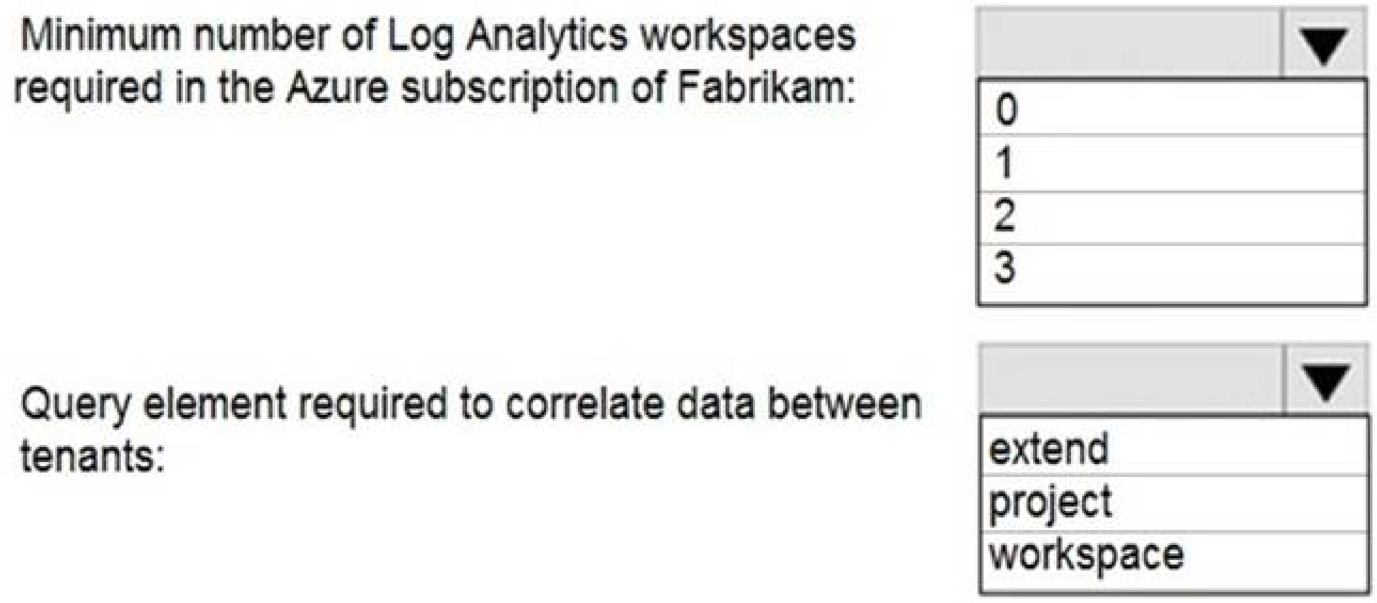
Exam Questions SC-200

Microsoft Security Operations Analyst

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

NEW QUESTION 1
HOTSPOT - (Topic 1)
You need to implement Azure 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.



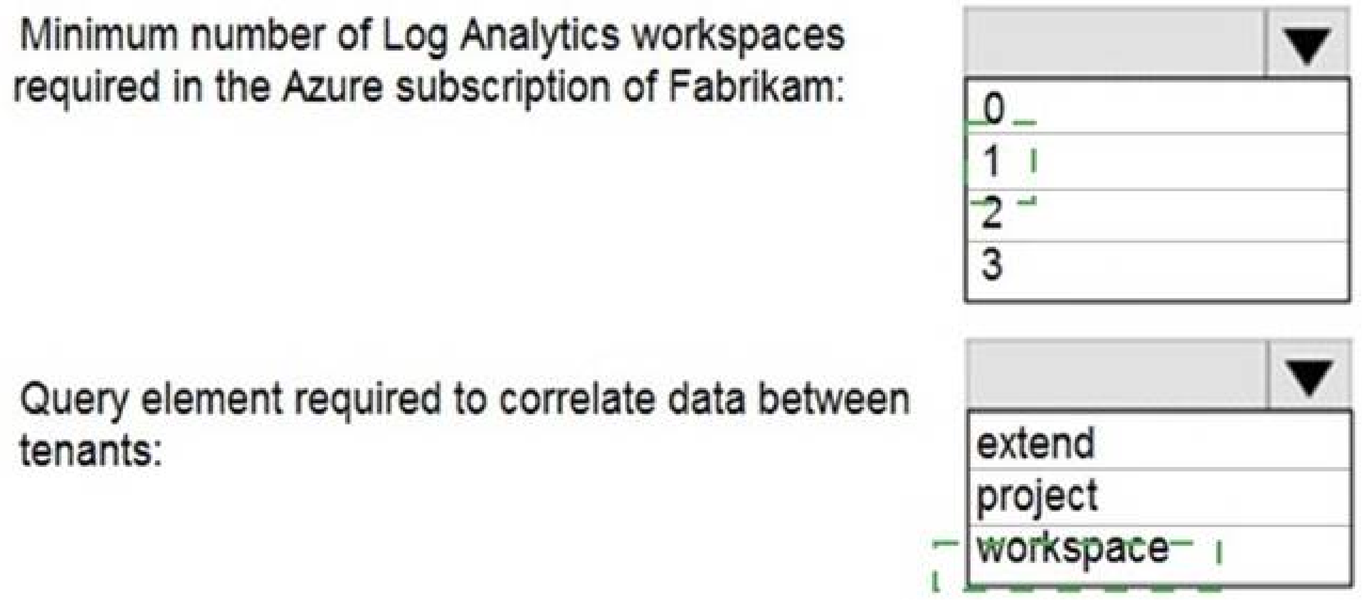
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: ▼
0
1
2
3

Query element required to correlate data between tenants: ▼
extend
project
workspace

A. Mastered
B. Not Mastered

Answer: A

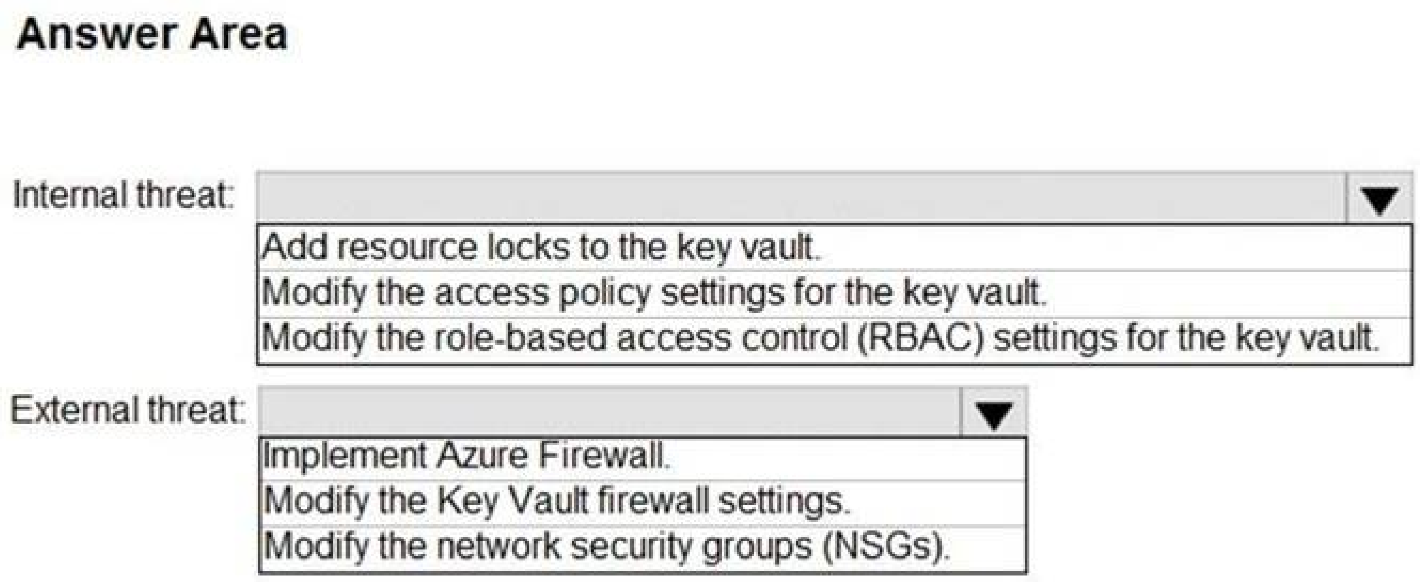
Explanation:



Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: ▼
0
[✓ 1]
2
3

Query element required to correlate data between tenants: ▼
extend
project
[✓ workspace]

NEW QUESTION 2
HOTSPOT - (Topic 1)
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

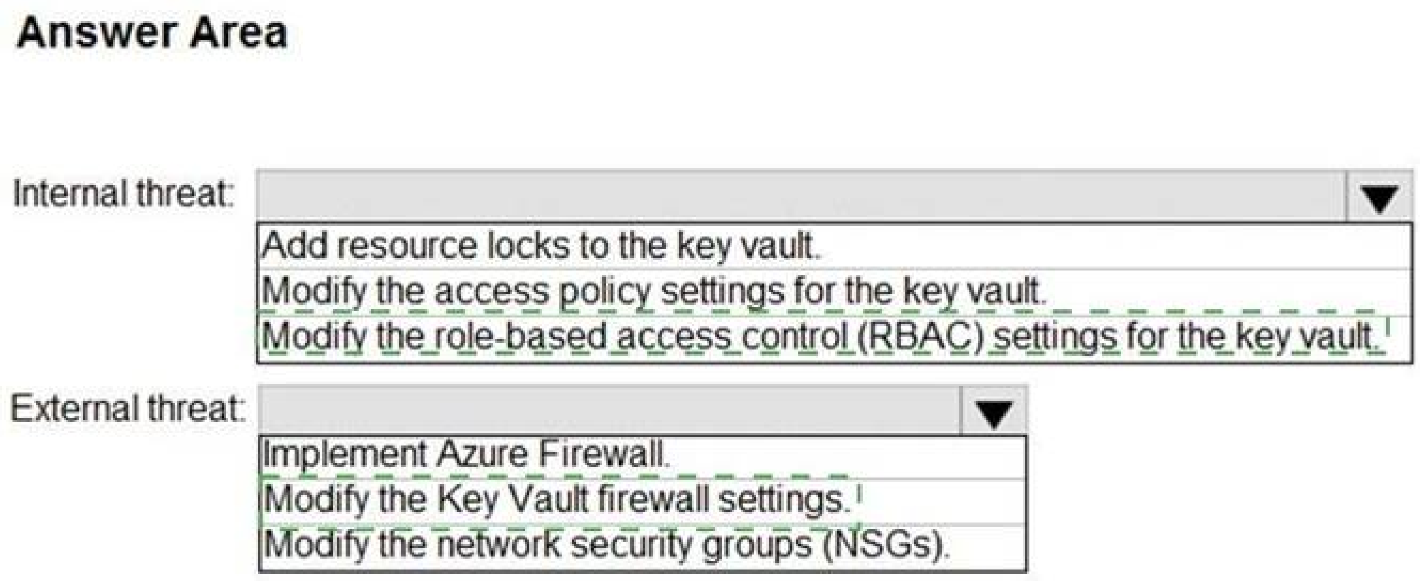
Internal threat: ▼
Add resource locks to the key vault.
Modify the access policy settings for the key vault.
Modify the role-based access control (RBAC) settings for the key vault.

External threat: ▼
Implement Azure Firewall.
Modify the Key Vault firewall settings.
Modify the network security groups (NSGs).

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Internal threat:
- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- [✓ Modify the role-based access control (RBAC) settings for the key vault.]

External threat:
- Implement Azure Firewall.
- [✓ Modify the Key Vault firewall settings.]
- Modify the network security groups (NSGs).

NEW QUESTION 3
- (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

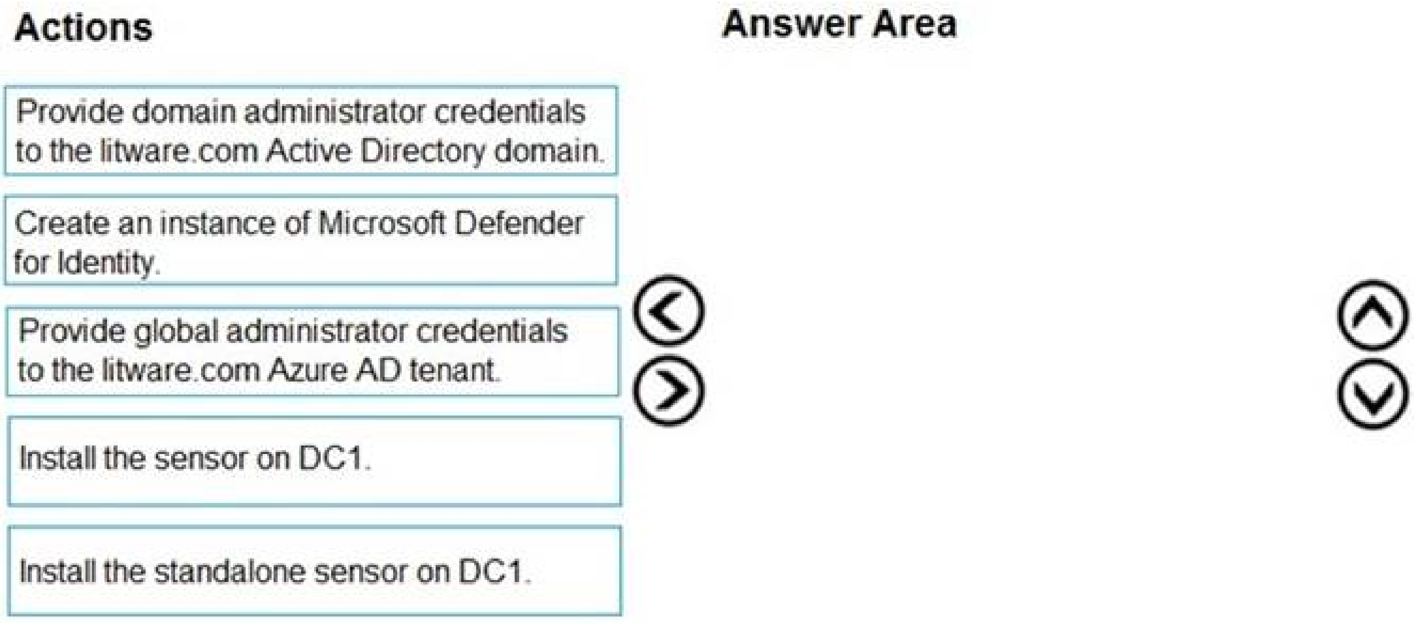
NEW QUESTION 4
- (Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive
B. sales
C. marketing

Answer: B

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

NEW QUESTION 5
DRAG DROP - (Topic 2)
You need to configure DC1 to meet the business requirements.
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

- Provide domain administrator credentials to the litware.com Active Directory domain.
- Create an instance of Microsoft Defender for Identity.
- Provide global administrator credentials to the litware.com Azure AD tenant.
- Install the sensor on DC1.
- Install the standalone sensor on DC1.

Answer Area

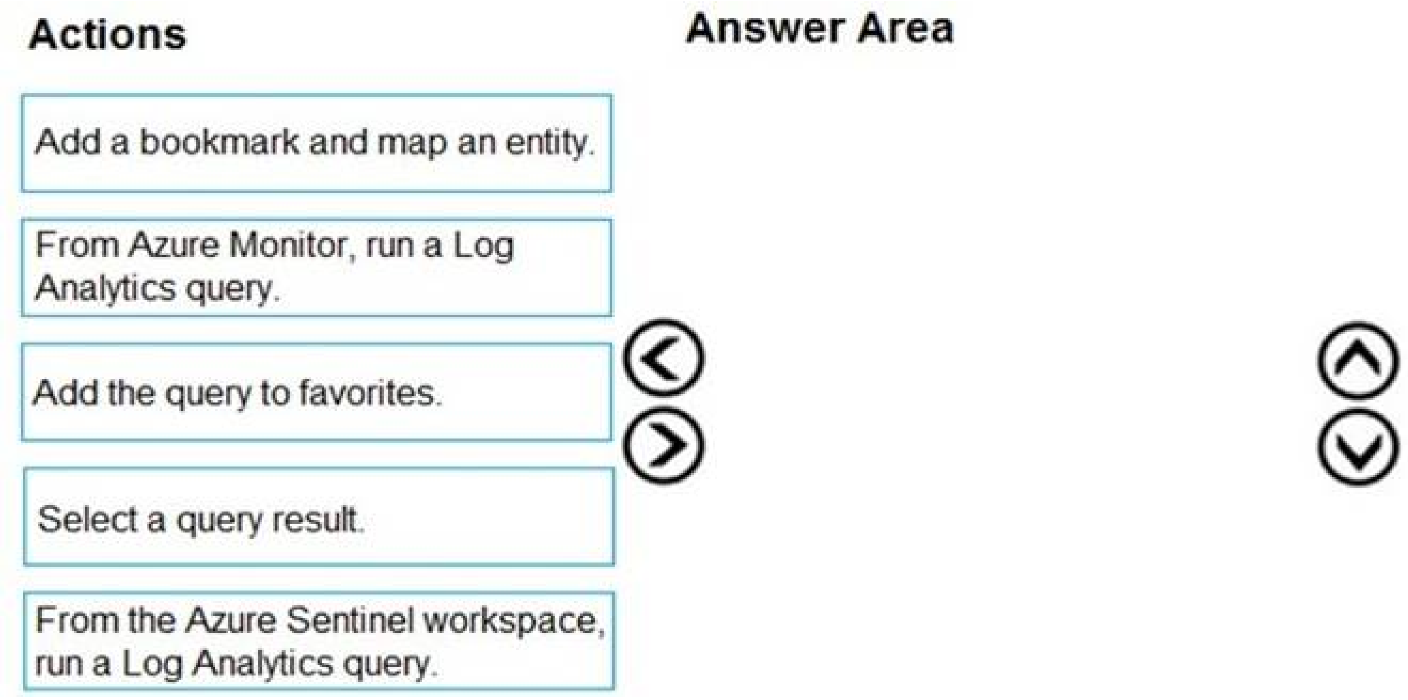
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence

Step 1: log in to https://portal.atp.azure.com as a global admin
Step 2: Create the instance
Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor.

NEW QUESTION 6
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

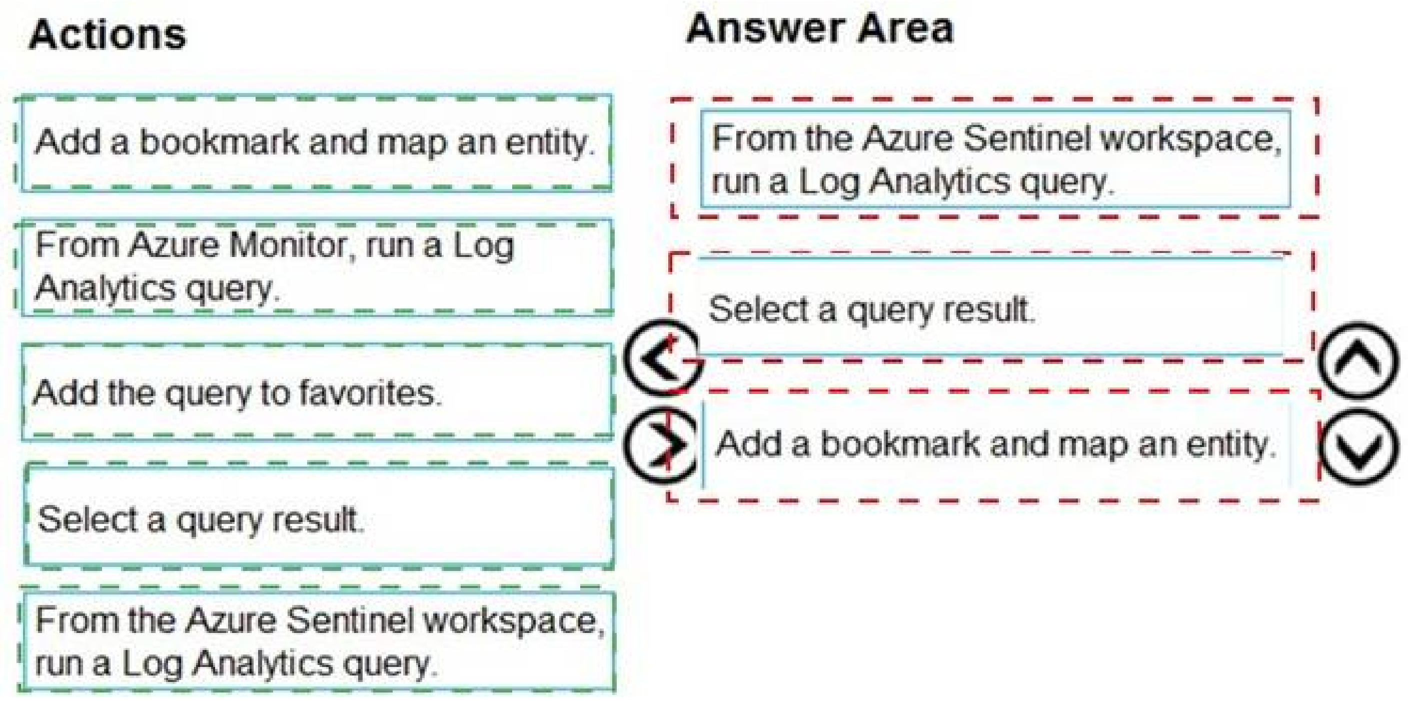
- Add a bookmark and map an entity.
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
- Select a query result.
- From the Azure Sentinel workspace, run a Log Analytics query.

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

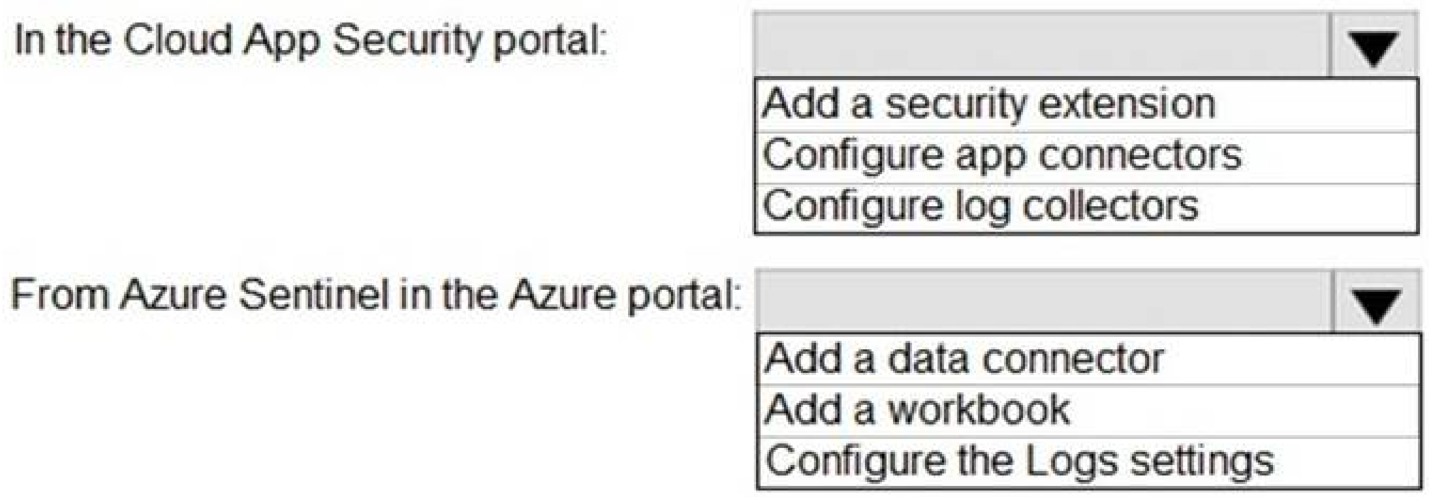
- From the Azure Sentinel workspace, run a Log Analytics query.
- Select a query result.
- Add a bookmark and map an entity.

NEW QUESTION 7
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.
Which policy should you modify?

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

Answer: D

NEW QUESTION 8
HOTSPOT - (Topic 2)
You need to configure the Azure Sentinel integration 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.



