Exam Questions SC-200

Microsoft Security Operations Analyst

https://www.2passeasy.com/dumps/SC-200/

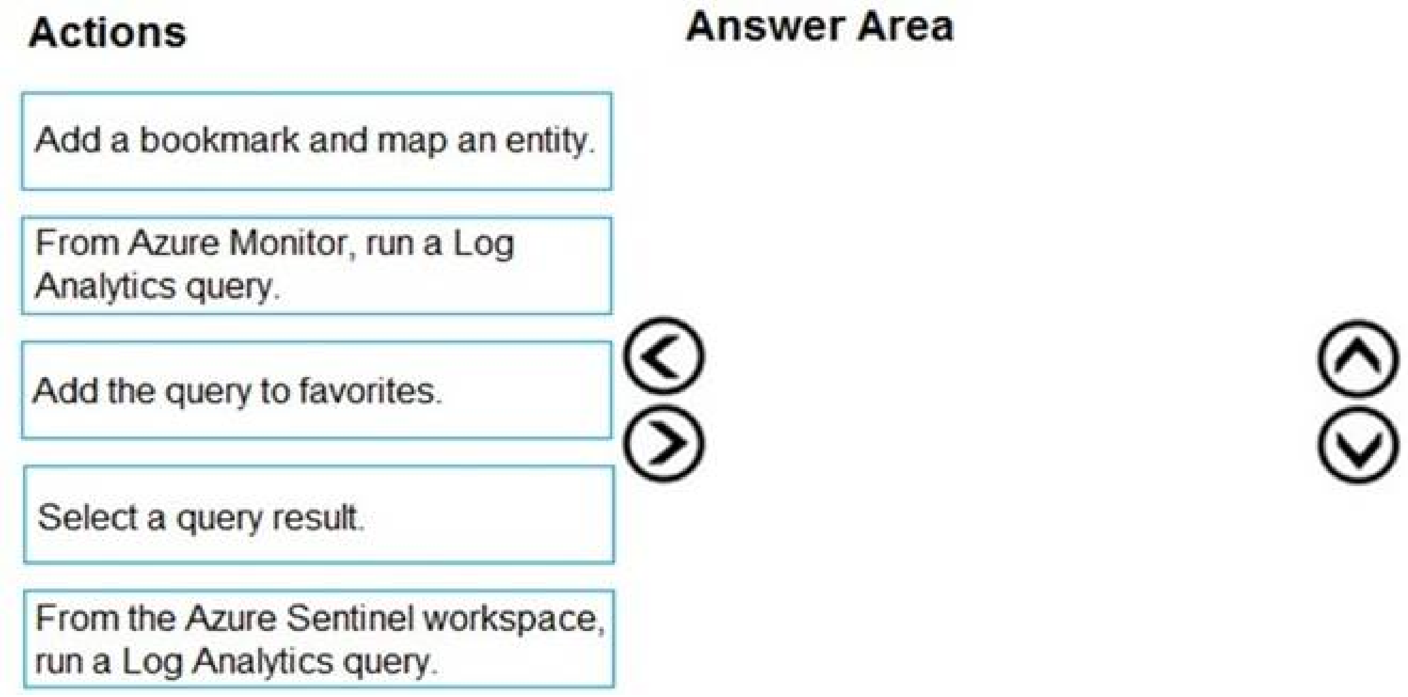
NEW QUESTION 1
- (Topic 1)
You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure FunctionsD Azure Sentinel livestreams

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

NEW QUESTION 2
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

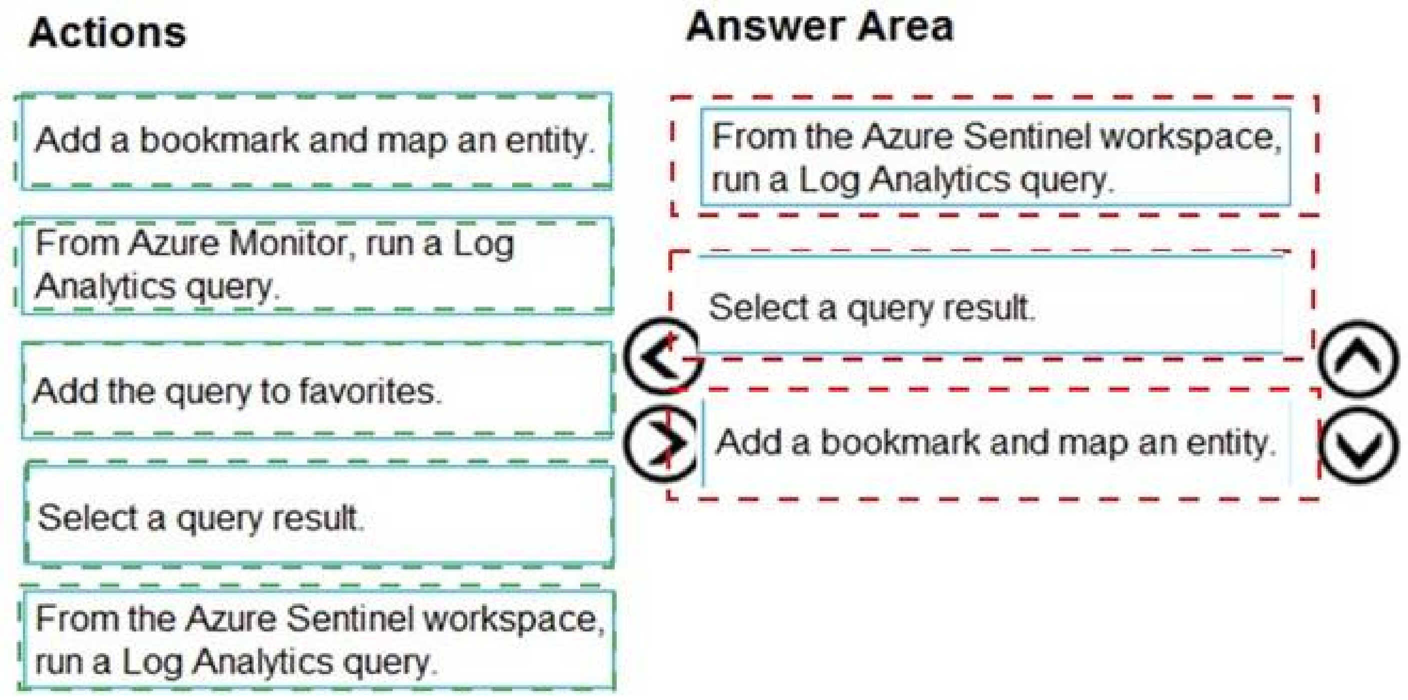
From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

From the Azure Sentinel workspace, run a Log Analytics query.

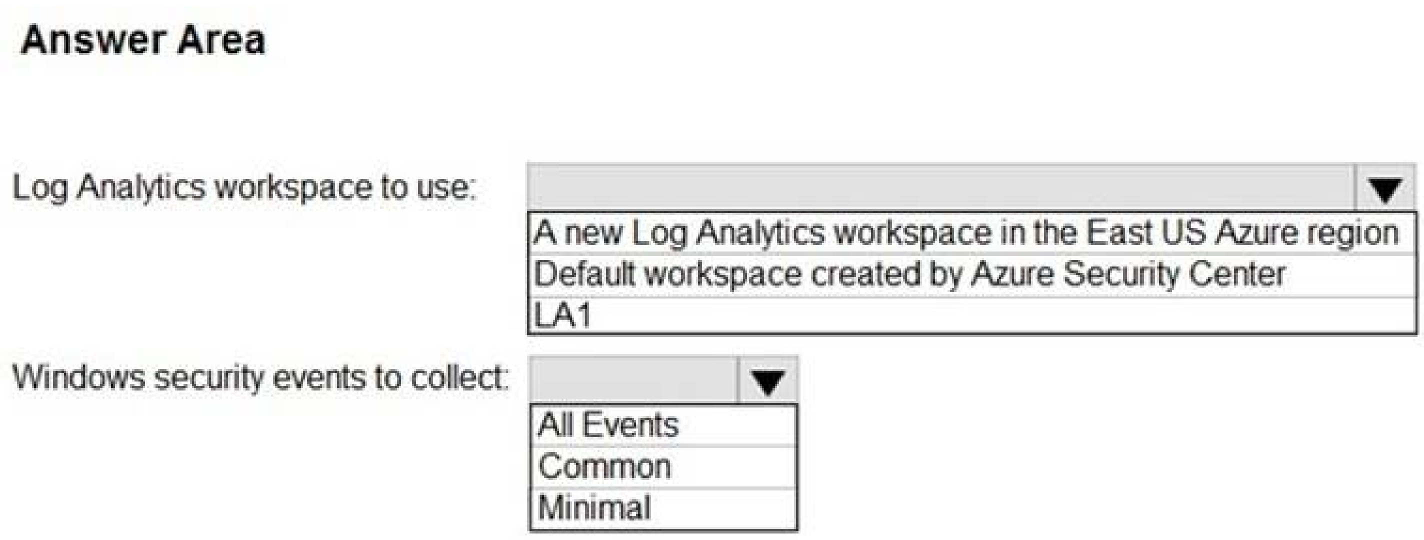
Answer Area

From the Azure Sentinel workspace, run a Log Analytics query.

Select a query result.

Add a bookmark and map an entity.

NEW QUESTION 3
HOTSPOT - (Topic 2)
You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. 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.



Answer Area

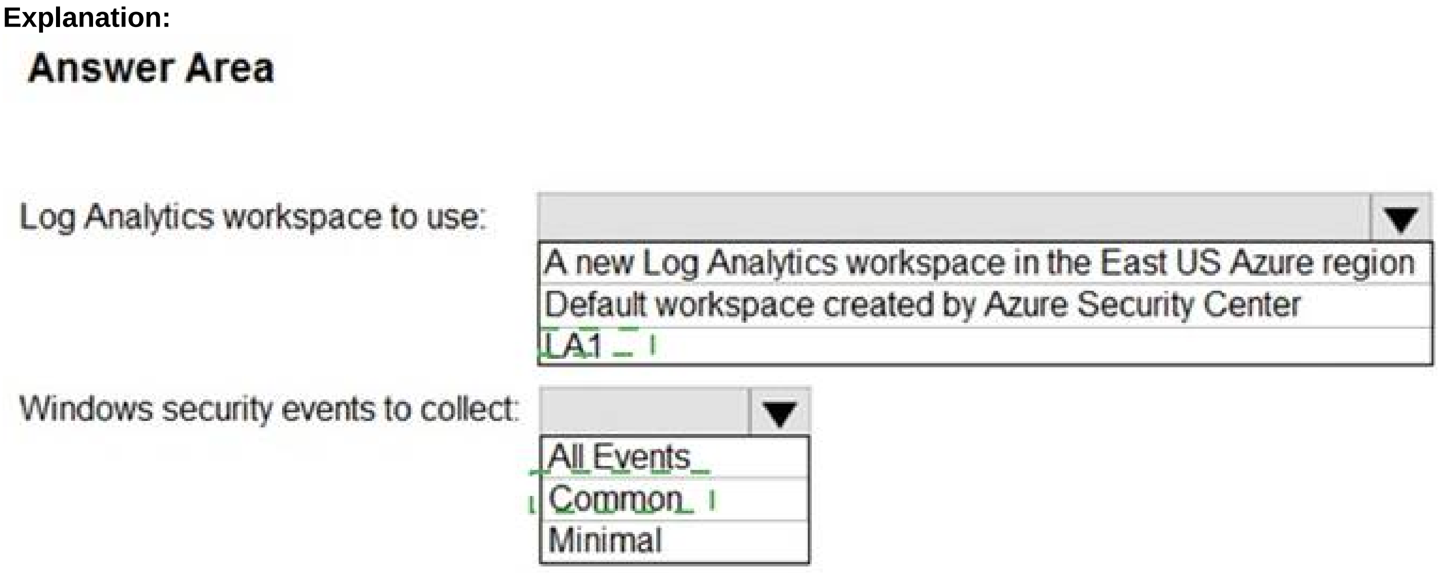
Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- LA1

Windows security events to collect:
- All Events
- Common
- Minimal

A. Mastered
B. Not Mastered

Answer: A

Explanation:

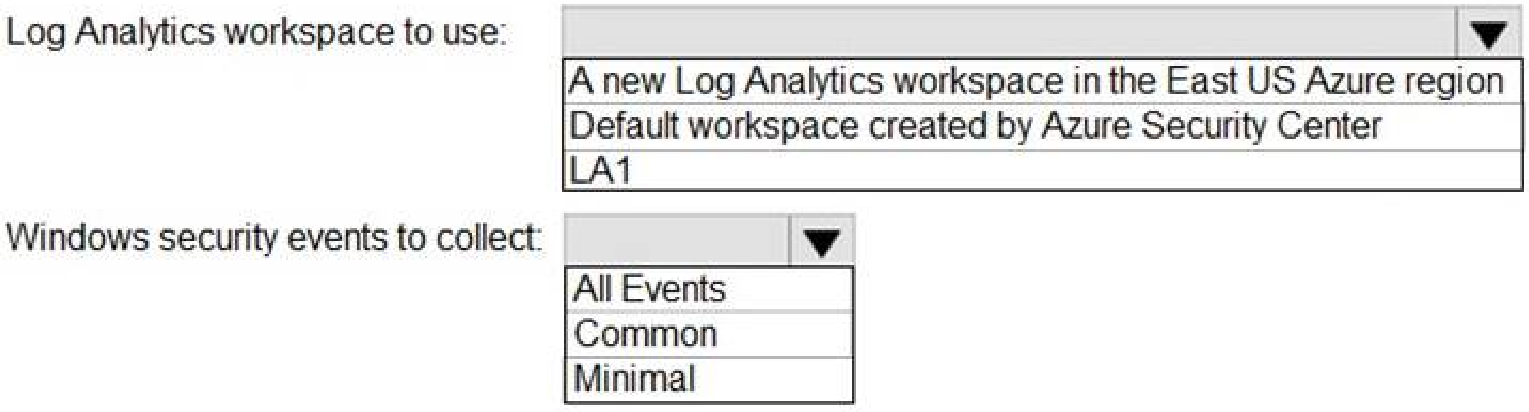


Answer Area

Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- [✓ LA1]

Windows security events to collect:
- All Events
- [✓ Common]
- Minimal

NEW QUESTION 4
HOTSPOT - (Topic 2)
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
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.



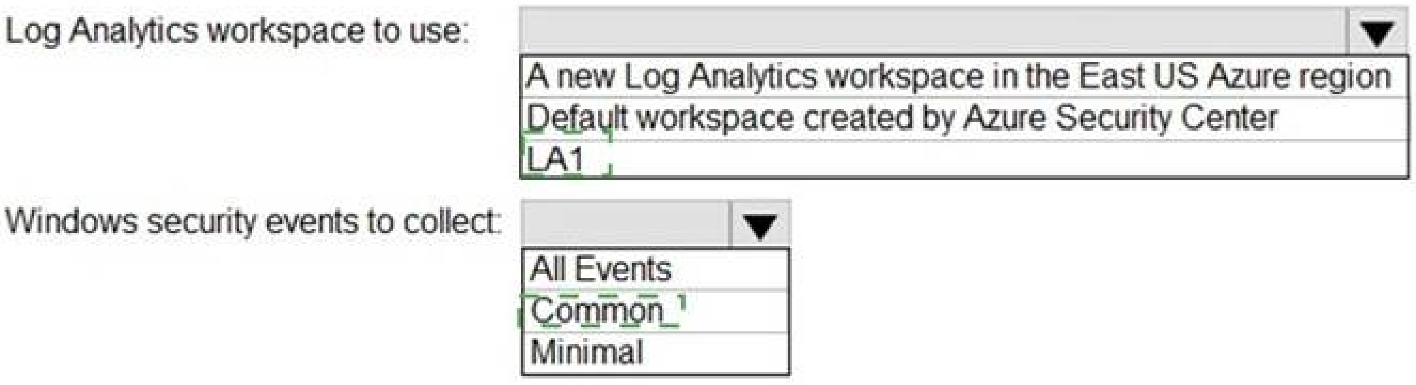
Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- LA1

Windows security events to collect:
- All Events
- Common
- Minimal

A. Mastered
B. Not Mastered

Answer: A

Explanation:

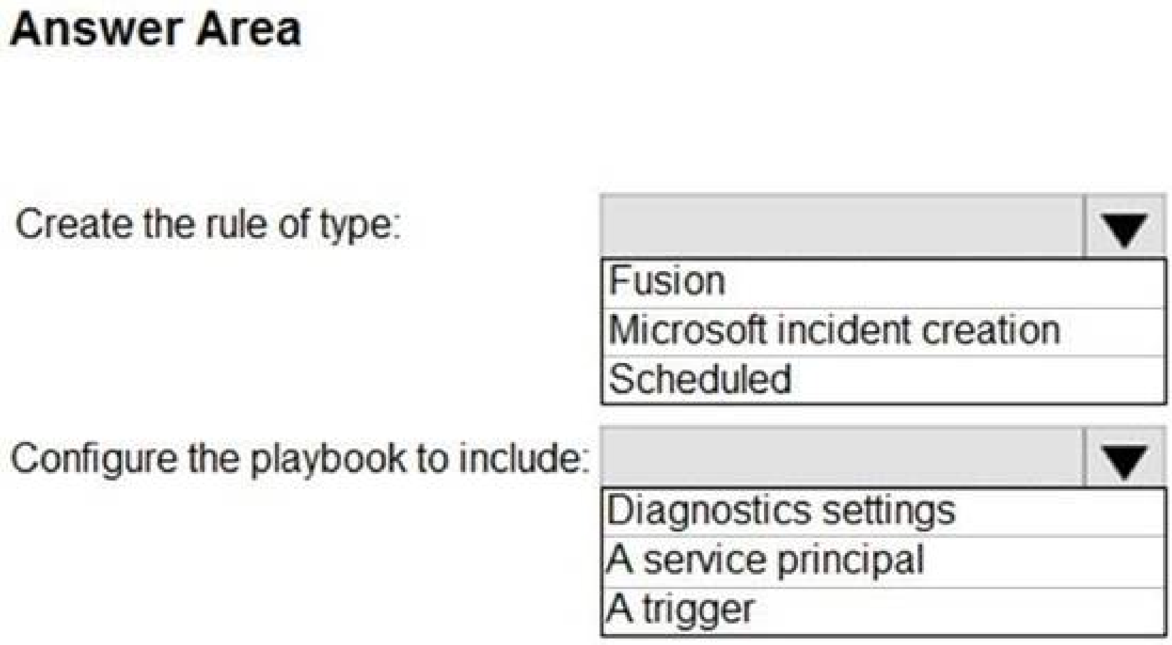


Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- [✓ LA1]

Windows security events to collect:
- All Events
- [✓ Common]
- Minimal

NEW QUESTION 5

HOTSPOT - (Topic 2)
You need to create the analytics rule to meet the Azure Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

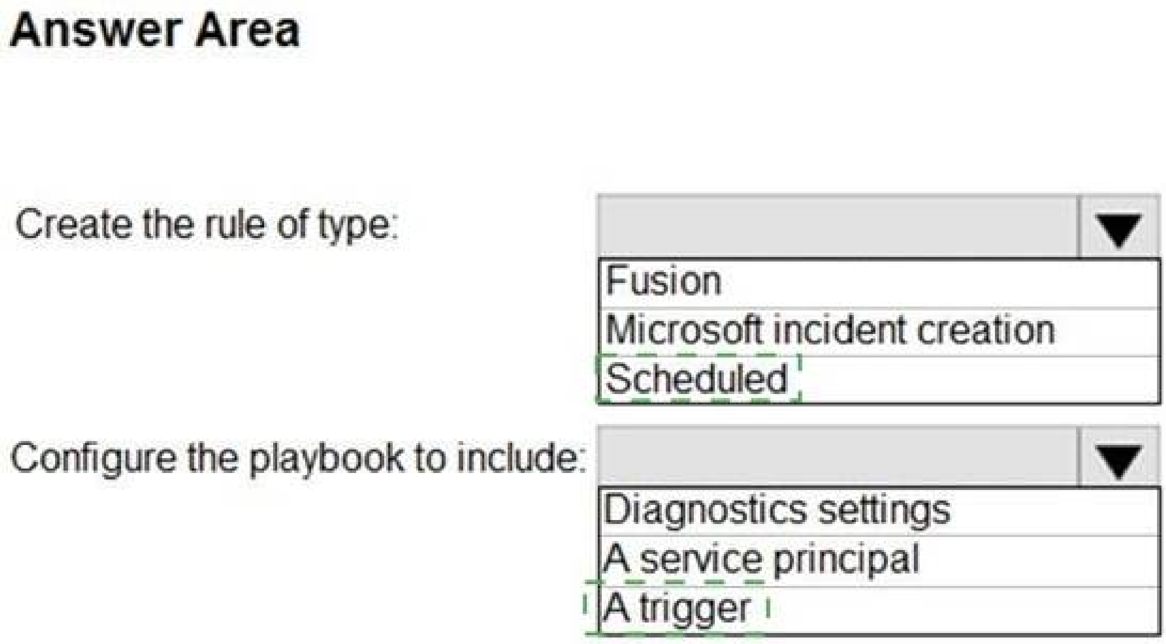
Create the rule of type:
- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include:
- Diagnostics settings
- A service principal
- A trigger

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Create the rule of type:
- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include:
- Diagnostics settings
- A service principal
- A trigger

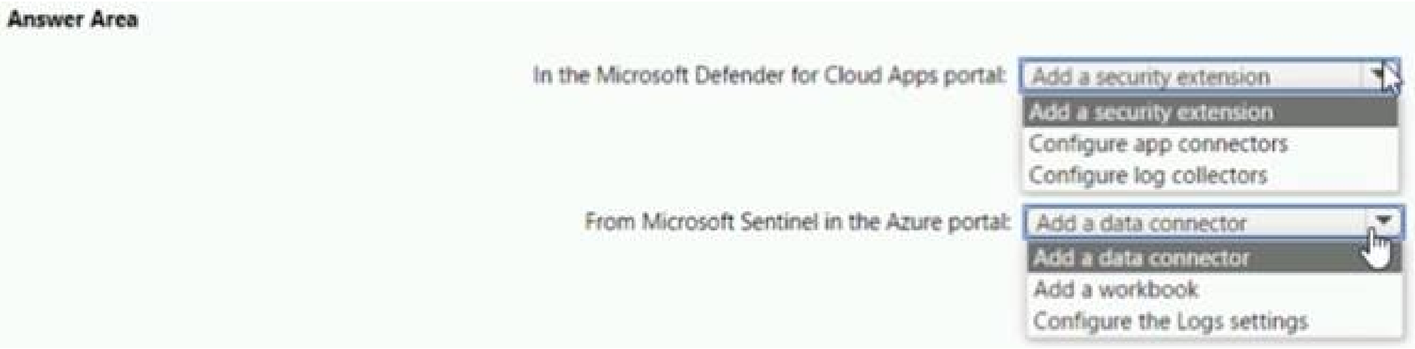
NEW QUESTION 6
- (Topic 2)
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center
B. Cloud App Security anomaly detection policies
C. Advanced features from Settings in Microsoft Defender Security Center
D. the Cloud Discovery settings in Cloud App Security

Answer: CD

Explanation:
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

NEW QUESTION 7
HOTSPOT - (Topic 2)
You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

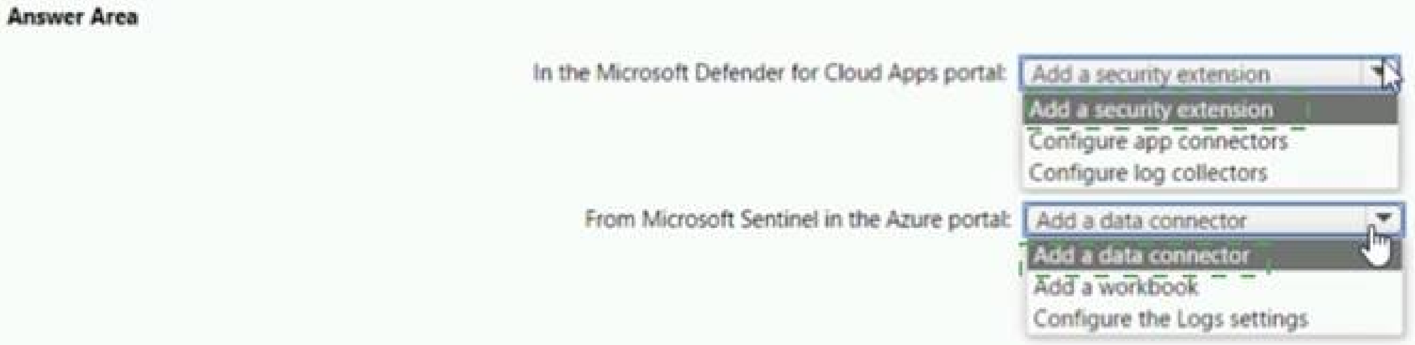
In the Microsoft Defender for Cloud Apps portal: Add a security extension
- Add a security extension
- Configure app connectors
- Configure log collectors

From Microsoft Sentinel in the Azure portal: Add a data connector
- Add a data connector
- Add a workbook
- Configure the Logs settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

In the Microsoft Defender for Cloud Apps portal: Add a security extension
- Add a security extension
- Configure app connectors
- Configure log collectors

From Microsoft Sentinel in the Azure portal: Add a data connector
- Add a data connector
- Add a workbook
- Configure the Logs settings

NEW QUESTION 8
- (Topic 2)
You need to implement the Azure Information Protection requirements. What should you configure first?

A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center

Answer: D

Explanation:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/information- protection-in-windows-overview

NEW QUESTION 9
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel
D. Risky sign-in

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

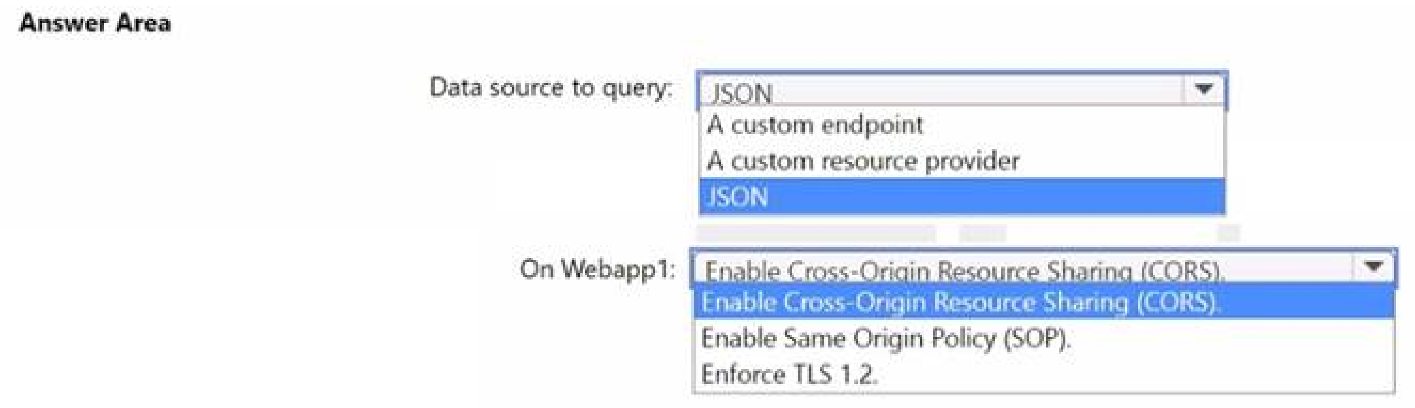
NEW QUESTION 10
- (Topic 2)
You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A. Automation Operator
B. Automation Runbook Operator
C. Azure Sentinel Contributor
D. Logic App Contributor

Answer: C

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

NEW QUESTION 10
HOTSPOT - (Topic 3)
You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query?
To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Data source to query: JSON

A custom endpoint
A custom resource provider
JSON

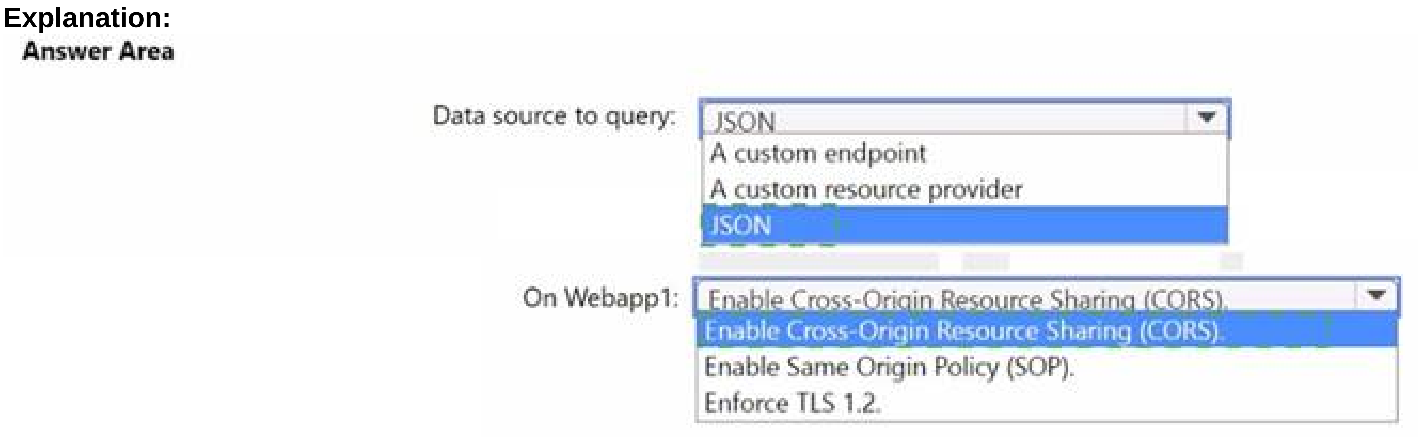
On Webapp1: Enable Cross-Origin Resource Sharing (CORS).

Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Data source to query: JSON

A custom endpoint
A custom resource provider
JSON

On Webapp1: Enable Cross-Origin Resource Sharing (CORS).

Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

NEW QUESTION 13
- (Topic 3)
You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.
What should you create first?

A. a playbook with an incident trigger
B. a playbook with an entity trigger
C. an Azure Automation rule
D. a playbook with an alert trigger

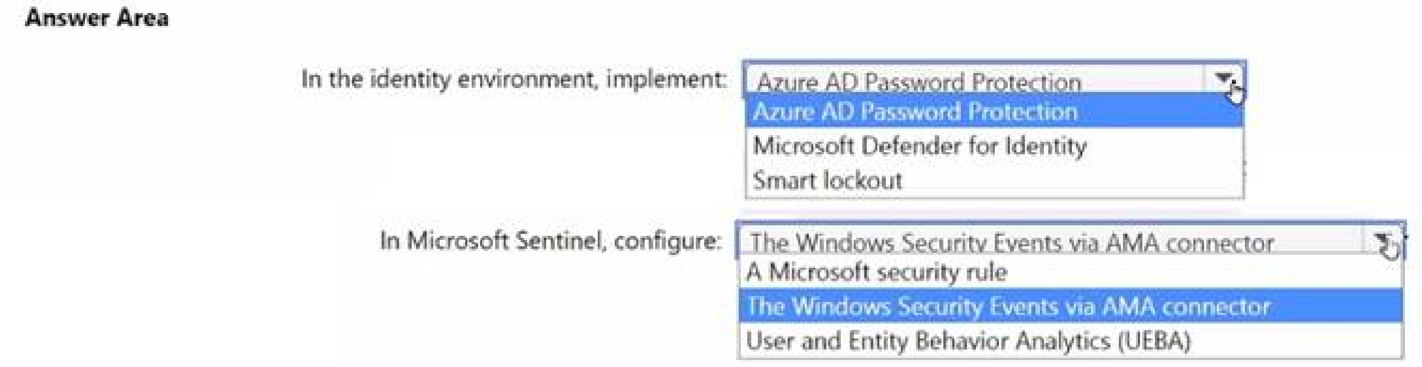
Answer: A

NEW QUESTION 14
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

A. entity mapping
B. custom details
C. event grouping
D. alert details

Answer: D

NEW QUESTION 17
HOTSPOT - (Topic 3)
You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

In the identity environment, implement: Azure AD Password Protection

Azure AD Password Protection
Microsoft Defender for Identity
Smart lockout

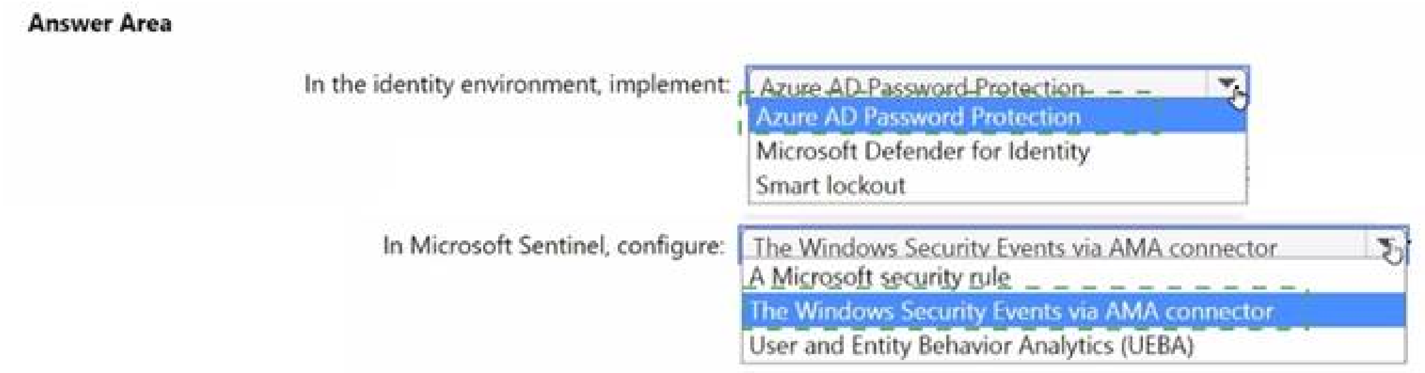
In Microsoft Sentinel, configure: The Windows Security Events via AMA connector

A Microsoft security rule
The Windows Security Events via AMA connector
User and Entity Behavior Analytics (UEBA)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

In the identity environment, implement: Azure AD Password Protection

Azure AD Password Protection
Microsoft Defender for Identity
Smart lockout

In Microsoft Sentinel, configure: The Windows Security Events via AMA connector

A Microsoft security rule
The Windows Security Events via AMA connector
User and Entity Behavior Analytics (UEBA)

NEW QUESTION 22
- (Topic 4)
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader

Answer: A

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

NEW QUESTION 24
- (Topic 4)
Your company uses Azure Security Center and Azure Defender.
The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

A. Security solutions
B. Security policy
C. Pricing & settings
D. Security alerts
E. Azure Defender

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security- contact-details

NEW QUESTION 29
- (Topic 4)
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.
B. The number of alerts exceeded 10,000 within two minutes.
C. The rule query takes too long to run and times out.
D. Permissions to one of the data sources of the rule query were modified.

Answer: D

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

NEW QUESTION 30
- (Topic 4)
You use Microsoft Sentinel.
You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point

A. Create a bookmark.
B. Create an analytics rule.
C. Create a livestream.
D. Create a hunting query.
E. Add a data connector.

Answer: DE

NEW QUESTION 32
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 hunting bookmark. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 33
- (Topic 4)
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

A. the Details tab of the alert
B. Management log
C. the Sensitive Info Types tab of the alert
D. the Events tab of the alert

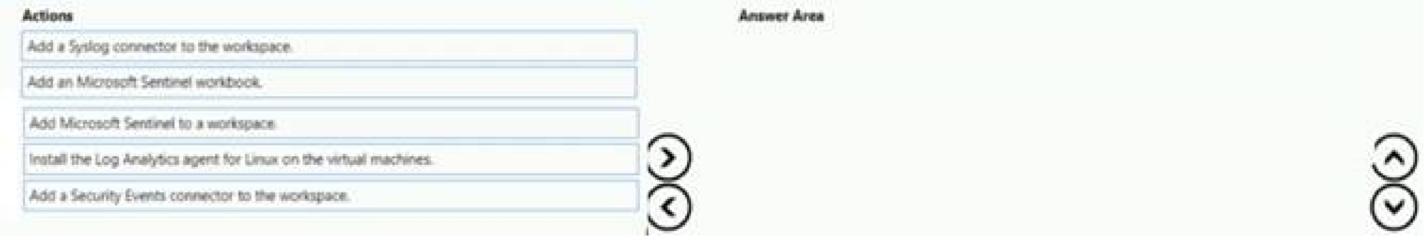
Answer: B

NEW QUESTION 37
- (Topic 4)
You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

A. Modify the properties of the connector.
B. Create a Data Collection Rule (DCR).
C. Create a scheduled query rule.
D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

NEW QUESTION 38
DRAG DROP - (Topic 4)
You have an Azure subscription that contains 100 Linux virtual machines.
You need to configure Microsoft Sentinel to collect event logs from the virtual machines. 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.



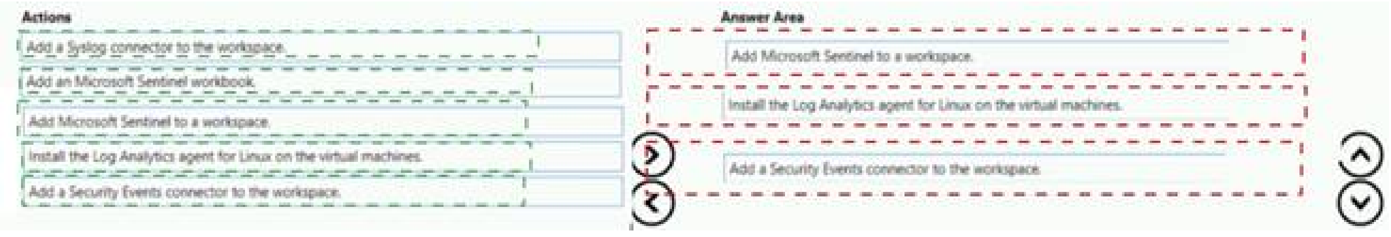
Actions
Add a Syslog connector to the workspace.
Add an Microsoft Sentinel workbook.
Add Microsoft Sentinel to a workspace.
Install the Log Analytics agent for Linux on the virtual machines.
Add a Security Events connector to the workspace.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions
Add a Syslog connector to the workspace.
Add an Microsoft Sentinel workbook.
Add Microsoft Sentinel to a workspace.
Install the Log Analytics agent for Linux on the virtual machines.
Add a Security Events connector to the workspace.

Answer Area
Add Microsoft Sentinel to a workspace.
Install the Log Analytics agent for Linux on the virtual machines.
Add a Security Events connector to the workspace.

NEW QUESTION 41
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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

Answer: B

Explanation:

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

NEW QUESTION 43
- (Topic 4)
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.

Answer: B

Explanation:

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

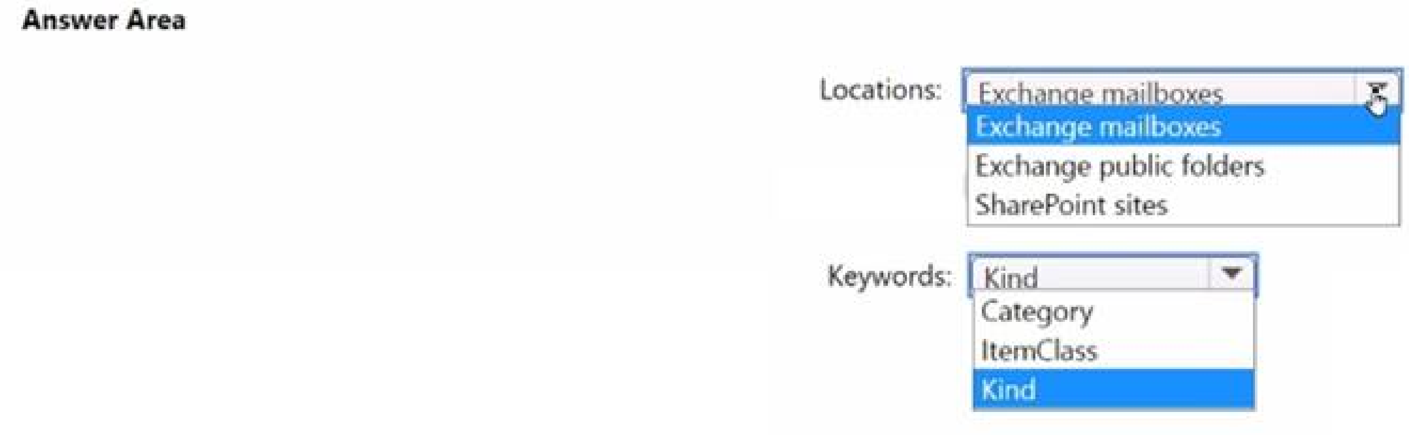
NEW QUESTION 46
- (Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.
What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365
B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

Answer: A

Explanation:
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

NEW QUESTION 51
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.
How should you configure the content search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

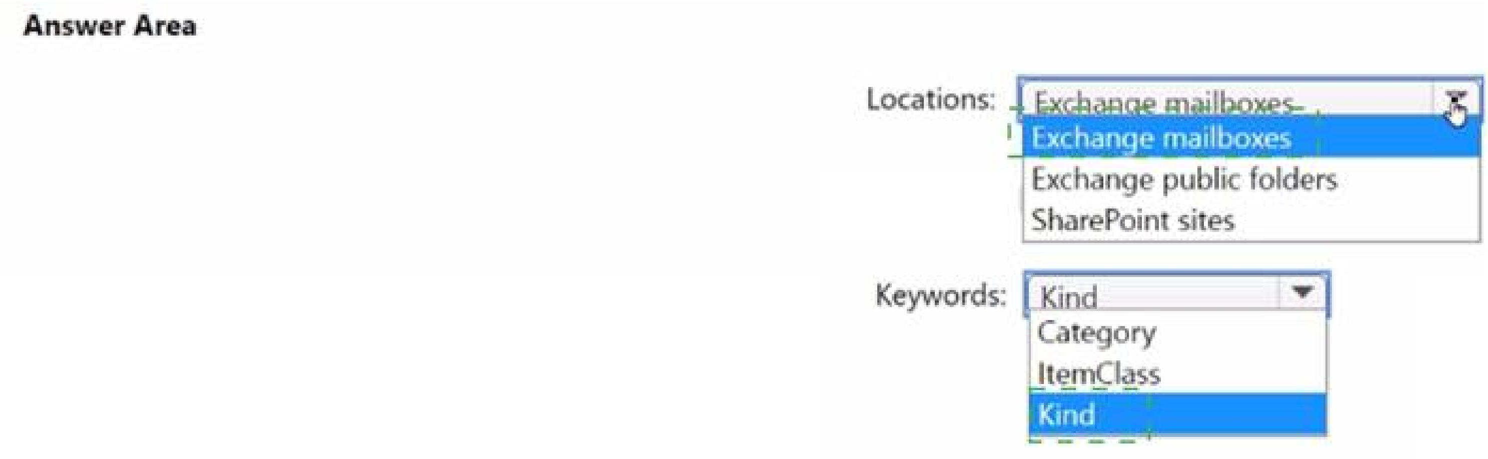
Locations: Exchange mailboxes

Keywords: Kind

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

Locations: Exchange mailboxes

Keywords: Kind

NEW QUESTION 52
- (Topic 4)
You have the following environment:
? Azure Sentinel
? A Microsoft 365 subscription
? Microsoft Defender for Identity
? An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.
D. Configure Windows Event Forwarding on the domain controllers.

Answer: AD

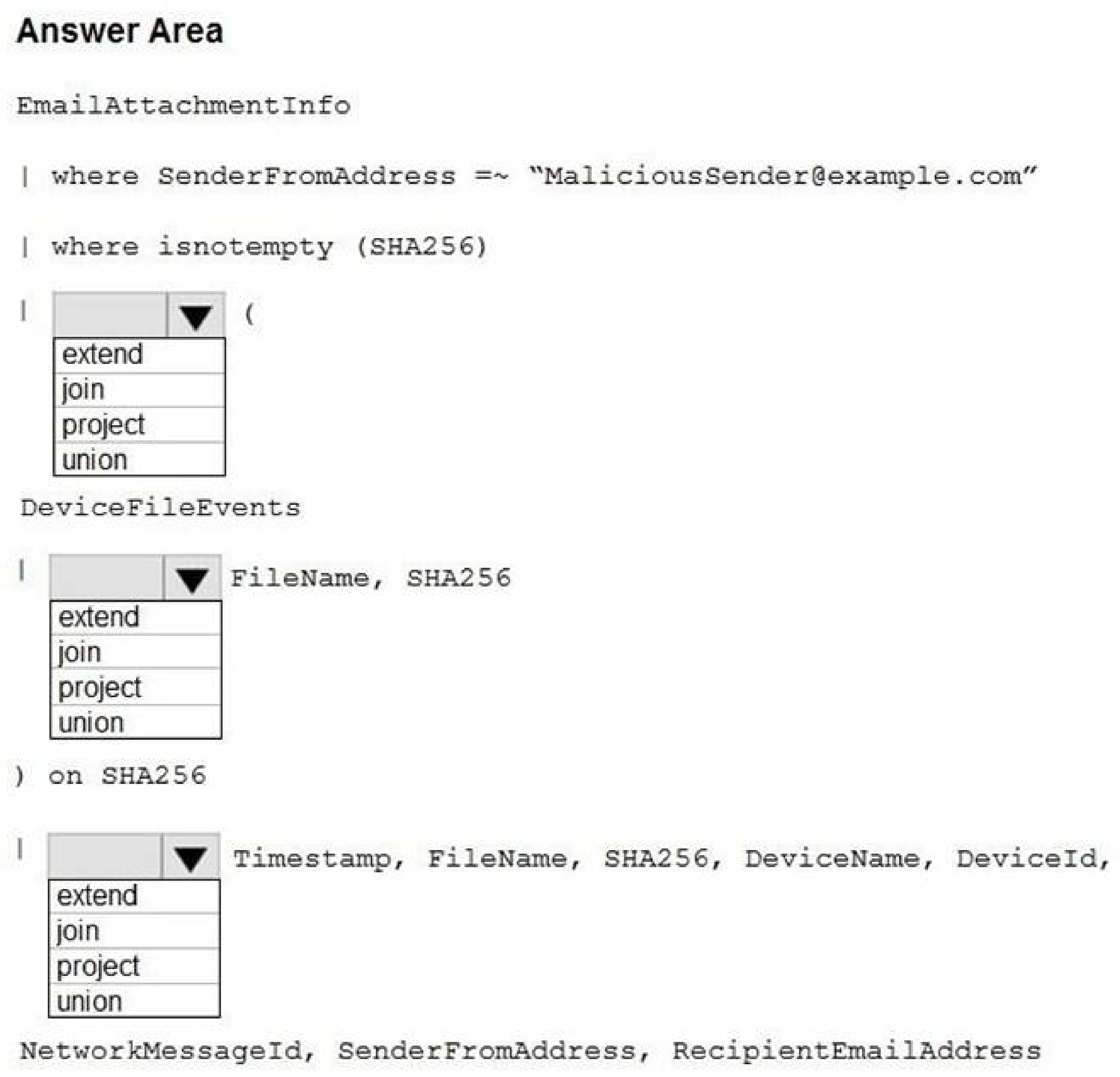
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

NEW QUESTION 56
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

A. From Defender for Cloud, enable agentless scanning.
B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
C. Onboard the virtual machines to Microsoft Defender for Endpoint.
D. From Defender for Cloud, configure auto-provisioning.
E. From Defender for Cloud, configure the AWS connector.

Answer: BC

NEW QUESTION 61
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



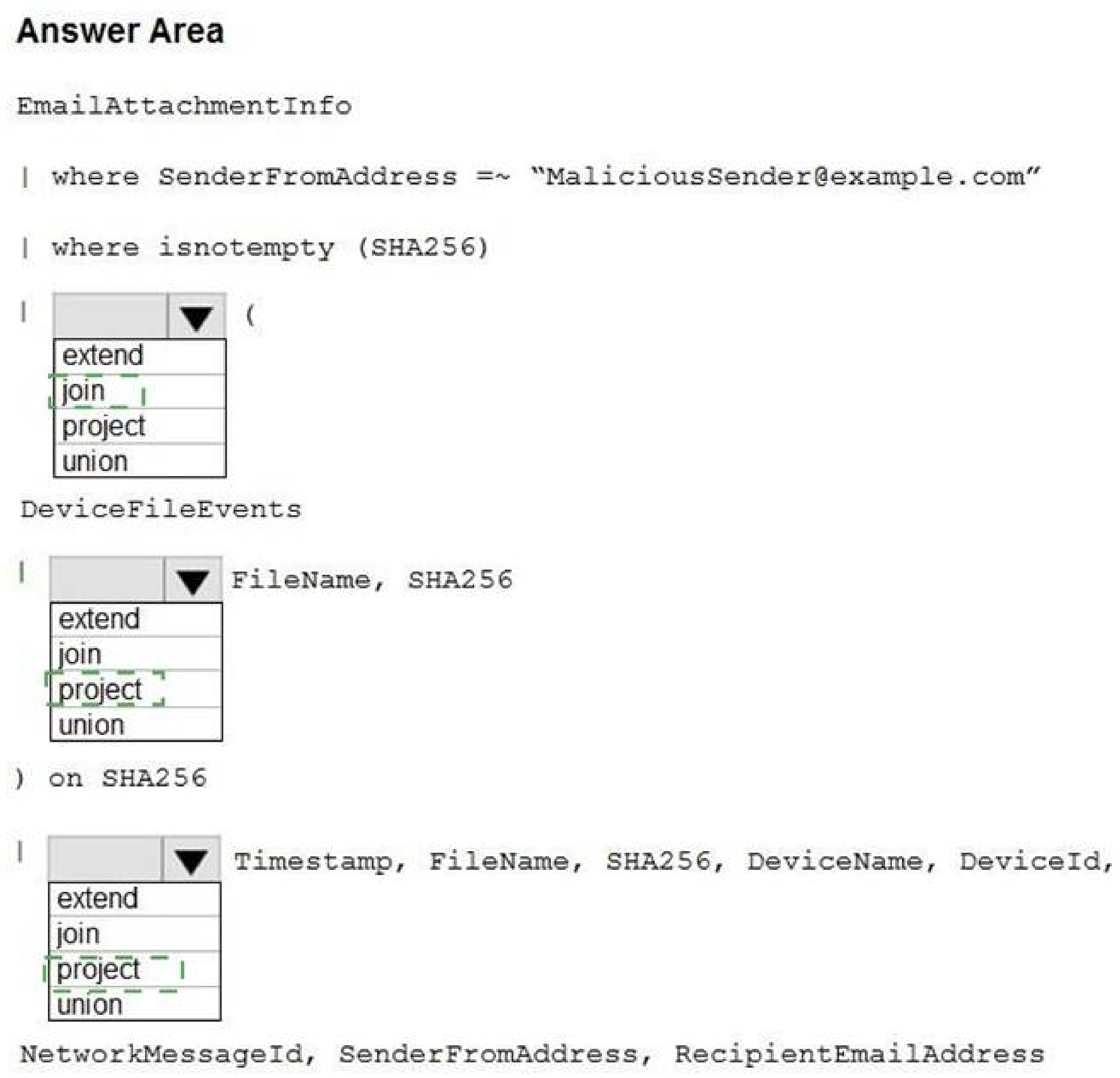
Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [▼] (
DeviceFileEvents
| [▼] FileName, SHA256
) on SHA256
| [▼] Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

A. Mastered
B. Not Mastered

Answer: A

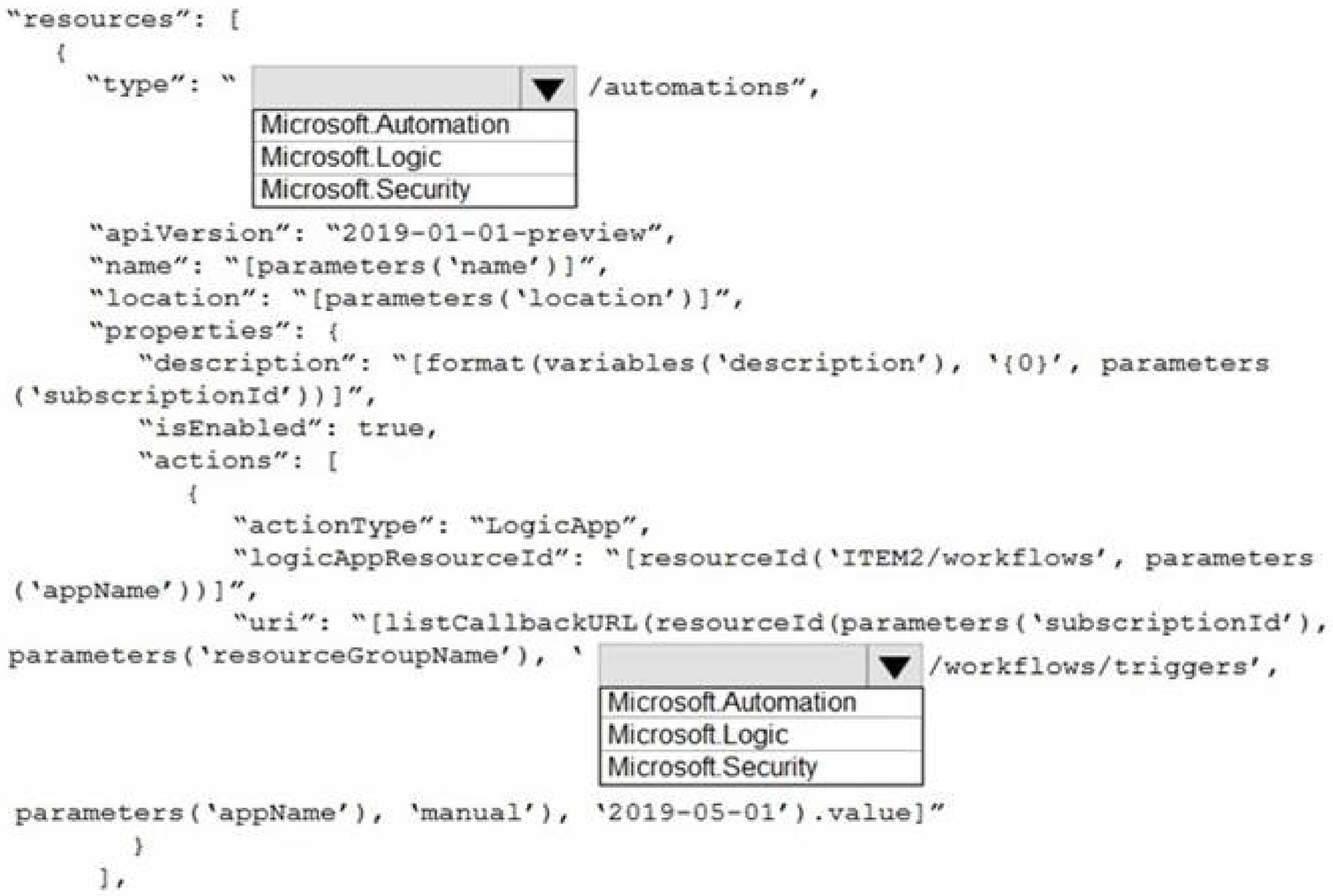
Explanation:



Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [extend / [✓ join] / project / union] (
DeviceFileEvents
| [extend / join / [✓ project] / union] FileName, SHA256
) on SHA256
| [extend / join / [✓ project] / union] Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

NEW QUESTION 65
HOTSPOT - (Topic 4)
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

