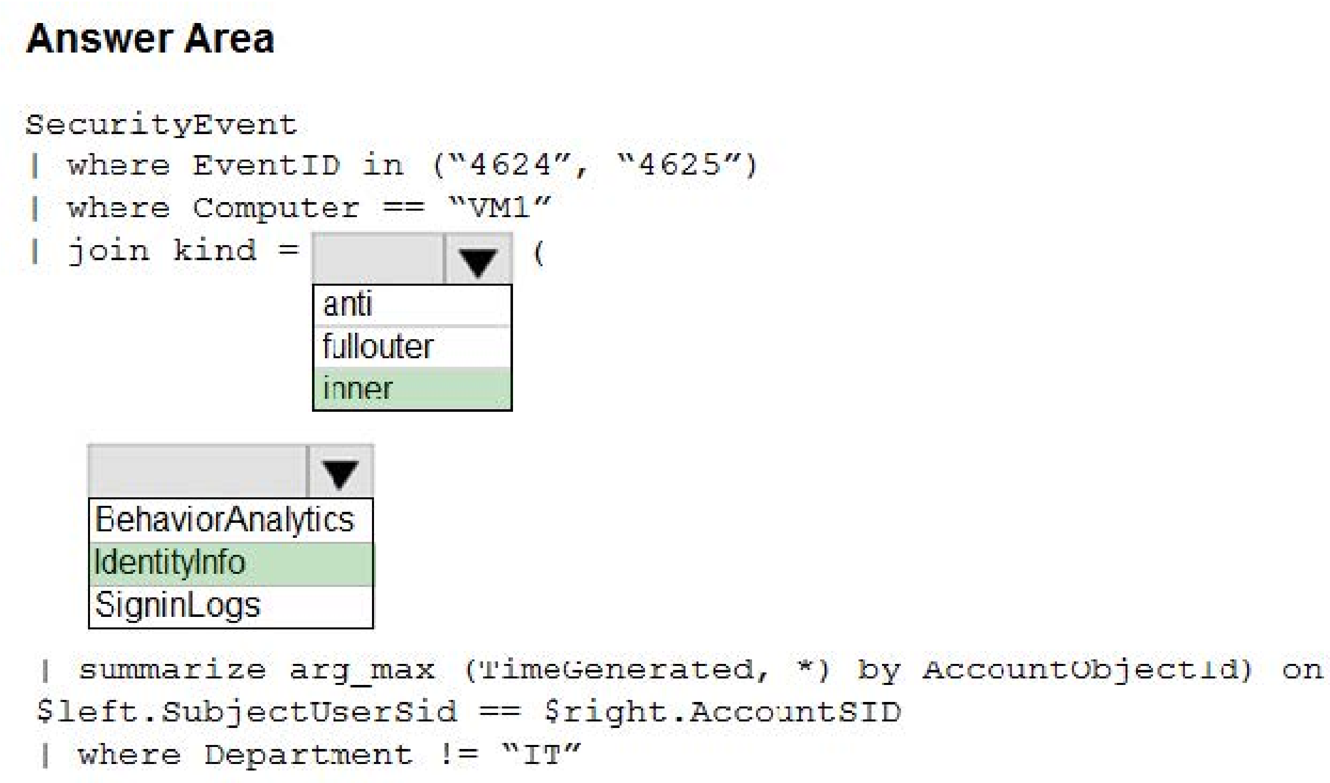
Hot Area:



```
SecurityEvent
| where EventID in (“4624”, “4625”)
| where Computer == “VM1”
| join kind =                (

| summarize arg_max (TimeGenerated, *) by AccountObjectId) on
$left.SubjectUserSid == $right.AccountSID
| where Department != “IT”
```

Correct Answer:



Answer Area

```
SecurityEvent
| where EventID in ("4624", "4625")
| where Computer == "VM1"
| join kind = [          ] (
    [          ]
 | summarize arg_max (TimeGenerated, *) by AccountObjectId) on
$left.SubjectUserSid == $right.AccountSID
 | where Department != "IT"
```

Box 1: inner

Use inner join to minimize false positives.