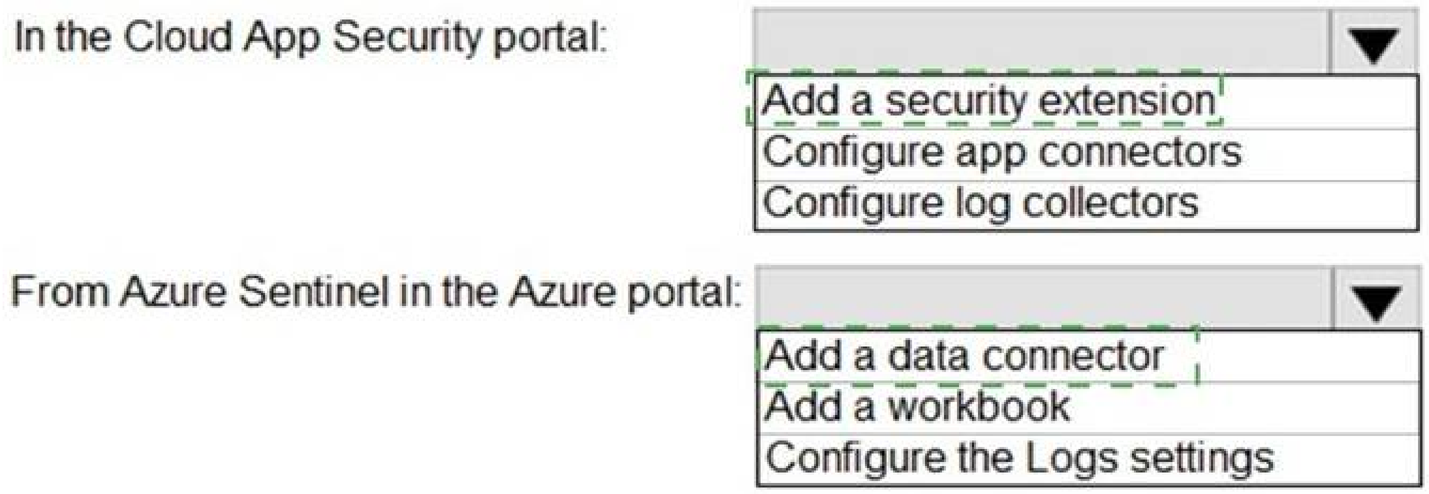
In the Cloud App Security portal:
Add a security extension
Configure app connectors
Configure log collectors

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



In the Cloud App Security portal:
Add a security extension
Configure app connectors
Configure log collectors

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

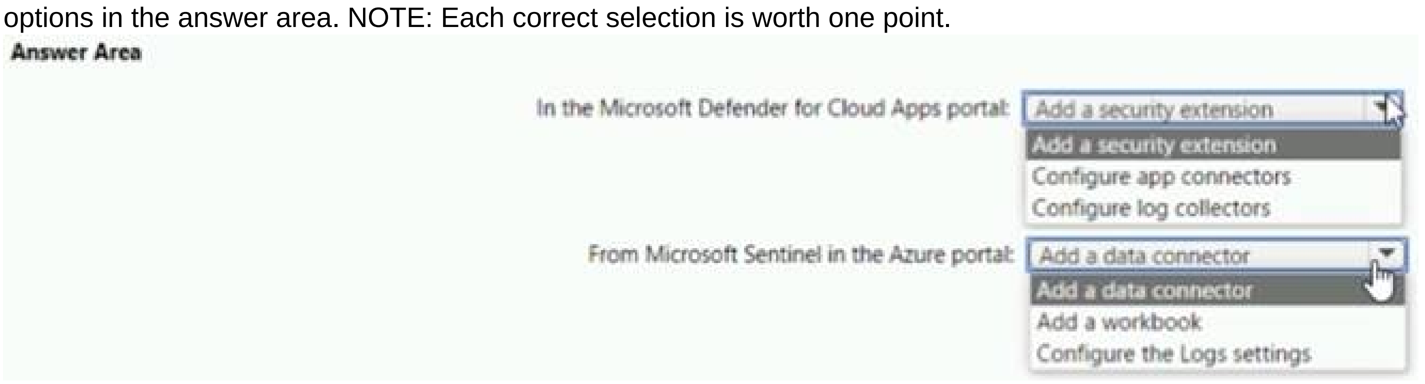
NEW QUESTION 9
- (Topic 2)
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the
solution.
NOTE: Each correct selection is worth one point.

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 10
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

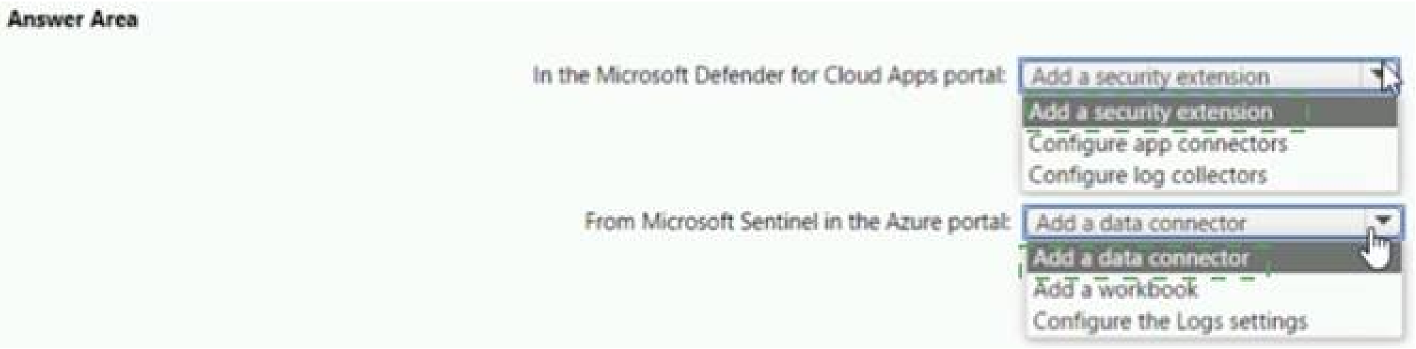
In the Microsoft Defender for Cloud Apps portal: Add a security extension
Add a security extension
Configure app connectors
Configure log collectors

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

From Microsoft Sentinel in the Azure portal: Add a data connector

NEW QUESTION 10
- (Topic 2)
Which rule setting should you configure to meet the Microsoft Sentinel requirements?

A. From Set rule logic, turn off suppression.
B. From Analytic rule details, configure the tactics.
C. From Set rule logic, map the entities.
D. From Analytic rule details, configure the severity.

Answer: C

NEW QUESTION 15
- (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 19
- (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

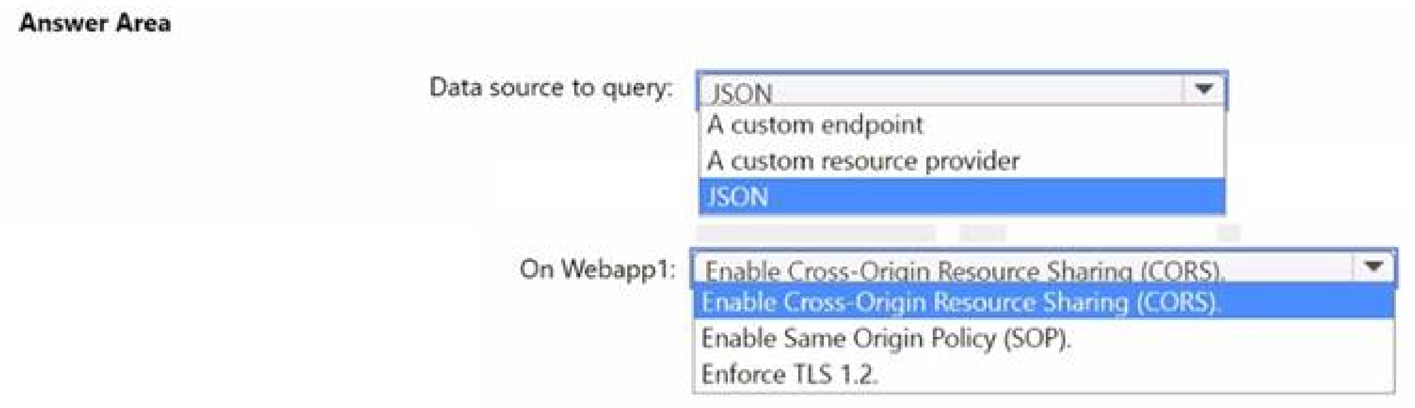
NEW QUESTION 22
- (Topic 2)
You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

A. From Set rule logic, turn off suppression.
B. From Analytics rule details, configure the tactics.
C. From Set rule logic, map the entities.
D. From Analytics rule details, configure the severity.

Answer: C

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

NEW QUESTION 24
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

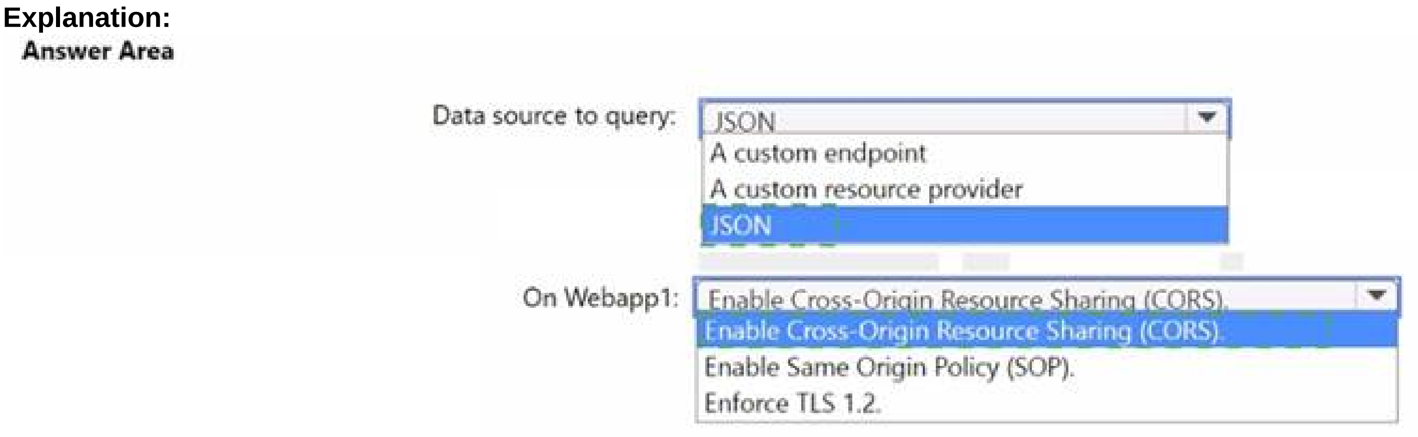
Data source to query: JSON
A custom endpoint
A custom resource provider
JSON

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 28

- (Topic 3)

You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?

A. a Microsoft Sentinel automation rule
B. a Microsoft Sentinel scheduled query rule
C. a Data Collection Rule (DCR)
D. an Azure Event Grid topic

Answer: C

NEW QUESTION 31

- (Topic 3)

You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

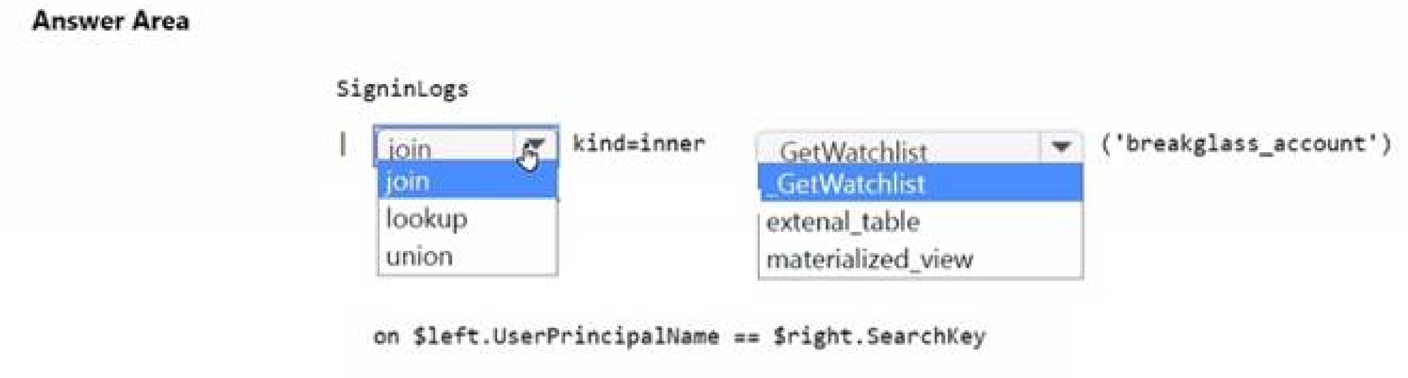
A. Microsoft Sentinel Automation Contributor
B. Logic App Contributor
C. Automation Operator
D. Microsoft Sentinel Playbook Operator

Answer: D

NEW QUESTION 34

HOTSPOT - (Topic 3)

You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The solution must meet the Microsoft Sentinel requirements.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

```
SigninLogs
| [join ▼] kind=inner [GetWatchlist ▼] ('breakglass_account')
on $left.UserPrincipalName == $right.SearchKey
```

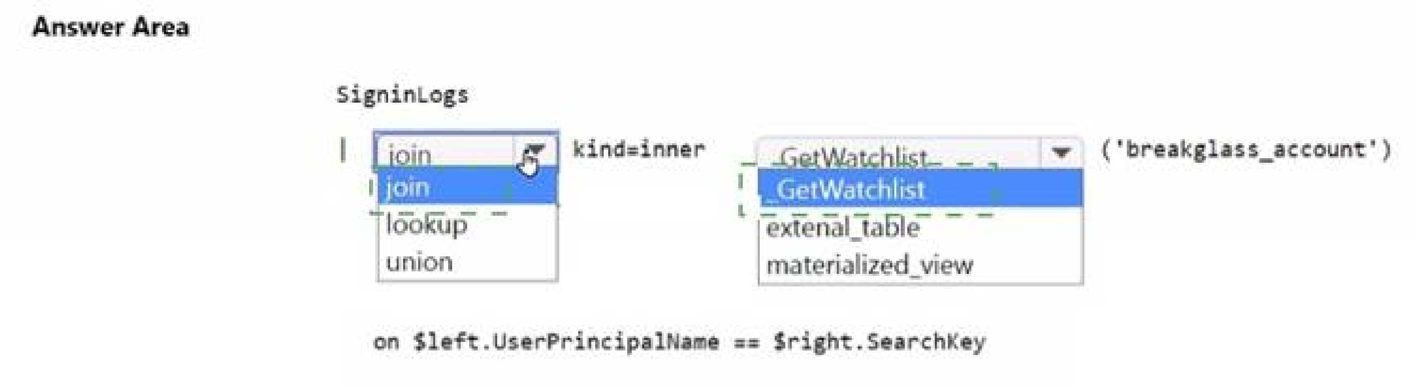
join
lookup
union

GetWatchlist
extenal_table
materialized_view

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 35
- (Topic 3)
You need to implement the Defender for Cloud requirements. What should you configure for Server2?

A. the Microsoft Antimalware extension
B. an Azure resource lock
C. an Azure resource tag
D. the Azure Automanage machine configuration extension for Windows

Answer: D

NEW QUESTION 39
- (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

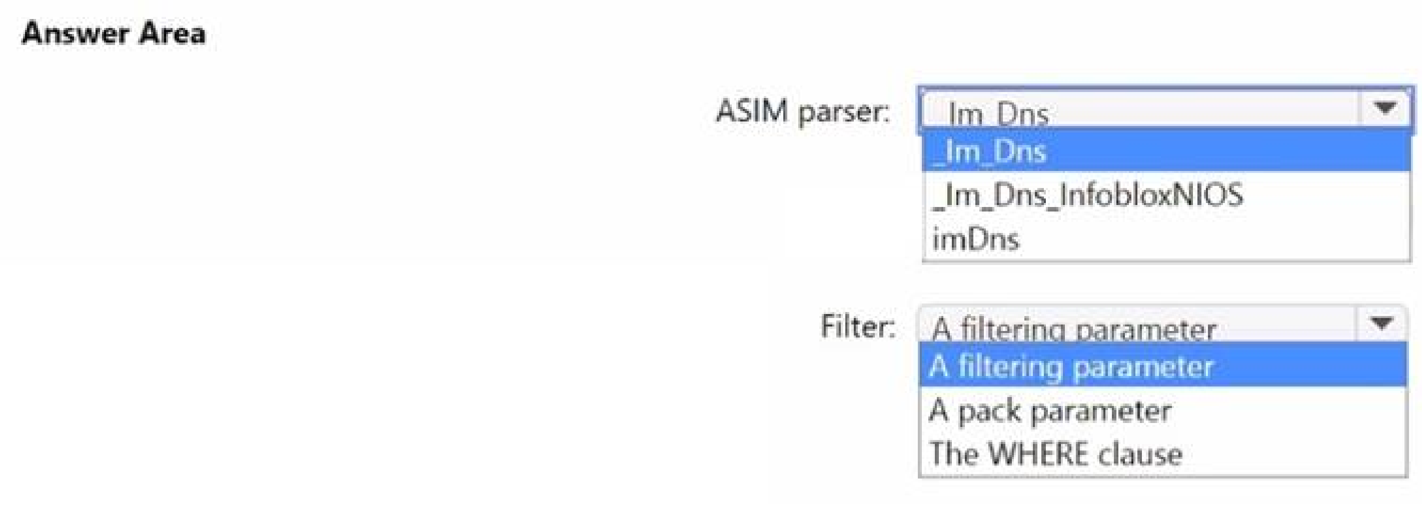
Answer: A

NEW QUESTION 40
- (Topic 3)
You need to implement the Defender for Cloud requirements. Which subscription-level role should you assign to Group1?

A. Security Admin
B. Owner
C. Security Assessment Contributor
D. Contributor

Answer: B

NEW QUESTION 44
HOTSPOT - (Topic 3)
You need to implement the ASIM query for DNS requests. 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

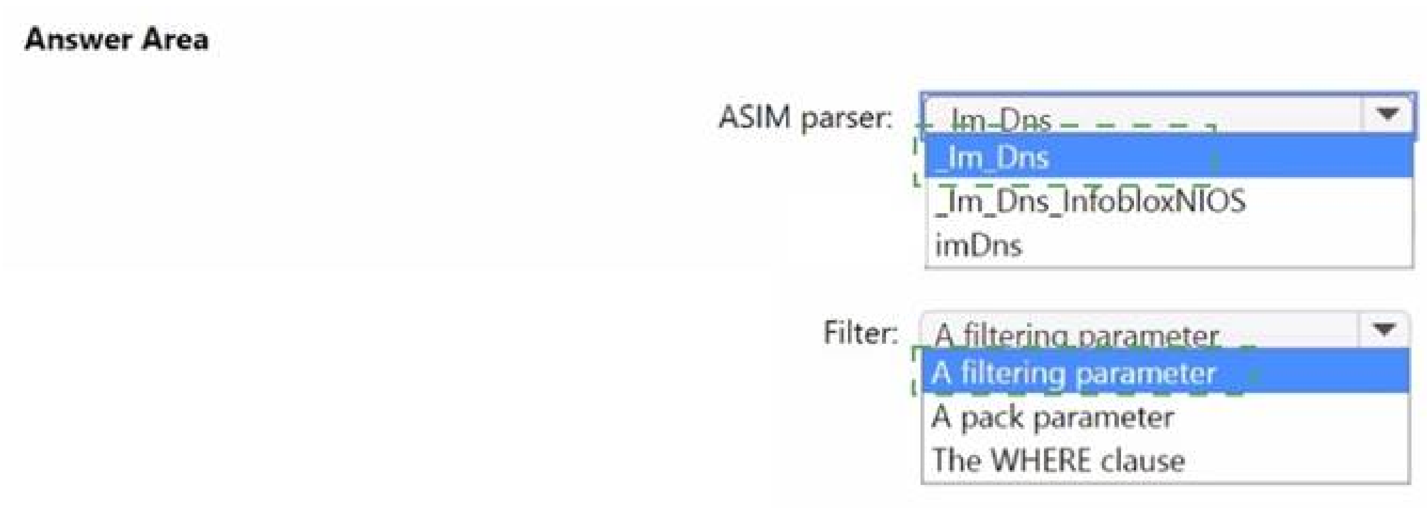
ASIM parser: _Im_Dns

Filter: A filtering parameter

A. Mastered
B. Not Mastered

Answer: A

Explanation:

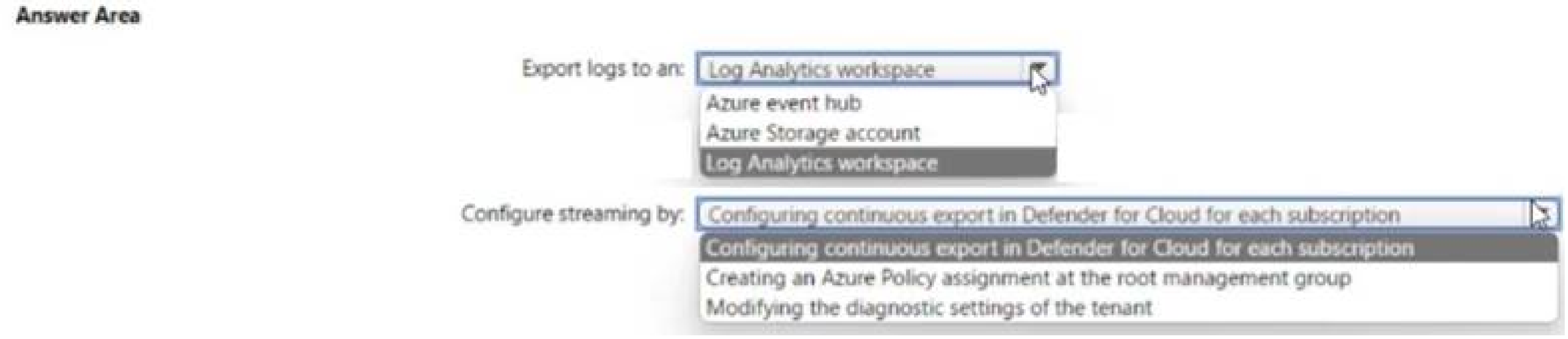


Answer Area

ASIM parser: _Im_Dns

Filter: A filtering parameter

NEW QUESTION 47
HOTSPOT - (Topic 4)
You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point



Answer Area

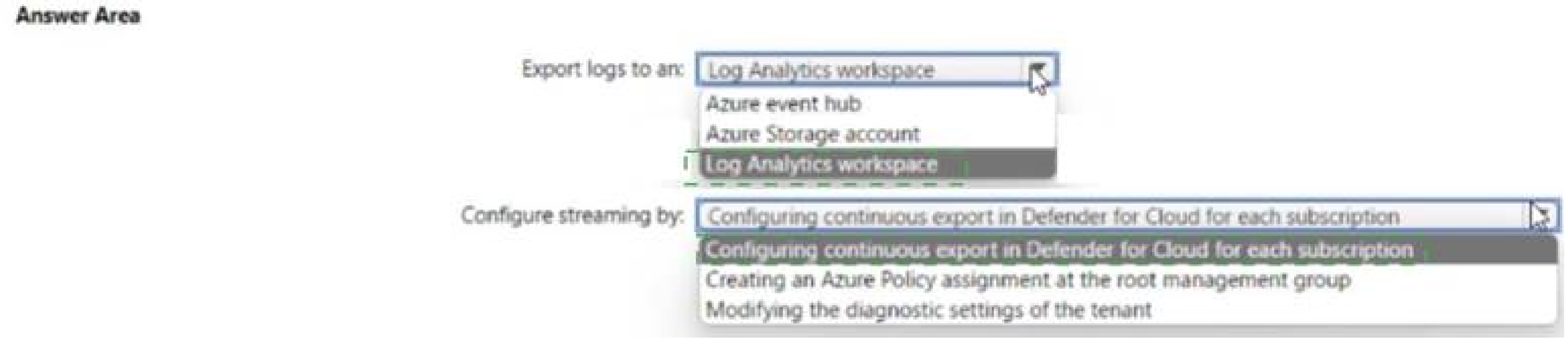
Export logs to an: Log Analytics workspace
Azure event hub
Azure Storage account
Log Analytics workspace