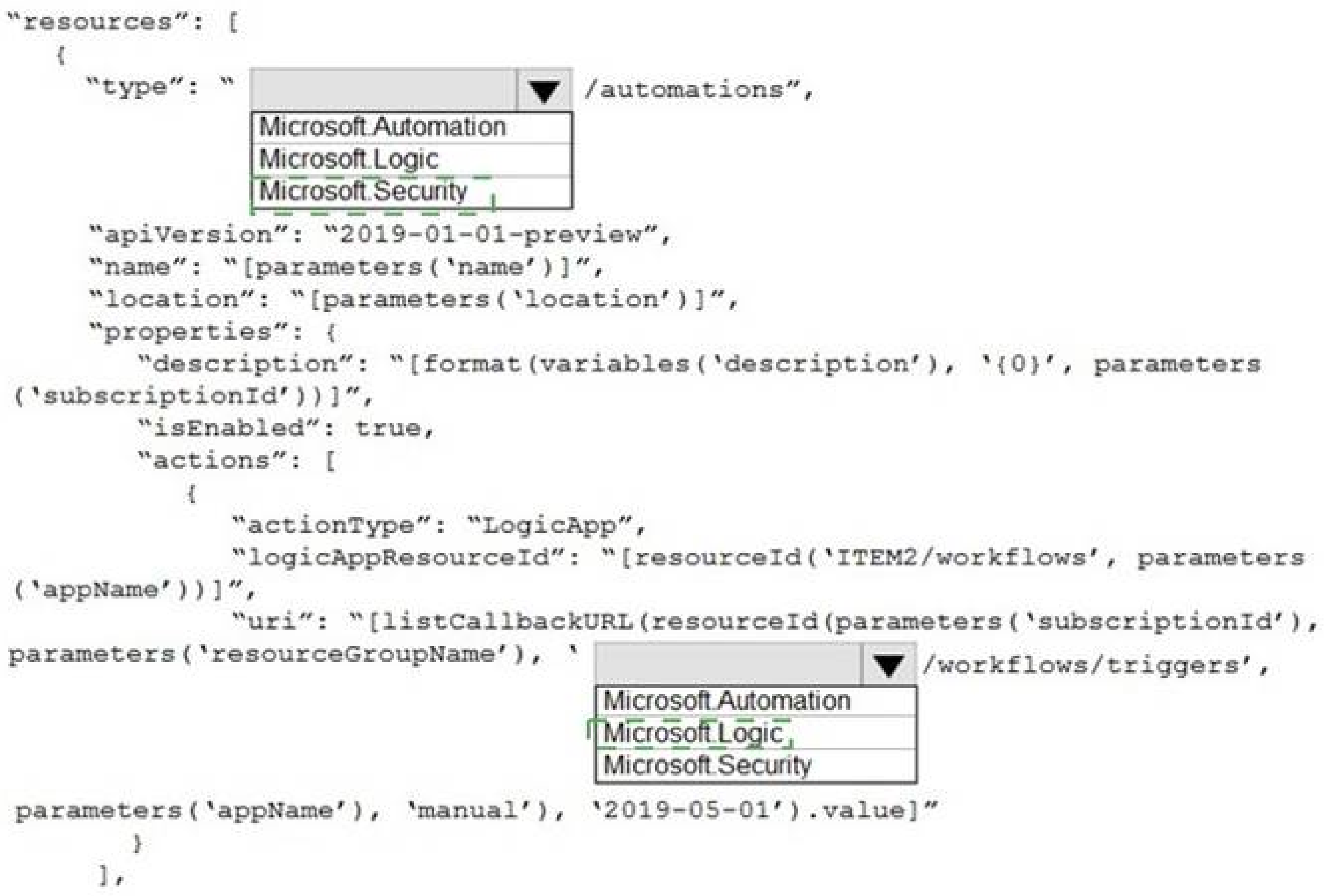


```
"resources": [
   {
    "type": "  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security] /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
               "actionType": "LogicApp",
               "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
               "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), ' [Microsoft.Automation / Microsoft.Logic / Microsoft.Security] /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
        ],
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



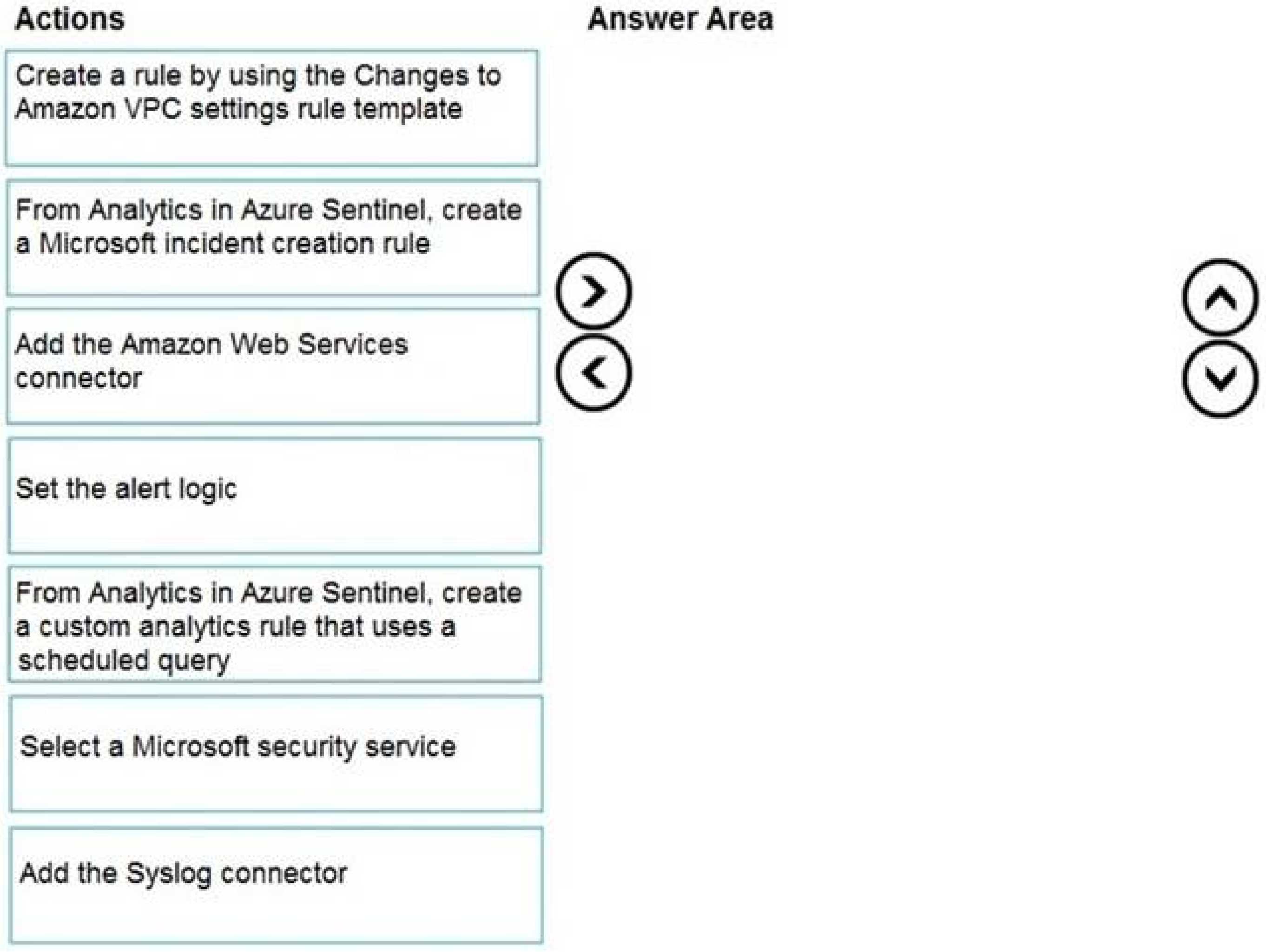
```
"resources": [
   {
     "type": "  ▼ /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('name')]",
      "location": "[parameters('location')]",
      "properties": {
         "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
         "isEnabled": true,
         "actions": [
            {
               "actionType": "LogicApp",
               "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
               "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '  ▼ /workflows/triggers',
                                    Microsoft.Automation
                                    Microsoft.Logic
                                    Microsoft.Security
 parameters('appName'), 'manual'), '2019-05-01').value]"
         }
      ],
```

NEW QUESTION 68
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You have a GitHub account named Account1 that contains 10 repositories.
You need to ensure that Defender for Cloud can assess the repositories in Account1. What should you do first in the Microsoft Defender for Cloud portal?

A. Add an environment.
B. Enable security policies.
C. Enable integrations.
D. Enable a plan.

Answer: A

NEW QUESTION 69
DRAG DROP - (Topic 4)
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.
a Microsoft 365 E5



Actions

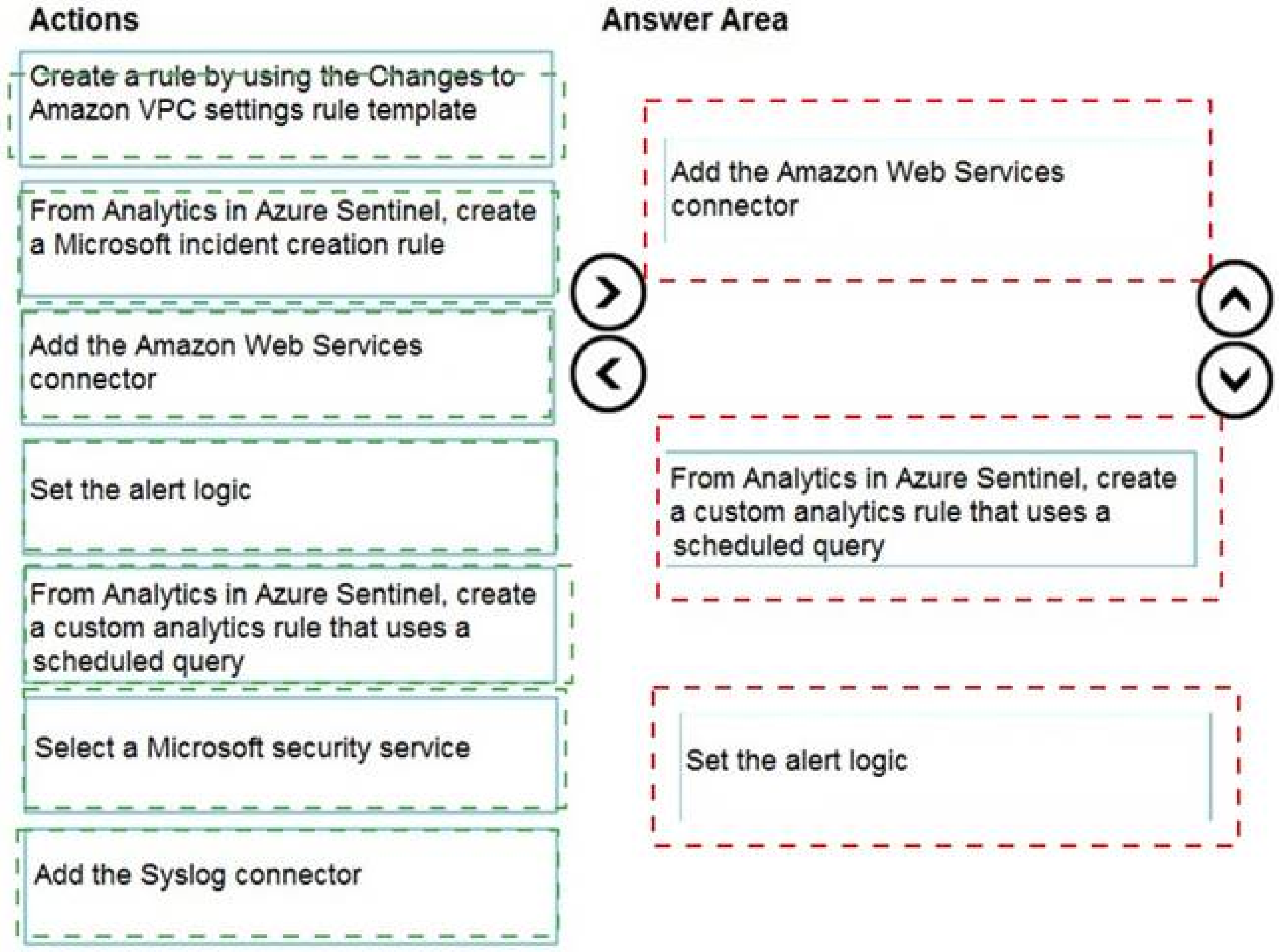
- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

1. Add the Amazon Web Services connector
2. From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
3. Set the alert logic

NEW QUESTION 74
- (Topic 4)
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?

A. notebooks in Azure Sentinel
B. Microsoft Cloud App Security
C. Azure Monitor
D. hunting queries in Azure Sentinel

Answer: A

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

NEW QUESTION 76
- (Topic 4)
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

A. Impossible travel
B. Activity from anonymous IP addresses
C. Activity from infrequent country
D. Malware detection

Answer: C

Explanation:
Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION 80
- (Topic 4)
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook
B. a notebook
C. a livestream
D. a bookmark

Answer: C

Explanation:
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

NEW QUESTION 85
- (Topic 4)
You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

A. the status update time
B. the alert status
C. the certainty of the source computer
D. the resolution method of the source computer

Answer: B

NEW QUESTION 88
- (Topic 4)
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.

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

Answer: AB

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

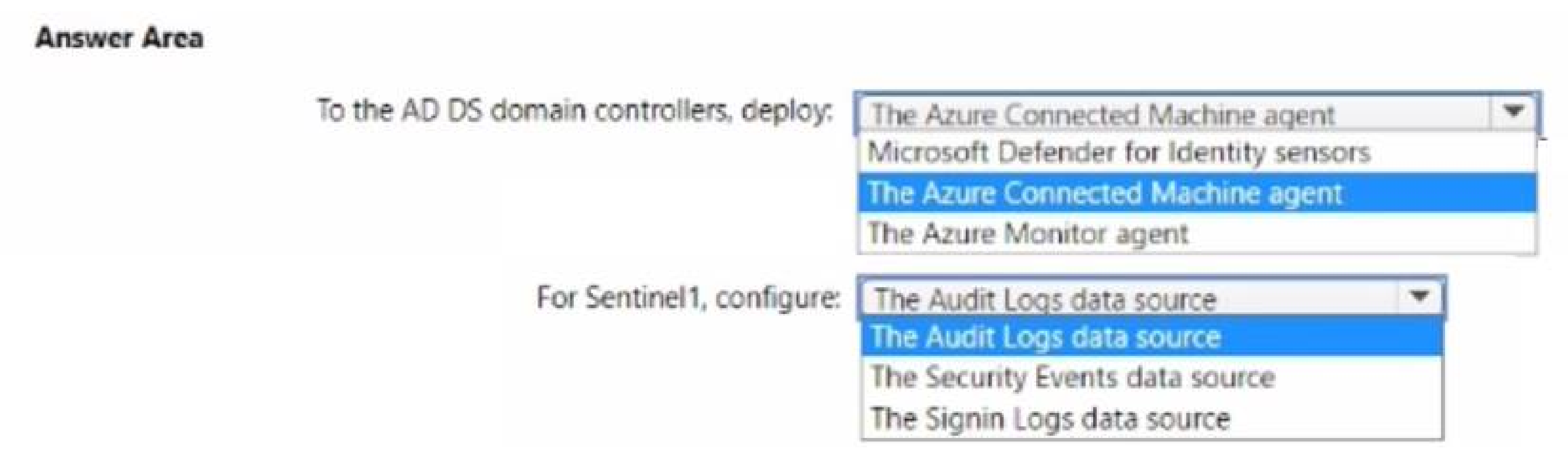
NEW QUESTION 91
- (Topic 4)
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?

A. extend
B. bin
C. count
D. workspace

Answer: B

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

NEW QUESTION 94
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

To the AD DS domain controllers, deploy: The Azure Connected Machine agent

- Microsoft Defender for Identity sensors
- [✓ The Azure Connected Machine agent]
- The Azure Monitor agent

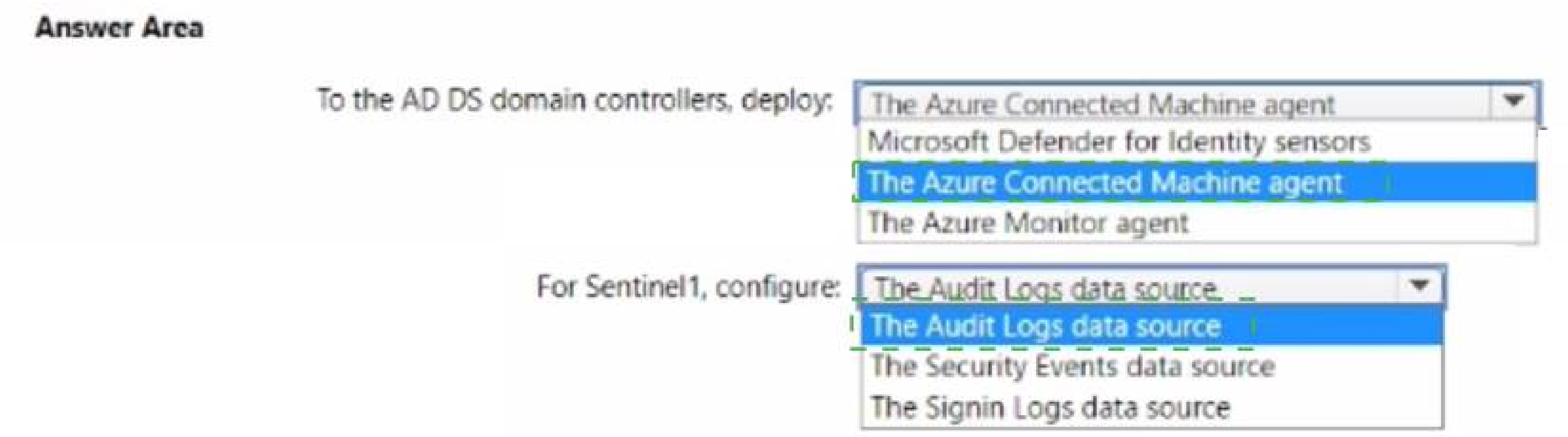
For Sentinel1, configure: The Audit Logs data source

- [✓ The Audit Logs data source]
- The Security Events data source
- The Signin Logs data source

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

To the AD DS domain controllers, deploy: The Azure Connected Machine agent

- Microsoft Defender for Identity sensors
- [✓ The Azure Connected Machine agent]
- The Azure Monitor agent

For Sentinel1, configure: The Audit Logs data source

- [✓ The Audit Logs data source]
- The Security Events data source
- The Signin Logs data source

NEW QUESTION 96

HOTSPOT - (Topic 4)

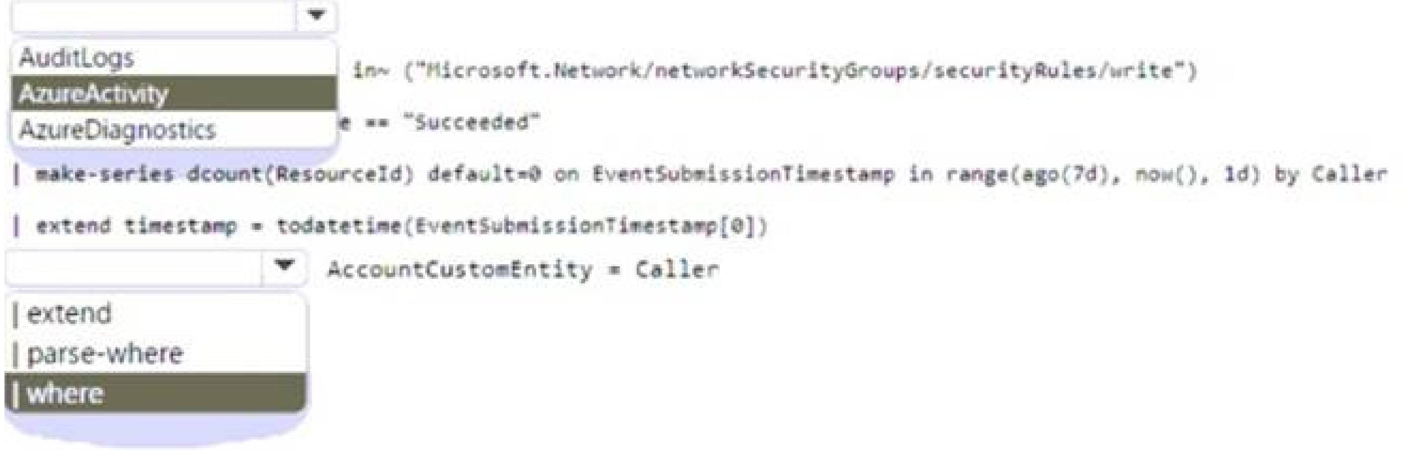
You have an Azure subscription that contains an Microsoft Sentinel workspace.

You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:

• Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal

• Automatically associates the security principal with an Microsoft Sentinel entity

How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- AuditLogs
- [✓ AzureActivity]
- AzureDiagnostics

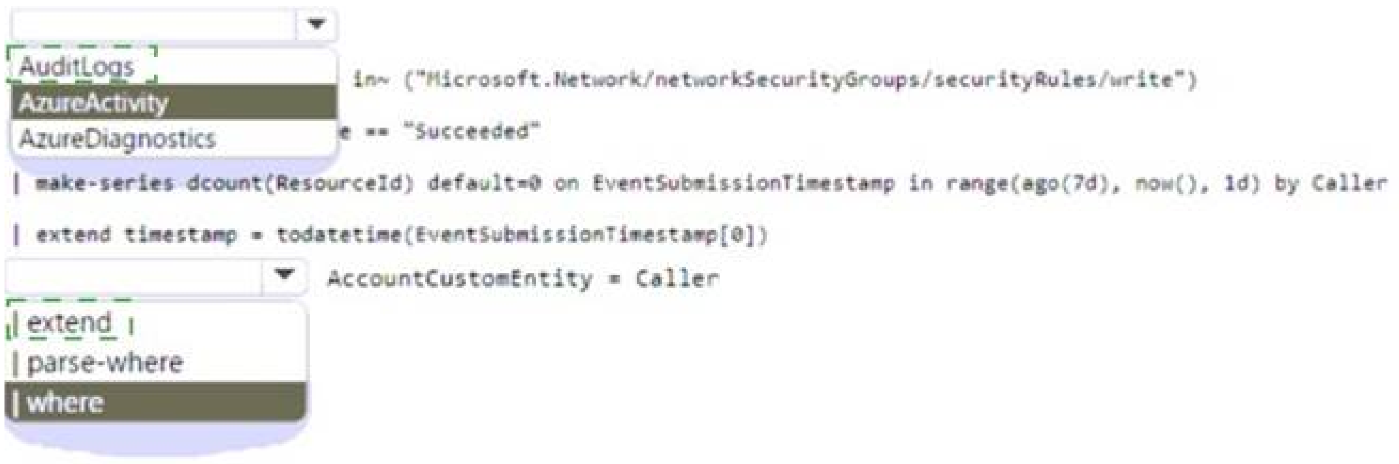
```
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
```

- | extend
- | parse-where
- [✓ | where]

A. Mastered
B. Not Mastered

Answer: A

Explanation:



```
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
```

NEW QUESTION 98

- (Topic 4)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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 Microsoft incident creation rule for a data connector. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 101

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

A. the activity logs of storage1
B. the Azure Storage Analytics logs
C. the alert details
D. the related entities of the alert

Answer: A

Explanation:
To identify which blobs were deleted, you should review the activity logs of the storage account. The activity logs contain information about all the operations that have taken place in the storage account, including delete operations. These logs can be accessed in the Azure portal by navigating to the storage account, selecting "Activity log" under the "Monitoring" section, and filtering by the appropriate time range. You can also use Azure Monitor and Log Analytics to query and analyze the activity logs data. References:
? https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs
? https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure- storage

NEW QUESTION 104

- (Topic 4)

You create an Azure subscription.

You enable Azure Defender for the subscription.

You need to use Azure Defender to protect on-premises computers. What should you do on the on-premises computers?

A. Install the Log Analytics agent.
B. Install the Dependency agent.
C. Configure the Hybrid Runbook Worker role.
D. Install the Connected Machine agent.

Answer: A

Explanation:
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data- collection

NEW QUESTION 105
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 108
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You need to add threat indicators for all the IP addresses in a range of 171.23.3432- 171.2334.63. The solution must minimize administrative effort.
What should you do in the Microsoft 365 Defender portal?

A. Create an import file that contains the IP address of 171.23.34.32/27. Select Importand import the file.
B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.
C. Select Add indicator and set the IP address to 171.23.34.32/27
D. Create an import file that contains the individual IP addresses in the rang
E. SelectImport and import the file.

Answer: D

Explanation:
This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.
Reference: [1] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence-manage-indicators

NEW QUESTION 111
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender fof Ctoud.
You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.
You need to onboard EC2-1 to Defender for Cloud. What should you install on EC2-1?

A. the Log Analytics agent
B. the Azure Connected Machine agent
C. the unified Microsoft Defender for Endpoint solution package
D. Microsoft Monitoring Agent

Answer: A

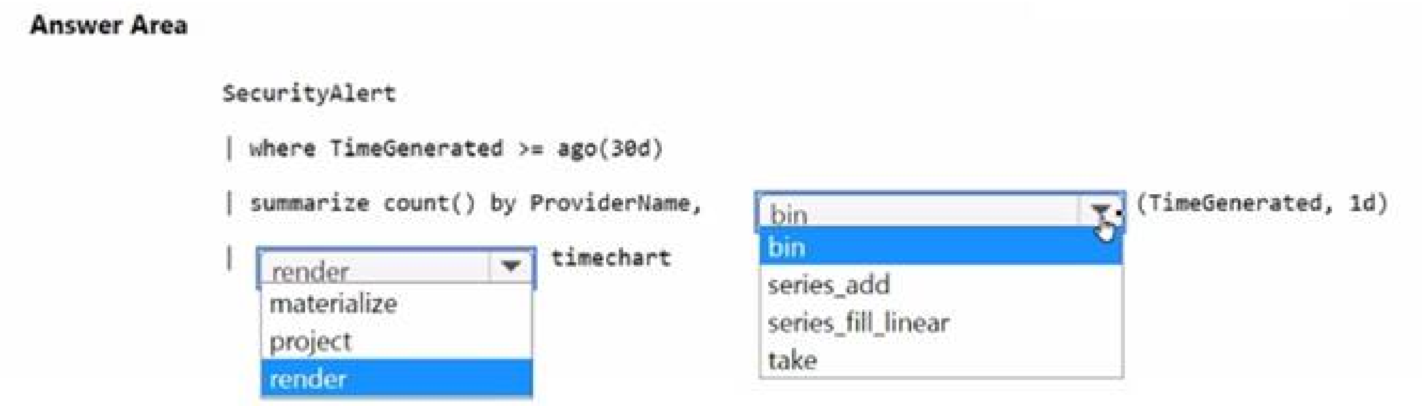
NEW QUESTION 112
- (Topic 4)
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure
Sentinel deployment to generate alerts based 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 Microsoft Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

Answer: C

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

NEW QUESTION 117
HOTSPOT - (Topic 4)
You have an Microsoft Sentinel workspace named SW1.
You plan to create a custom workbook that will include a time chart.
You need to create a query that will identify the number of security alerts per day for each provider.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



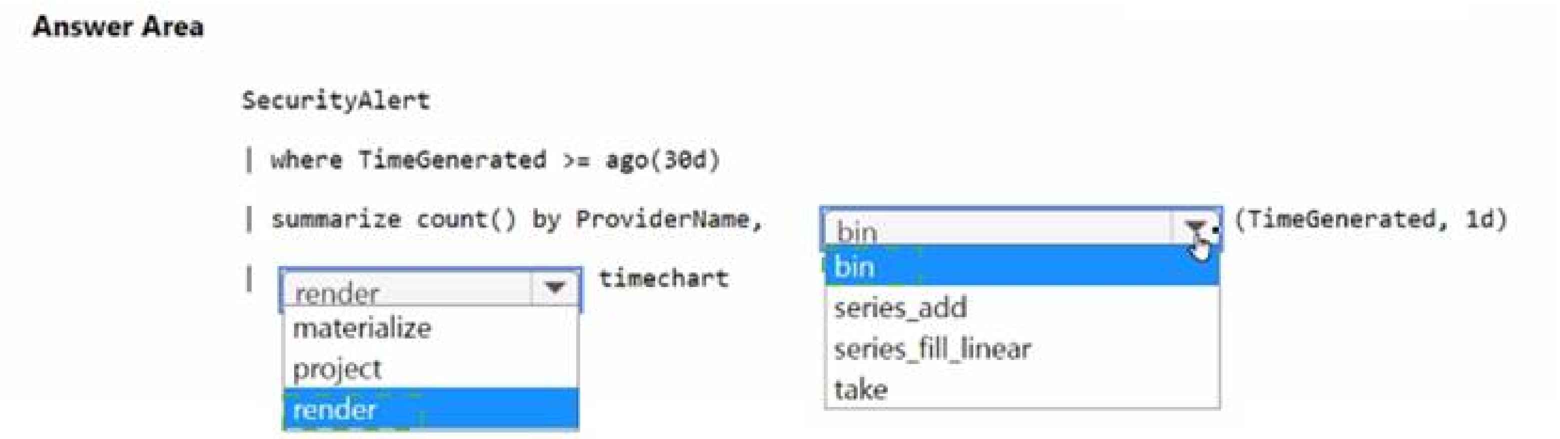
Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName, [bin] (TimeGenerated, 1d)
| [render] timechart
```