Example:

The following query resolves user and peer identifier fields:

UserPeerAnalytics

| where TimeGenerated > ago(24h)

// join to resolve user identifier fields

| join kind=inner (IdentityInfo | where TimeGenerated > ago(14d) | distinct AccountTenantId, AccountObjectId, AccountUPN, AccountDisplayName | extend UserPrincipalNameIdentityInfo = AccountUPN | extend UserNameIdentityInfo = AccountDisplayName | project AccountTenantId, AccountObjectId, UserPrincipalNameIdentityInfo, UserNameIdentityInfo

) on $left.AADTenantId == $right.AccountTenantId, $left.UserId == $right.AccountObjectId

Box 2: IdentityInfo

IdentityInfo table

After you enable UEBA for your Microsoft Sentinel workspace, data from your Azure Active Directory is synchronized to the IdentityInfo table in Log Analytics for use in Microsoft Sentinel. You can embed user data synchronized from your

Azure AD in your analytics rules to enhance your analytics to fit your use cases and reduce false positives.

The following table describes the user identity data included in the IdentityInfo table in Log Analytics.

AccountObjectId string

The Azure Active Directory object ID for the user account.

AccountSID string

The on-premises security identifier of the user account.

Etc.

Reference:

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-active-directory-identity-protection-user-account/ba-p/3695968

https://learn.microsoft.com/en-us/azure/sentinel/ueba-reference?source=recommendations#identityinfo-table

QUESTION 10

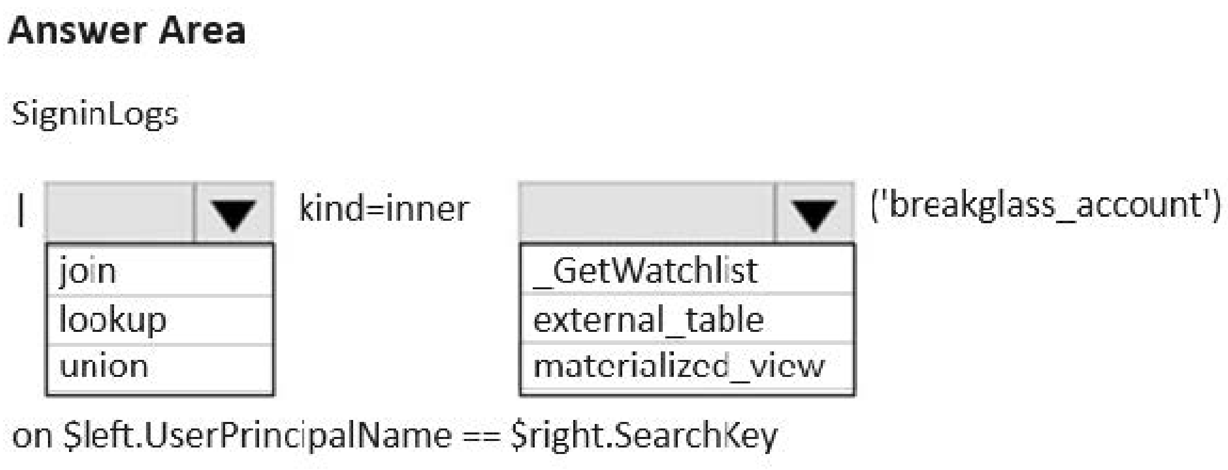
HOTSPOT

You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. 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.