Configure streaming by: Configuring continuous export in Defender for Cloud for each subscription
Configuring continuous export in Defender for Cloud for each subscription
Creating an Azure Policy assignment at the root management group
Modifying the diagnostic settings of the tenant

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Export logs to an: Log Analytics workspace
Azure event hub
Azure Storage account
Log Analytics workspace

Configure streaming by: Configuring continuous export in Defender for Cloud for each subscription
Configuring continuous export in Defender for Cloud for each subscription
Creating an Azure Policy assignment at the root management group
Modifying the diagnostic settings of the tenant

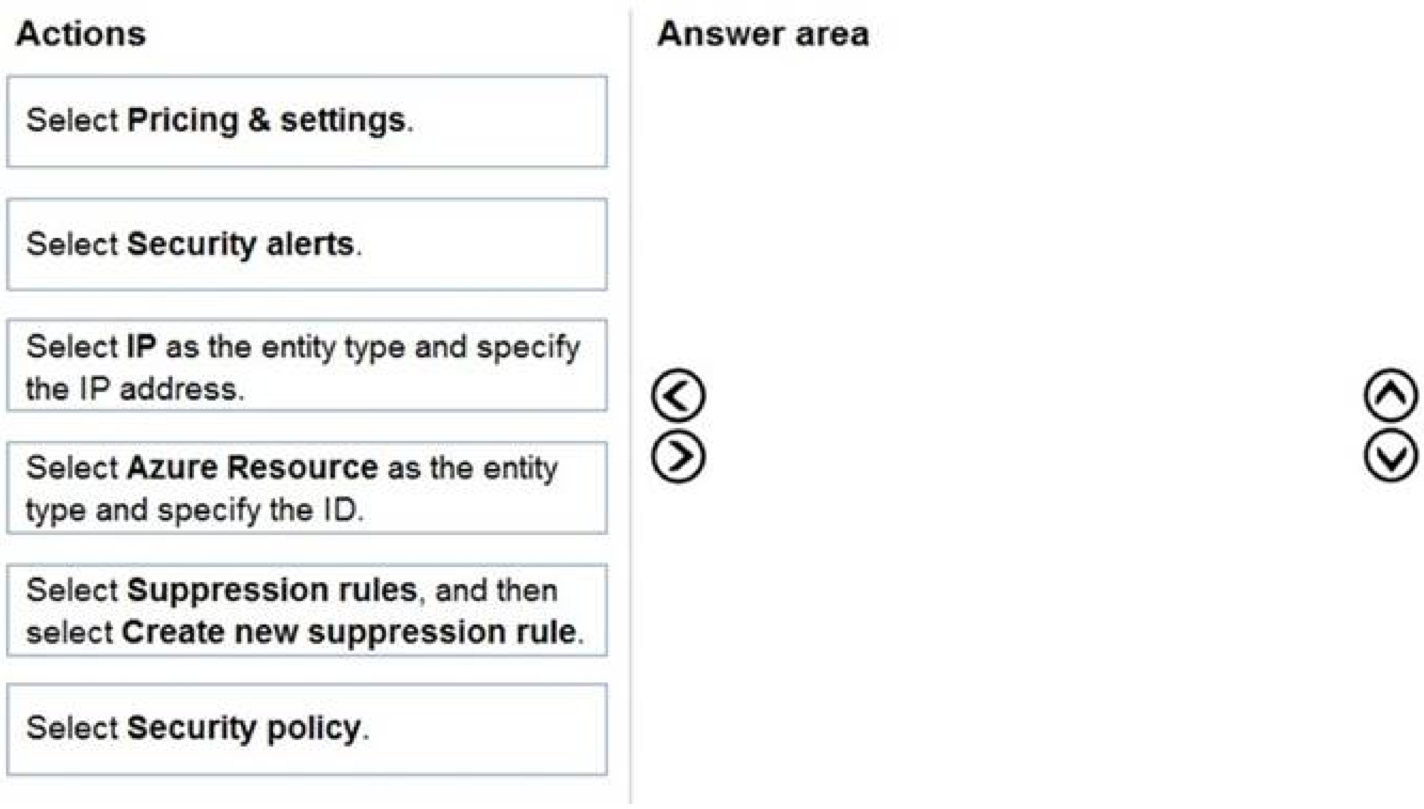
NEW QUESTION 50
- (Topic 4)
You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery
B. Replace
C. Block and Enable redirect
D. Monitor and Enable redirect

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

NEW QUESTION 54
DRAG DROP - (Topic 4)
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.



Actions

Select **Pricing & settings**.

Select **Security alerts**.

Select **IP** as the entity type and specify the IP address.

Select **Azure Resource** as the entity type and specify the ID.

Select **Suppression rules**, and then select **Create new suppression rule**.

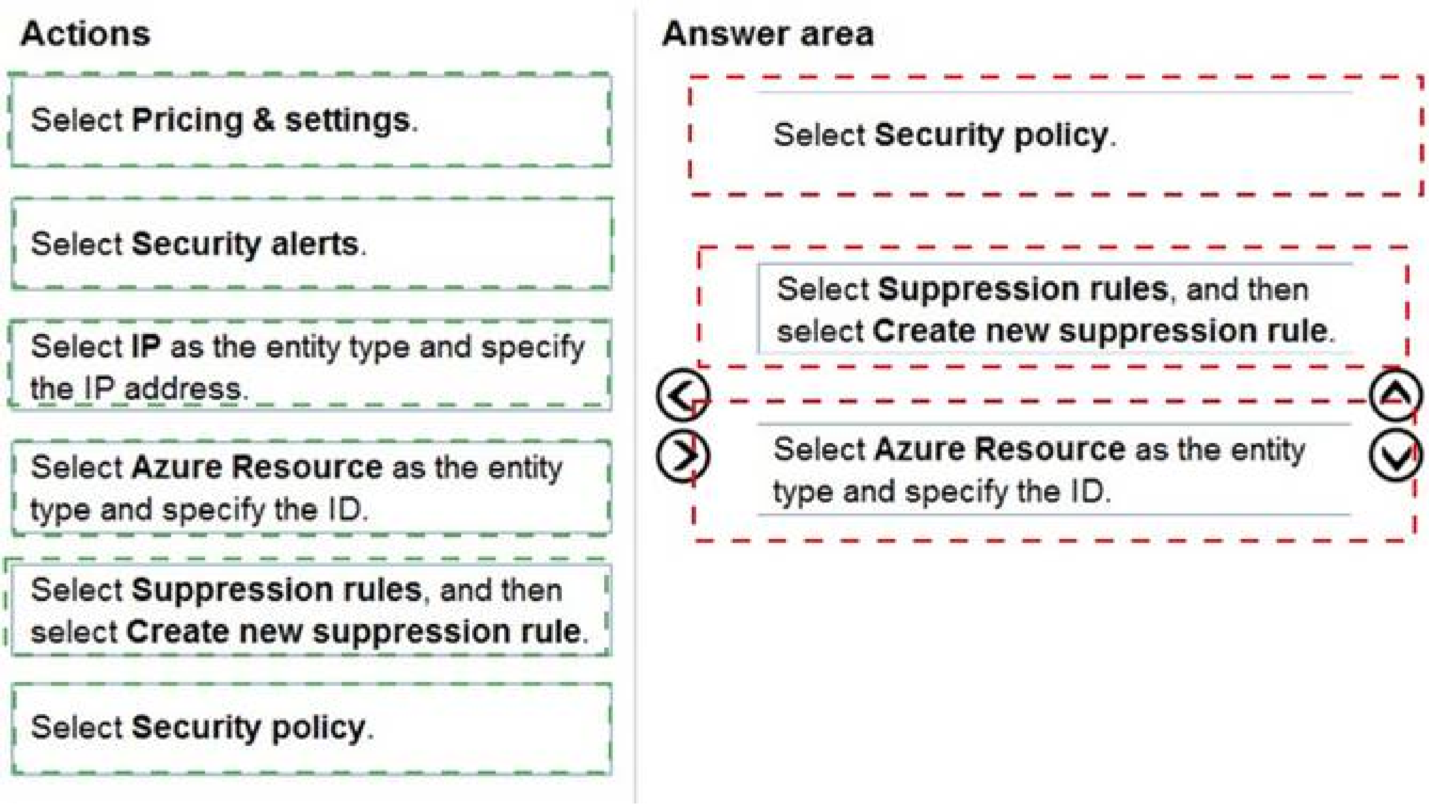
Select **Security policy**.

Answer area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

Select **Pricing & settings**.

Select **Security alerts**.

Select **IP** as the entity type and specify the IP address.

Select **Azure Resource** as the entity type and specify the ID.

Select **Suppression rules**, and then select **Create new suppression rule**.

Select **Security policy**.

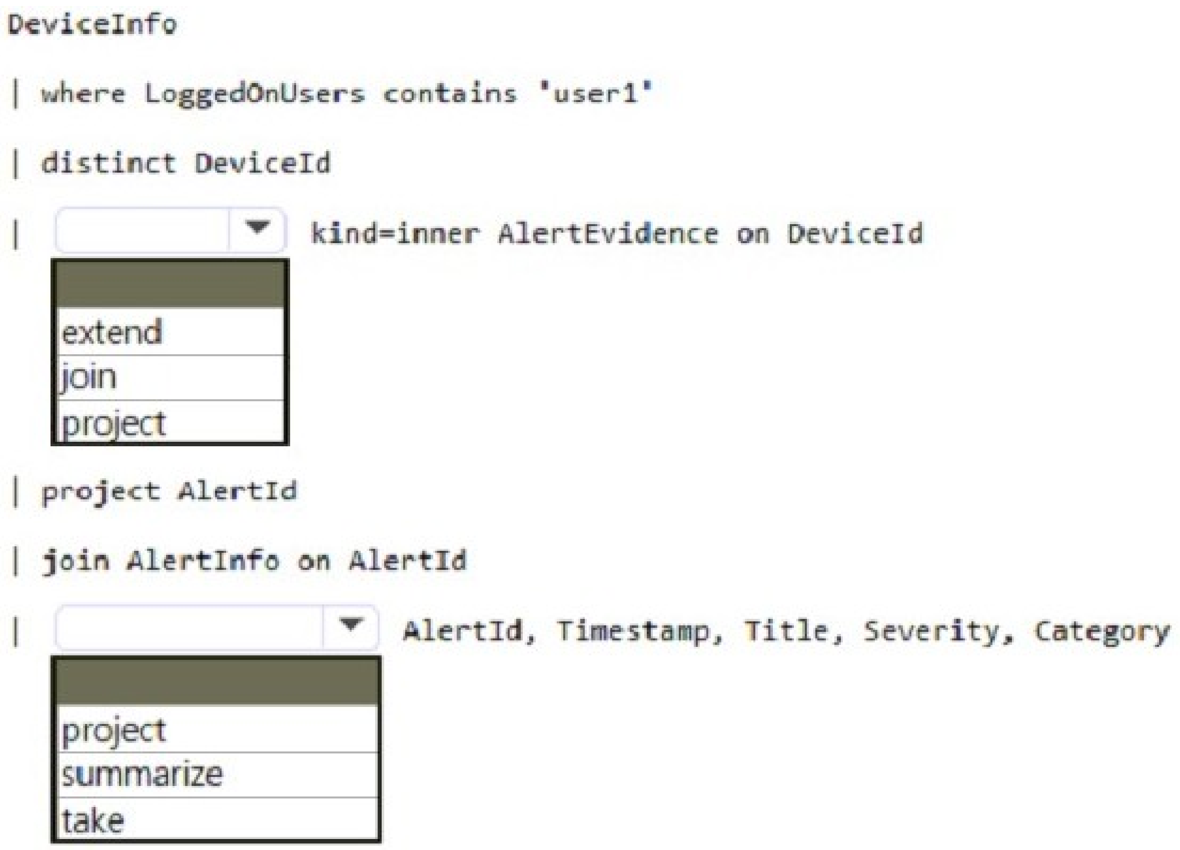
Answer area

Select **Security policy**.

Select **Suppression rules**, and then select **Create new suppression rule**.

Select **Azure Resource** as the entity type and specify the ID.

NEW QUESTION 58
HOTSPOT - (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.
You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: join An inner join.
This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.
This query uses the DeviceInfo table to check if a potentially compromised user (<account- name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID" Box 2: project

NEW QUESTION 60
- (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 63
- (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

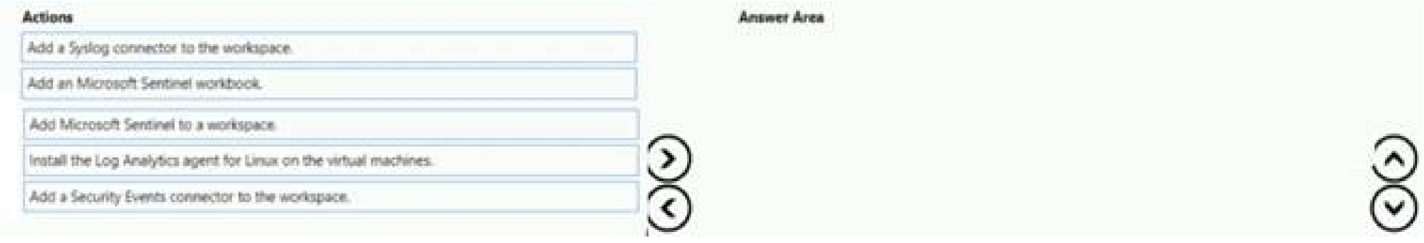
Answer: B

NEW QUESTION 65
- (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 68
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

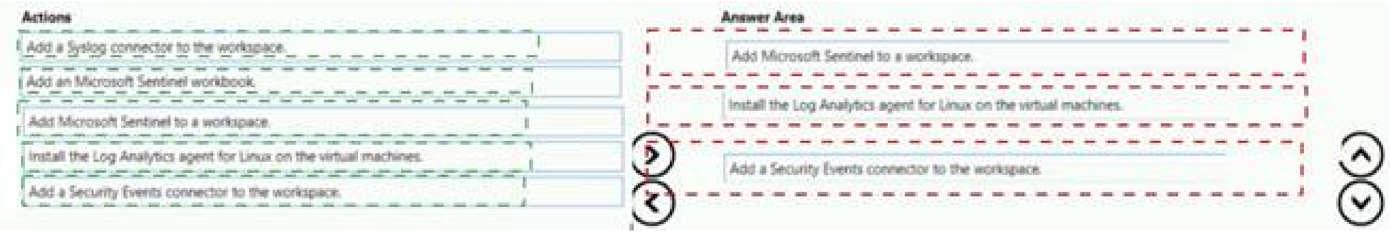
Add a Syslog connector to the workspace.
Add an Microsoft Sentinel workbook.
Add Microsoft Sentinel to a workspace.
Install the Log Analytics agent for Linux on the virtual machines.
Add a Security Events connector to the workspace.

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 73
- (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 74
- (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?

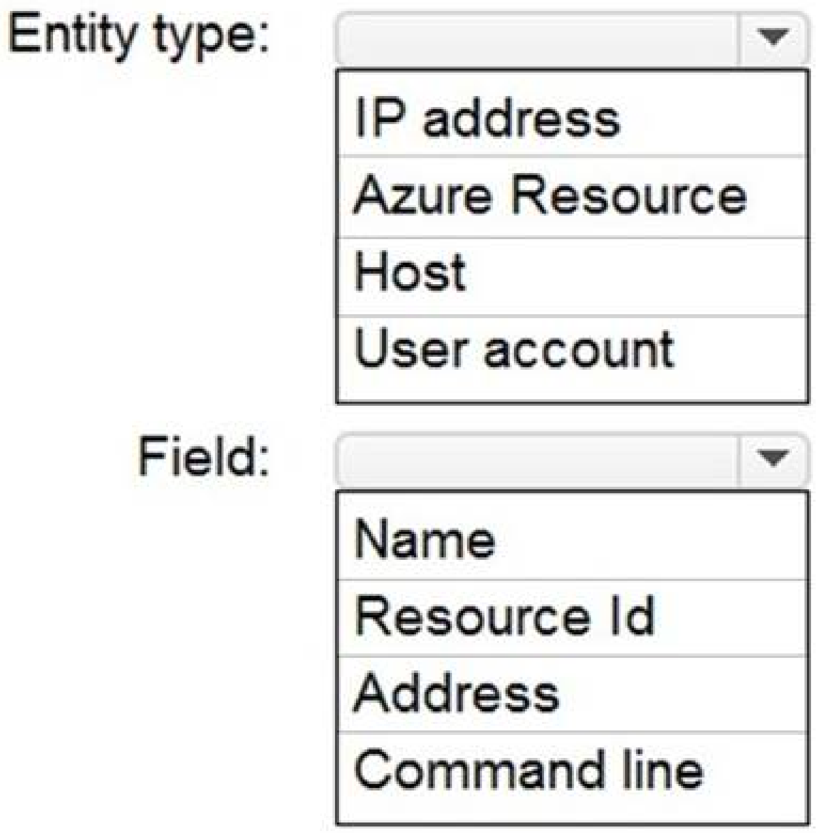
A. the Threat Protection Status report in Microsoft Defender for Office 365
B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

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 78

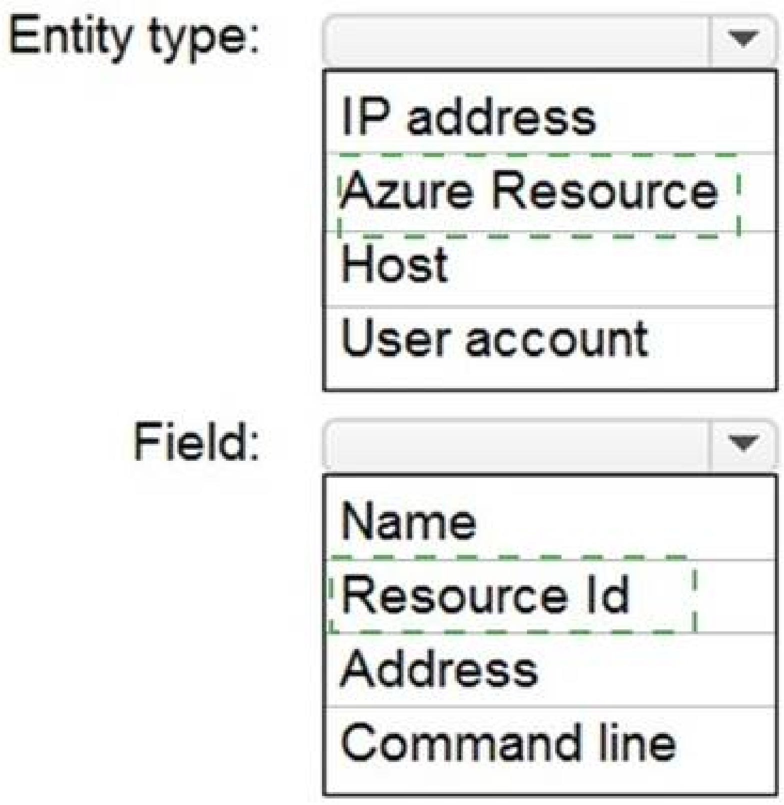
HOTSPOT - (Topic 4)
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 82

- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:

- App name: App1
- IP address: 192.168.1.2
- Computer name: Device1
- Used client app: Microsoft Edge
- Email address: user1@company.com
- Sign-in URL: https://www.company.com

Which entities can be investigated by using UEBA?

A. app name, computer name, IP address, email address, and used client app only
B. IP address and email address only
C. used client app and app name only
D. IP address only

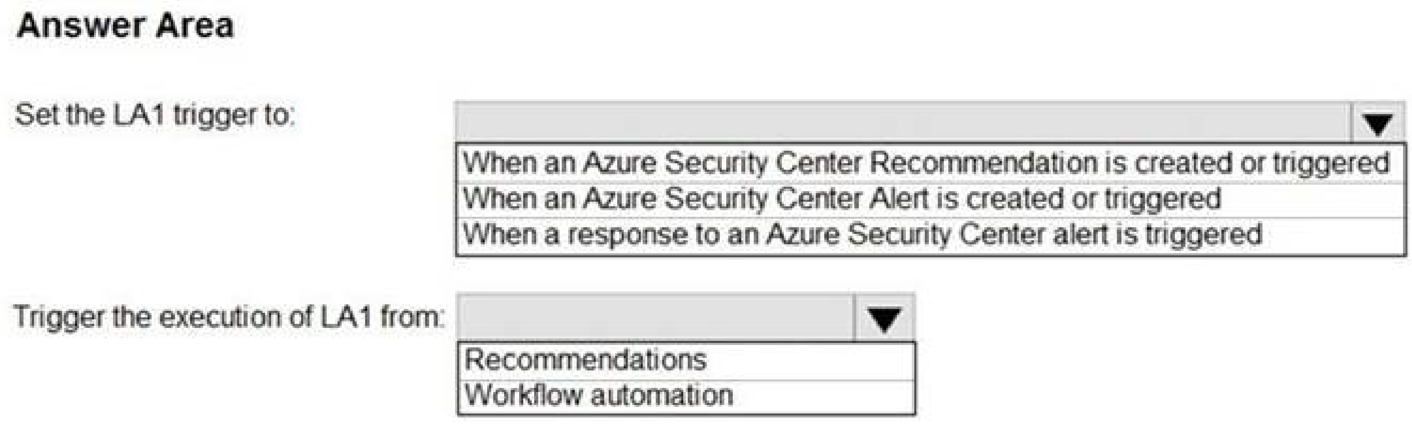
Answer: D

NEW QUESTION 83
- (Topic 4)
You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.
You need to identify all the changes made to Domain Admins group during the past 30 days.
What should you use?