A. Mastered
B. Not Mastered

Answer: A

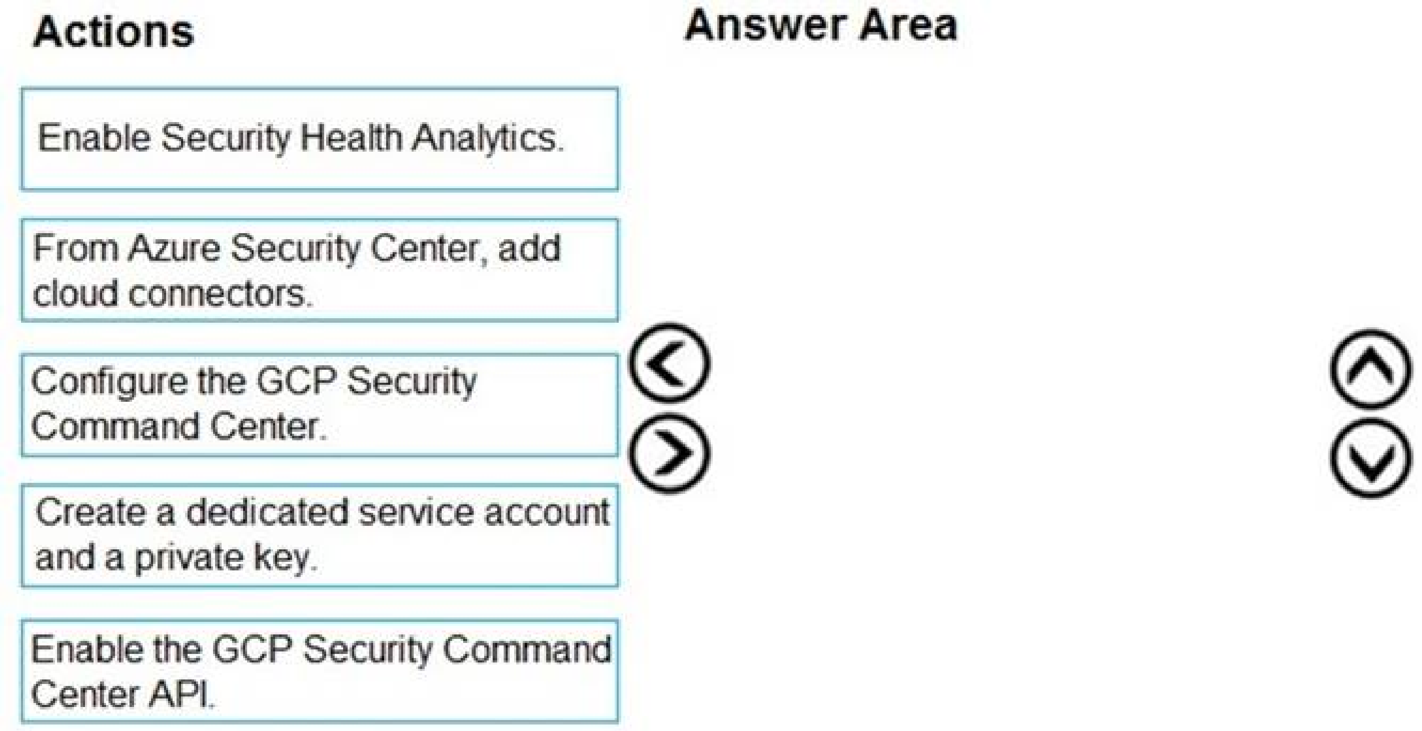
Explanation:



Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName, [bin] (TimeGenerated, 1d)
| [render] timechart
```

NEW QUESTION 118
DRAG DROP - (Topic 4)
You have resources in Azure and Google cloud.
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



Actions

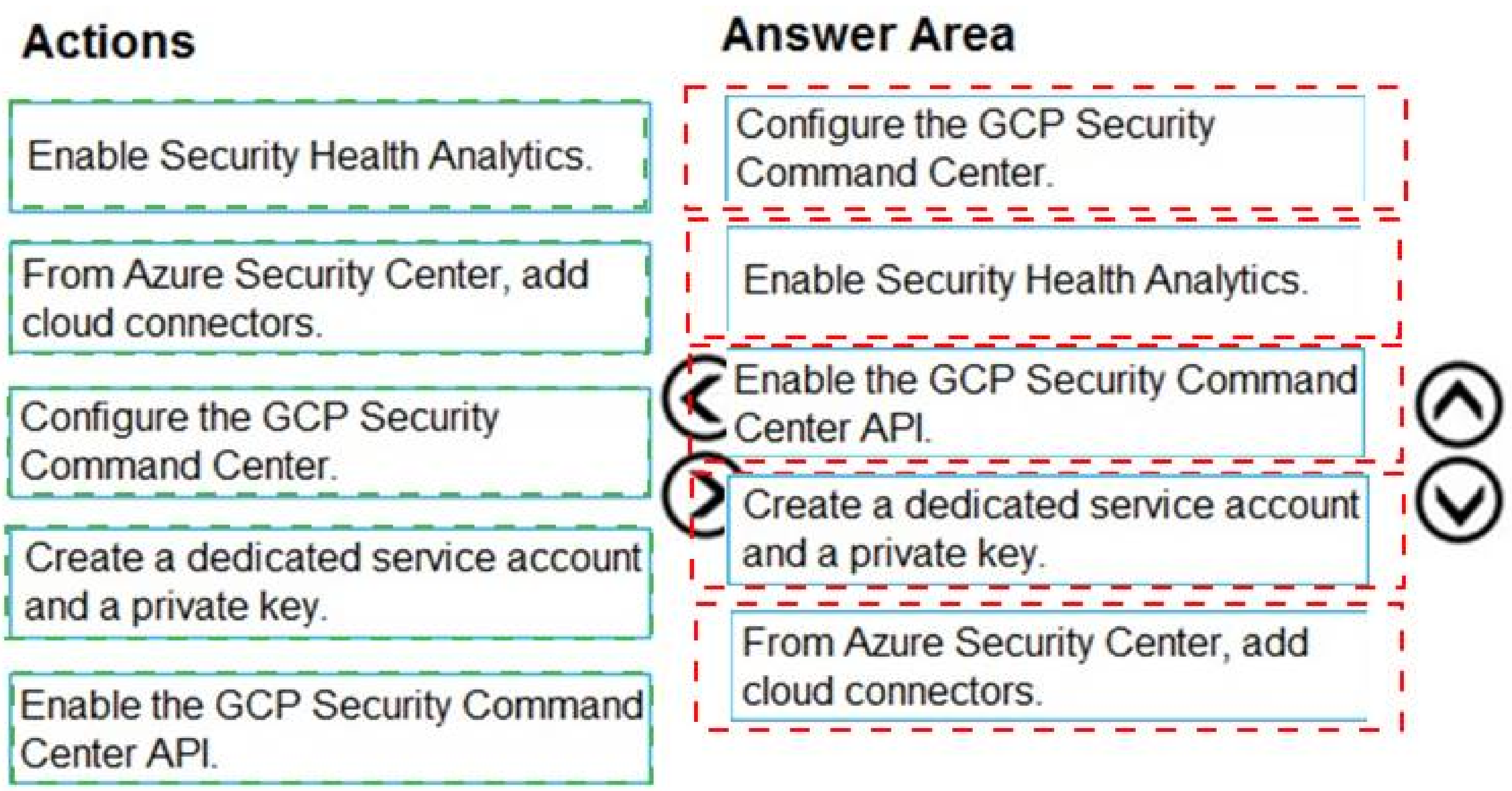
- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



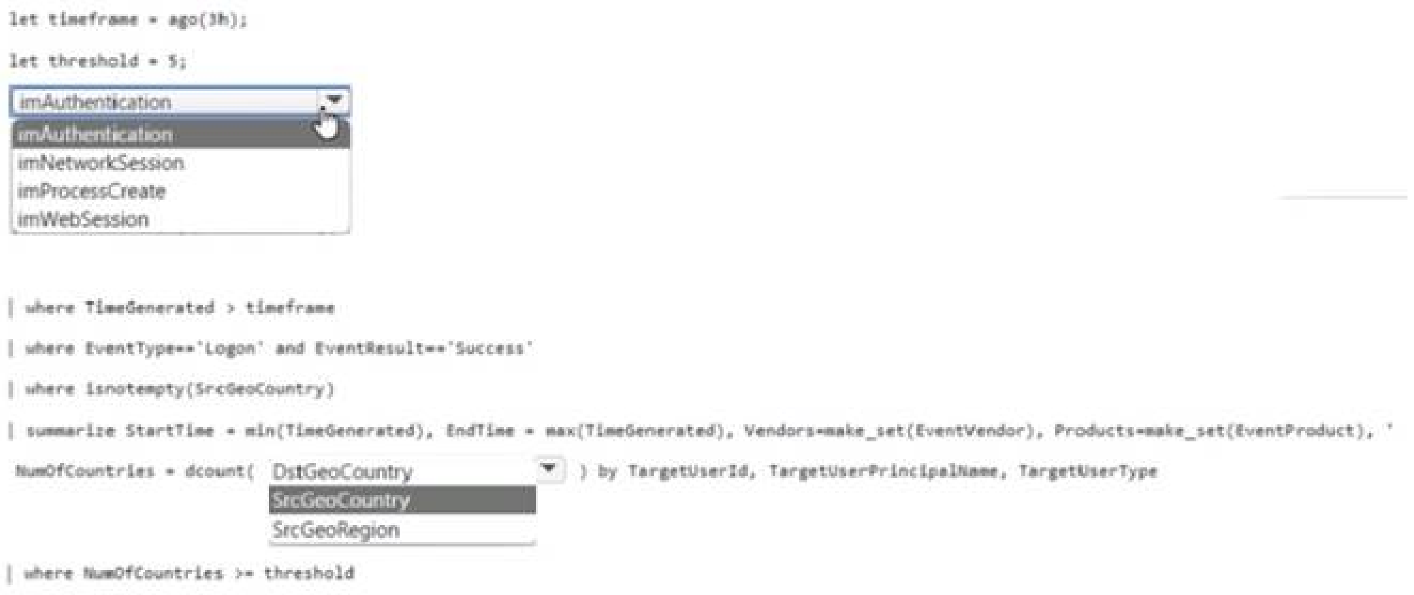
Actions

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.

Answer Area

1. Configure the GCP Security Command Center.
2. Enable Security Health Analytics.
3. Enable the GCP Security Command Center API.
4. Create a dedicated service account and a private key.
5. From Azure Security Center, add cloud connectors.

NEW QUESTION 122
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.
How should you complete the query? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point

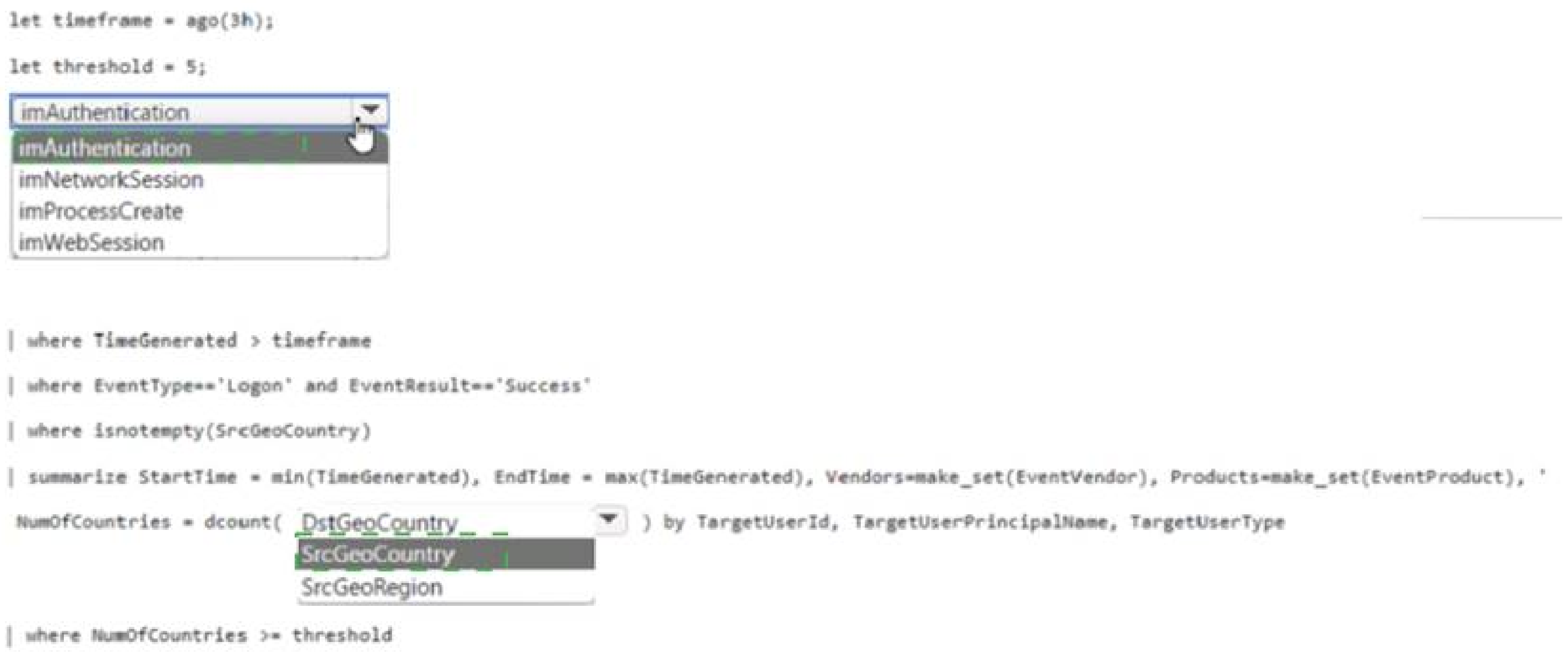


```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
  imAuthentication
  imNetworkSession
  imProcessCreate
  imWebSession
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
                         SrcGeoCountry
                         SrcGeoRegion
| where NumOfCountries >= threshold
```

A. Mastered
B. Not Mastered

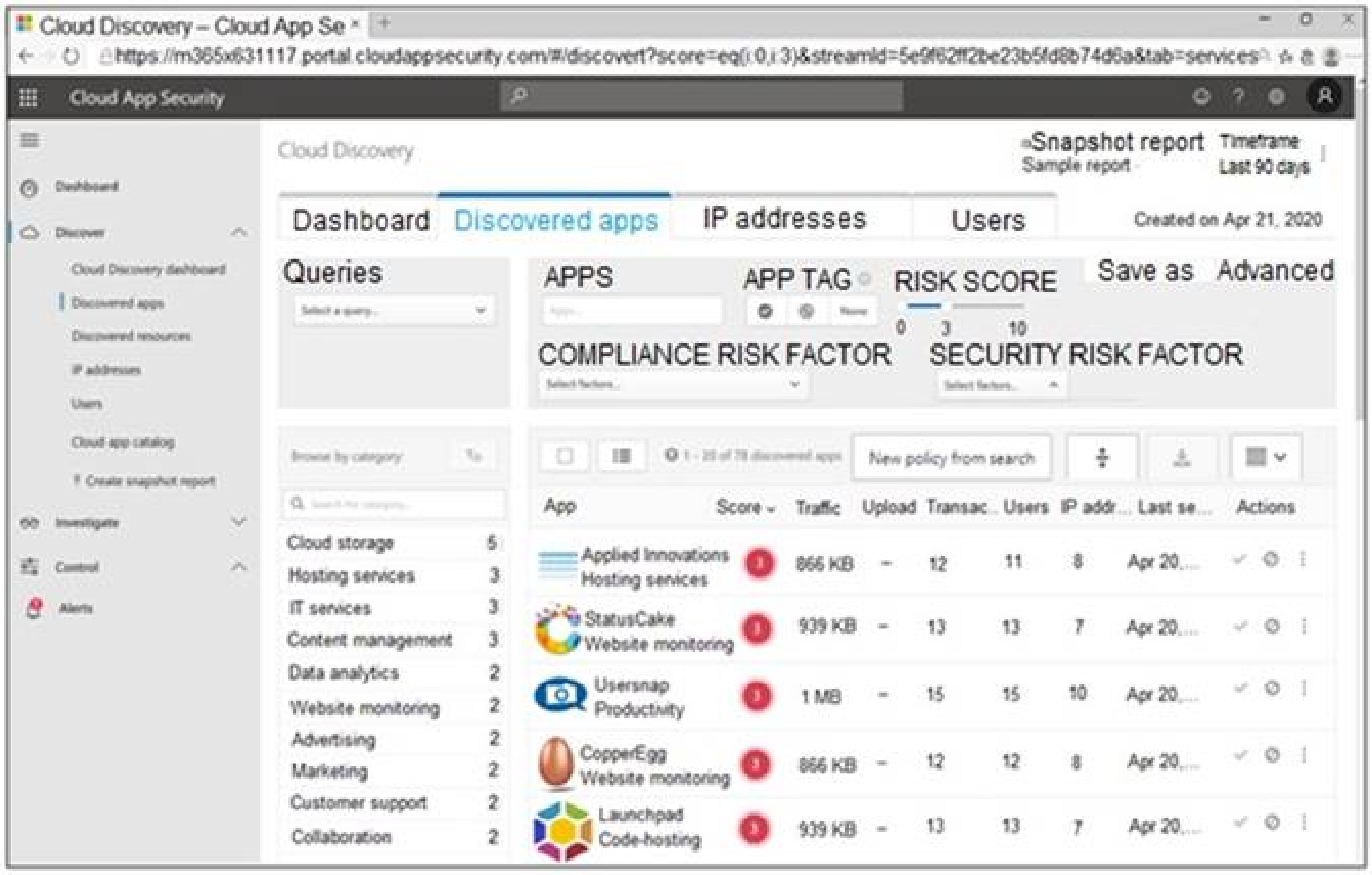
Answer: A

Explanation:



```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
  imAuthentication
  imNetworkSession
  imProcessCreate
  imWebSession
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '
NumOfCountries = dcount( DstGeoCountry ) by TargetUserId, TargetUserPrincipalName, TargetUserType
                         SrcGeoCountry
                         SrcGeoRegion
| where NumOfCountries >= threshold
```

NEW QUESTION 127
DRAG DROP - (Topic 4)
You open the Cloud App Security portal as shown in the following exhibit.



Cloud Discovery – Cloud App Se
https://m365x631117.portal.cloudappsecurity.com/#/discover?score=eq(i:0,i:3)&streamId=5e9f62ff2be23b5fd8b74d6a&tab=services

Cloud App Security

Cloud Discovery — Snapshot report, Sample report — Timeframe: Last 90 days

Dashboard | Discovered apps | IP addresses | Users — Created on Apr 21, 2020

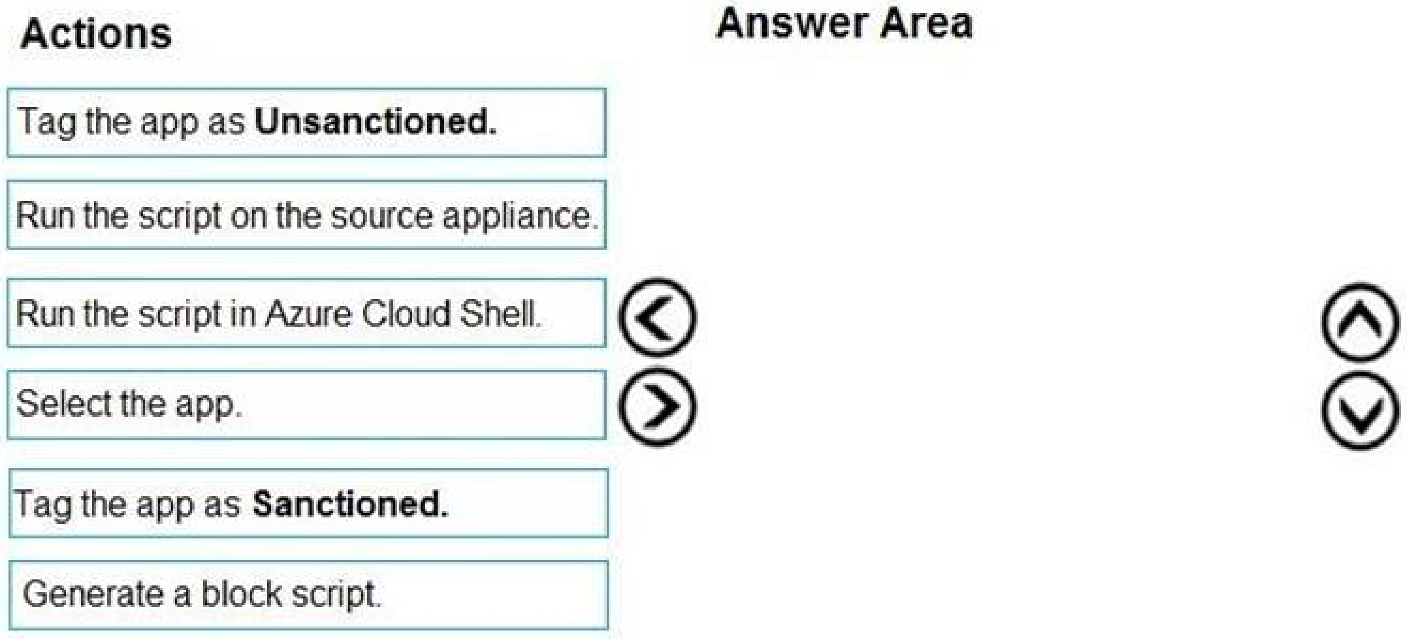
Queries: Select a query...
APPS | APP TAG | RISK SCORE 0 3 10 | Save as | Advanced
COMPLIANCE RISK FACTOR: Select factors... | SECURITY RISK FACTOR: Select factors...

1 - 20 of 78 discovered apps | New policy from search

Browse by category	
Cloud storage	5
Hosting services	3
IT services	3
Content management	3
Data analytics	2
Website monitoring	2
Advertising	2
Marketing	2
Customer support	2
Collaboration	2

App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	-	12	11	8	Apr 20,...	
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20,...	
Usersnap Productivity	3	1 MB	-	15	15	10	Apr 20,...	
CopperEgg Website monitoring	3	866 KB	-	12	12	8	Apr 20,...	
Launchpad Code-hosting	3	939 KB	-	13	13	7	Apr 20,...	

You need to remediate the risk for the Launchpad app.
Which four 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.



Actions

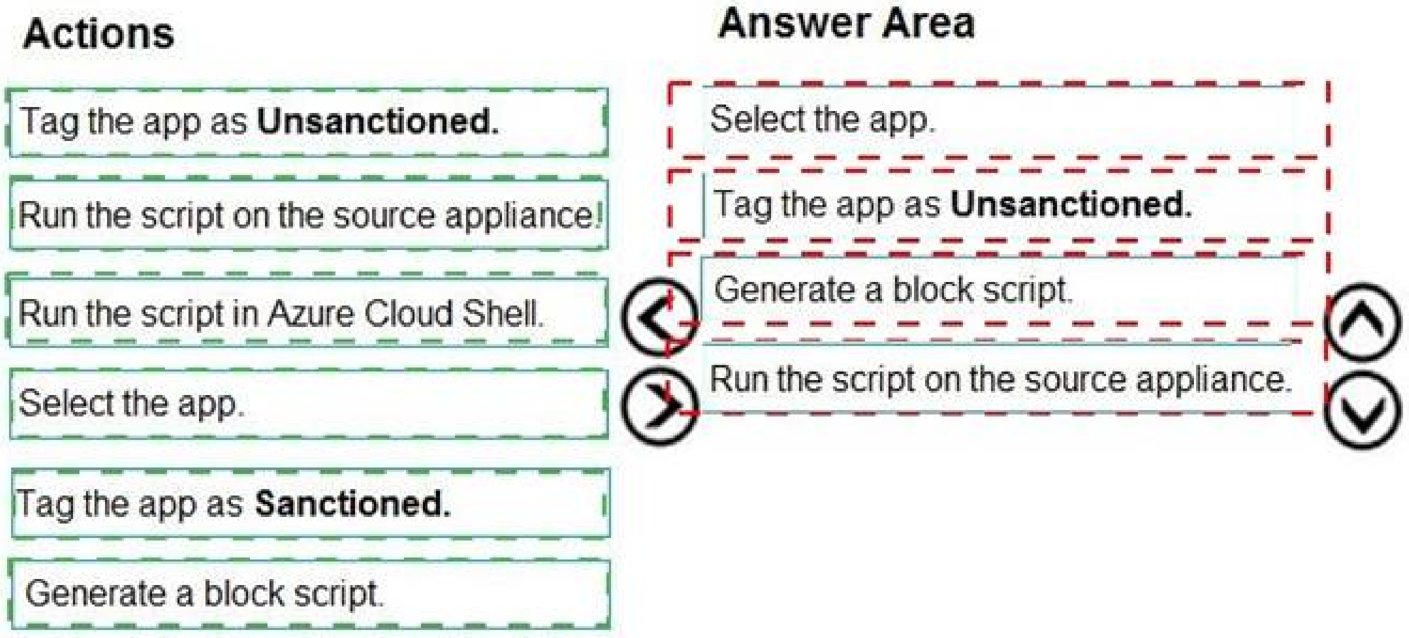
- Tag the app as **Unsanctioned.**
- Run the script on the source appliance.
- Run the script in Azure Cloud Shell.
- Select the app.
- Tag the app as **Sanctioned.**
- Generate a block script.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

- Tag the app as **Unsanctioned.**
- Run the script on the source appliance!
- Run the script in Azure Cloud Shell.
- Select the app.
- Tag the app as **Sanctioned.**
- Generate a block script.

Answer Area

- Select the app.
- Tag the app as **Unsanctioned.**
- Generate a block script.
- Run the script on the source appliance.

NEW QUESTION 128

- (Topic 4)
You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

A. Analytics Efficiency
B. Security Operations Efficiency
C. Event Analyzer
D. Investigation insights

Answer: C

NEW QUESTION 129
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.
You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common
B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.
C. From the Azure portal, create an Azure Event Grid subscription.
D. From the workspace created by Defender for Cloud, set the data collection level to All Events
E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Answer: DE

NEW QUESTION 130
- (Topic 4)
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

A. And a new scheduled query rule.
B. Add a data connector to Azure Sentinel.
C. Configure a custom Threat Intelligence connector in Azure Sentinel.
D. Modify the trigger in the logic app.

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

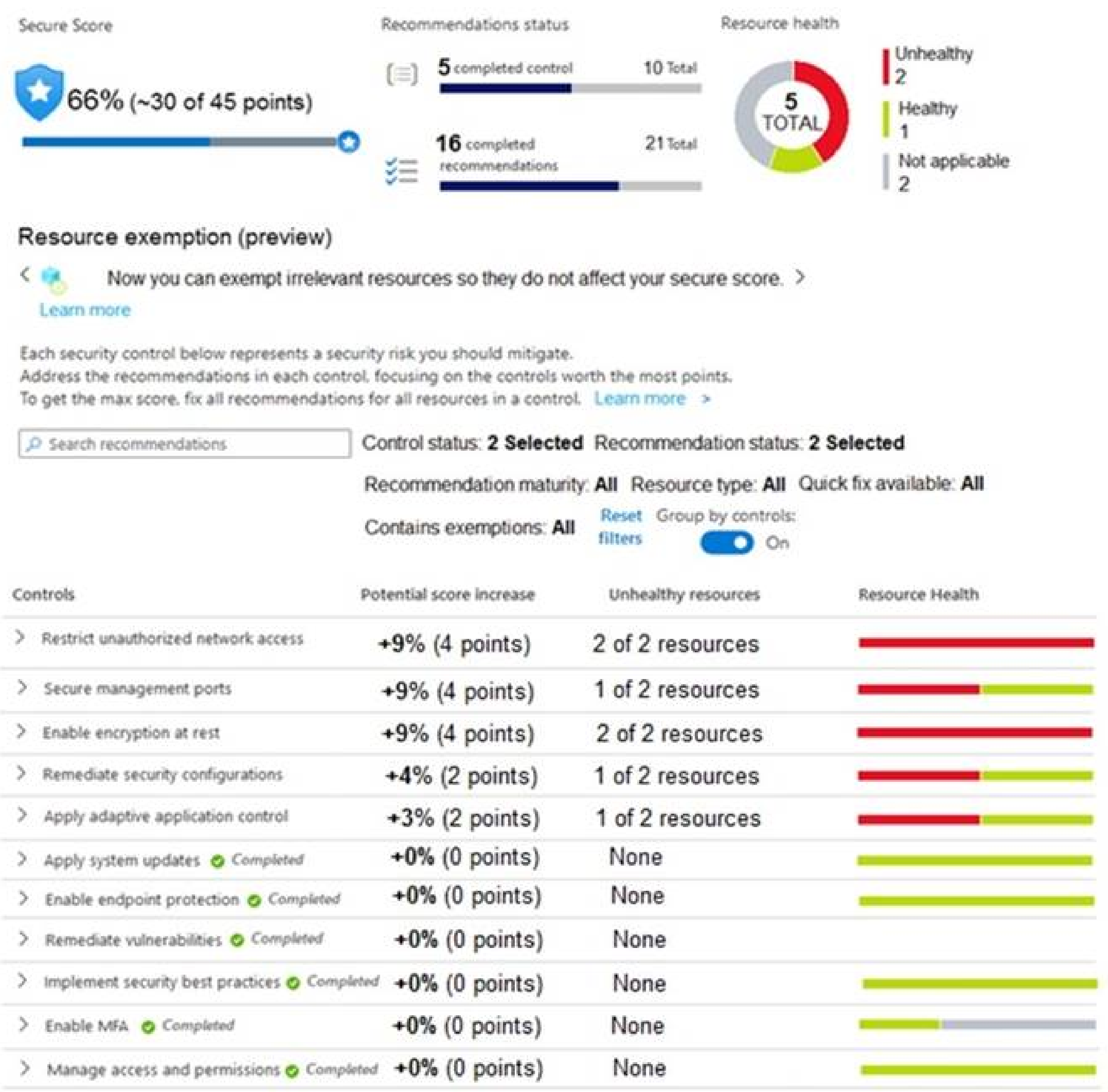
NEW QUESTION 131
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

NEW QUESTION 132
HOTSPOT - (Topic 4)
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

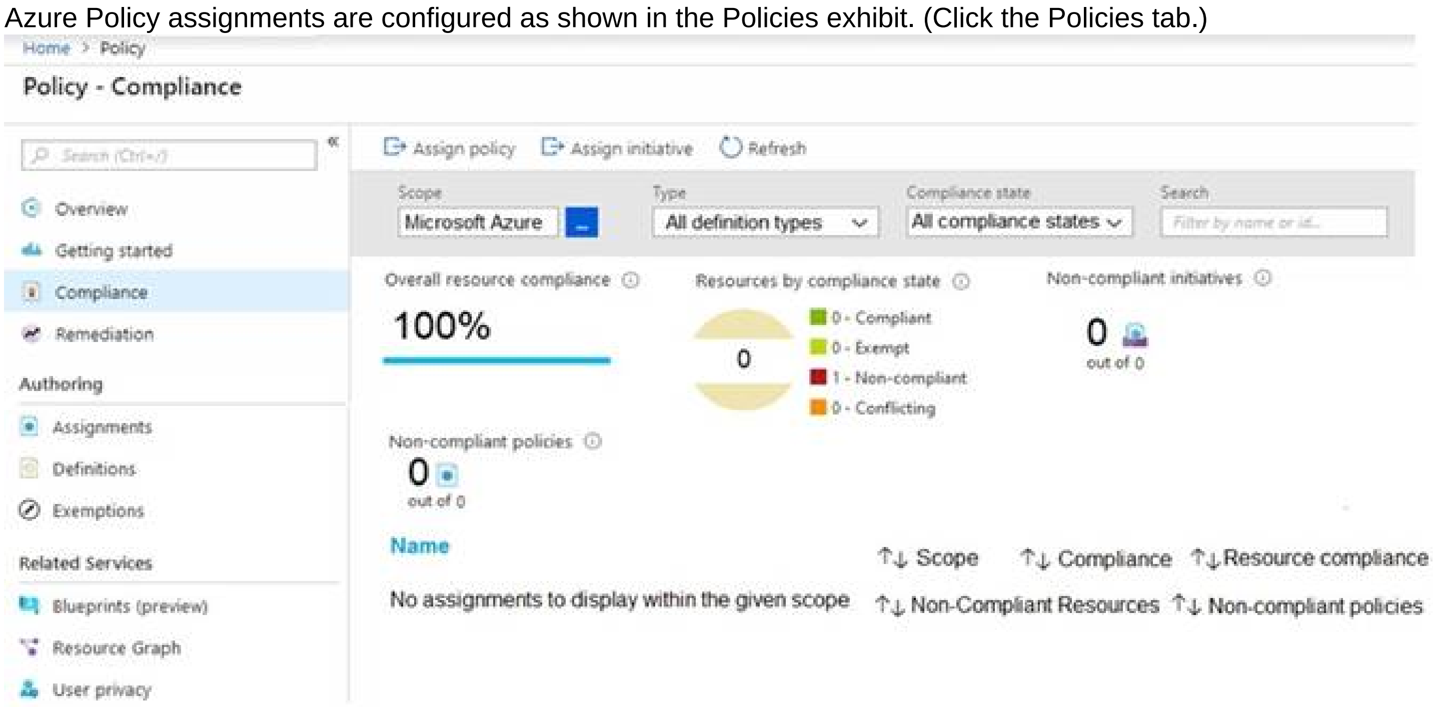
Control status: **2 Selected** Recommendation status: **2 Selected**

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.)



Home > Policy

Policy - Compliance

Search (Ctrl+/)

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

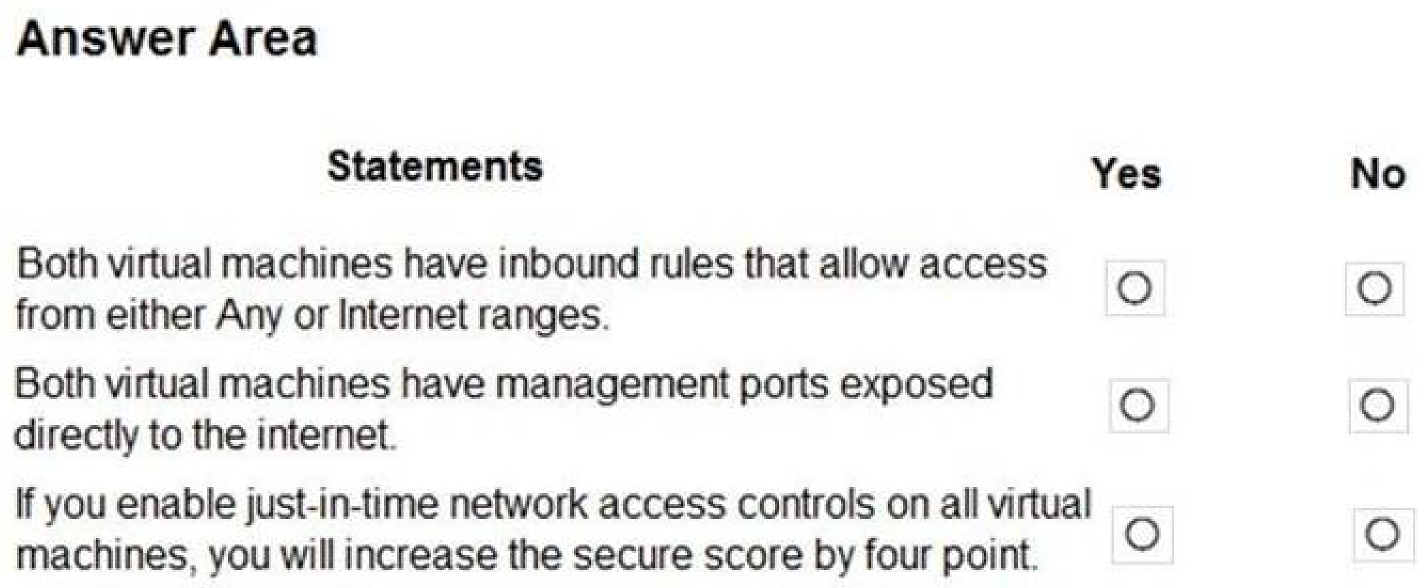
- 0 - Compliant
- 0 - Exempt
- 1 - Non-compliant
- 0 - Conflicting

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.



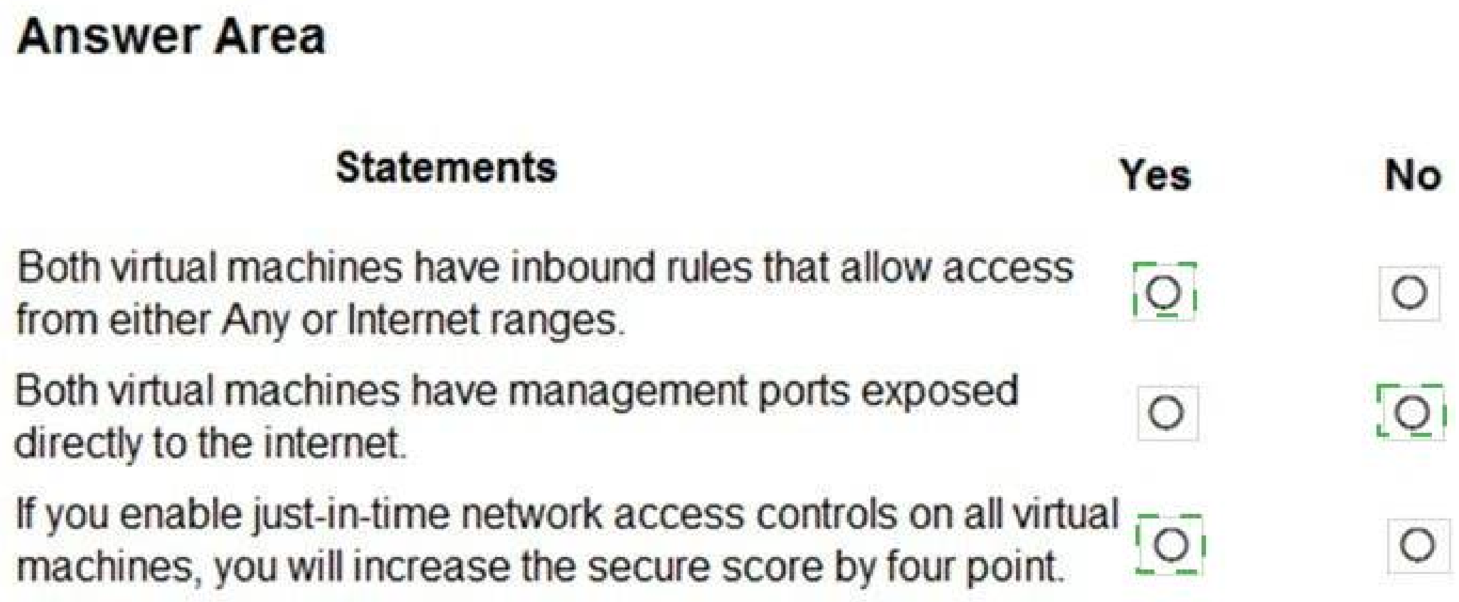
Answer Area

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.	○	○

A. Mastered
B. Not Mastered

Answer: A

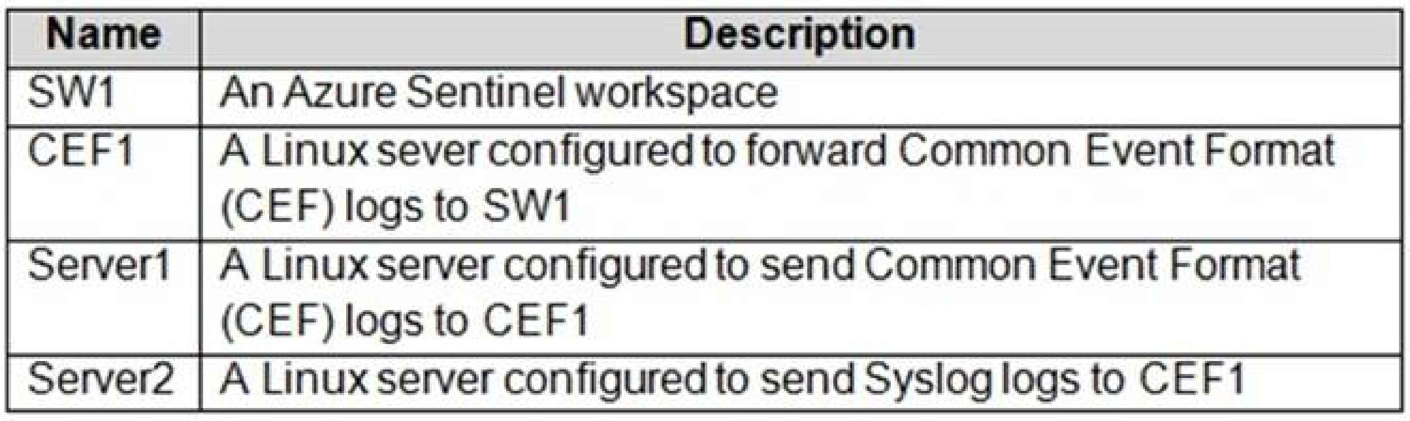
Explanation:



Answer Area

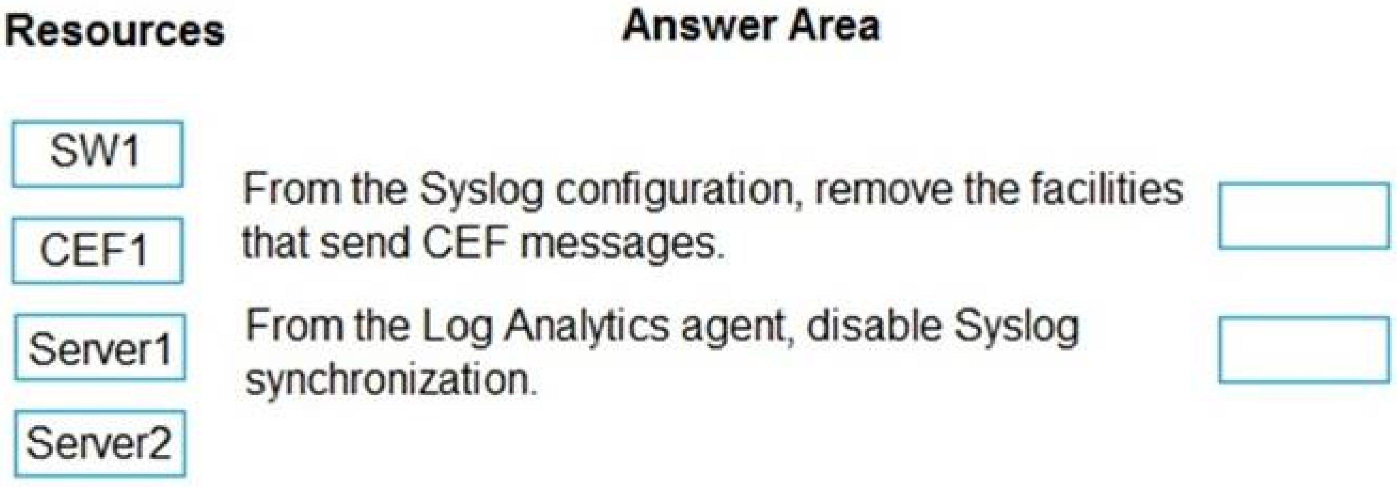
Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	[✓ ○]	○
Both virtual machines have management ports exposed directly to the internet.	○	[✓ ○]
If you enable just-in-time network access controls on all virtual machines, you will increase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

NEW QUESTION 137
DRAG DROP - (Topic 4)
You have the resources shown in the following table.



Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

You need to prevent duplicate events from occurring in SW1.
What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource 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.



Resources

SW1
CEF1
Server1
Server2

Answer Area

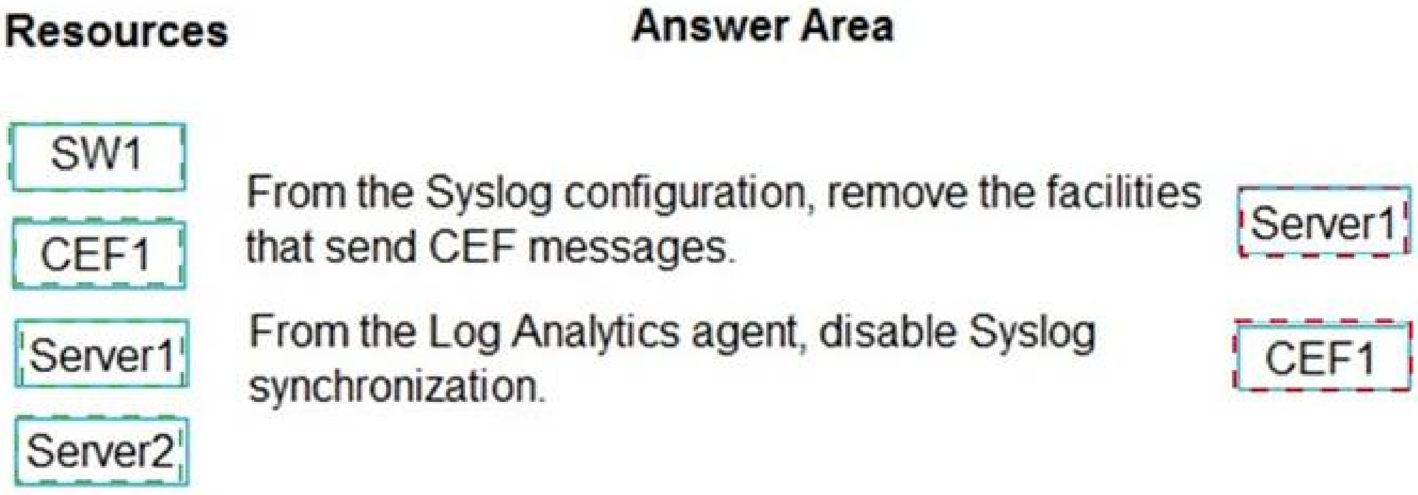
From the Syslog configuration, remove the facilities that send CEF messages. □

From the Log Analytics agent, disable Syslog synchronization. □

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Resources

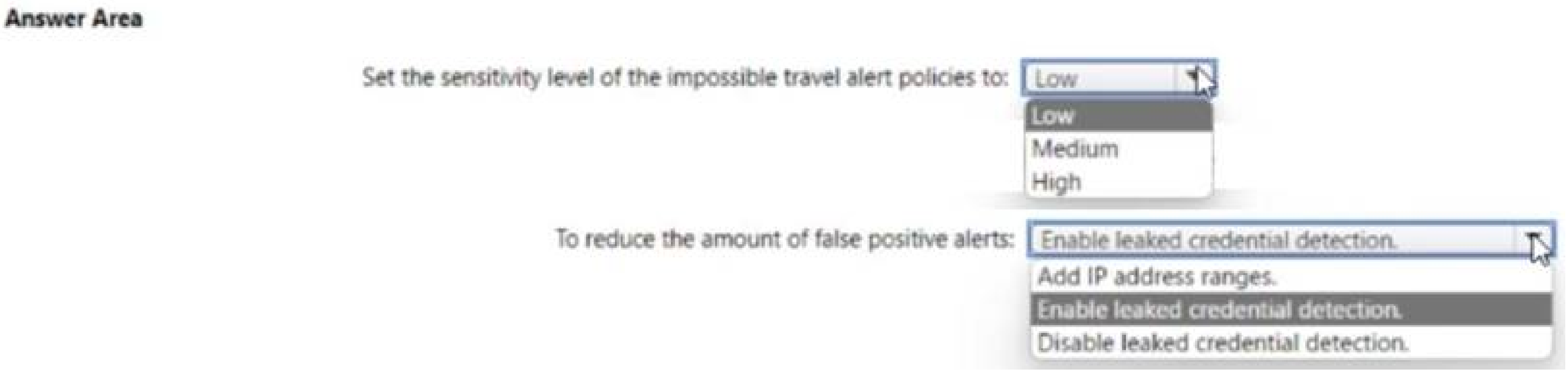
SW1
CEF1
Server1
Server2

Answer Area

From the Syslog configuration, remove the facilities that send CEF messages. Server1

From the Log Analytics agent, disable Syslog synchronization. CEF1

NEW QUESTION 140
HOTSPOT - (Topic 4)
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.



Answer Area

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

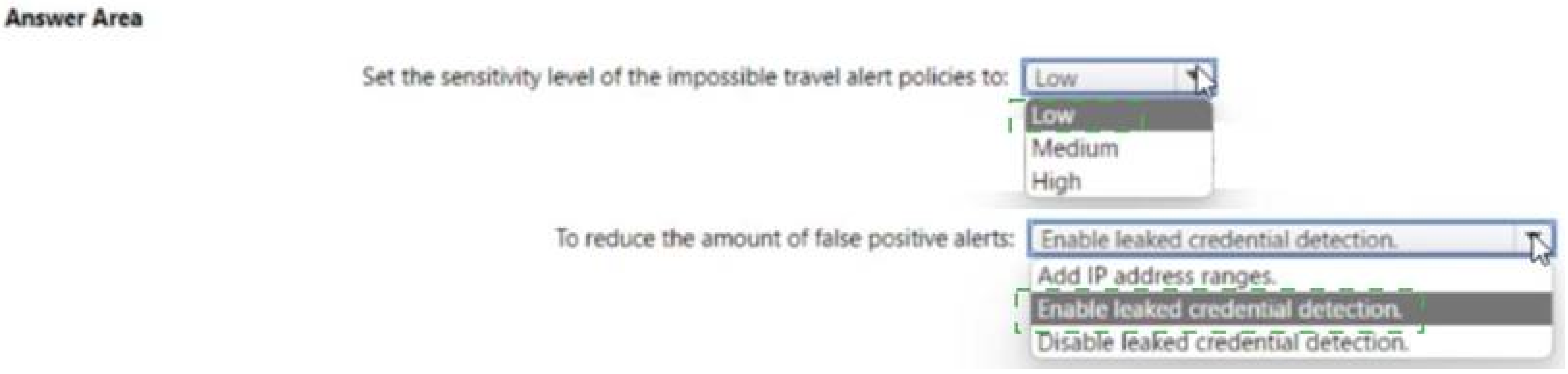
To reduce the amount of false positive alerts: Enable leaked credential detection.

Add IP address ranges.
Enable leaked credential detection.
Disable leaked credential detection.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

To reduce the amount of false positive alerts: Enable leaked credential detection.

Add IP address ranges.
Enable leaked credential detection.
Disable leaked credential detection.

NEW QUESTION 145
- (Topic 4)
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate files, and then select New policy from search
D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
E. From Settings, select Information Protection, select Files, and then enable file monitoring.
F. Select Investigate files, and then filter File Type to Document.

Answer: DE

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

NEW QUESTION 150
- (Topic 4)
You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

Answer: C

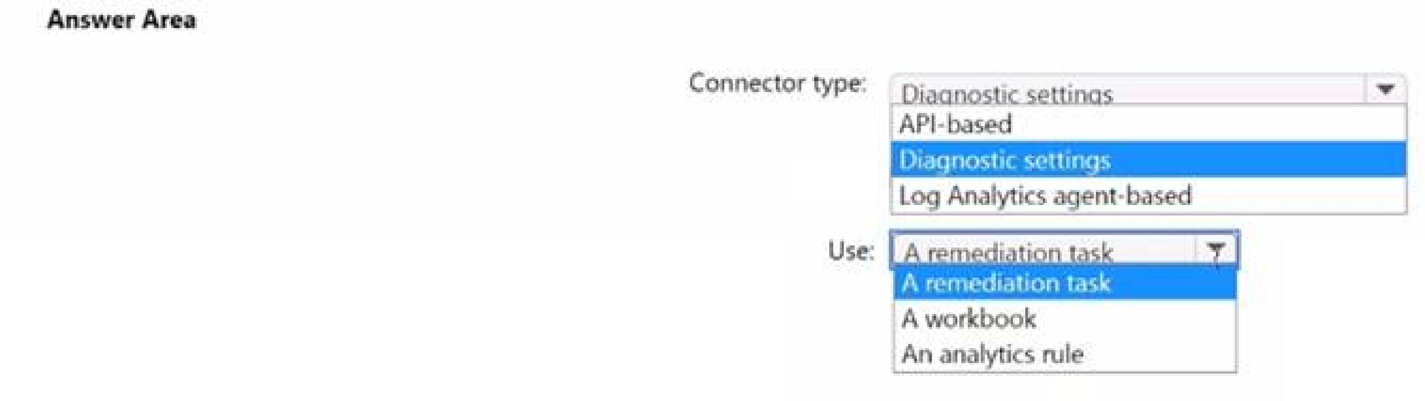
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

NEW QUESTION 151
- (Topic 4)
You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

A. an API connection
B. a trigger
C. an connector
D. authorization

Answer: B

NEW QUESTION 154
HOTSPOT - (Topic 4)
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

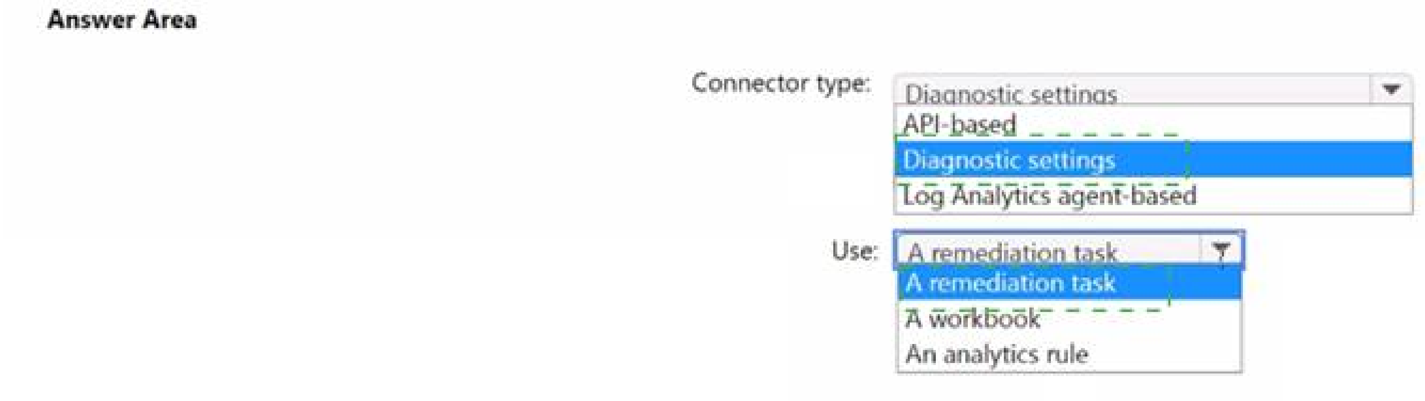
Connector type: Diagnostic settings
- API-based
- Diagnostic settings
- Log Analytics agent-based

Use: A remediation task
- A remediation task
- A workbook
- An analytics rule

A. Mastered
B. Not Mastered

Answer: A

Explanation:

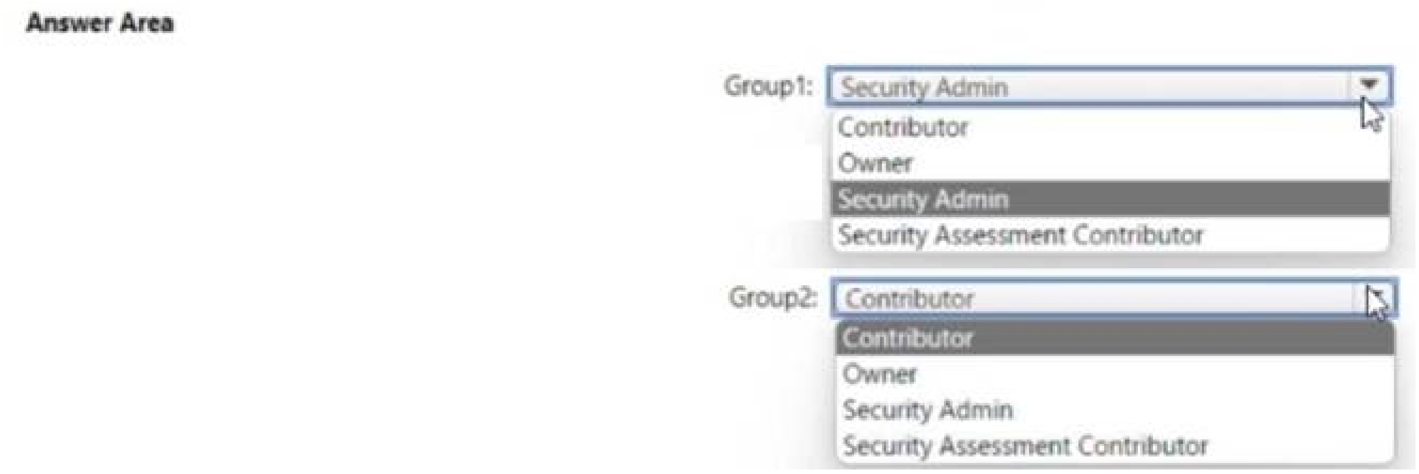


Answer Area

Connector type: Diagnostic settings
- API-based
- Diagnostic settings
- Log Analytics agent-based

Use: A remediation task
- A remediation task
- A workbook
- An analytics rule

NEW QUESTION 156
HOTSPOT - (Topic 4)
You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.



Answer Area

Group1: Security Admin
- Contributor
- Owner
- Security Admin
- Security Assessment Contributor

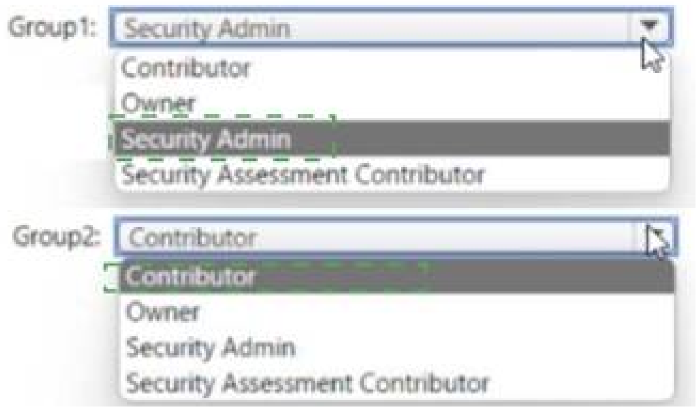
Group2: Contributor
- Contributor
- Owner
- Security Admin
- Security Assessment Contributor

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



Group1: Security Admin

Contributor
Owner
Security Admin
Security Assessment Contributor

Group2: Contributor

Contributor
Owner
Security Admin
Security Assessment Contributor

NEW QUESTION 157
- (Topic 4)
You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender. Which two Bash commands should you run on the virtual machine? Each correct answer
presents part of the solution.
NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n
B. ./alerttest testing eicar pipe
C. cp /bin/echo ./alerttest
D. ./asc_alerttest_662jfi039n testing eicar pipe

Answer: AD

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your- azure-vms-linux-

NEW QUESTION 158
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.
You enable agentless scanning.
You need to prevent Server1 from being scanned. The solution must minimize administrative effort.
What should you do?

A. Create an exclusion tag.
B. Upgrade the subscription to Defender for Servers Plan 2.
C. Create a governance rule.
D. Create an exclusion group.

Answer: D

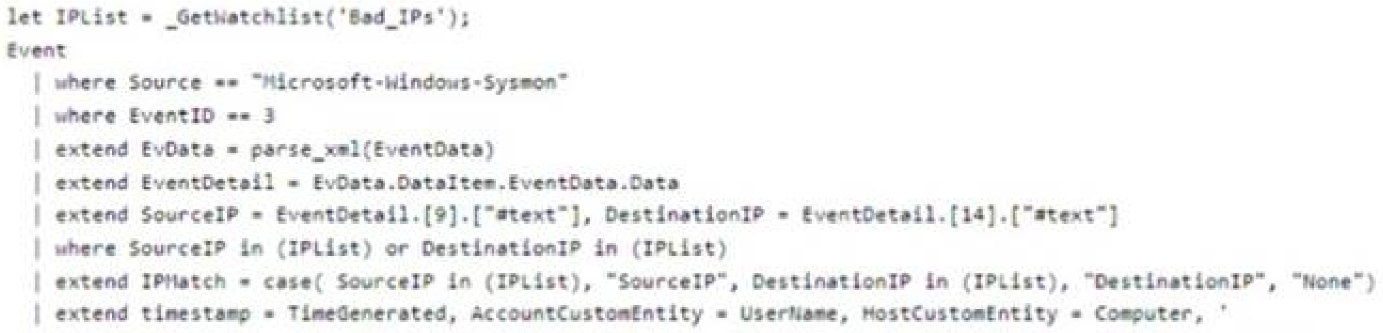
NEW QUESTION 160
- (Topic 4)
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level
B. at the workspace level
C. at the resource level

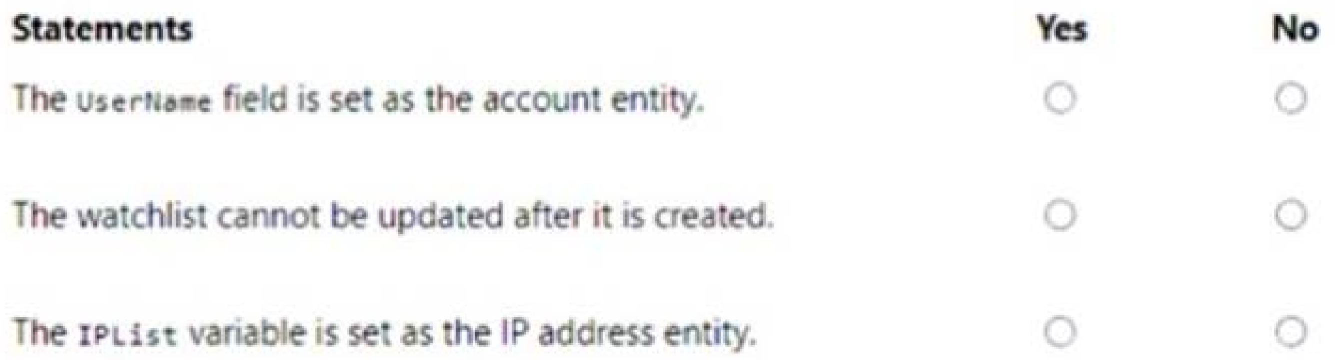
Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

NEW QUESTION 164
HOTSPOT - (Topic 4)
You have the following KQL query.