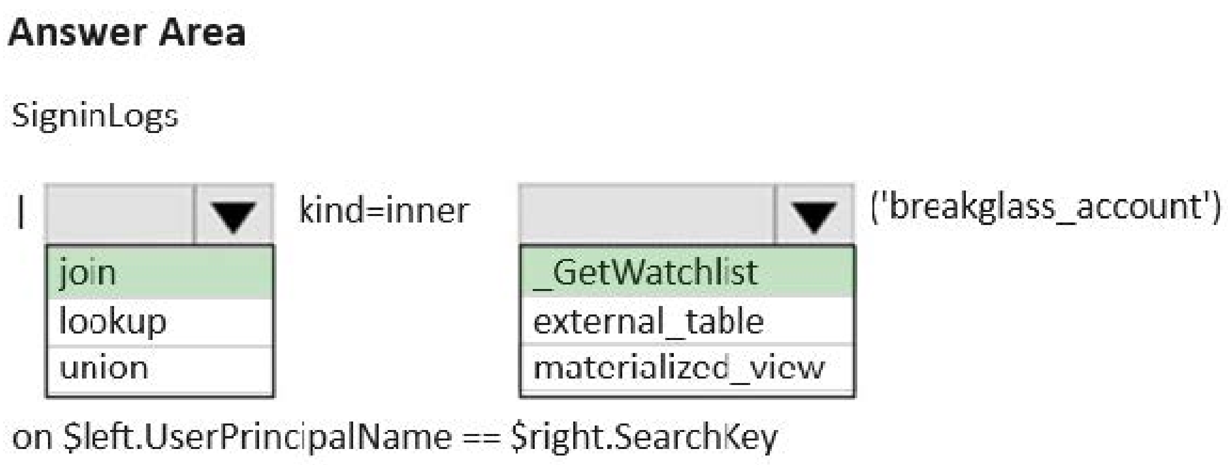
Hot Area:



Answer Area

```
SigninLogs
|            kind=inner            ('breakglass_account')
on $left.UserPrincipalName == $right.SearchKey
```

Correct Answer:



Answer Area

SigninLogs

| [✓ join] / lookup / union kind=inner [✓ _GetWatchlist] / external_table / materialized_view ('breakglass_account')

on $left.UserPrincipalName == $right.SearchKey

QUESTION 11

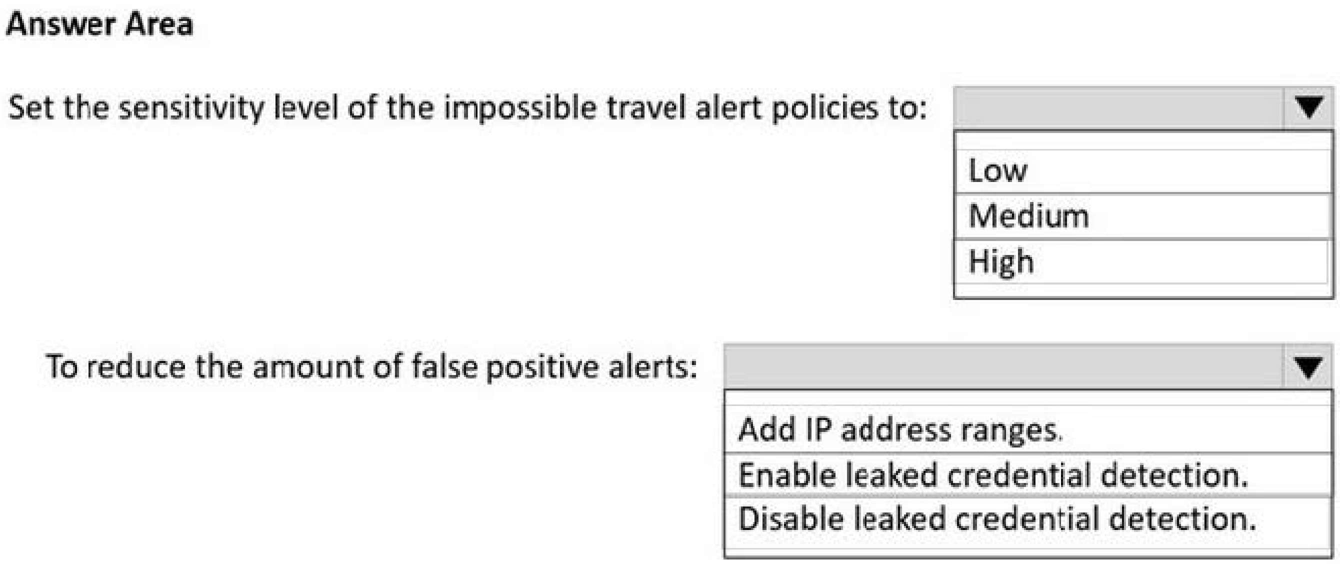
HOTSPOT

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.