A. the Azure Active Directory Provisioning Analysis workbook
B. the Overview settings of Insider risk management
C. the Modifications of sensitive groups report in Microsoft Defender for Identity
D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 85
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 Azure Security Center.
View the window
You need to test LA1 in Security Center.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

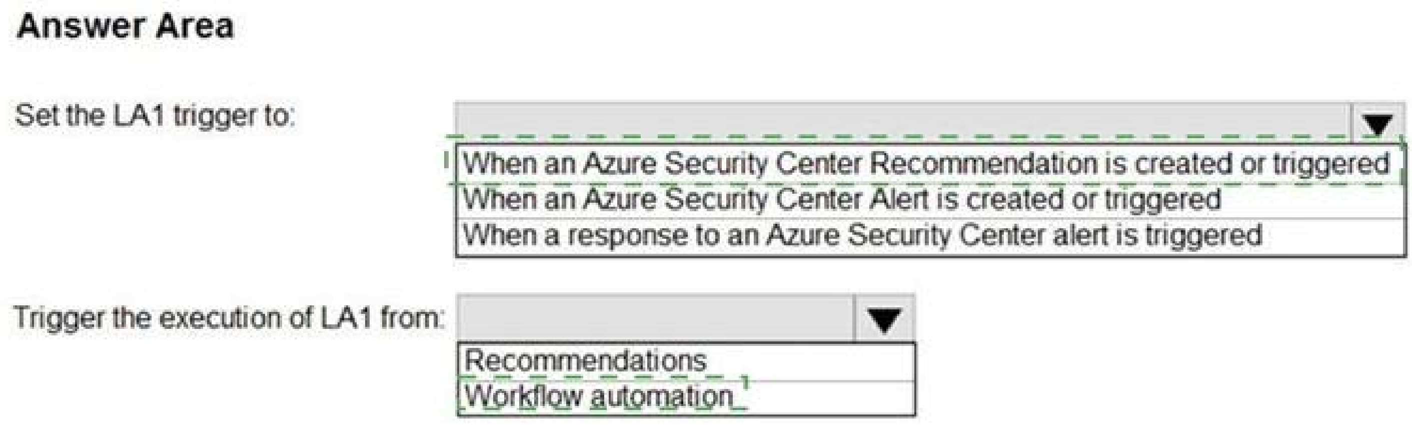
Set the LA1 trigger to:
- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:
- Recommendations
- Workflow automation

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Set the LA1 trigger to:
- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:
- Recommendations
- Workflow automation

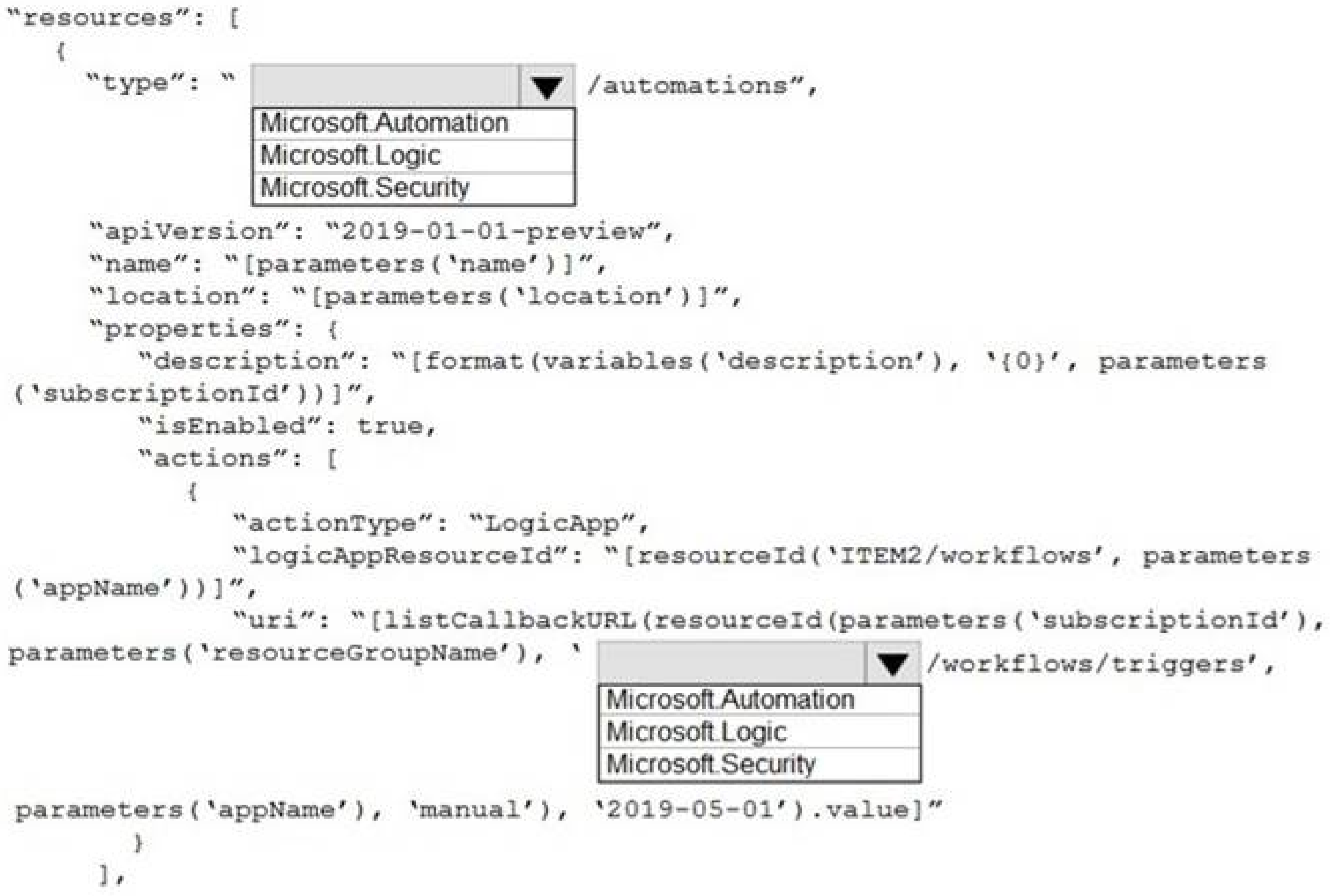
NEW QUESTION 87
- (Topic 4)
You have the following environment:
? Azure Sentinel
? A Microsoft 365 subscription
? Microsoft Defender for Identity
? An Azure Active Directory (Azure AD) tenant
You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain 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 90
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.

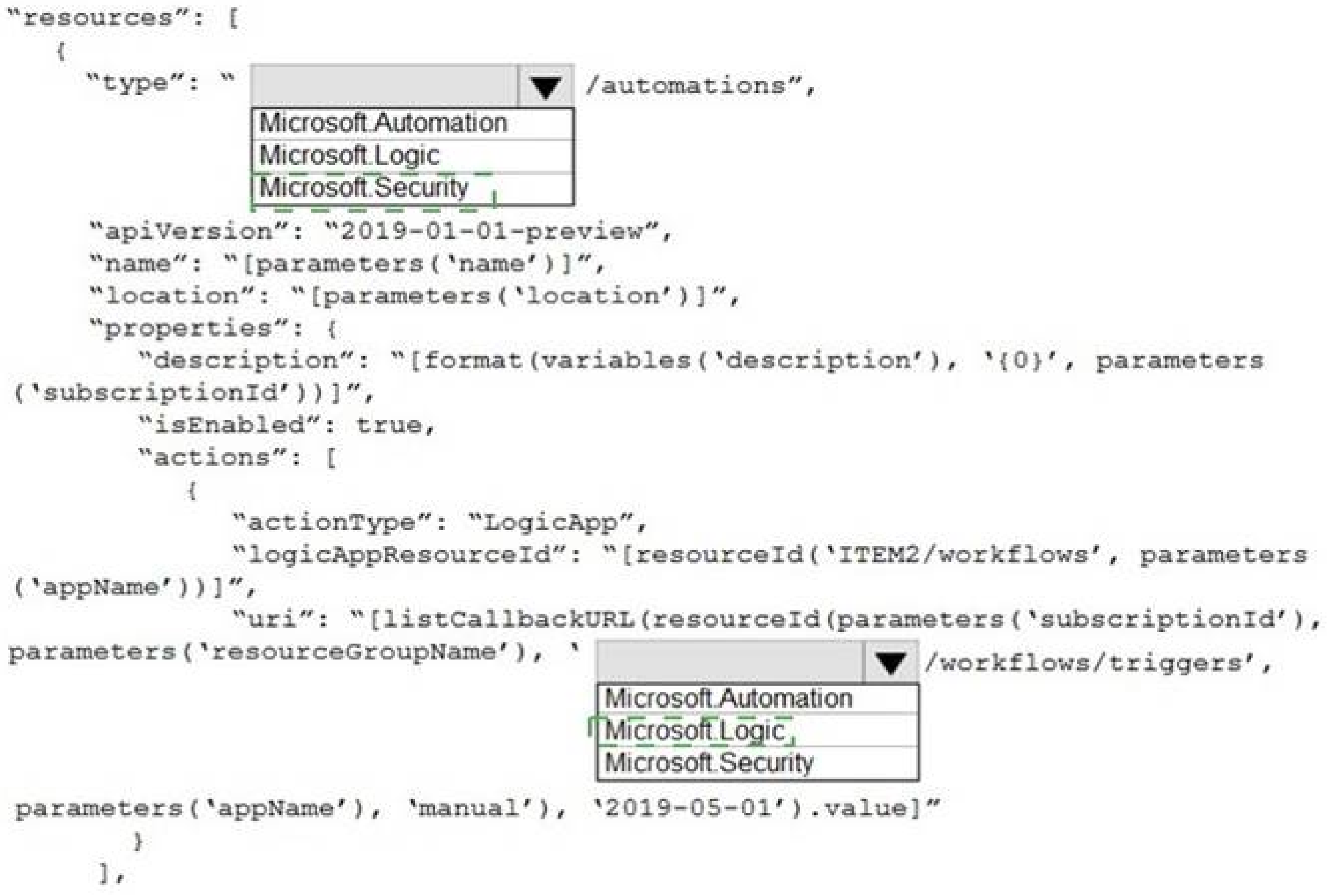


```
"resources": [
   {
    "type": "  [▼] /automations",
               Microsoft.Automation
               Microsoft.Logic
               Microsoft.Security
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
       "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]"
          }
        ],
```

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 93

- (Topic 4)
You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

A. Create an Azure Policy assignment.
B. Modify the Workload protections settings in Defender for Cloud.
C. Create an alert rule in Azure Monitor.
D. Modify the alert settings in Defender for Cloud.

Answer: D

Explanation:
You can use alerts suppression rules to suppress false positives or other unwanted
security alerts from Defender for Cloud.
Note: To create a rule directly in the Azure portal:
* 1. From Defender for Cloud's security alerts page:
Select the specific alert you don't want to see anymore, and from the details pane, select Take action.
Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:
* 2. In the new suppression rule pane, enter the details of your new rule.
Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.
Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.
* 3. Enter details of the rule.
* 4. Save the rule.
Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression- rules

NEW QUESTION 96
- (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.

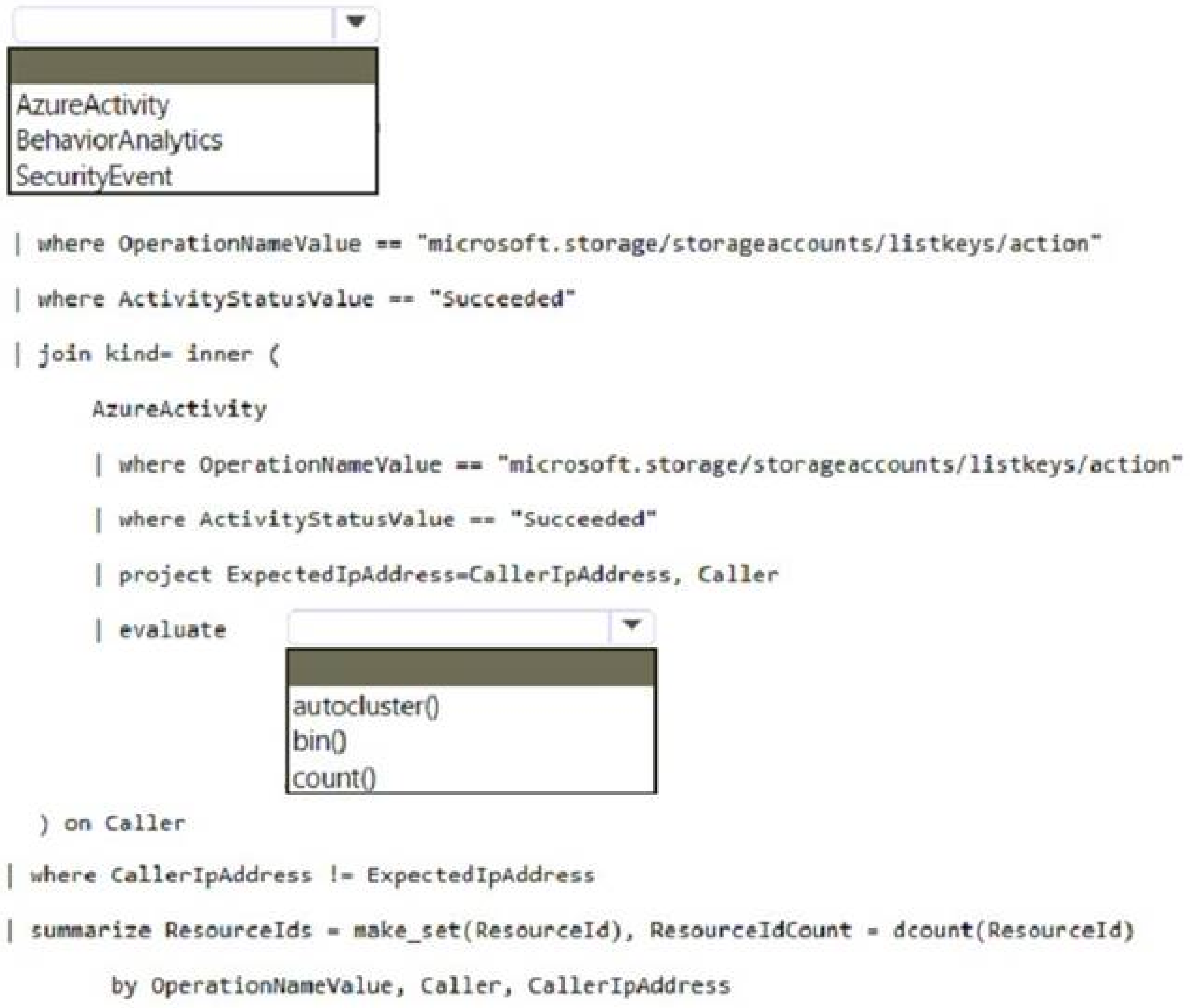
Answer: A

NEW QUESTION 99
- (Topic 4)
You have a Microsoft Sentinel workspace.
You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.
What are two ways to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Redeploy the built-in parse and specify a CallerContext parameter of any and a SourceSpecificParse parameter of any.
B. Create a hunting query that references the built-in parse.
C. Redeploy the built-in parse and specify a CallerContext parameter of built-in.
D. Build a custom unify parse and include the build- parse version
E. Create an analytics rule that includes the built-in parse

Answer: AD

NEW QUESTION 103
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
      AzureActivity
      | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
      | where ActivityStatusValue == "Succeeded"
      | project ExpectedIpAddress=CallerIpAddress, Caller
      | evaluate
```

```
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
        by OperationNameValue, Caller, CallerIpAddress
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: AzureActivity
The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:
Box 2: autocluster()
Example: description: |
'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this
type, it would be interesting to see if the account performing this activity or the source IP address from
which it is being done is anomalous.
The query below generates known clusters of ip address per caller, notice that users which only had single
operations do not appear in this list as we cannot learn from it their normal activity (only based on a single
event). The activities for listing storage account keys is correlated with this learned
clusters of expected activities and activity which is not expected is returned.'
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress

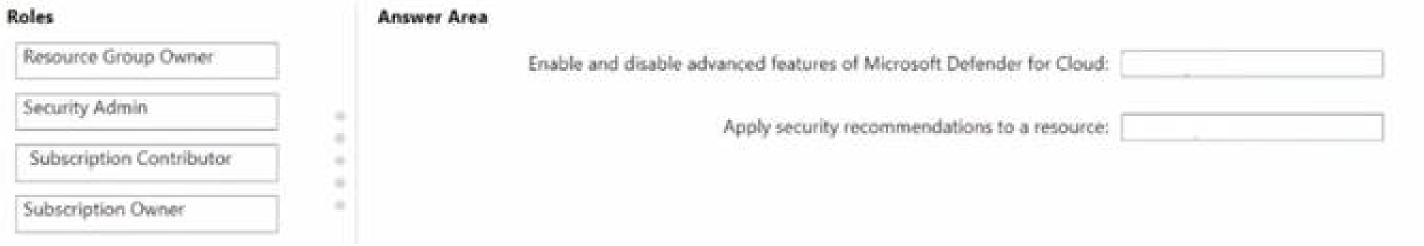
NEW QUESTION 107
- (Topic 4)
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

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 112
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
• Enable and disable advanced features of Microsoft Defender for Cloud.
• Apply security recommendations to a resource. The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



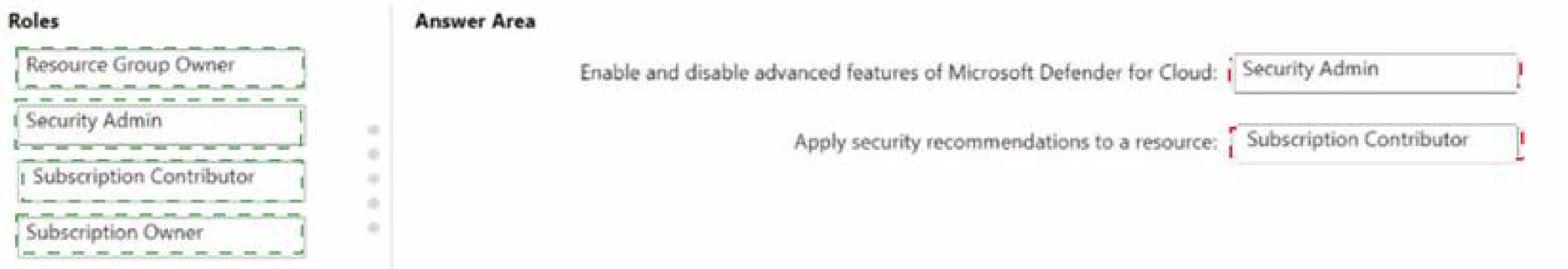
Roles
Resource Group Owner
Security Admin
Subscription Contributor
Subscription Owner

Answer Area
Enable and disable advanced features of Microsoft Defender for Cloud:
Apply security recommendations to a resource:

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Roles
Resource Group Owner
Security Admin
Subscription Contributor
Subscription Owner

Answer Area
Enable and disable advanced features of Microsoft Defender for Cloud: Security Admin
Apply security recommendations to a resource: Subscription Contributor

NEW QUESTION 116
- (Topic 4)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation. You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

A. Create a Microsoft incident creation rule
B. Share the incident URL
C. Create a scheduled query rule
D. Assign the incident

Answer: D

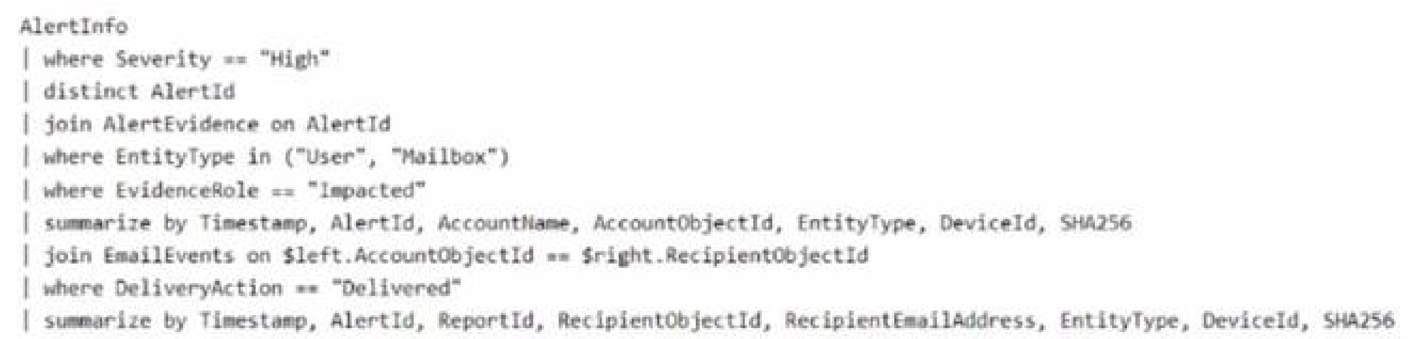
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

NEW QUESTION 121
- (Topic 4)
You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEBA. Which Log Analytics table should you use?