```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

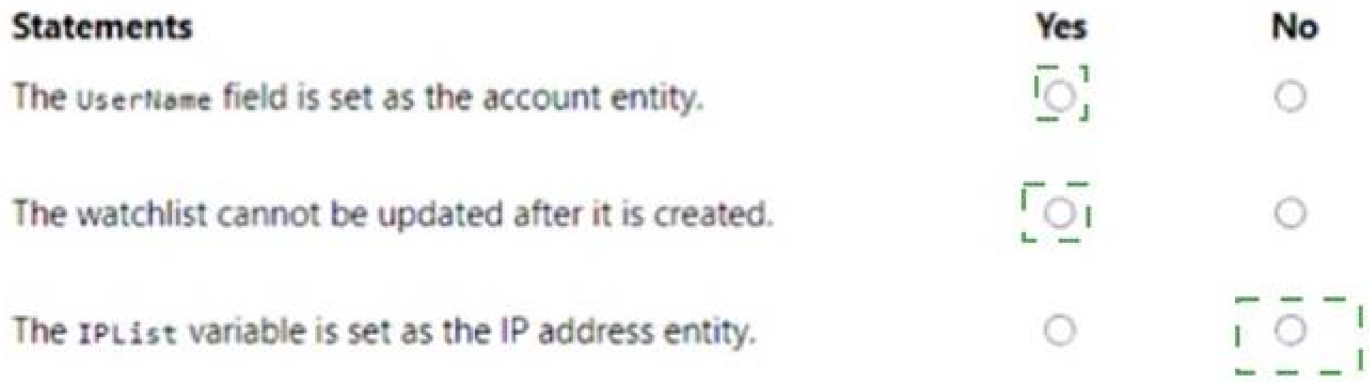


Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

A. Mastered
B. Not Mastered

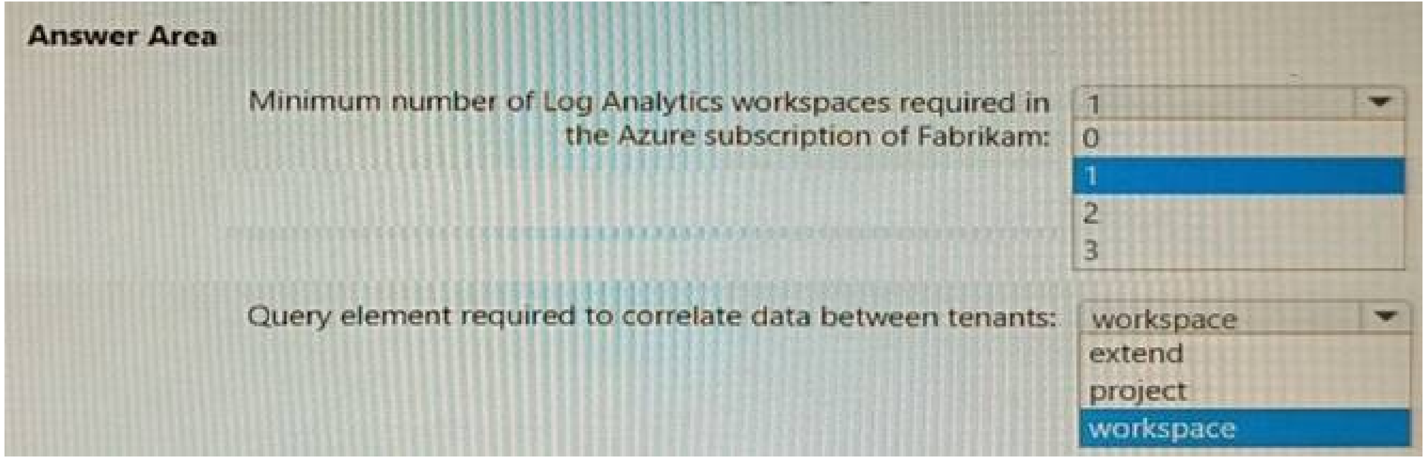
Answer: A

Explanation:



Statements	Yes	No
The UserName field is set as the account entity.	[✓ ○]	○
The watchlist cannot be updated after it is created.	[✓ ○]	○
The IPList variable is set as the IP address entity.	○	[✓ ○]

NEW QUESTION 167
HOTSPOT - (Topic 4)
You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
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.



Answer Area

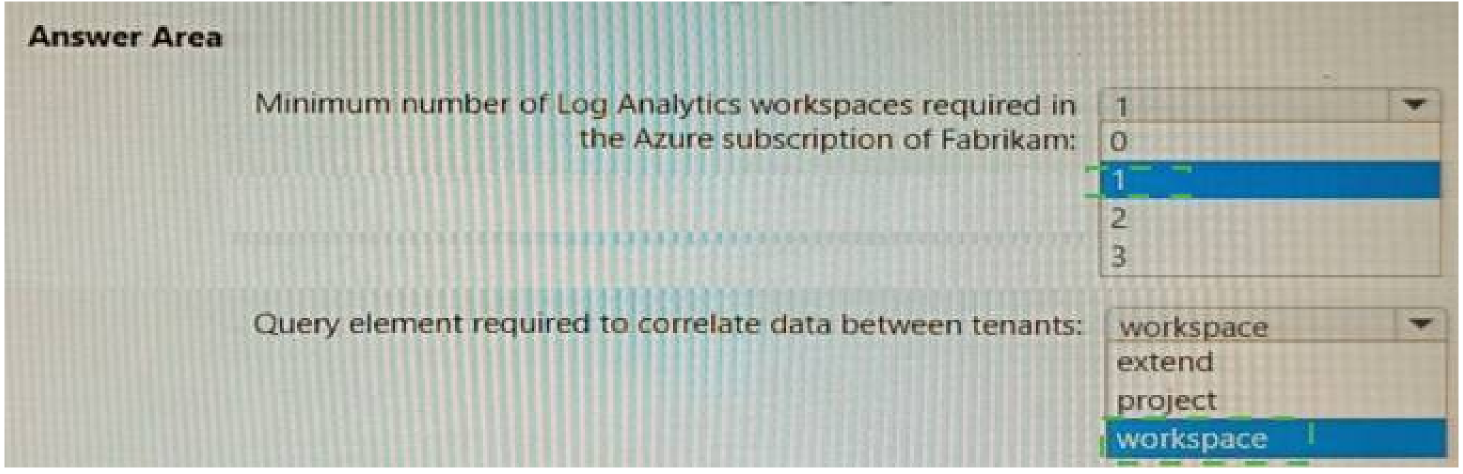
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

NEW QUESTION 168
- (Topic 4)
You have five on-premises Linux servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

Answer: B

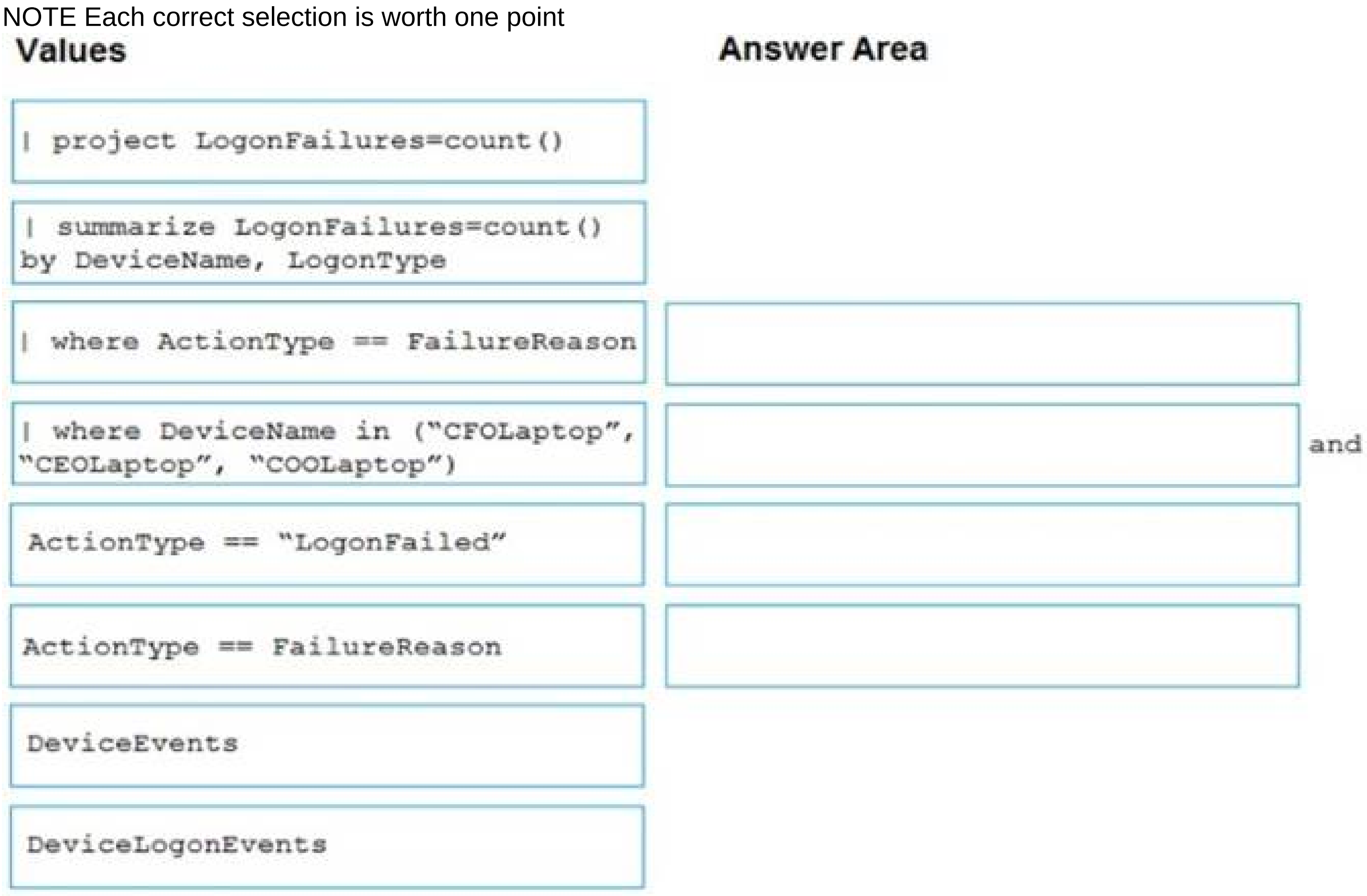
Explanation:
Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

NEW QUESTION 173
- (Topic 4)
You have an Azure subscription that uses resource type 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?

A. Informational
B. Low
C. Medium
D. High

Answer: C

NEW QUESTION 178
DRAG DROP - (Topic 4)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point



Values

```
| project LogonFailures=count()
| summarize LogonFailures=count() by DeviceName, LogonType
| where ActionType == FailureReason
| where DeviceName in (”CFOLaptop”, ”CEOLaptop”, ”COOLaptop”)
ActionType == ”LogonFailed”
ActionType == FailureReason
DeviceEvents
DeviceLogonEvents
```

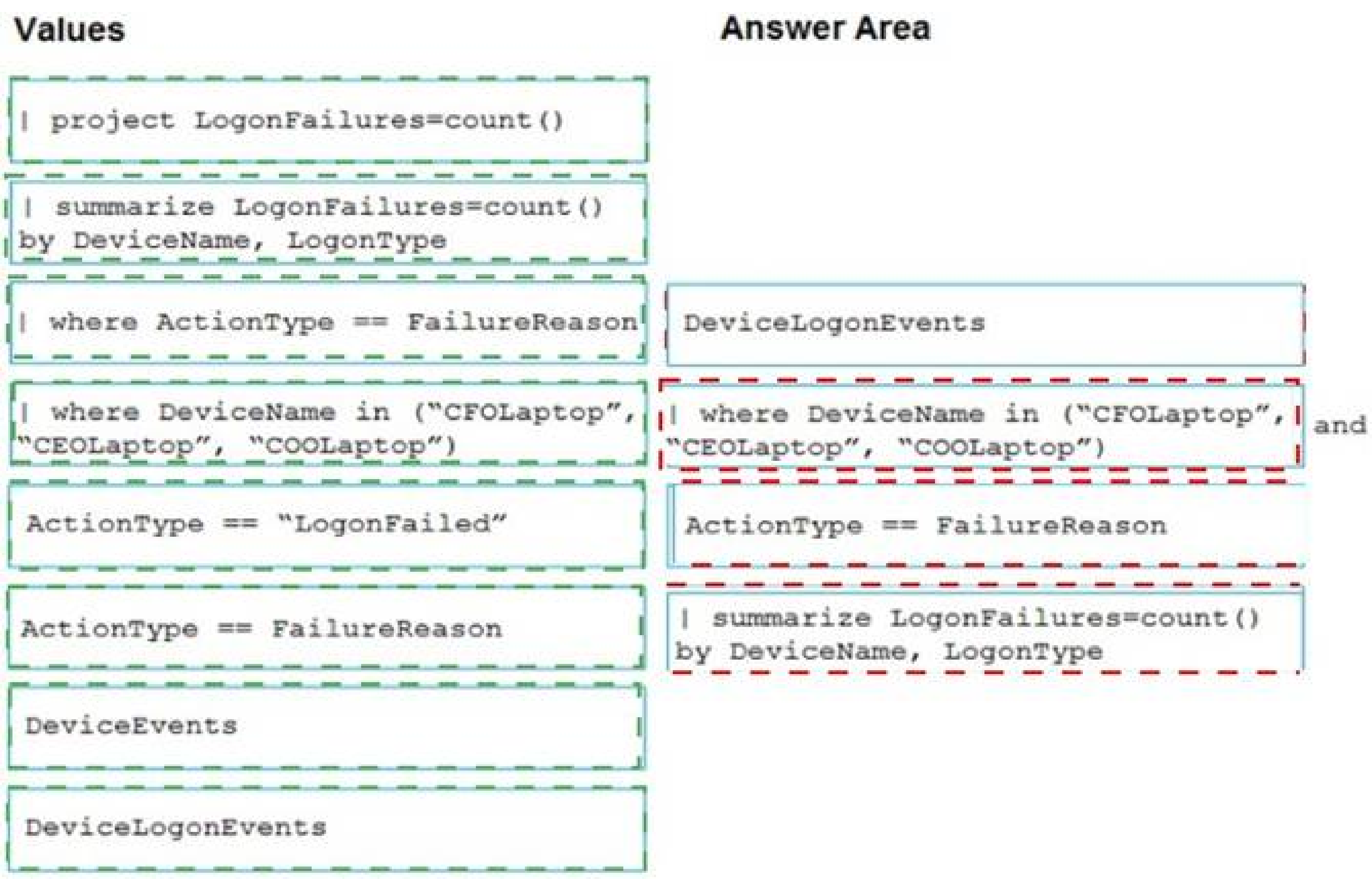
Answer Area

and

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Values

```
| project LogonFailures=count()
| summarize LogonFailures=count()
by DeviceName, LogonType
| where ActionType == FailureReason
| where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")
ActionType == "LogonFailed"
ActionType == FailureReason
DeviceEvents
DeviceLogonEvents
```

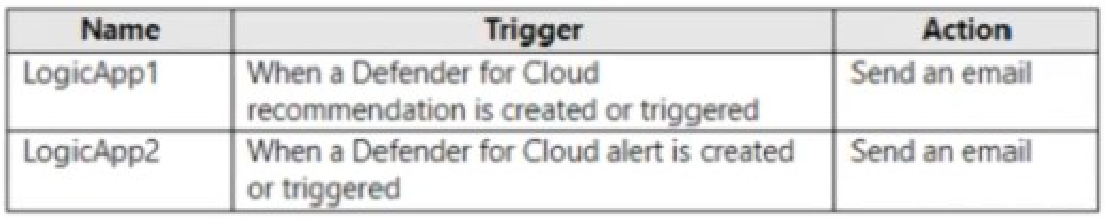
Answer Area

```
DeviceLogonEvents
| where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")              and
ActionType == FailureReason
| summarize LogonFailures=count()
by DeviceName, LogonType
```

NEW QUESTION 183

DRAG DROP - (Topic 4)

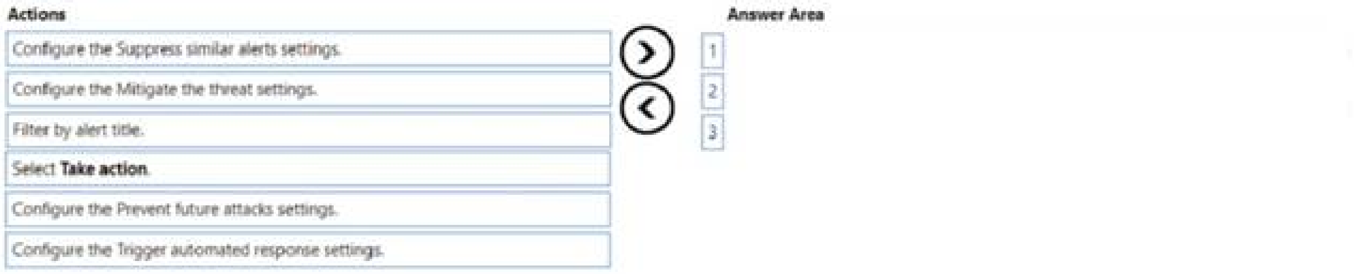
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.



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.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
* A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,
* B. Filter by alert title (e.g. "Suspicious process executed").
* C. Select "Take action" (e.g. "Mitigate the threat").

NEW QUESTION 187

- (Topic 4)

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine’s respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

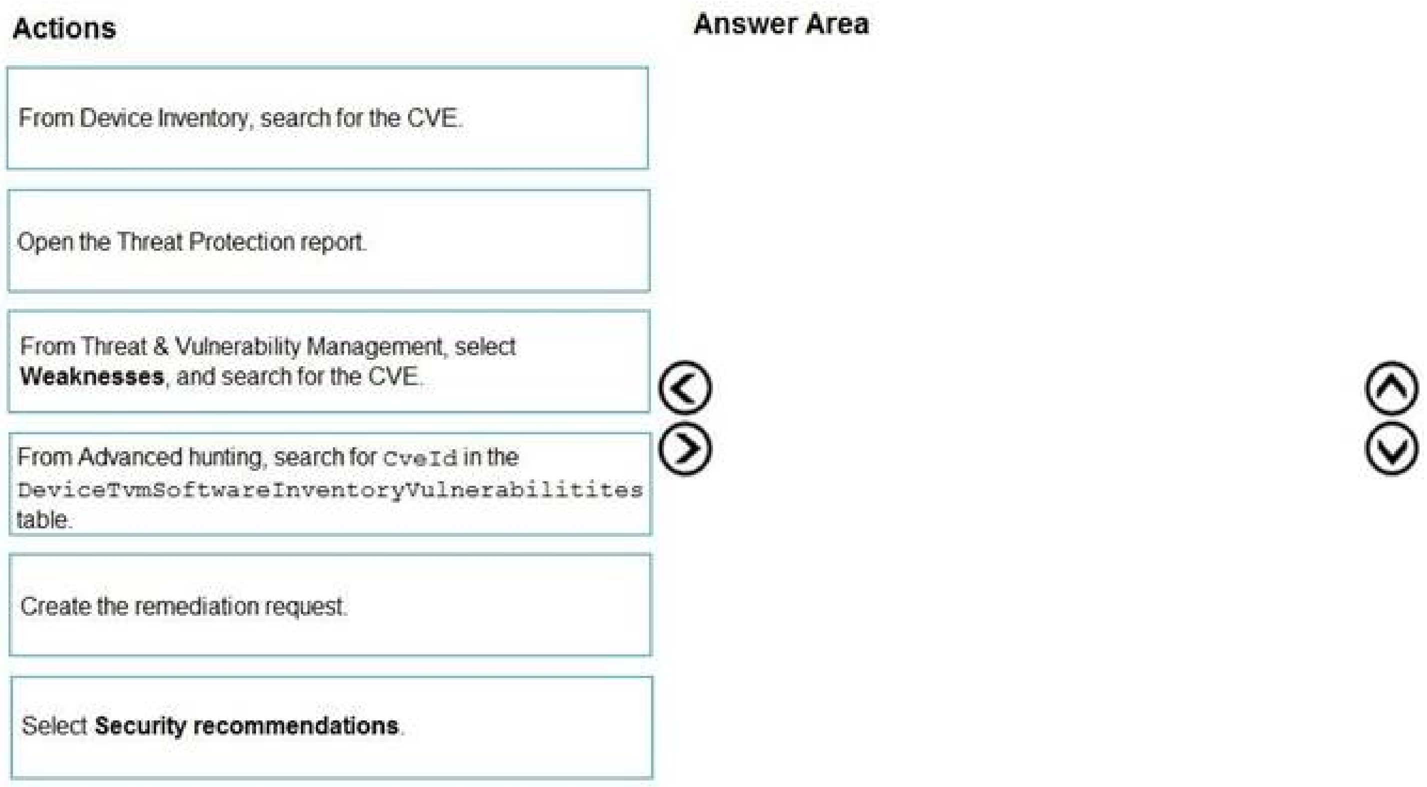
A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:
Reference:

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

NEW QUESTION 192
DRAG DROP - (Topic 4)
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
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.