Hot Area:

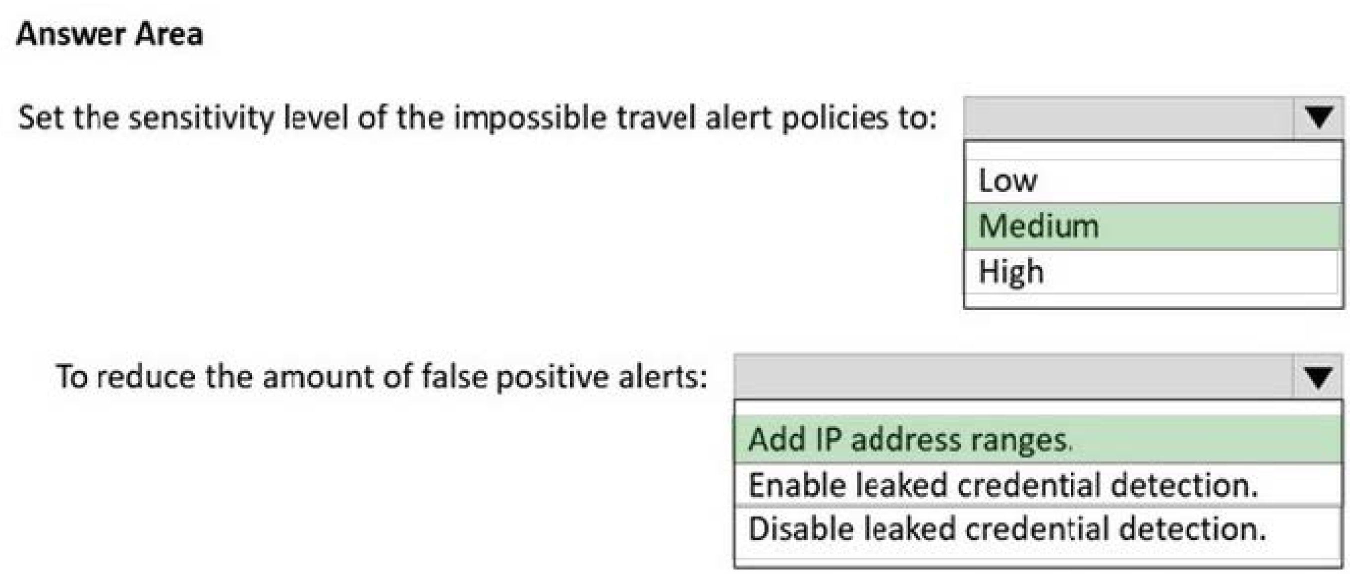


Answer Area

Set the sensitivity level of the impossible travel alert policies to:
- Low
- Medium
- High

To reduce the amount of false positive alerts:
- Add IP address ranges.
- Enable leaked credential detection.
- Disable leaked credential detection.

Correct Answer:



Answer Area

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

- Low
- [✓ Medium]
- High

To reduce the amount of false positive alerts: ▼

- [✓ Add IP address ranges.]
- Enable leaked credential detection.
- Disable leaked credential detection.

QUESTION 12

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

A. Azure Sentinel Contributor

B. Security Administrator

C. Azure Sentinel Responder

D. Logic App Contributor

Correct Answer: A

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION 13

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.

You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATTandCK tactic.

Which JSON key should you search?

A. Description

B. Intent

C. ExtendedProperies

D. Entities

Correct Answer: B

The "Intent" key is part of the JSON format used by Microsoft Defender for Cloud to transmit security alert data to third-party security information and event management (SIEM) solutions. The "Intent" key provides information on the type of attack or tactic that the alert is related to, and can be used to identify alerts that are specifically related to the Privilege Escalation tactic.