A. SentwlAuoNt
B. AADRiskyUsers
C. IdentityOirectoryEvents
D. Identityinfo

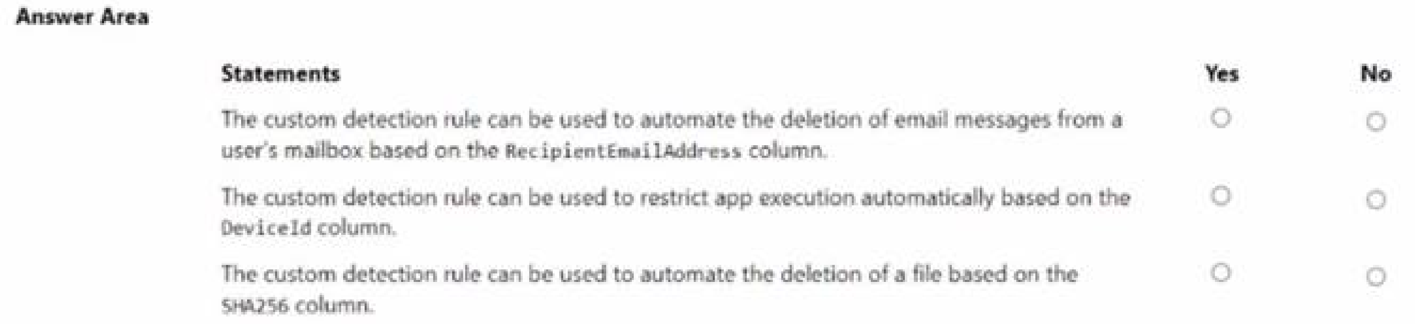
Answer: C

NEW QUESTION 122
HOTSPOT - (Topic 4)
You have a custom detection rule that includes the following KQL query.



```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

For each of the following statements, select Yes if True. Otherwise select No. NOTE: Each correct selection is worth one point.



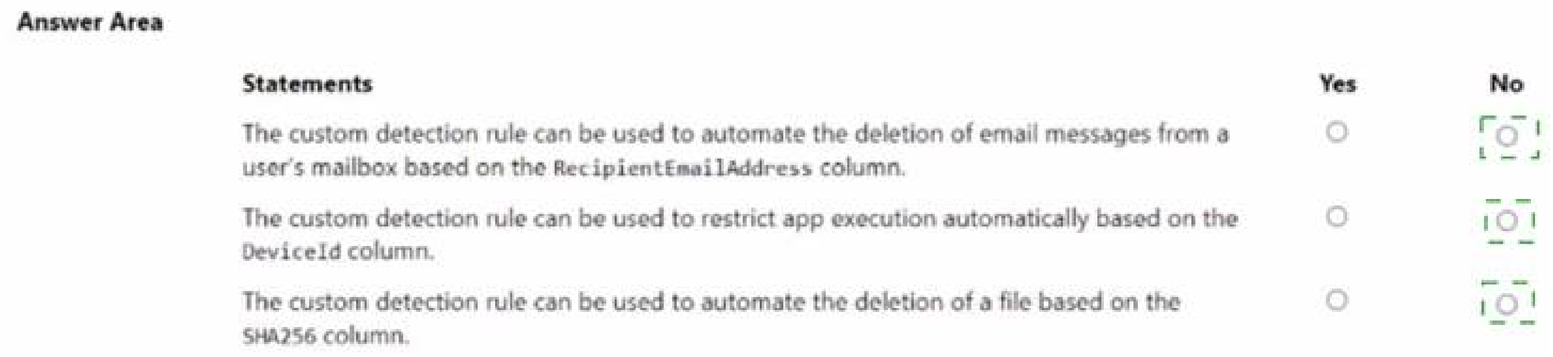
Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the RecipientEmailAddress column.	○	[✓ ○]
The custom detection rule can be used to restrict app execution automatically based on the DeviceId column.	○	[✓ ○]
The custom detection rule can be used to automate the deletion of a file based on the SHA256 column.	○	[✓ ○]

NEW QUESTION 126
- (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 128
- (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 131
- (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

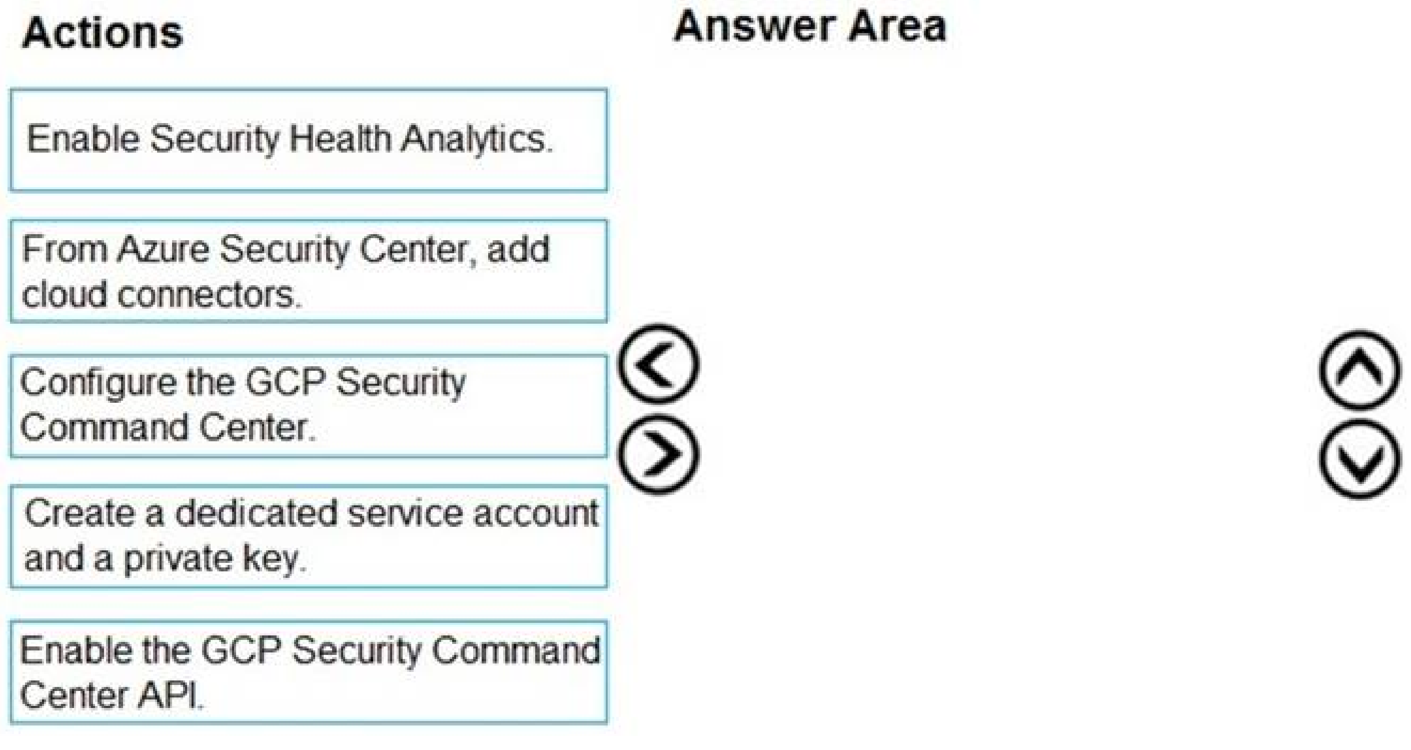
NEW QUESTION 134
- (Topic 4)
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure
Sentinel deployment to generate alerts based 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 136
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

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

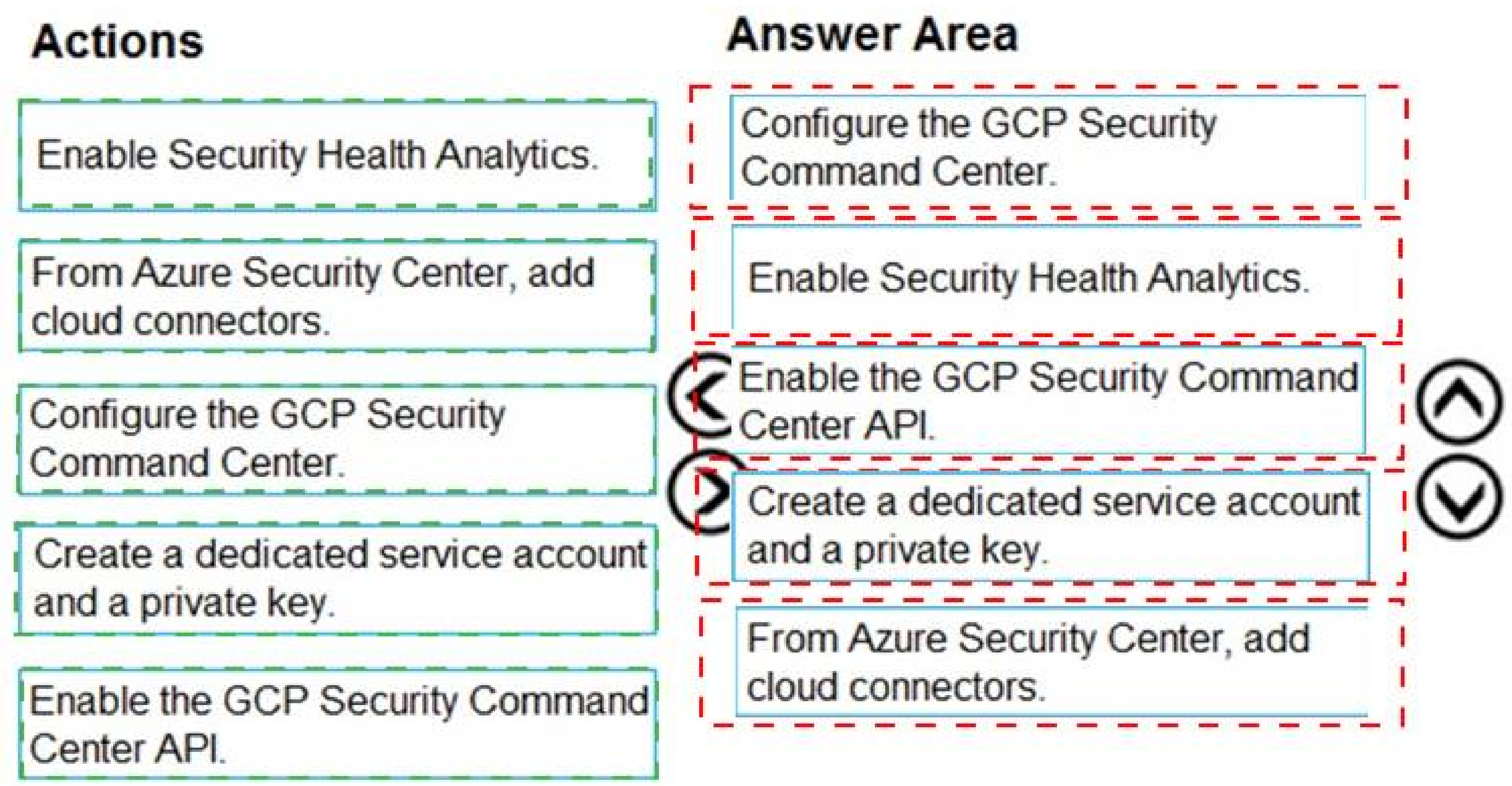
Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

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

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

NEW QUESTION 137

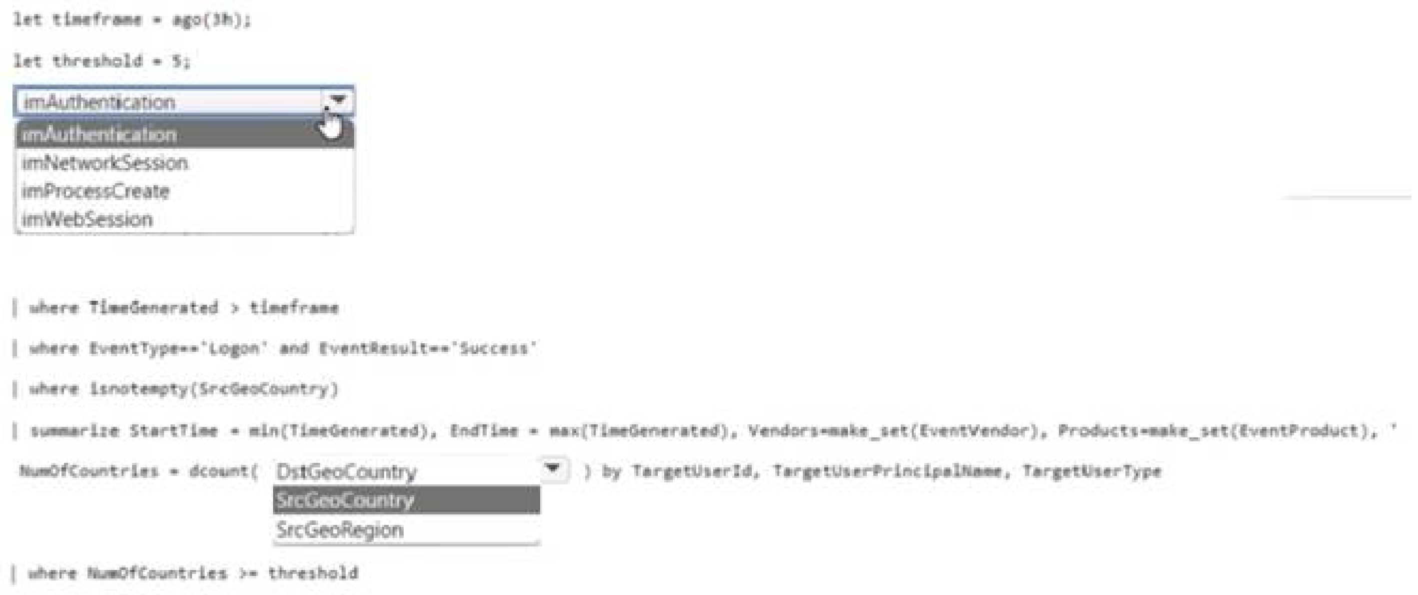
HOTSPOT - (Topic 4)

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

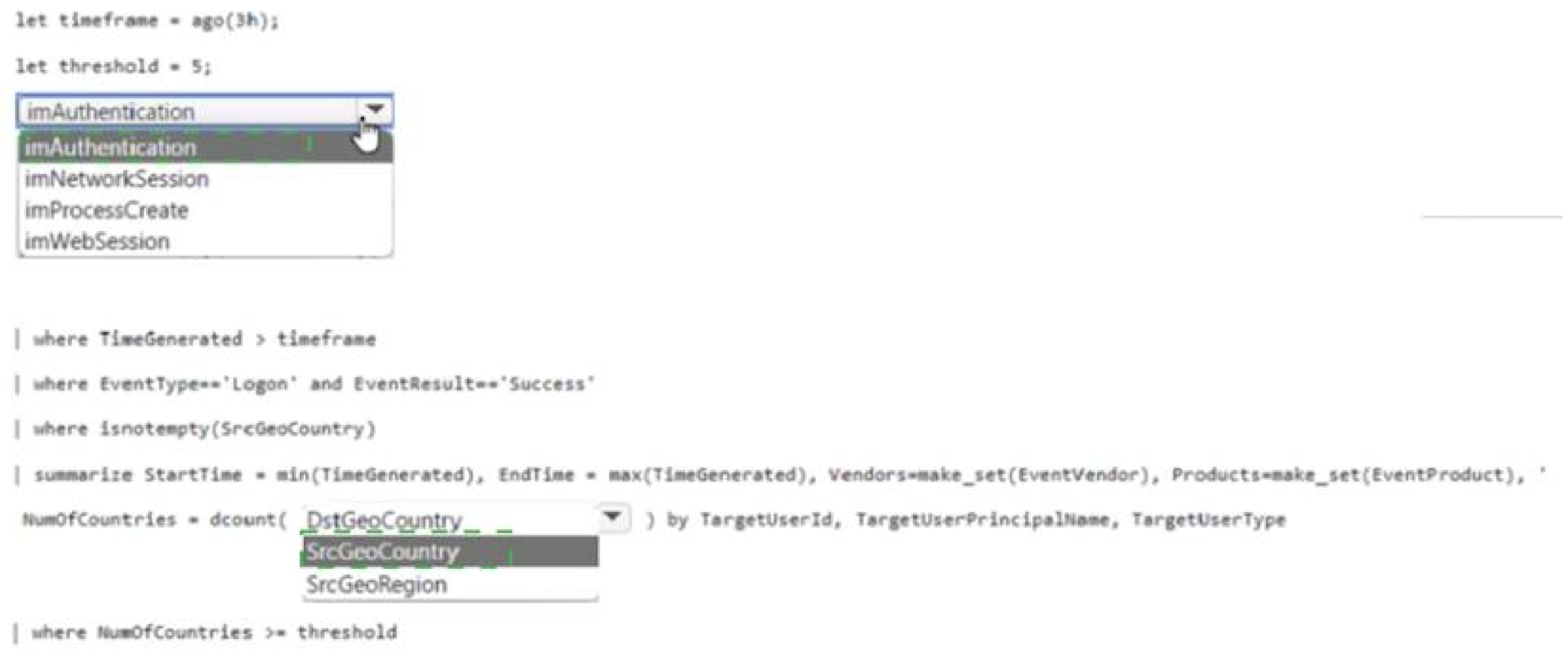


```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication ▼
  imAuthentication
  imNetworkSession
  imProcessCreate
  imWebSession
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), 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:



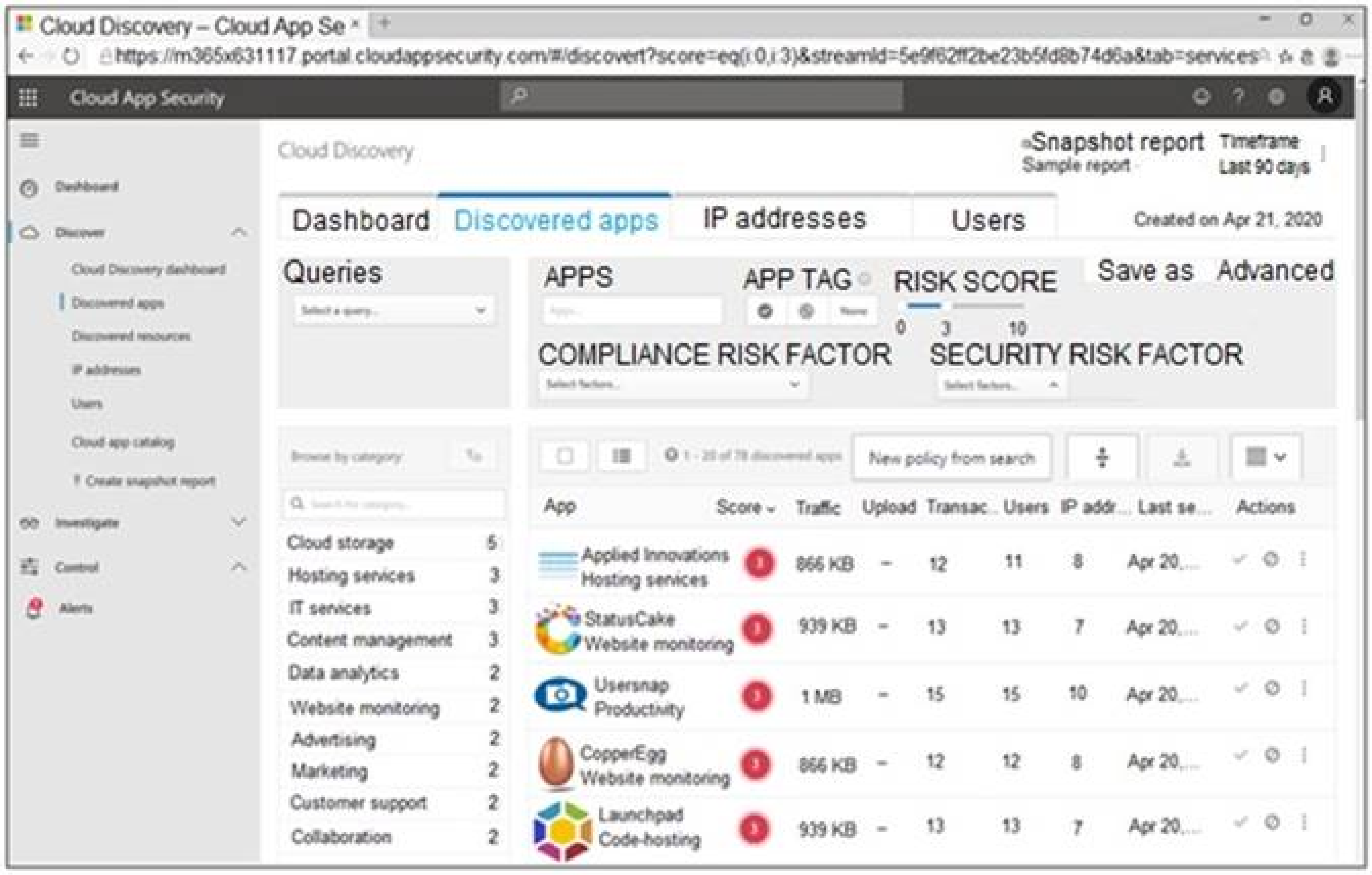
```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication ▼
  imAuthentication
  imNetworkSession
  imProcessCreate
  imWebSession
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), 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 140
- (Topic 4)
You have 50 Microsoft Sentinel workspaces.
You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.
Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents
B. Microsoft Sentinel - Workbooks
C. Microsoft Sentinel
D. Log Analytics workspaces

Answer: D

NEW QUESTION 142
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

Dashboard
Discover
Cloud Discovery dashboard
Discovered apps
Discovered resources
IP addresses
Users
Cloud app catalog
Create snapshot report
Investigate
Control
Alerts

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...

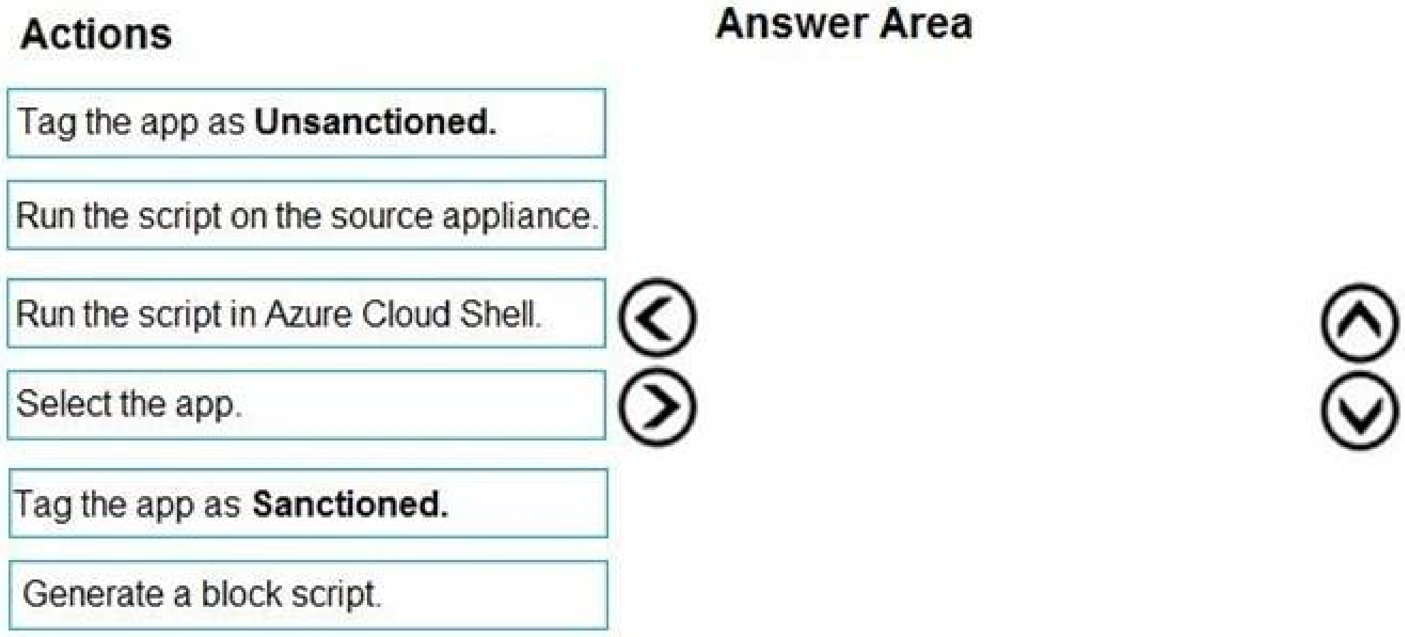
Browse by category

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

New policy from search

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

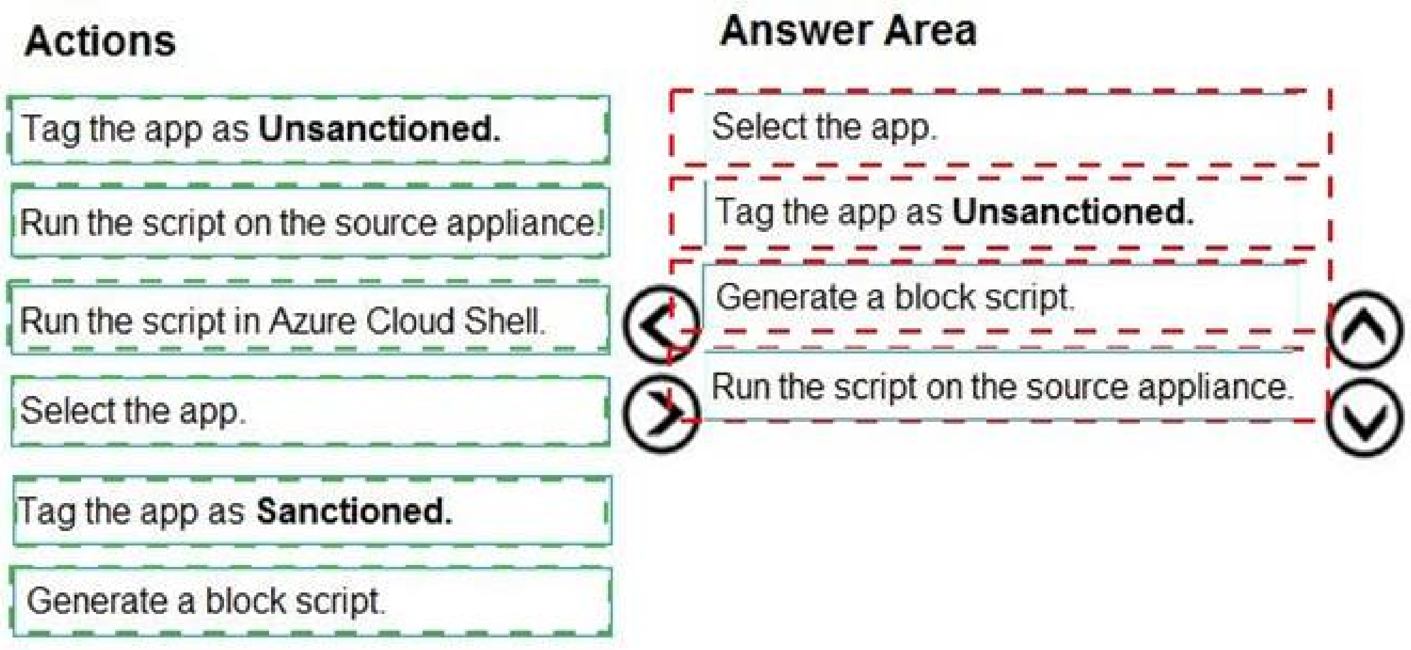
Generate a block script.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



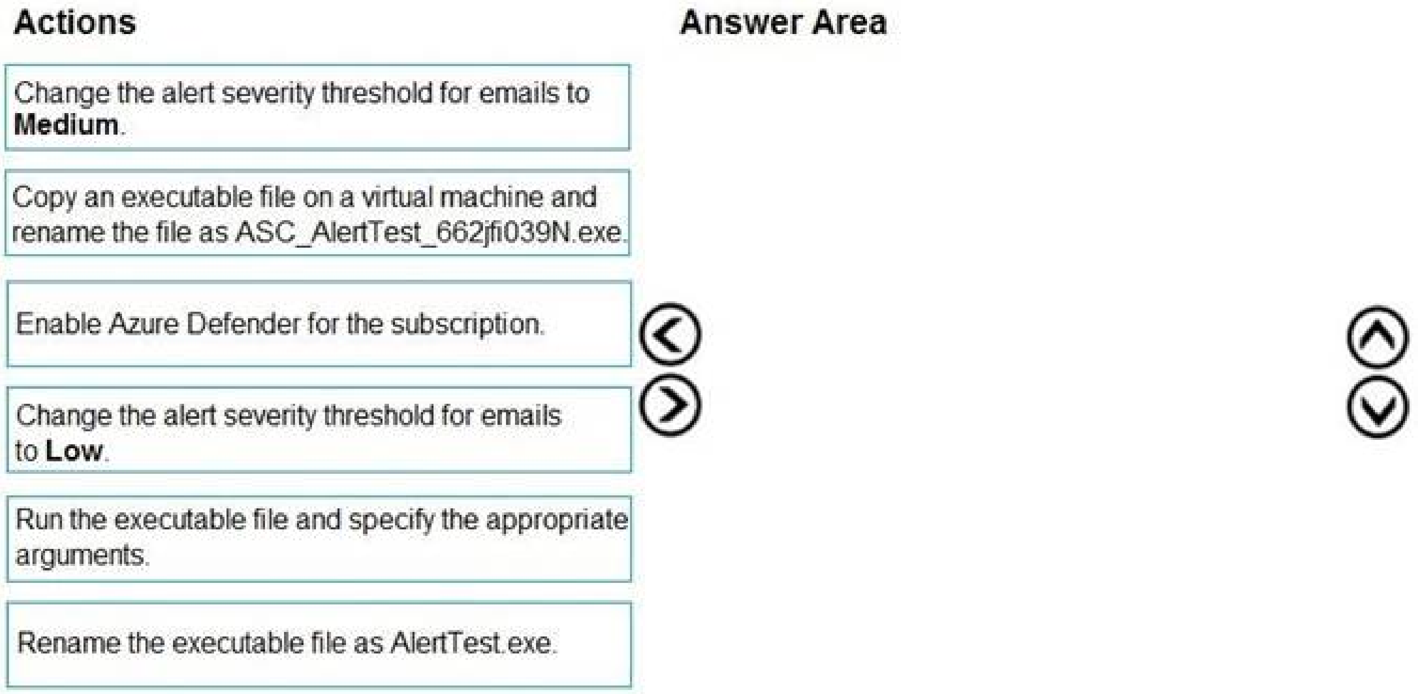
Actions

- 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 146
DRAG DROP - (Topic 4)
DRAG DROP
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

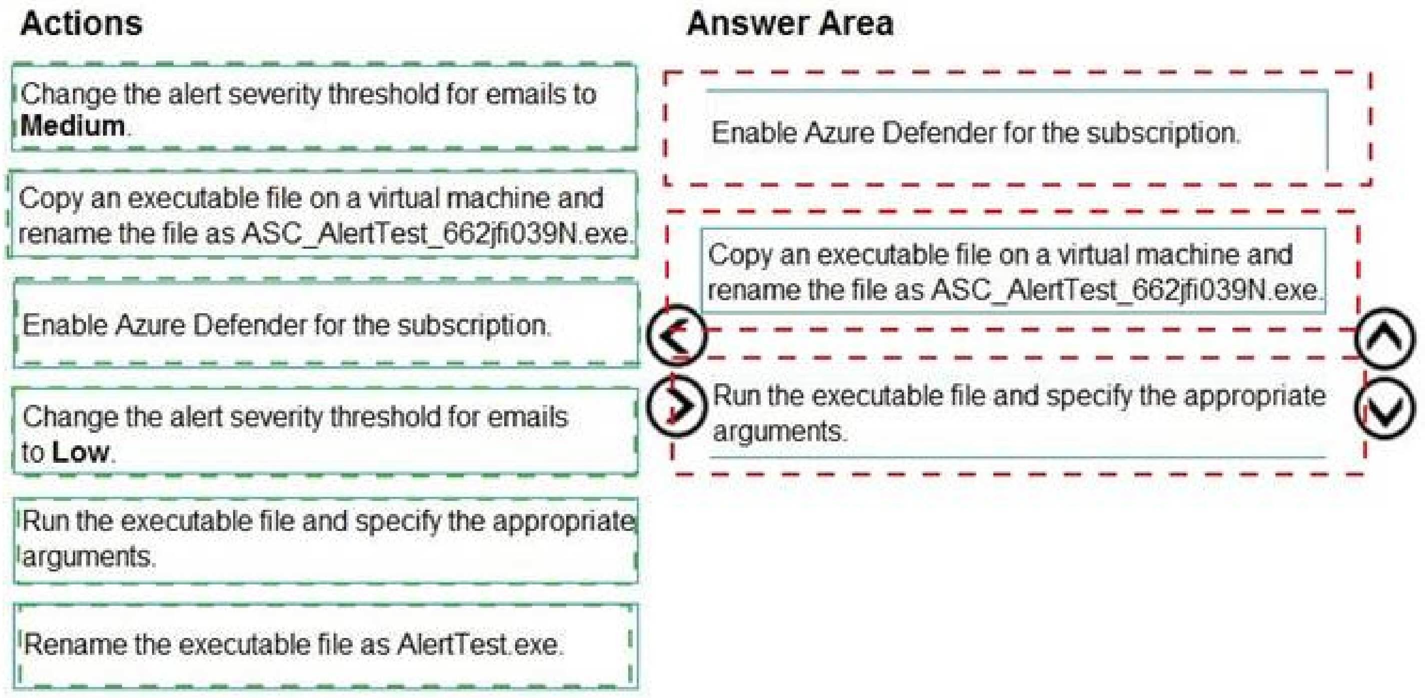
- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

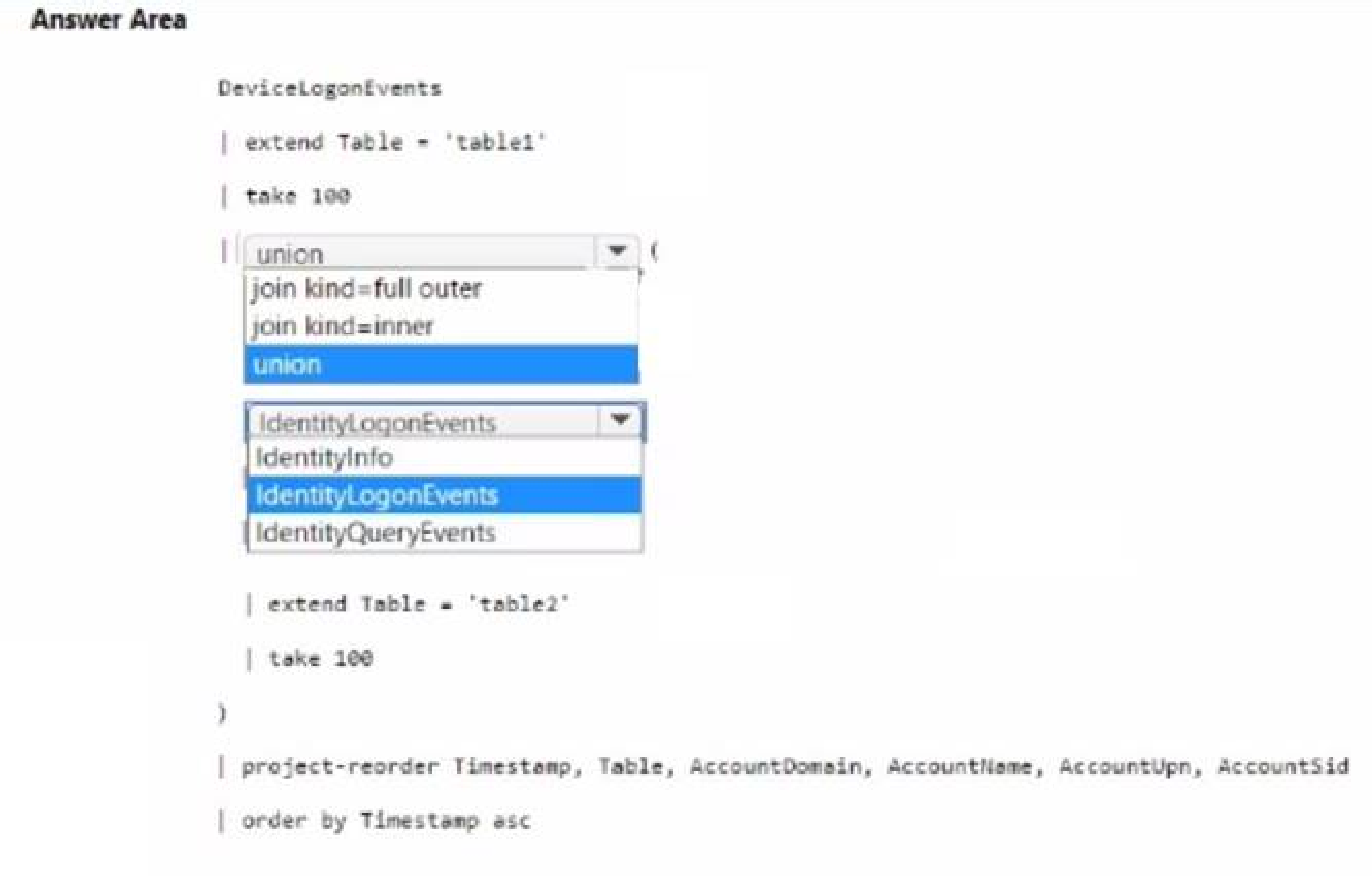
- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and specify the appropriate arguments.
- Rename the executable file as AlertTest.exe.

Answer Area

- Enable Azure Defender for the subscription.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Run the executable file and specify the appropriate arguments.

NEW QUESTION 151
HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.
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.



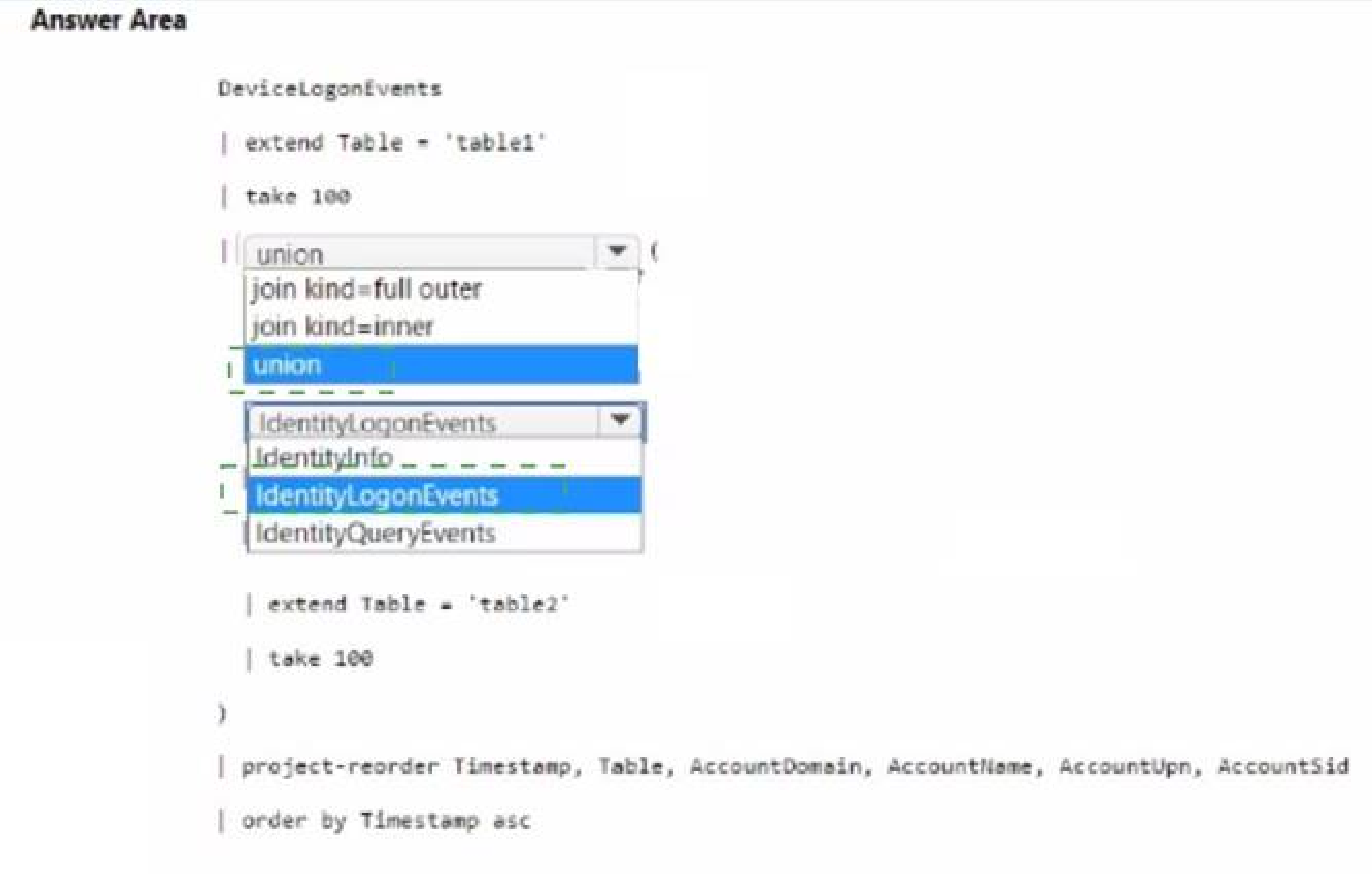
Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [union ▼] (
   join kind=full outer
   join kind=inner
   union
  [IdentityLogonEvents ▼]
   IdentityInfo
   IdentityLogonEvents
   IdentityQueryEvents
  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [union ▼] (
   join kind=full outer
   join kind=inner
   union
  [IdentityLogonEvents ▼]
   IdentityInfo
   IdentityLogonEvents
   IdentityQueryEvents
  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

NEW QUESTION 152

- (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:

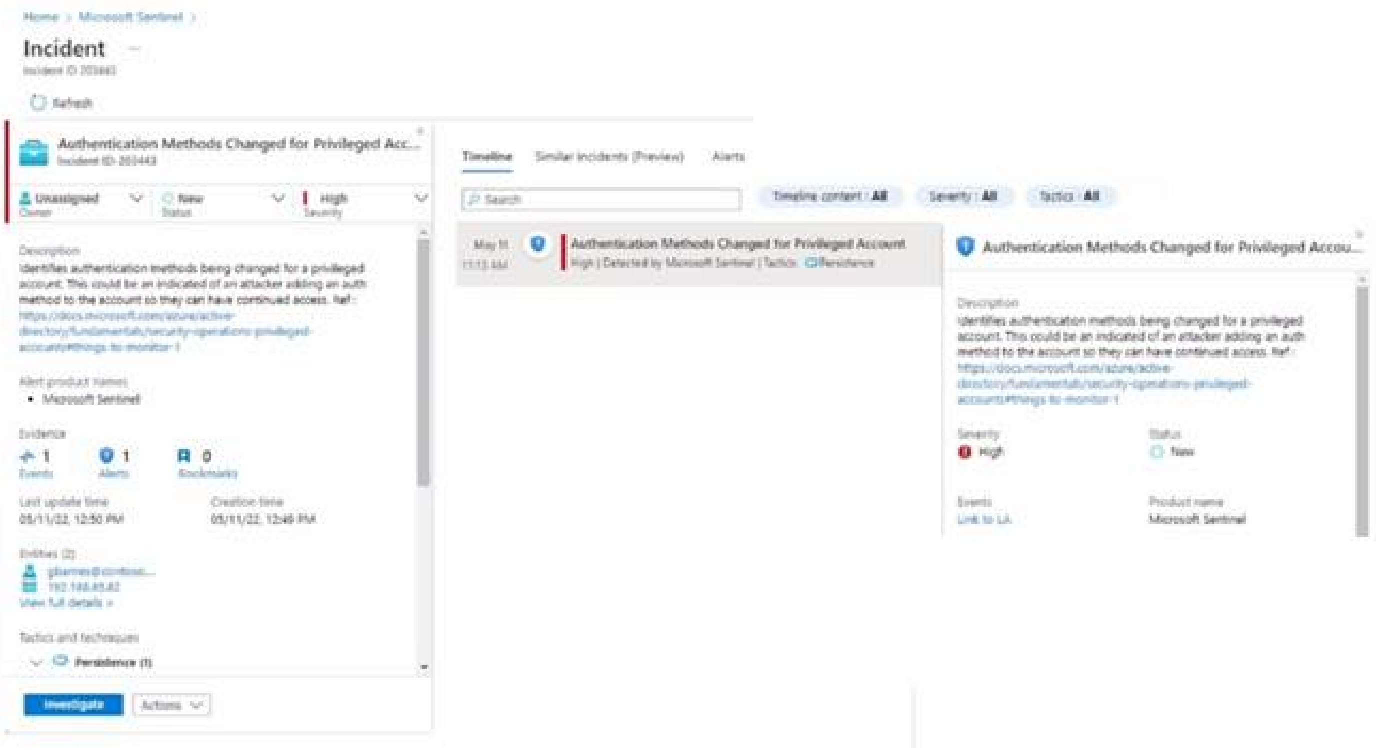
https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION 153

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace.

A Microsoft Sentinel incident is generated as shewn in the following exhibit.



Incident
Incident ID 203443

Authentication Methods Changed for Privileged Acc...
Incident ID: 203443

Unassigned
Owner

New
Status

High
Severity

Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

Alert product names
- Microsoft Sentinel

Evidence
1 Events
1 Alerts
0 Bookmarks

Last update time
05/11/22, 12:50 PM

Creation time
05/11/22, 12:49 PM

Entities (2)
gbarnes@contoso...
192.168.65.82
View full details >

Tactics and techniques
Persistence (1)

May 11
11:13 AM
Authentication Methods Changed for Privileged Account
High | Detected by Microsoft Sentinel | Tactics: Persistence

Authentication Methods Changed for Privileged Accou...

Description
Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

Severity
High

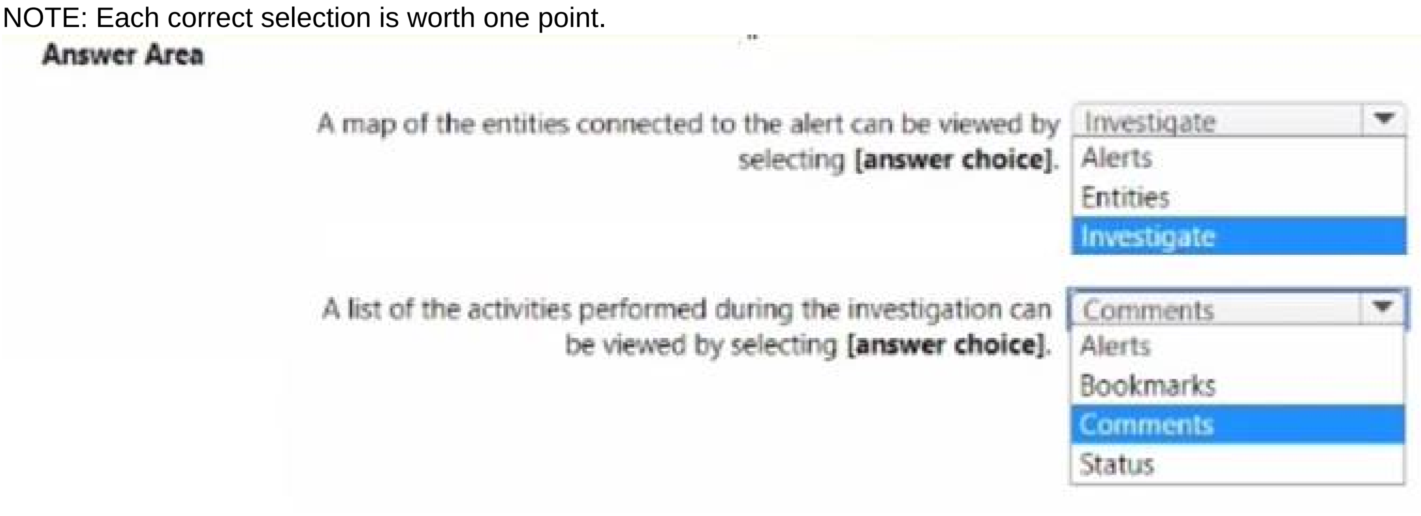
Status
New

Events
Link to LA

Product name
Microsoft Sentinel

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].

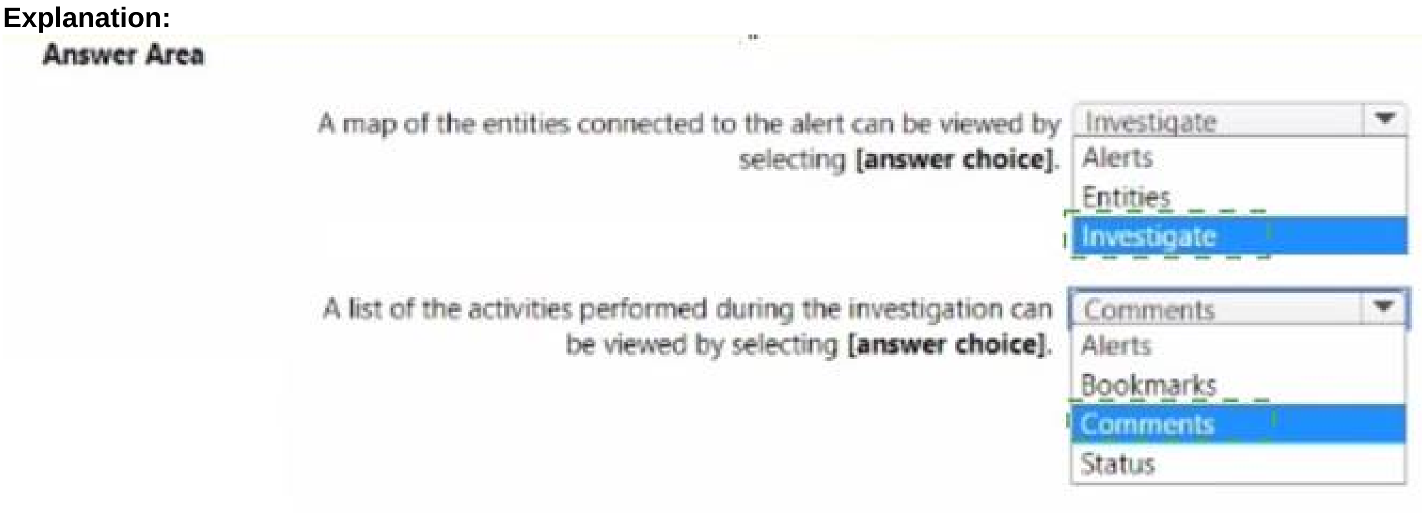
A list of the activities performed during the investigation can be viewed by selecting [answer choice].

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

A map of the entities connected to the alert can be viewed by selecting [answer choice].

A list of the activities performed during the investigation can be viewed by selecting [answer choice].

NEW QUESTION 157

- (Topic 4)

Your company has a single office in Istanbul and a Microsoft 365 subscription.

The company plans to use conditional access policies to enforce multi-factor authentication (MFA).

You need to enforce MFA for all users who work remotely. What should you include in the solution?

A. a fraud alert

B. a user risk policy

C. a named location

D. a sign-in user policy

Answer: C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

NEW QUESTION 161
- (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

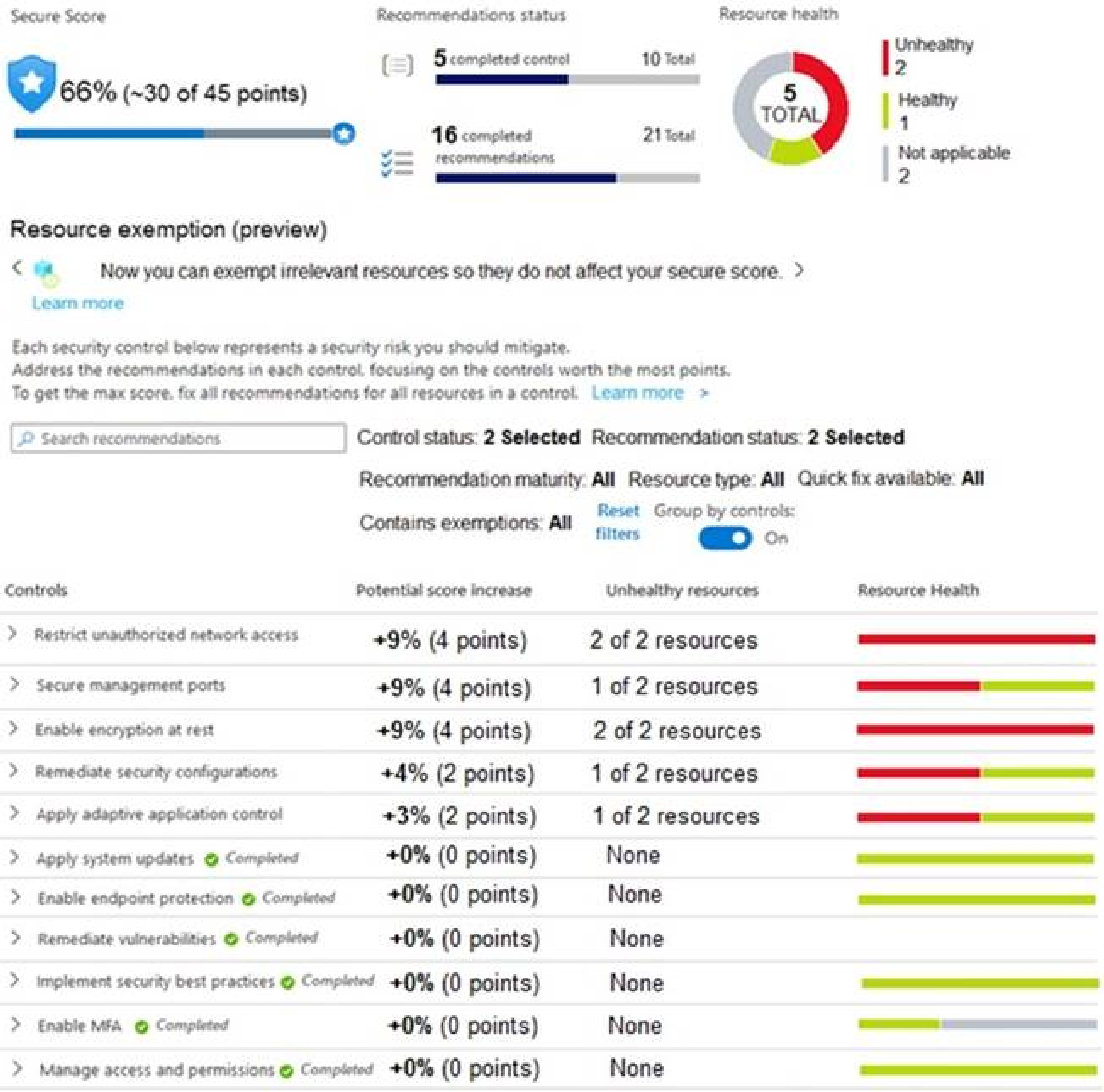
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

NEW QUESTION 164
- (Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned an Azure Active Directory Premium Plan 2 license
You need to identify whether the identity of User1 was compromised during the last 90 days.
What should you use?

A. the risk detections report
B. the risky users report
C. Identity Secure Score recommendations
D. the risky sign-ins report

Answer: B

NEW QUESTION 169
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

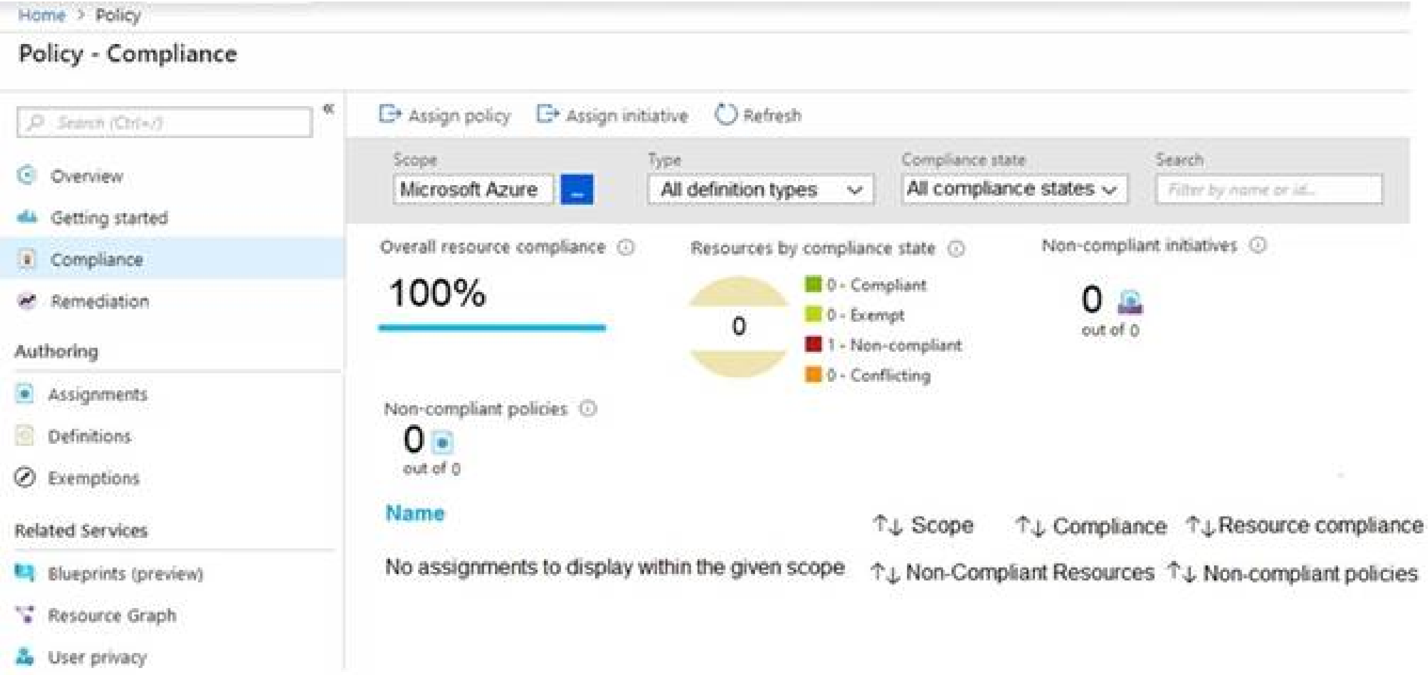
Resource exemption (preview)
Now you can exempt irrelevant resources so they do not affect your secure score.
Learn more

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

Scope: Microsoft Azure | Type: All definition types | Compliance state: All compliance states | Search: Filter by name or id...

Overall resource compliance: 100%

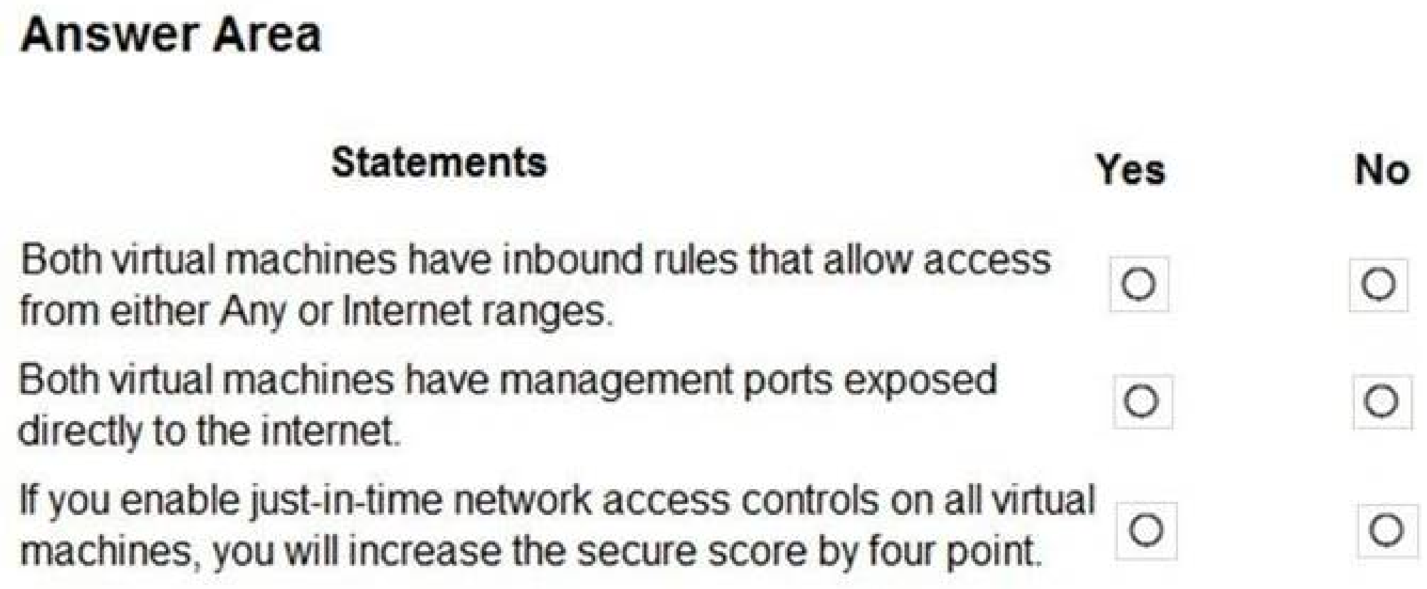
Resources by compliance state: 0
- 🟩 0 - Compliant
- 🟩 0 - Exempt
- 🟥 1 - Non-compliant
- 🟧 0 - Conflicting

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.



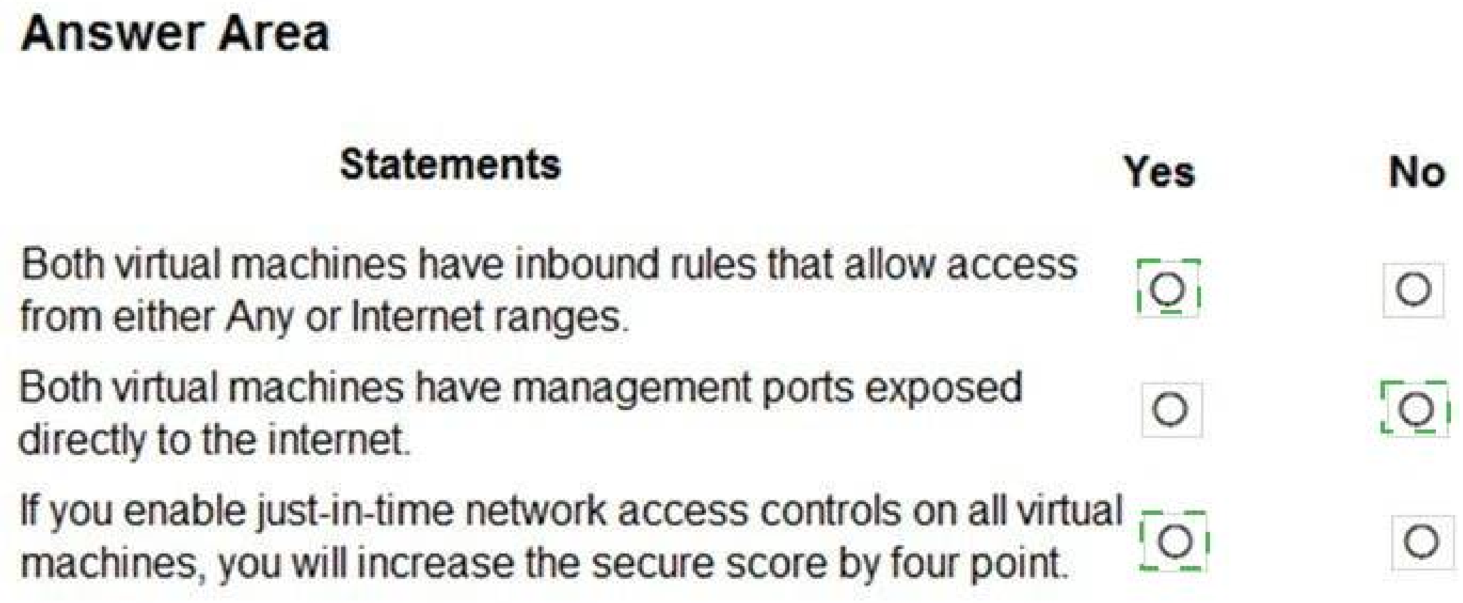
Answer Area

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.	[✓ ○]	○

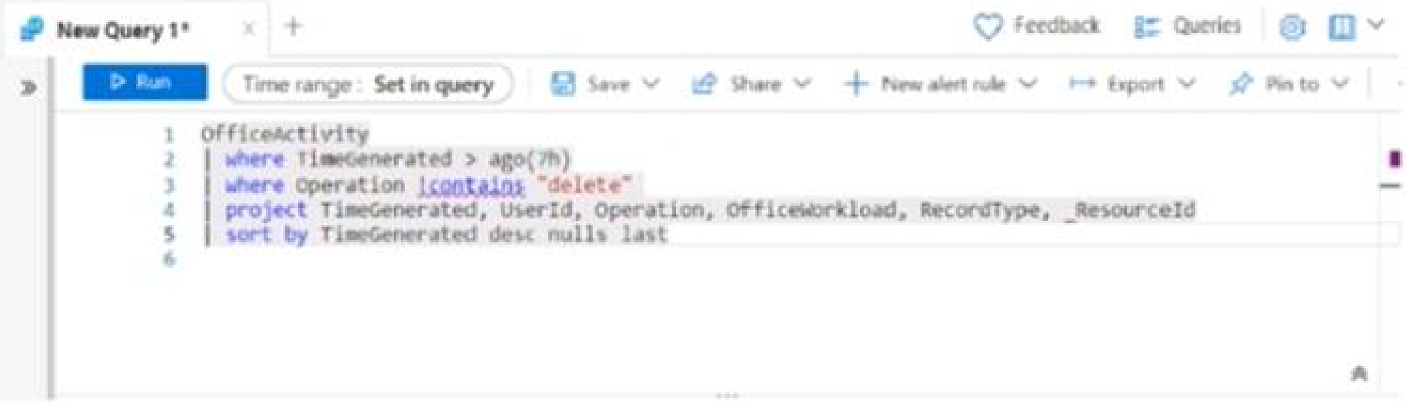
NEW QUESTION 171
- (Topic 4)
You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

A. Azure Synapse AnarytKS
B. AzureDalabricks
C. Azure Machine Learning
D. LogAnalytics

Answer: D

NEW QUESTION 173
- (Topic 4)
You have a Microsoft Sentinel workspace.

You have a query named Query1 as shown in the following exhibit.