Actions

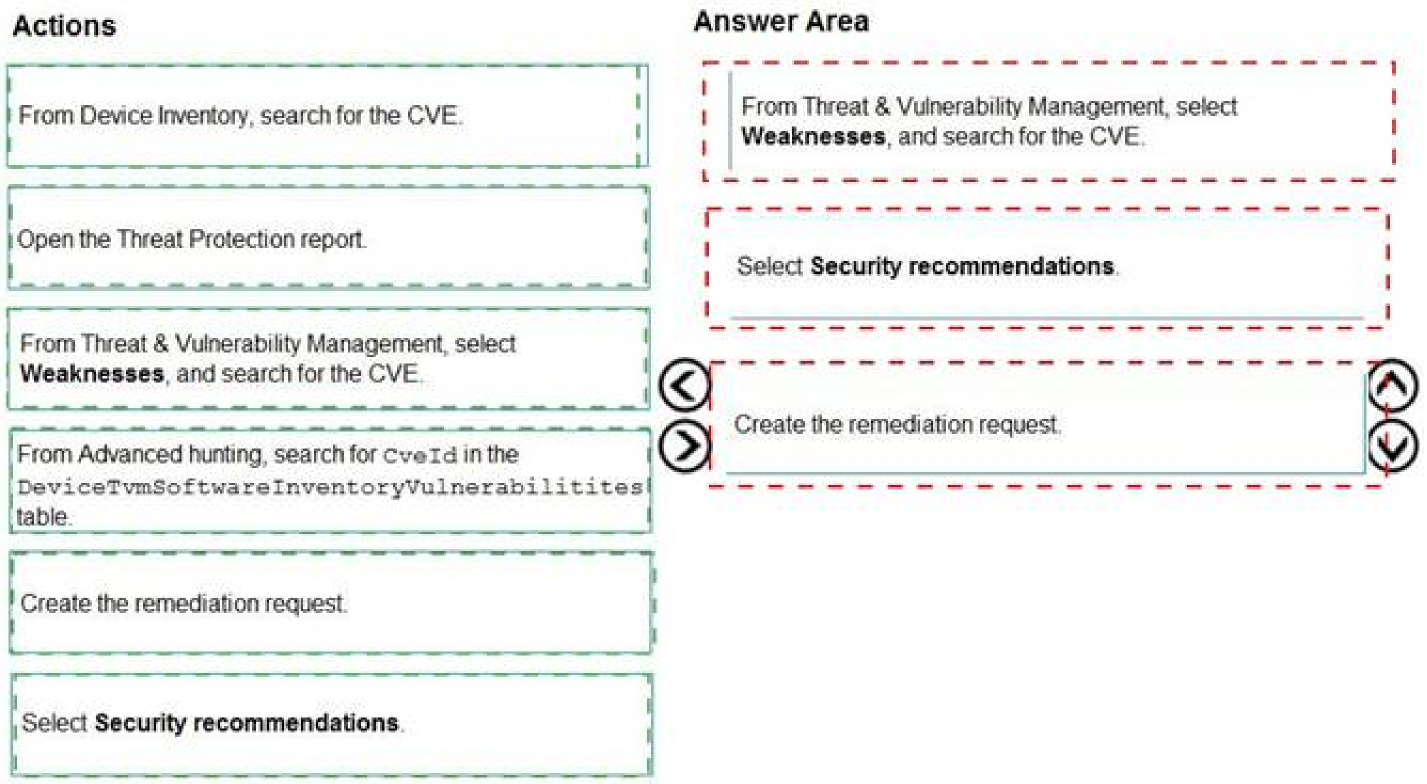
- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.
- Create the remediation request.
- Select **Security recommendations**.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



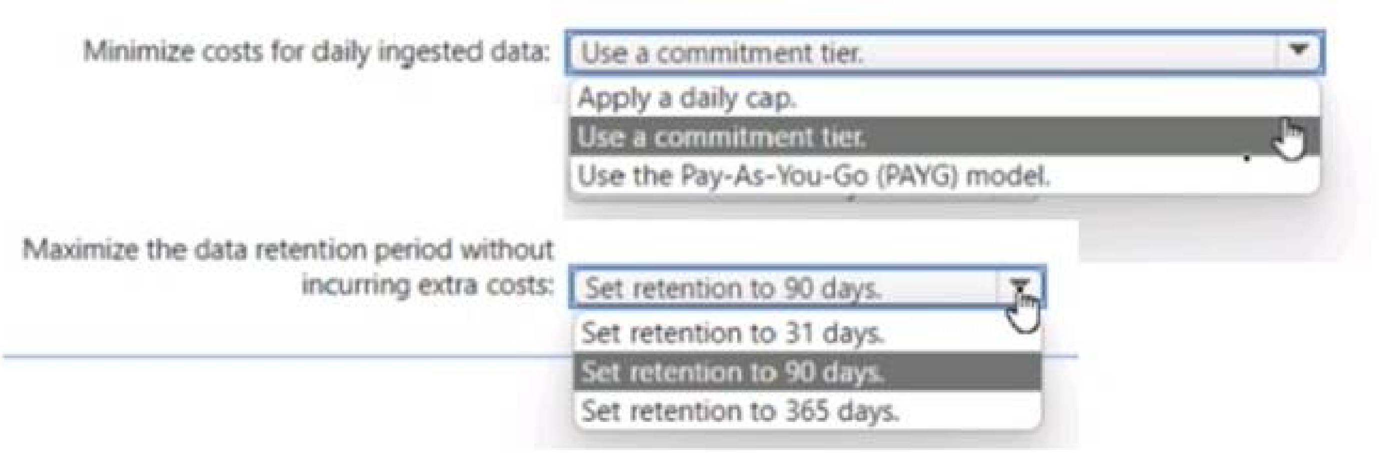
Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.
- Create the remediation request.
- Select **Security recommendations**.

Answer Area

1. From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
2. Select **Security recommendations**.
3. Create the remediation request.

NEW QUESTION 195
HOTSPOT - (Topic 4)
You have an Azure subscription.
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.
You need to configure storage for the workspace. The solution must meet the following requirements:
• Minimize costs for daily ingested data.
• Maximize the data retention period without incurring extra costs.
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



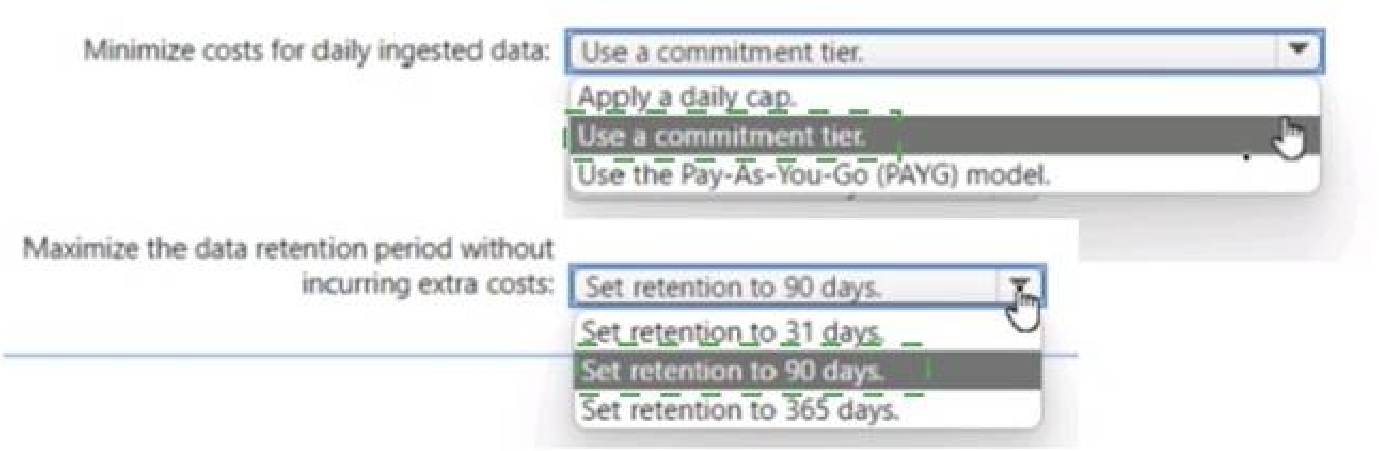
Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.
Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.
Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

NEW QUESTION 198
- (Topic 4)
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.

Answer: D

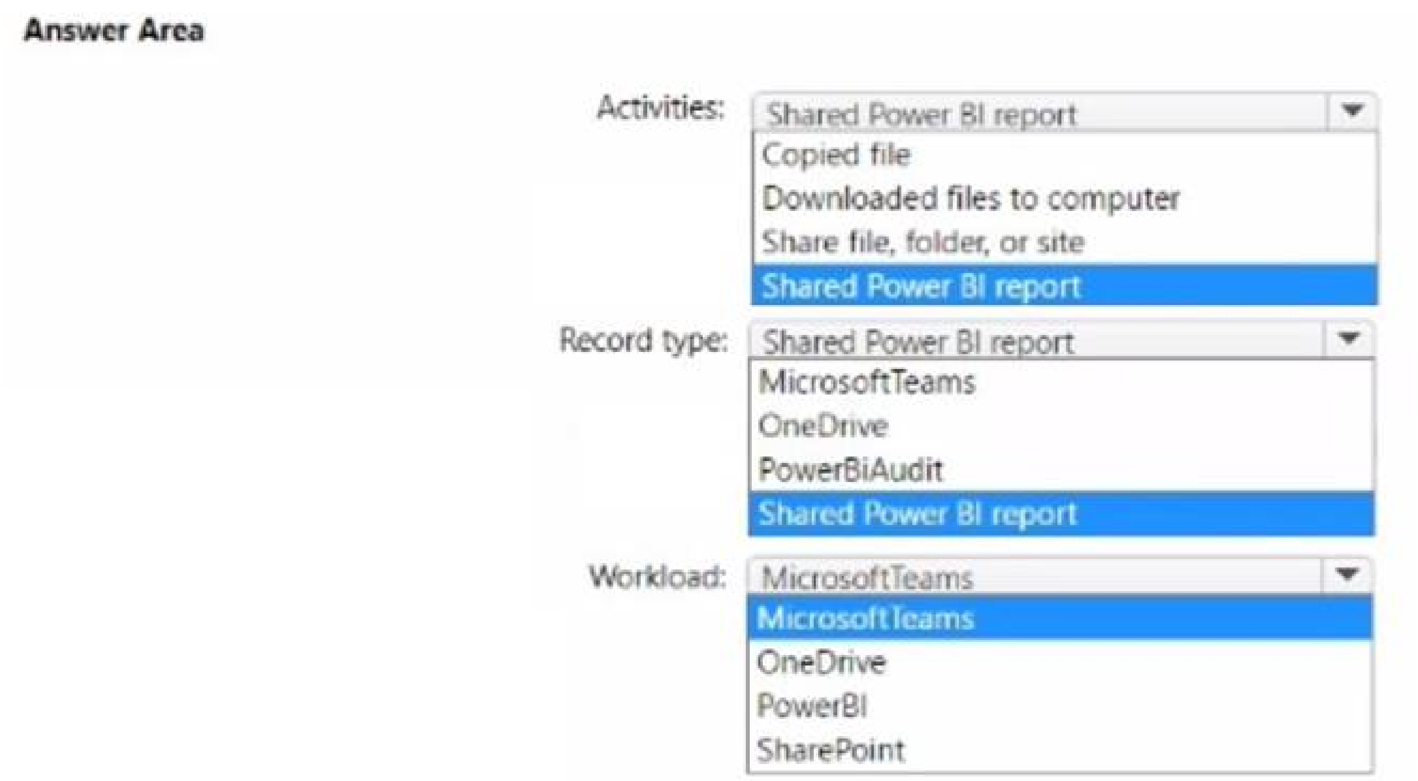
Explanation:
Reference:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email- automatically/

NEW QUESTION 202
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.
You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:
• Minimize administrative effort
• Minimize the parsing required to read log data What should you configure?

A. REST API integration
B. a SysJog connector
C. a Log Analytics Data Collector API
D. a Common Event Format (CEF) connector

Answer: B

NEW QUESTION 207
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.
User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.
You need to identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Activities: Shared Power BI report

Record type: Shared Power BI report

Workload: MicrosoftTeams

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To identify which Power BI report file was shared by User1, you should configure the search with the following parameters:
? Activities: Shared Power BI report
? Record Type: PowerBiAudit
? Workload: PowerBi
These parameters will filter the search results to show only the events where a Power BI report was shared by a user in your organization. You can then look for the event that has User1 as the user ID and an external user as the recipient. The event details will show the name and URL of the Power BI report file that was shared. For more information,
see Search the audit log for events in Power BI and Search for content in the Microsoft Purview compliance portal.

NEW QUESTION 208
- (Topic 4)
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.
B. Hide the alert.
C. Create a suppression rule scoped to any device.
D. Create a suppression rule scoped to a device group.
E. Generate the alert.

Answer: BCE

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/manage-alerts

NEW QUESTION 212
- (Topic 4)
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only
B. a URL/domain indicator that has Action set to Alert and block
C. a file hash indicator that has Action set to Alert and block
D. a certificate indicator that has Action set to Alert and block

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

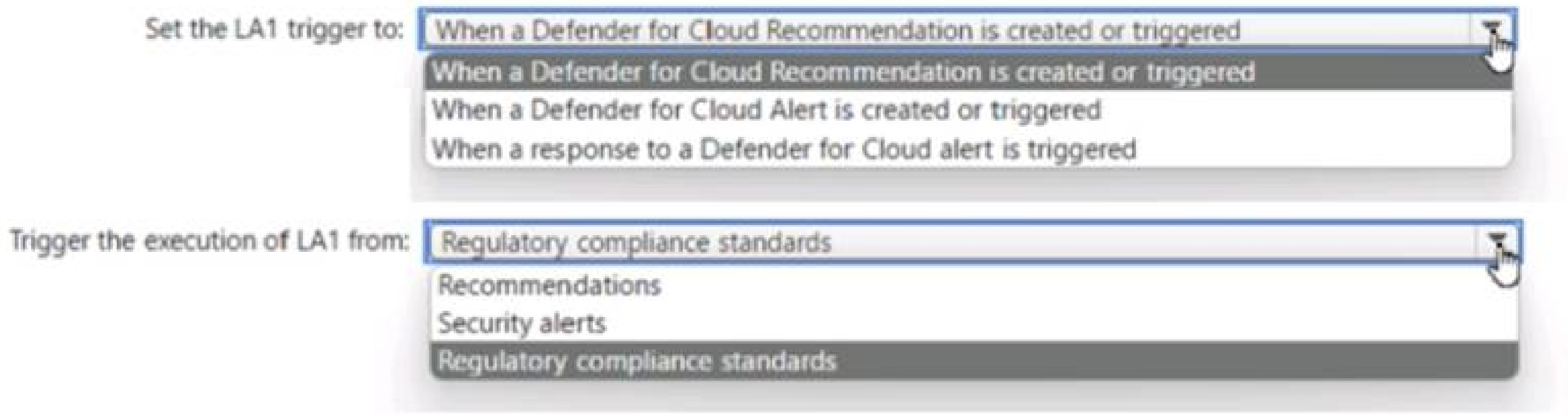
NEW QUESTION 214
- (Topic 4)
You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Override automatic data enrichment.
B. Add the IP addresses to the corporate address range category.
C. Increase the sensitivity level of the impossible travel anomaly detection policy.
D. Add the IP addresses to the other address range category and add a tag.
E. Create an activity policy that has an exclusion for the IP addresses.

Answer: AD

NEW QUESTION 217
HOTSPOT - (Topic 4)
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 Defenders for Cloud.
You need to test LA1 in Defender for Cloud.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

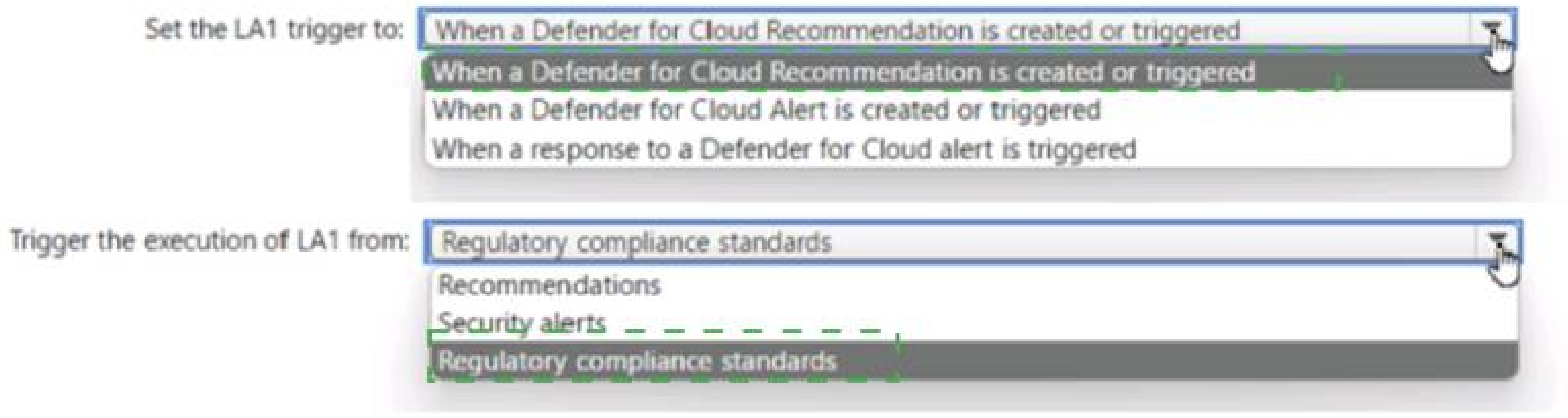

Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards
Recommendations
Security alerts
Regulatory compliance standards

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards
Recommendations
Security alerts
Regulatory compliance standards

NEW QUESTION 222
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

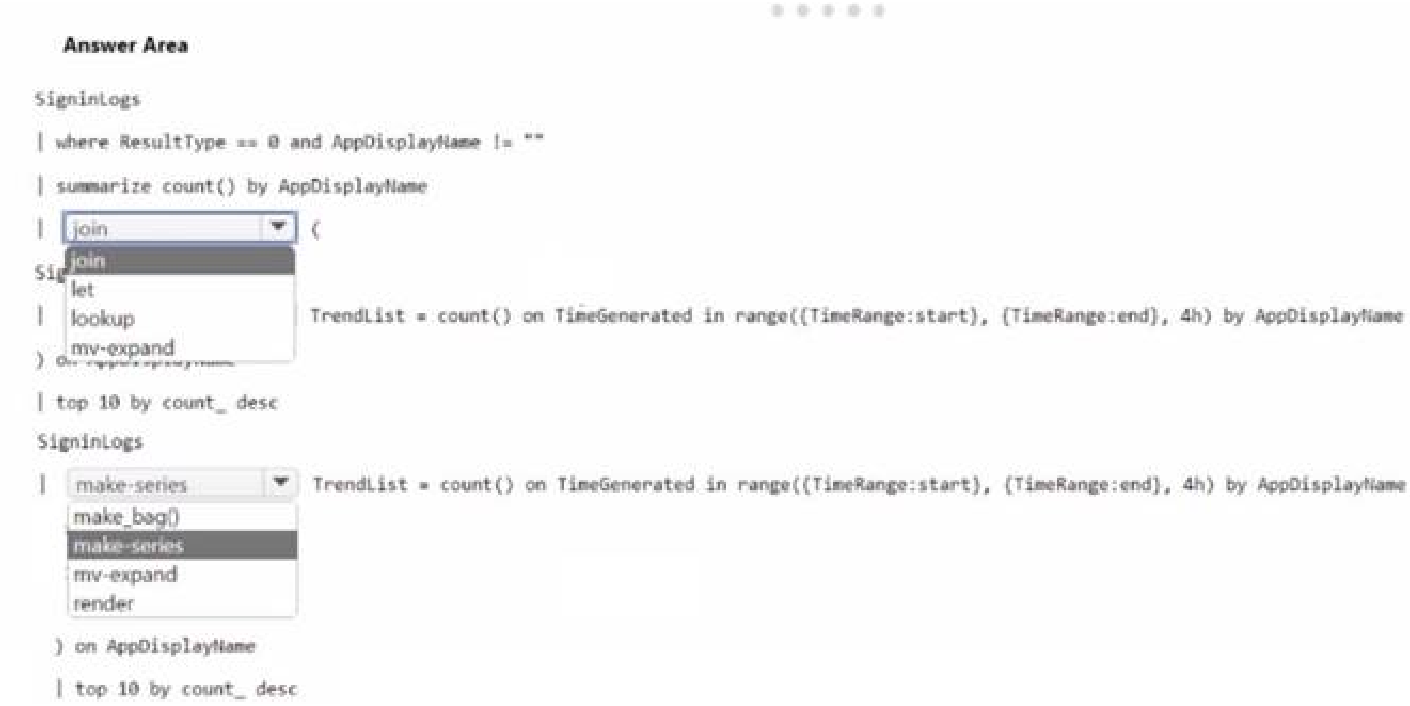
NEW QUESTION 227

- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

A. From Threat tracker, review the queries.
B. From the History tab in the Action center, revert the actions.
C. From the investigation page, review the AIR processes.
D. From Quarantine from the Review page, modify the rules.

Answer: B

NEW QUESTION 228
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to configure a report visual for a custom workbook. The solution must meet the following requirements:
• The count and usage trend of AppDisplayName must be included
• The TrendList column must be useable in a sparkline visual,
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