```
1  OfficeActivity
2  | where TimeGenerated > ago(7h)
3  | where Operation !contains "delete"
4  | project TimeGenerated, UserId, Operation, OfficeWorkload, RecordType, _ResourceId
5  | sort by TimeGenerated desc nulls last
6
```

You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

A. Remove line 2.
B. In line 4. remove the TimeGenerated predicate.
C. Remove line 5.
D. In line 3, replace the 'contains operator with the !has operator.

Answer: A

Explanation:
This can be confirmed by referring to the official Microsoft documentation on creating custom log queries in Azure Sentinel, which states that the “has” operator should not be used in the query, and that it is unnecessary.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/query-custom-logs

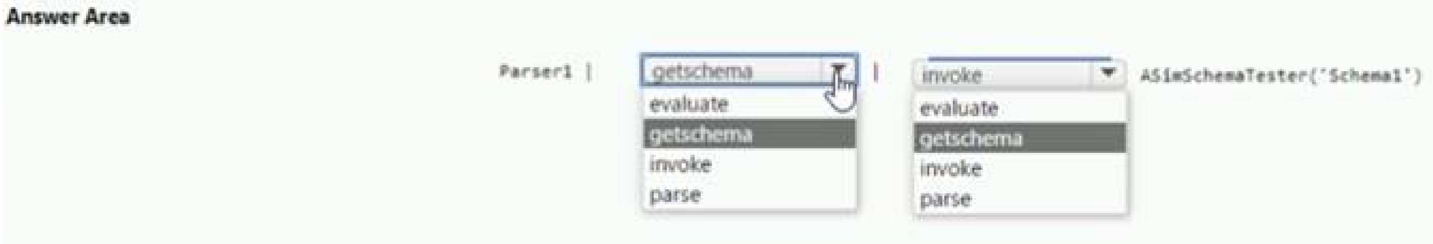
NEW QUESTION 174
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 scheduled query rule for a data connector. 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 175
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.
You need to validate Schema1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

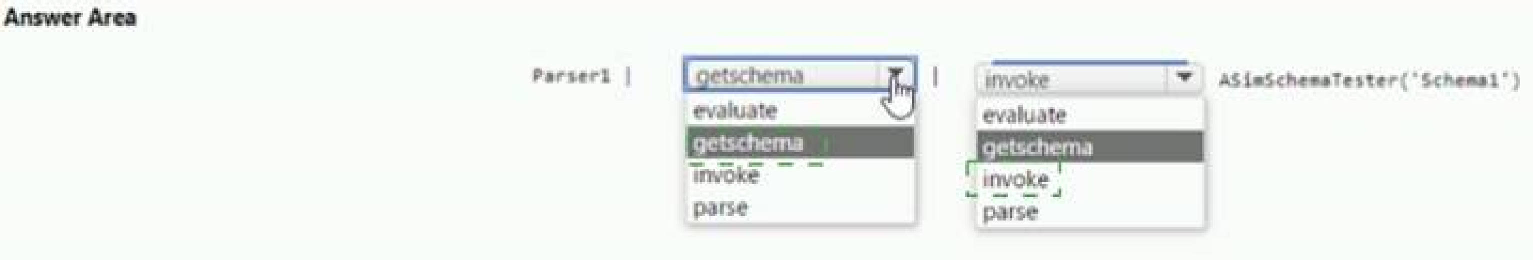

Answer Area

```
Parser1 | getschema | invoke ASimSchemaTester('Schema1')
```

A. Mastered
B. Not Mastered

Answer: A

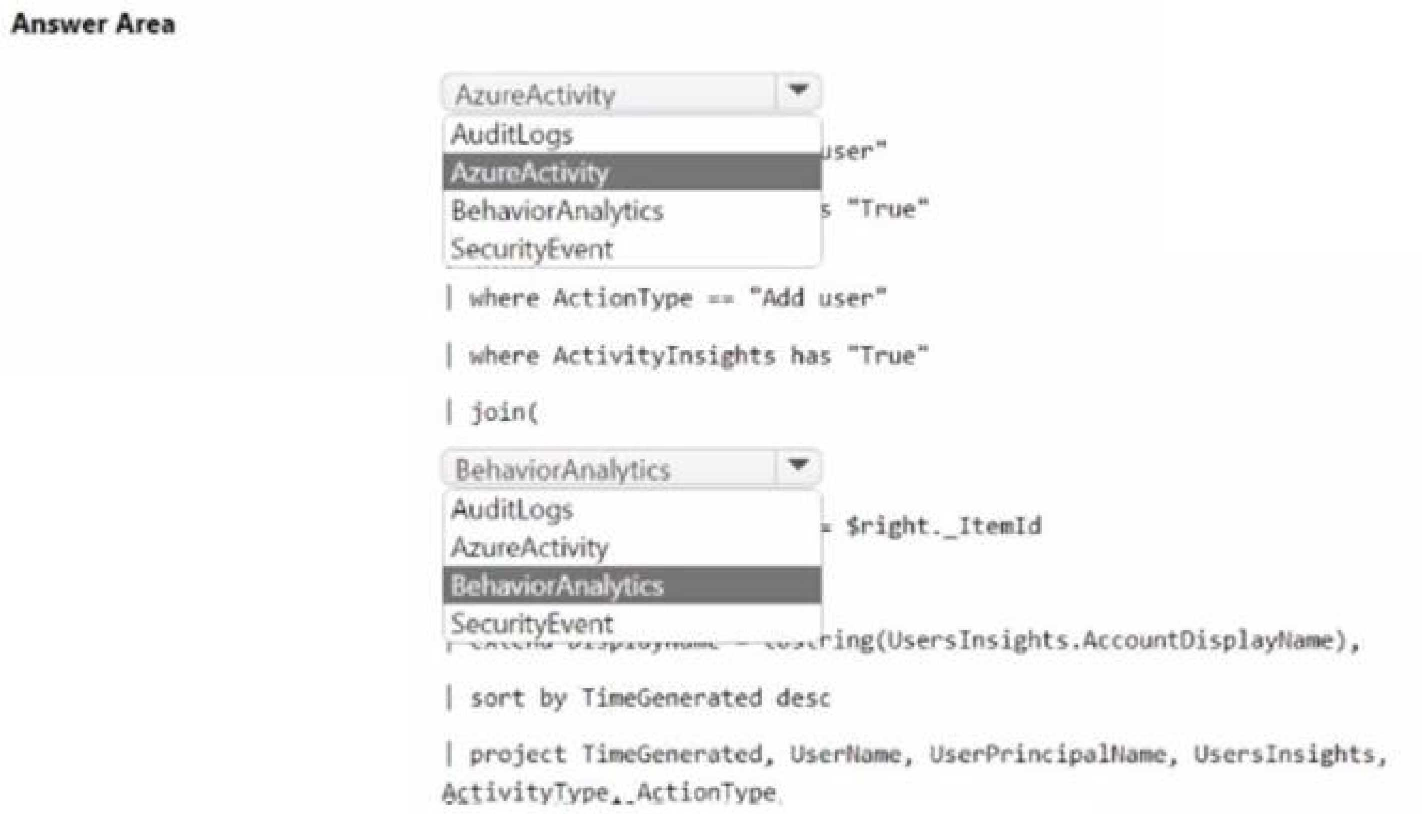
Explanation:


Answer Area

```
Parser1 | getschema | invoke ASimSchemaTester('Schema1')
```

NEW QUESTION 179
HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace named sws1.
You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



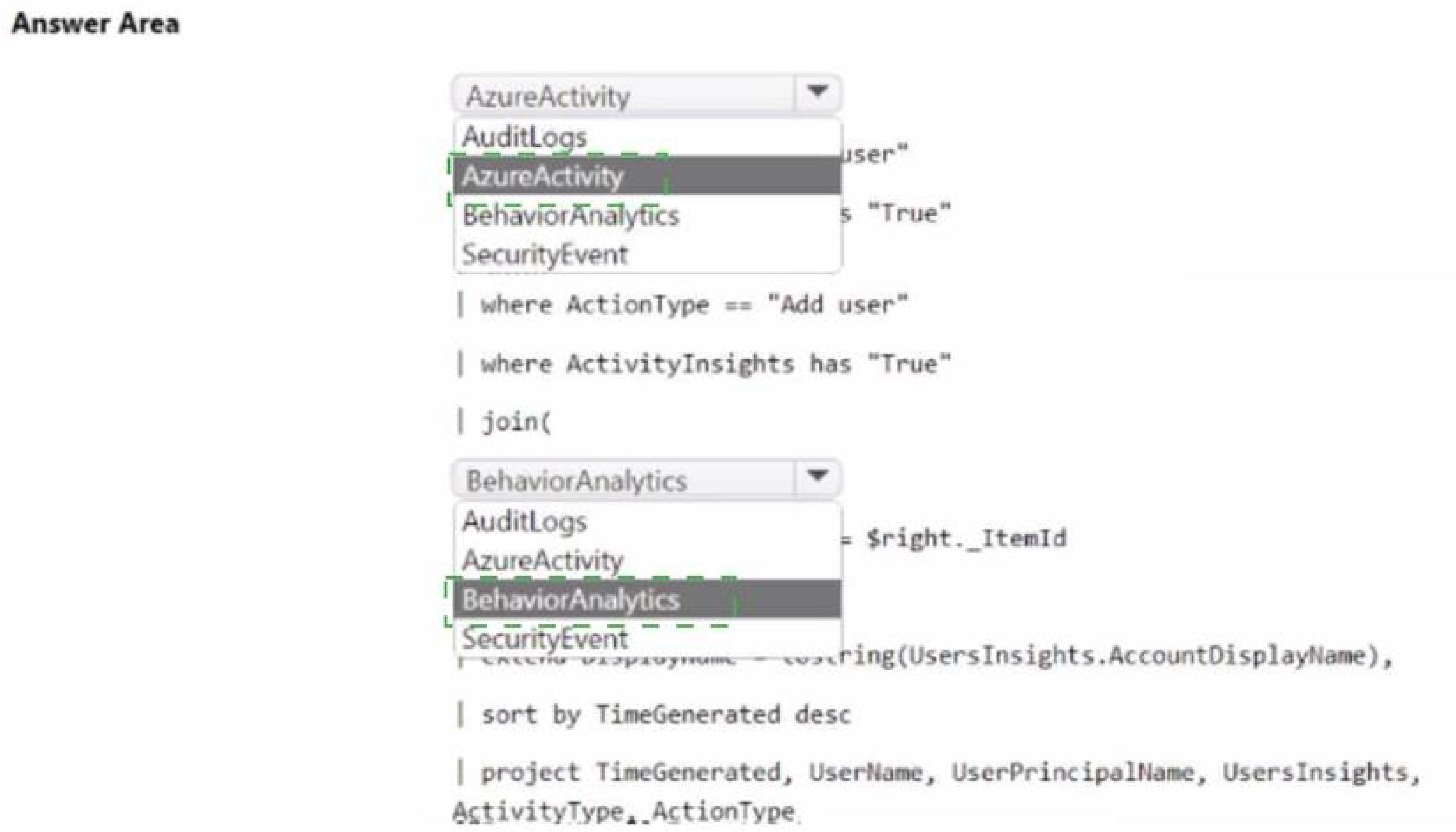
Answer Area