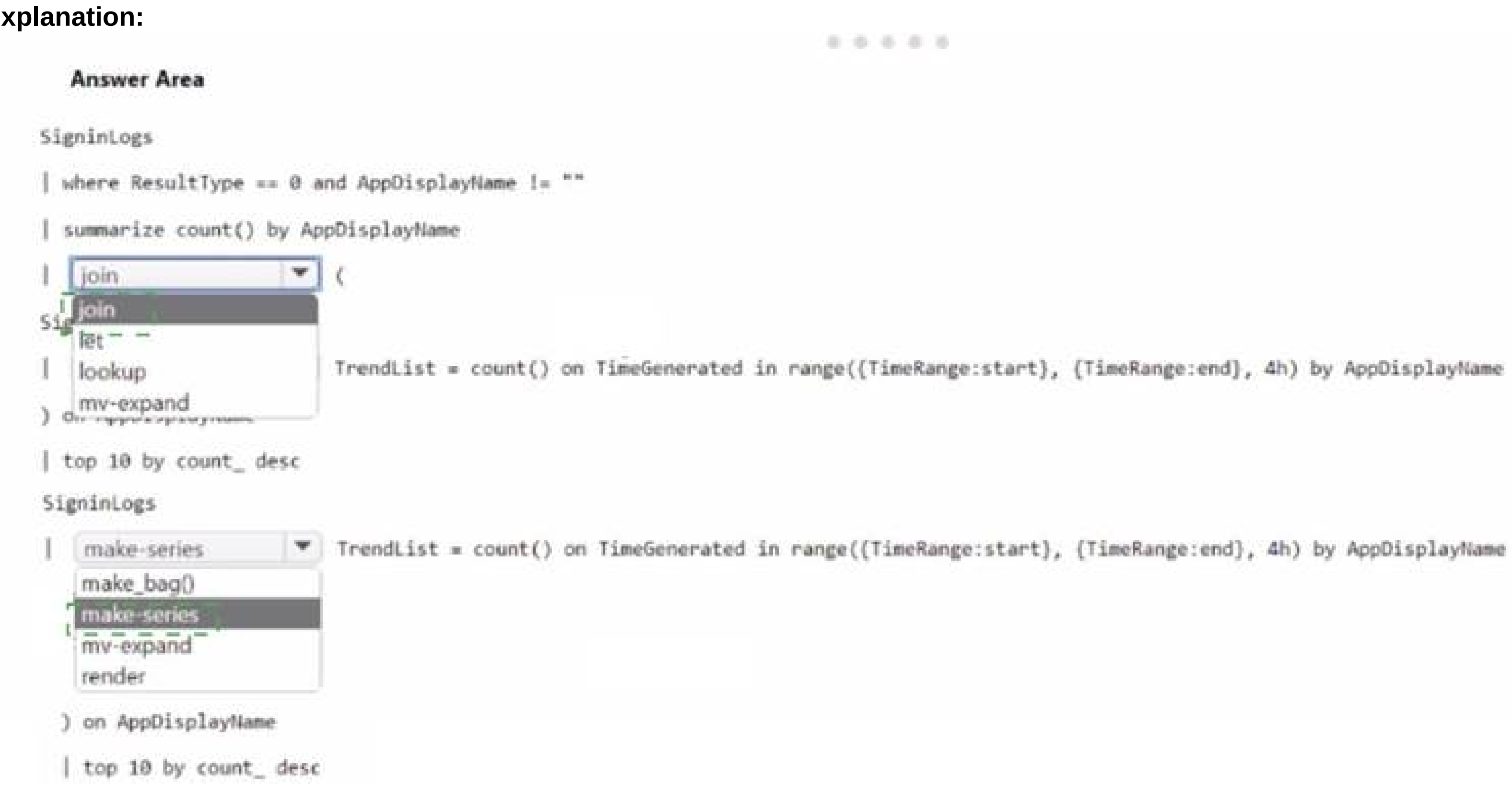
Answer Area

```
SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| join ▾ (
Sig
|        TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
) o
| top 10 by count_ desc
SigninLogs
| make-series ▾ TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
) on AppDisplayName
| top 10 by count_ desc
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

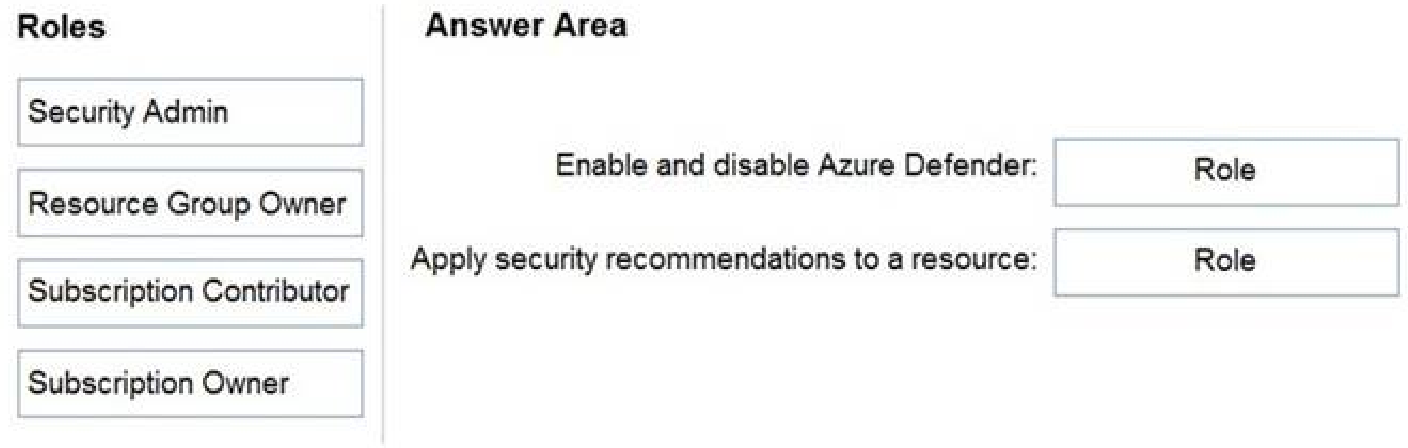
```
SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| join ▾ (
Si
|        TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
) o
| top 10 by count_ desc
SigninLogs
| make-series ▾ TrendList = count() on TimeGenerated in range({TimeRange:start}, {TimeRange:end}, 4h) by AppDisplayName
) on AppDisplayName
| top 10 by count_ desc
```

NEW QUESTION 232
- (Topic 4)
You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.
You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

A. the Incident automation settings
B. entity mapping
C. the query rule
D. the Alert automation settings

Answer: B

NEW QUESTION 234
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
? Enable and disable Azure Defender.
? Apply security recommendations to resource.
The solution must use the principle of least privilege.
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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.
NOTE: Each correct selection is worth one point.



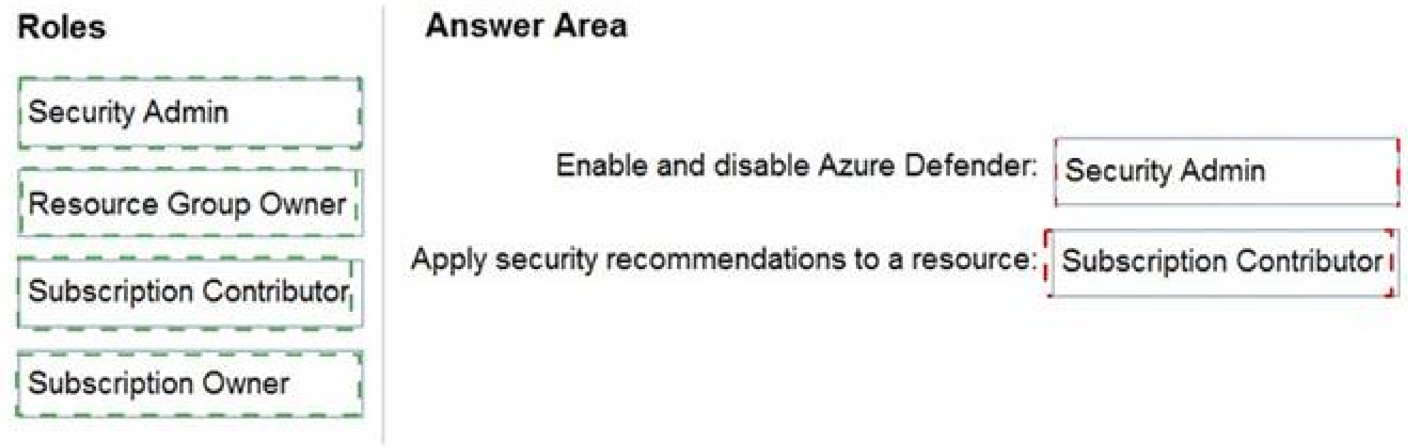
Roles
Security Admin
Resource Group Owner
Subscription Contributor
Subscription Owner

Answer Area
Enable and disable Azure Defender: Role
Apply security recommendations to a resource: Role

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Roles
Security Admin
Resource Group Owner
Subscription Contributor
Subscription Owner

Answer Area
Enable and disable Azure Defender: Security Admin
Apply security recommendations to a resource: Subscription Contributor

NEW QUESTION 236
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
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 have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 241
- (Topic 4)
A company uses Azure Sentinel.
You need to create an automated threat response. What should you use?

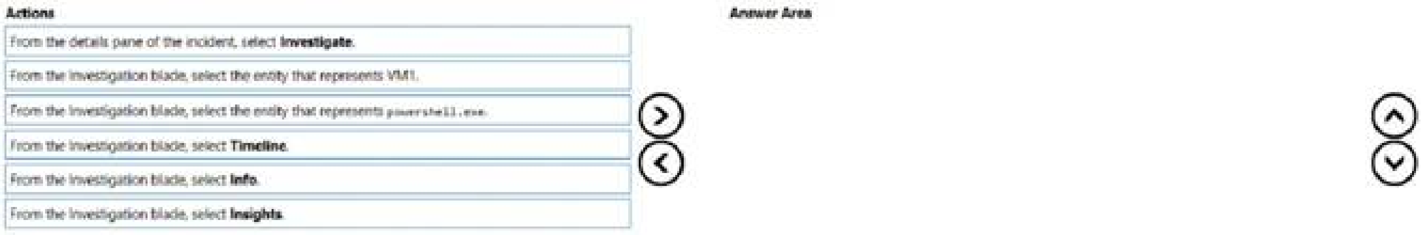
A. a data connector
B. a playbook
C. a workbook
D. a Microsoft incident creation rule

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION 242
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
? The modification of local group memberships
? The purging of event logs
Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

- From the details pane of the incident, select **Investigate**.
- From the investigation blade, select the entity that represents VM1.
- From the investigation blade, select the entity that represents `powershell.exe`.
- From the investigation blade, select **Timeline**.
- From the investigation blade, select **Info**.
- From the investigation blade, select **Insights**.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: From the Investigation blade, select Insights
The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.
Step 2: From the Investigation blade, select the entity that represents VM1.
The Investigation Insights workbook is broken up into 2 main sections, Incident Insights
and Entity Insights.
Incident Insights
The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.
Entity Insights
The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:
IP Address Account Host
URL
Step 3: From the details pane of the incident, select Investigate. Choose a single incident and click View full details or Investigate.

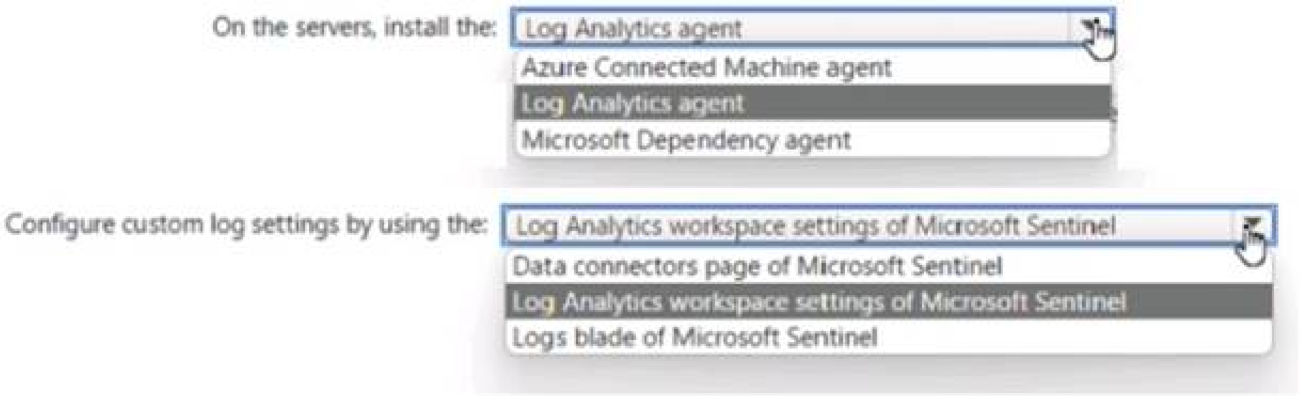
NEW QUESTION 246
- (Topic 4)
You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident. What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:
Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

NEW QUESTION 251
HOTSPOT - (Topic 4)
Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.
You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options m the answer area.



On the servers, install the: Log Analytics agent
- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel
- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

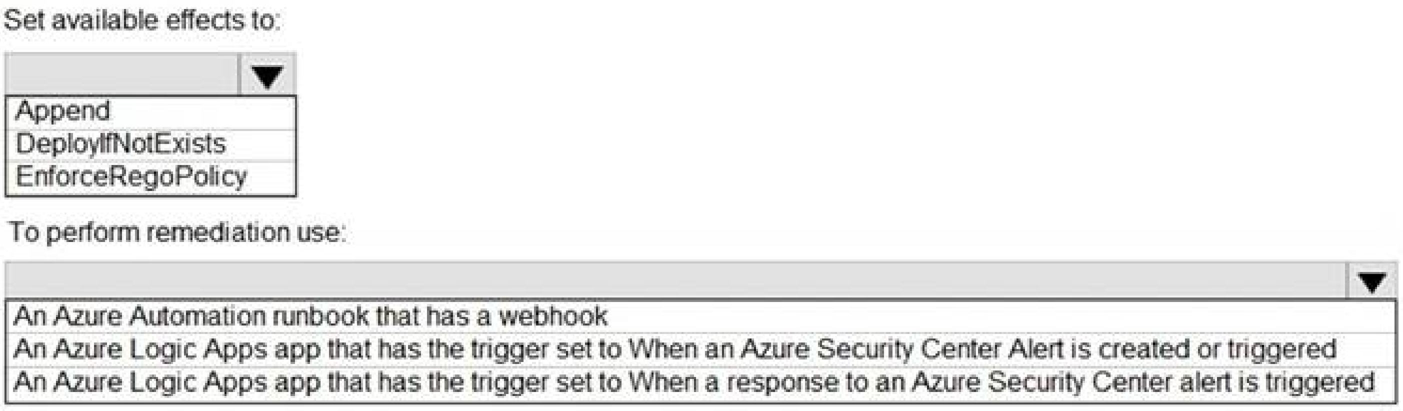
A. Mastered

B. Not Mastered

Answer: A

Explanation:
To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a
lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

NEW QUESTION 254
HOTSPOT - (Topic 4)
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.



Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

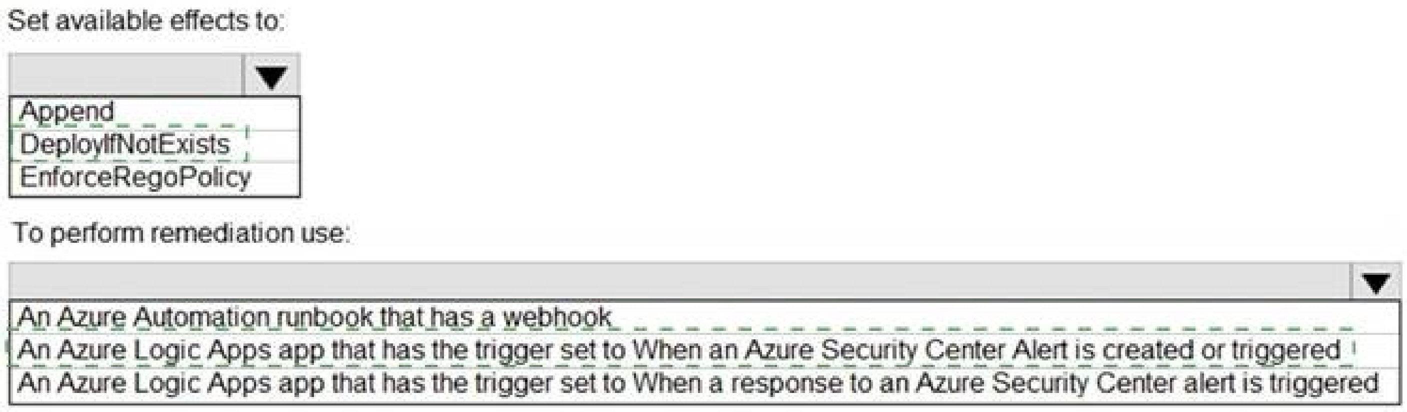
To perform remediation use:

- 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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



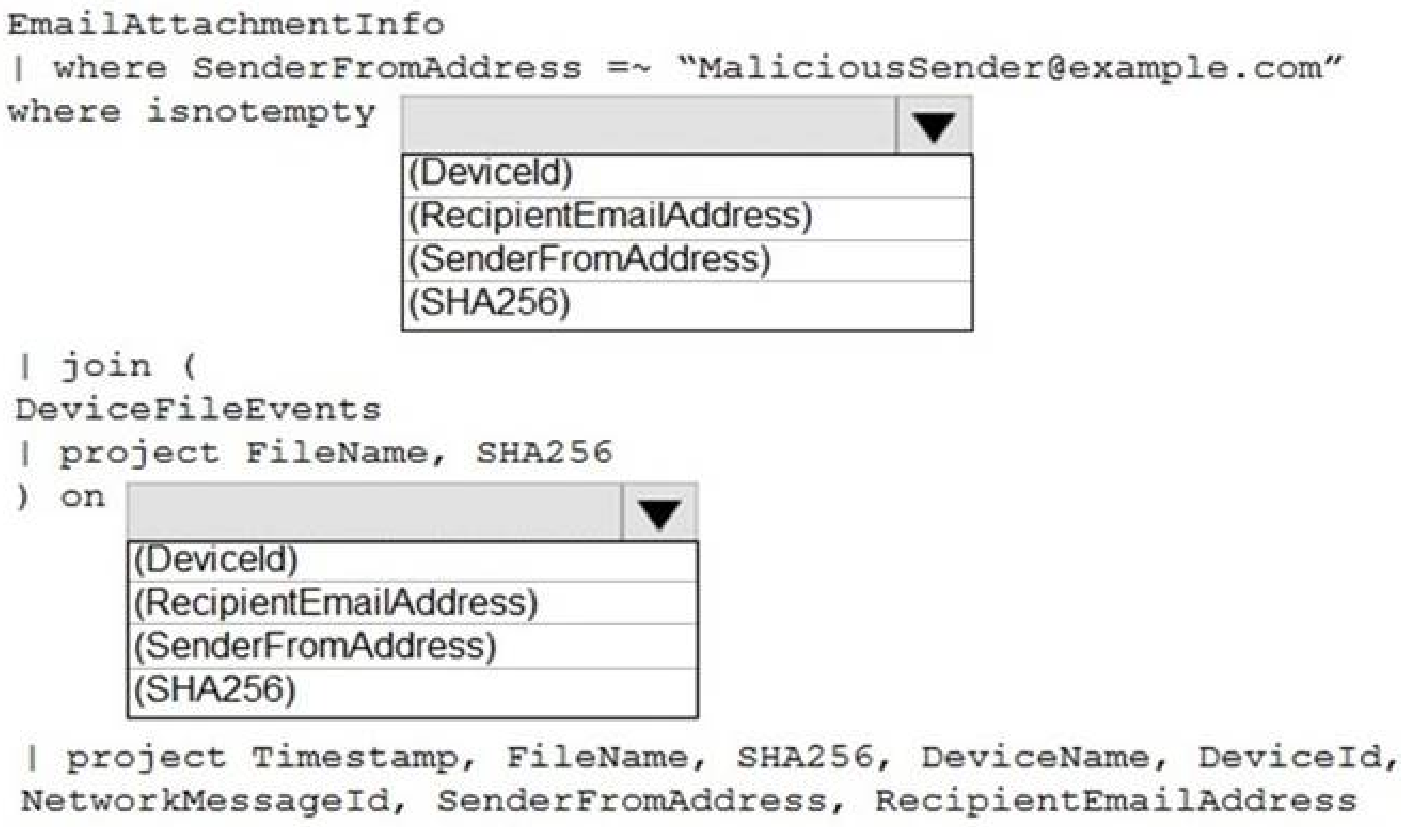
Set available effects to:

- 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

NEW QUESTION 259
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

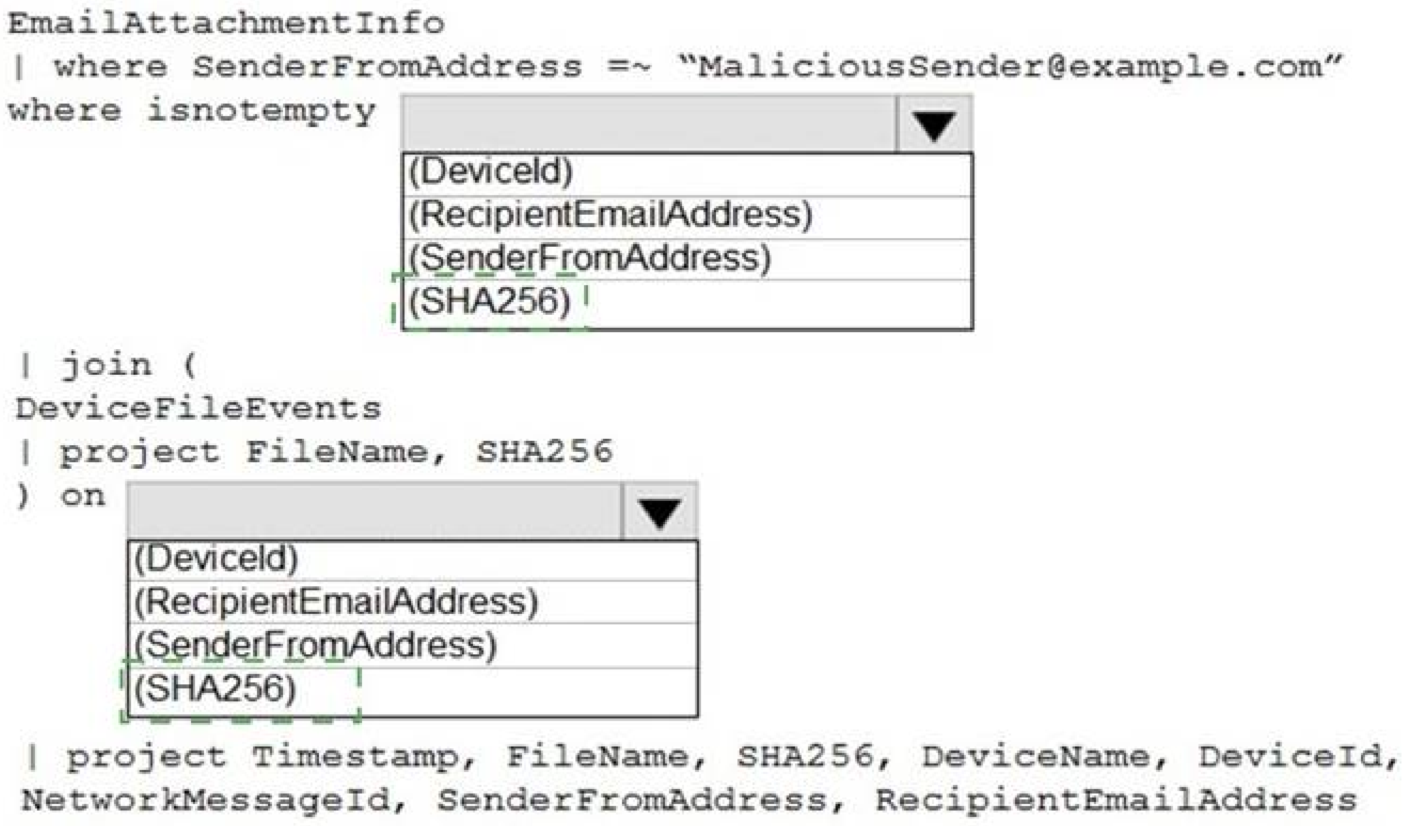


```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [▼]
                 (DeviceId)
                 (RecipientEmailAddress)
                 (SenderFromAddress)
                 (SHA256)
| join (
DeviceFileEvents
| project FileName, SHA256
) on [▼]
     (DeviceId)
     (RecipientEmailAddress)
     (SenderFromAddress)
     (SHA256)
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

A. Mastered
B. Not Mastered

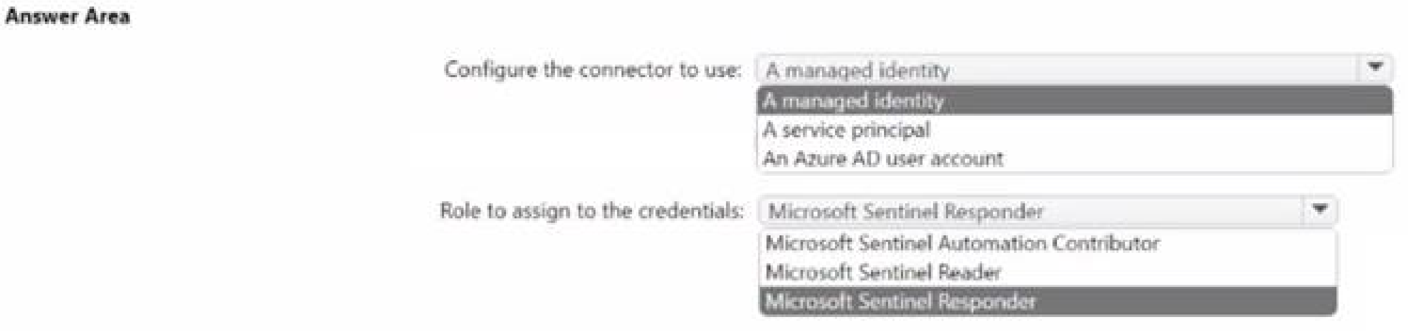
Answer: A

Explanation:



```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [▼]
                 (DeviceId)
                 (RecipientEmailAddress)
                 (SenderFromAddress)
                 (SHA256)
| join (
DeviceFileEvents
| project FileName, SHA256
) on [▼]
     (DeviceId)
     (RecipientEmailAddress)
     (SenderFromAddress)
     (SHA256)
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

NEW QUESTION 263
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:
• Minimize administrative effort.
• Use the principle of least privilege.
How should you configure the credentials? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

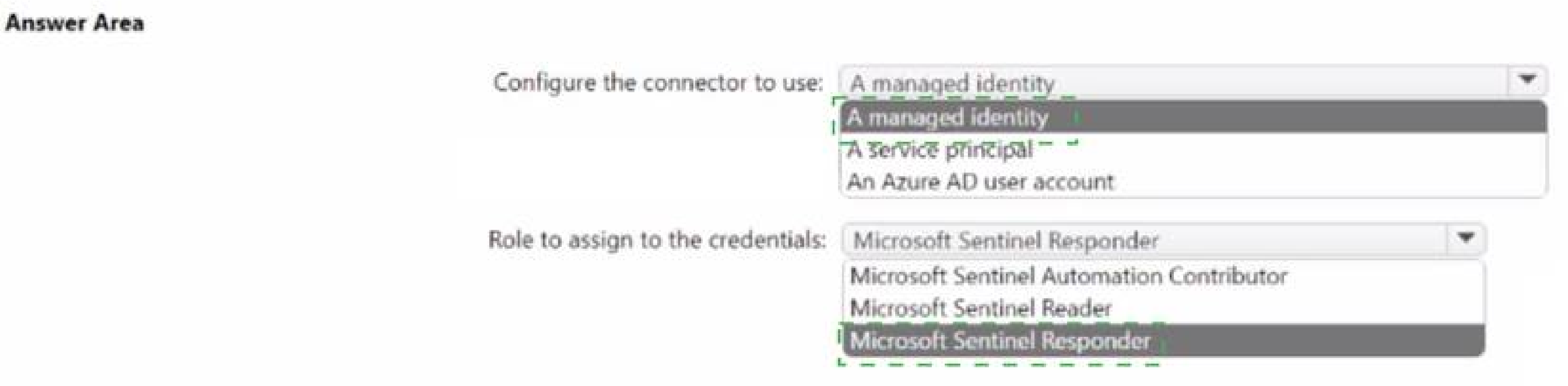
Configure the connector to use: A managed identity ▼
- A managed identity
- A service principal
- An Azure AD user account

Role to assign to the credentials: Microsoft Sentinel Responder ▼
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Configure the connector to use: A managed identity
- A managed identity
- A service principal
- An Azure AD user account

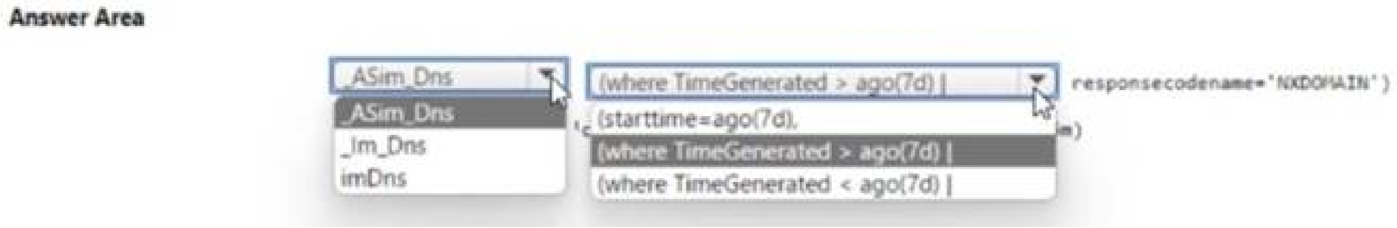
Role to assign to the credentials: Microsoft Sentinel Responder
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder

NEW QUESTION 268

HOTSPOT - (Topic 4)

You need to create a query to investigate DNS-related activity. 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.



Answer Area

_ASim_Dns
- _ASim_Dns
- _Im_Dns
- imDns

(where TimeGenerated > ago(7d) |
- (starttime=ago(7d),
- (where TimeGenerated > ago(7d) |
- (where TimeGenerated < ago(7d) |

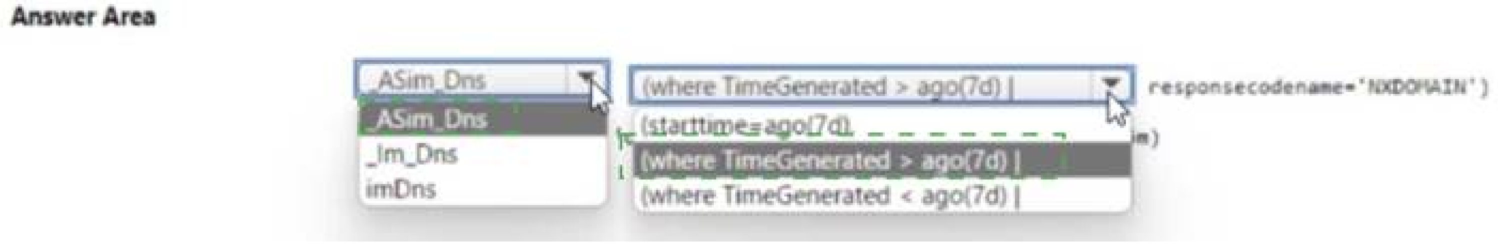
responsecodename='NXDOMAIN')

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

_ASim_Dns
- _ASim_Dns
- _Im_Dns
- imDns

(where TimeGenerated > ago(7d) |
- (starttime=ago(7d),
- (where TimeGenerated > ago(7d) |
- (where TimeGenerated < ago(7d) |

responsecodename='NXDOMAIN')

NEW QUESTION 270

- (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort

Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting

B. Threat analytics

C. Incidents & alerts

D. Learning hub

Answer: B

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment. Reference: https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender-threat-analytics

NEW QUESTION 272

- (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

A. Incidents

B. Investigations

C. Advanced hunting

D. Remediation

Answer: A

NEW QUESTION 273

......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-200 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-200 Product From:

https://www.2passeasy.com/dumps/SC-200/

Money Back Guarantee

SC-200 Practice Exam Features:

* SC-200 Questions and Answers Updated Frequently

* SC-200 Practice Questions Verified by Expert Senior Certified Staff

* SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year