```
AzureActivity ▼
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
                                   user"
                                 s "True"
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
BehaviorAnalytics ▼
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
                                 = $right._ItemId
                                 ring(UsersInsights.AccountDisplayName),
| sort by TimeGenerated desc
| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType, ActionType
```

A. Mastered
B. Not Mastered

Answer: A

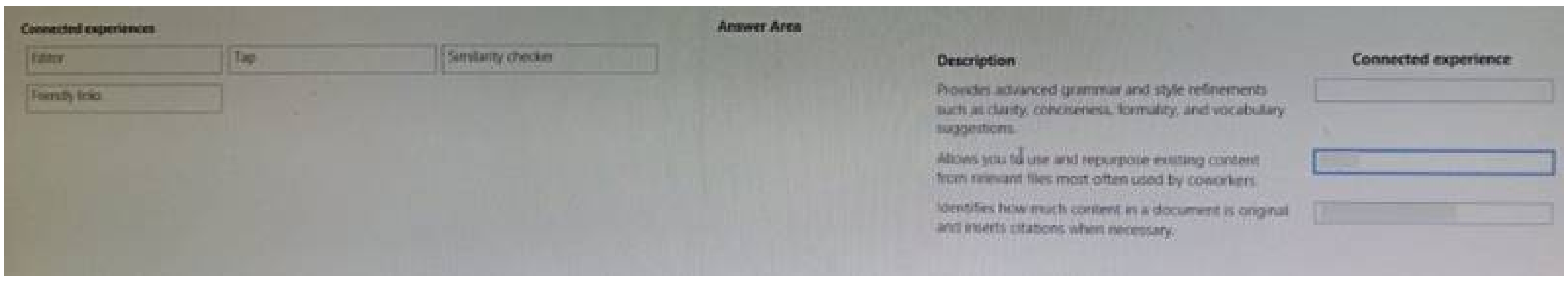
Explanation:



Answer Area

```
AzureActivity ▼
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
                                   user"
                                 s "True"
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
BehaviorAnalytics ▼
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent
                                 = $right._ItemId
                                 ring(UsersInsights.AccountDisplayName),
| sort by TimeGenerated desc
| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType, ActionType
```

NEW QUESTION 184
DRAG DROP - (Topic 4)
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Connected experiences

Editor | Tap | Similarity checker | Friendly links

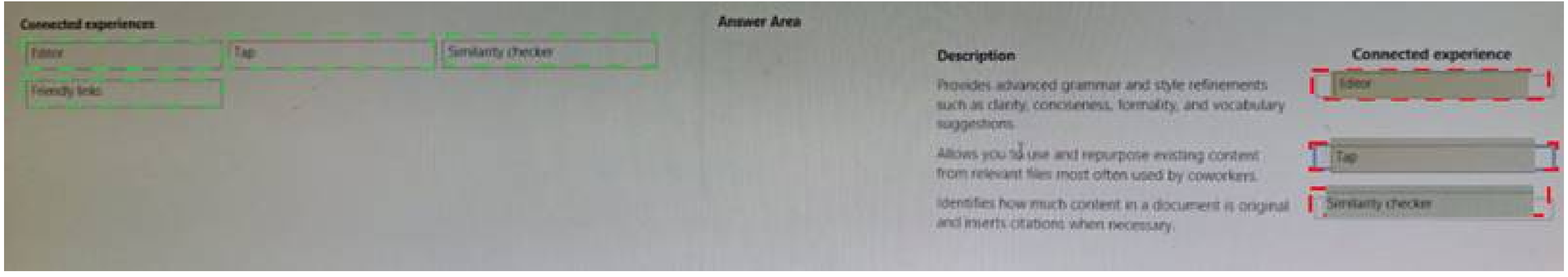
Answer Area

Description	Connected experience
Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.	
Allows you to use and repurpose existing content from relevant files most often used by coworkers.	
Identifies how much content in a document is original and inserts citations when necessary.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Connected experiences

Editor | Tap | Similarity checker | Friendly links

Answer Area

Description	Connected experience
Provides advanced grammar and style refinements such as clarity, conciseness, formality, and vocabulary suggestions.	Editor
Allows you to use and repurpose existing content from relevant files most often used by coworkers.	Tap
Identifies how much content in a document is original and inserts citations when necessary.	Similarity checker

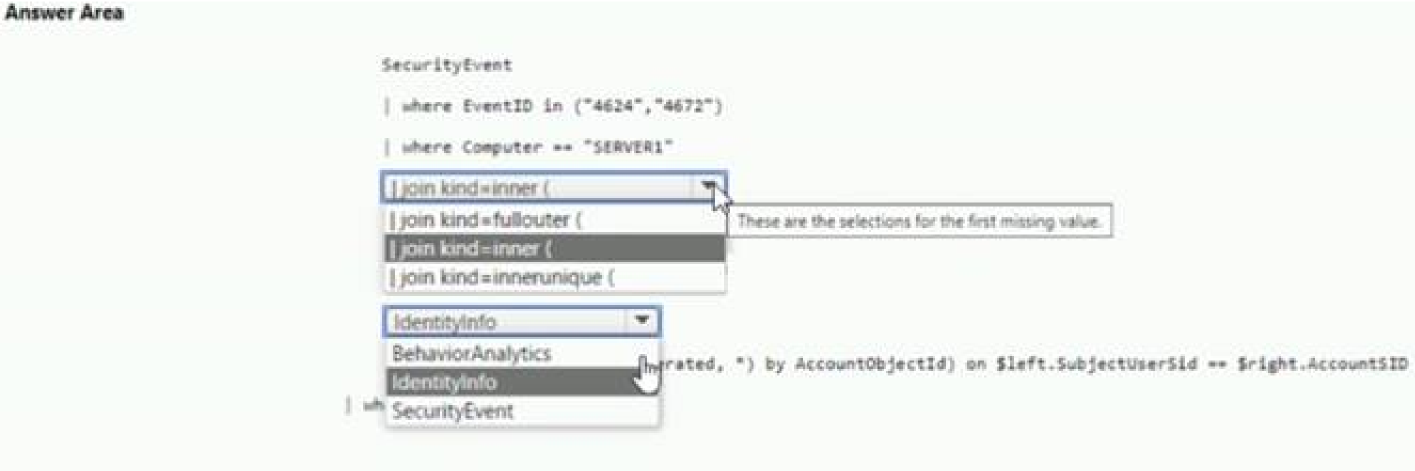
NEW QUESTION 186
- (Topic 4)
You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender. Which two Bash commands should you 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 190
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.
You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:
• Only include security-sensitive actions by users that are NOT members of the IT department.
• Minimize the number of false positives.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



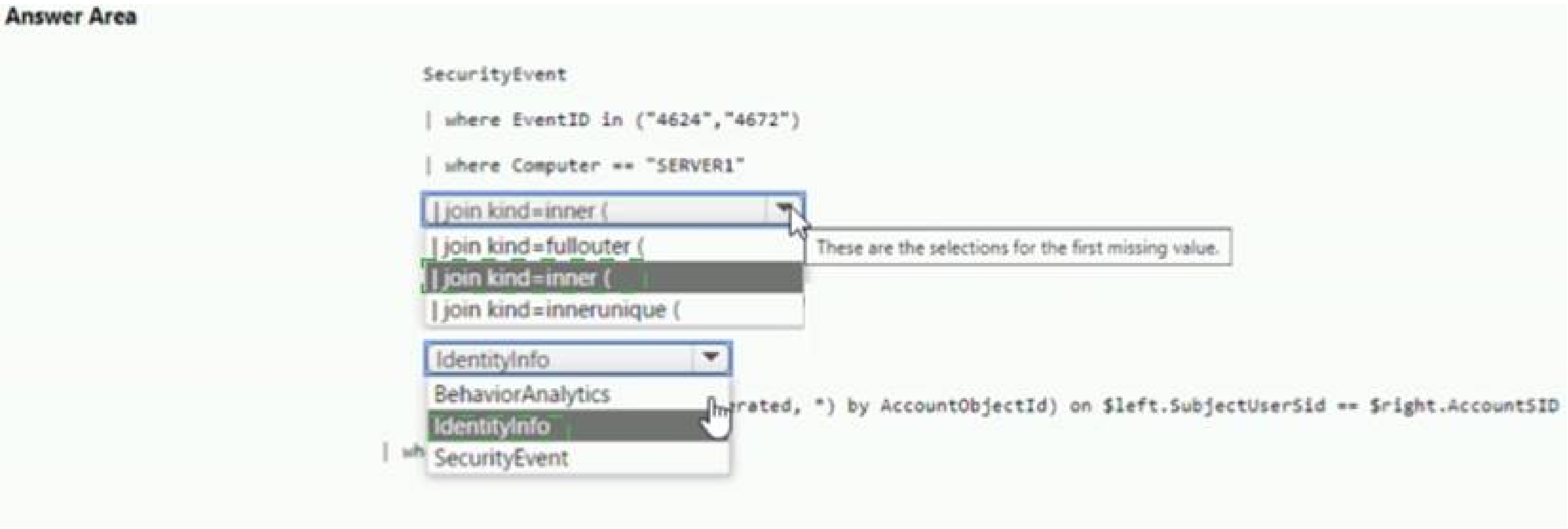
Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
IdentityInfo
...rated, ") by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| wh
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
```

```
rated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| wh
```

NEW QUESTION 195

- (Topic 4)

You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

A. Create an AWS user for Defender for Cloud.
B. Create an Access control (1AM) role for Defender for Cloud.
C. Configure AWS Security Hub.
D. Deploy the AWS Systems Manager (SSM) agent

Answer: D

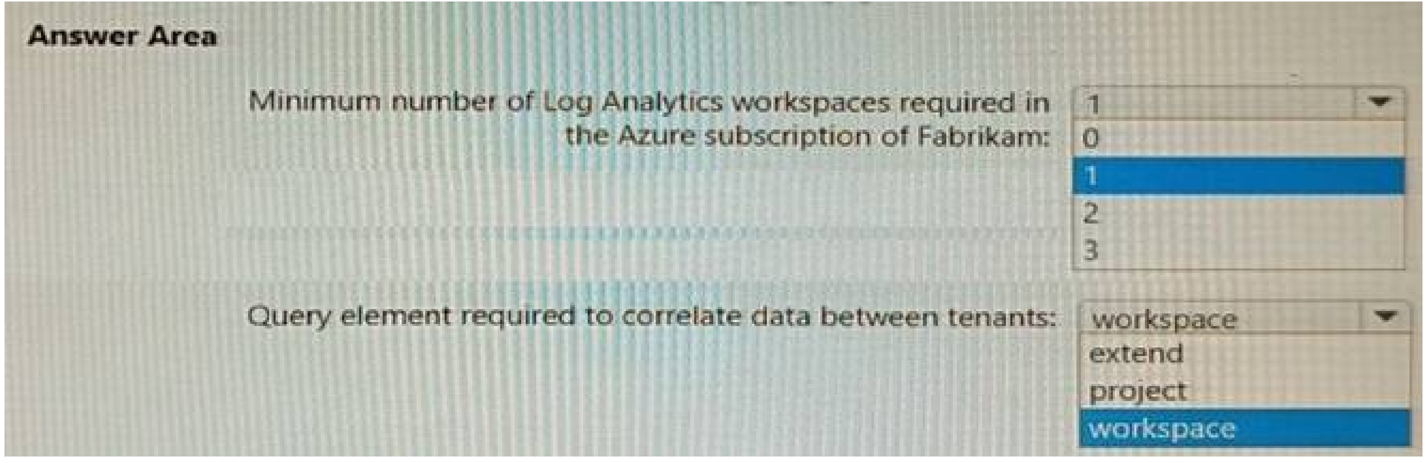
NEW QUESTION 196

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

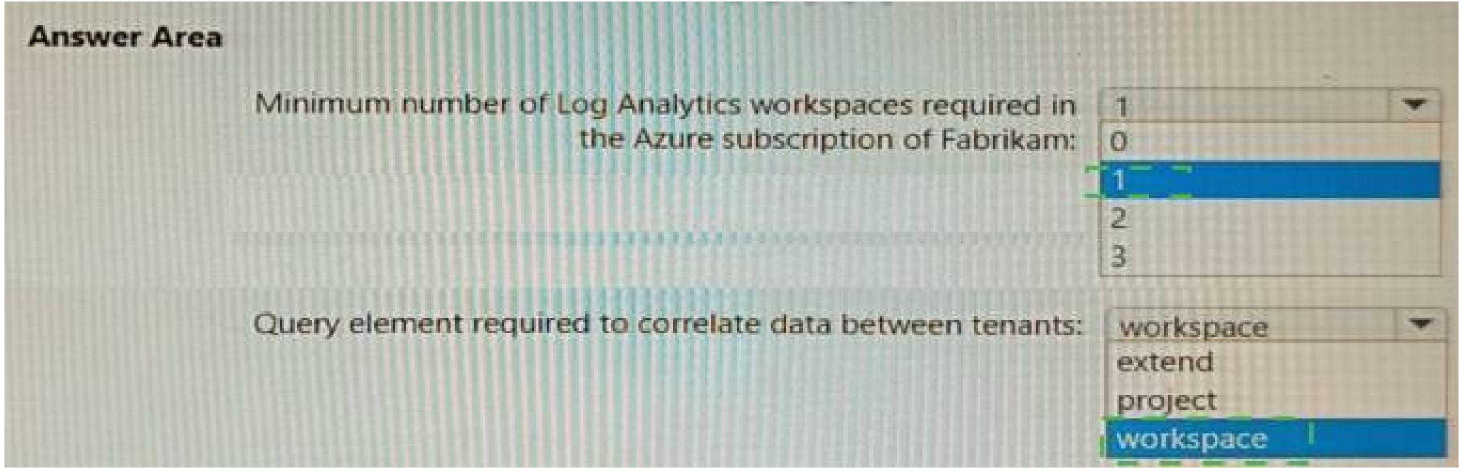
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

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 197

- (Topic 4)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

NOTE: Each correct selection is worth one point.

A. Add a playbook.
B. Associate a playbook to an incident.

C. Enable Entity behavior analytics.
D. Create a workbook.
E. Enable the Fusion rule.

Answer: AB

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

NEW QUESTION 199
- (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

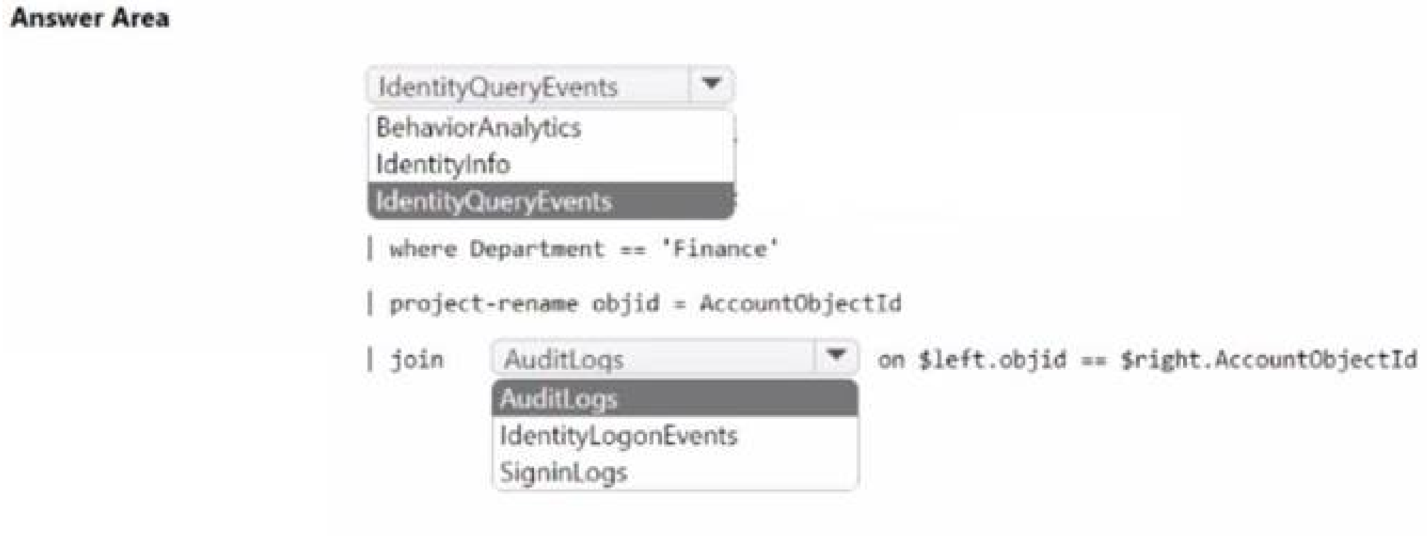
Explanation:
Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage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

NEW QUESTION 202
- (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 204
HOTSPOT - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to identify all the interactive authentication attempts by the users in the finance department of your company.
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.

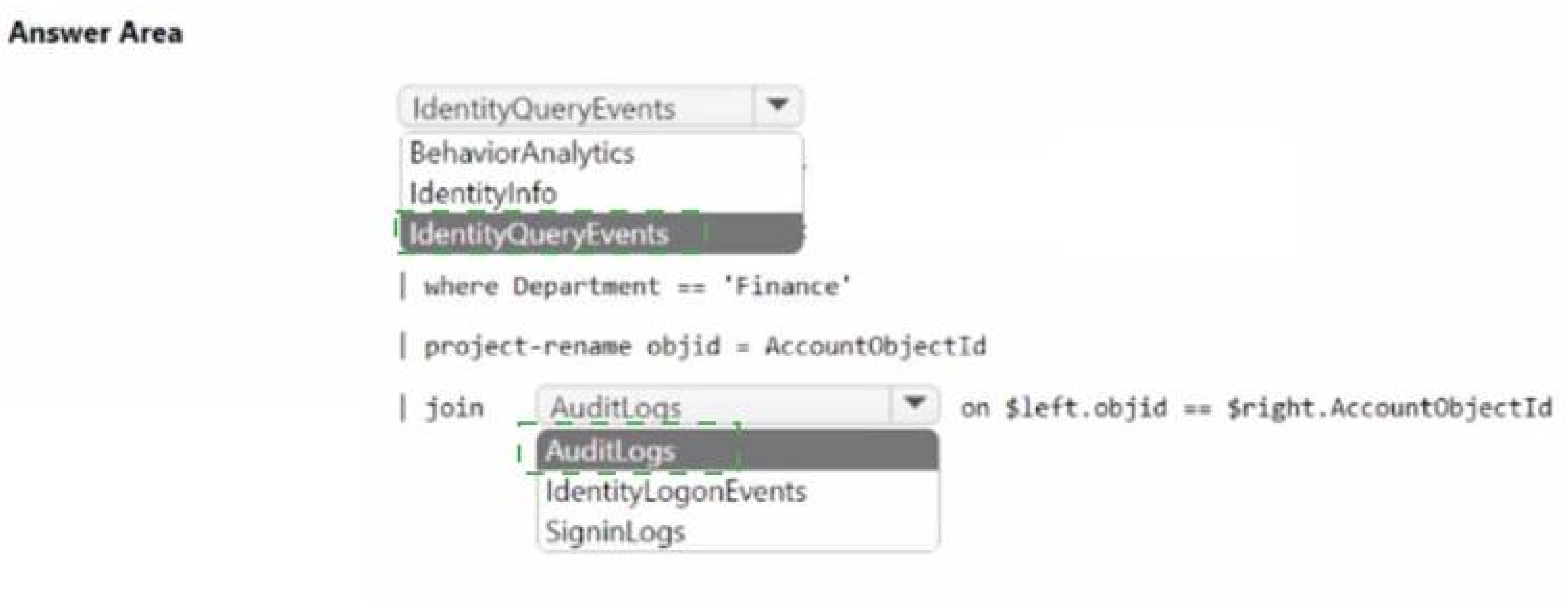


```
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join                on $left.objid == $right.AccountObjectId
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

```
IdentityQueryEvents
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join AuditLogs on $left.objid == $right.AccountObjectId
```

NEW QUESTION 208

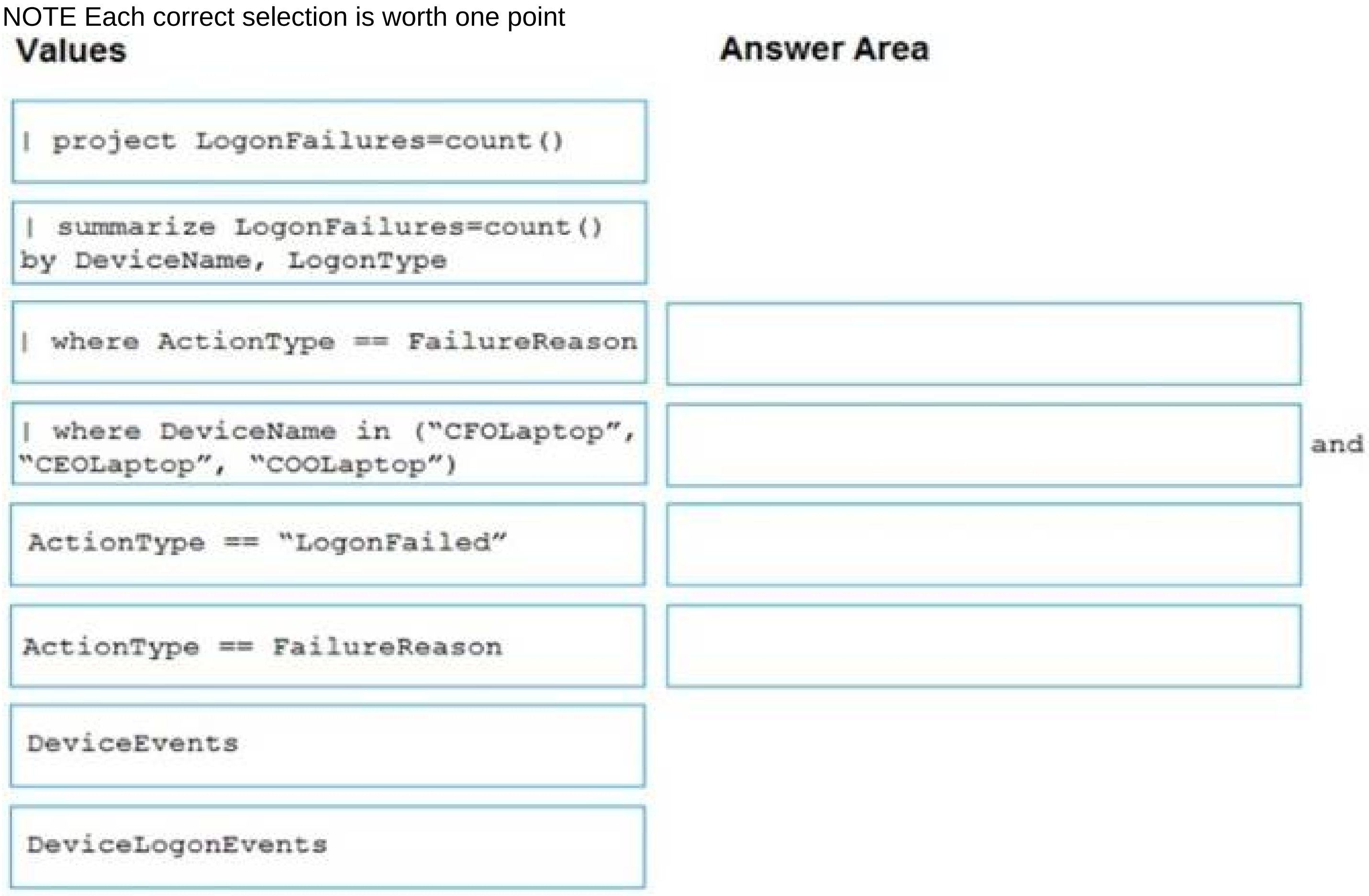
DRAG DROP - (Topic 4)

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
```

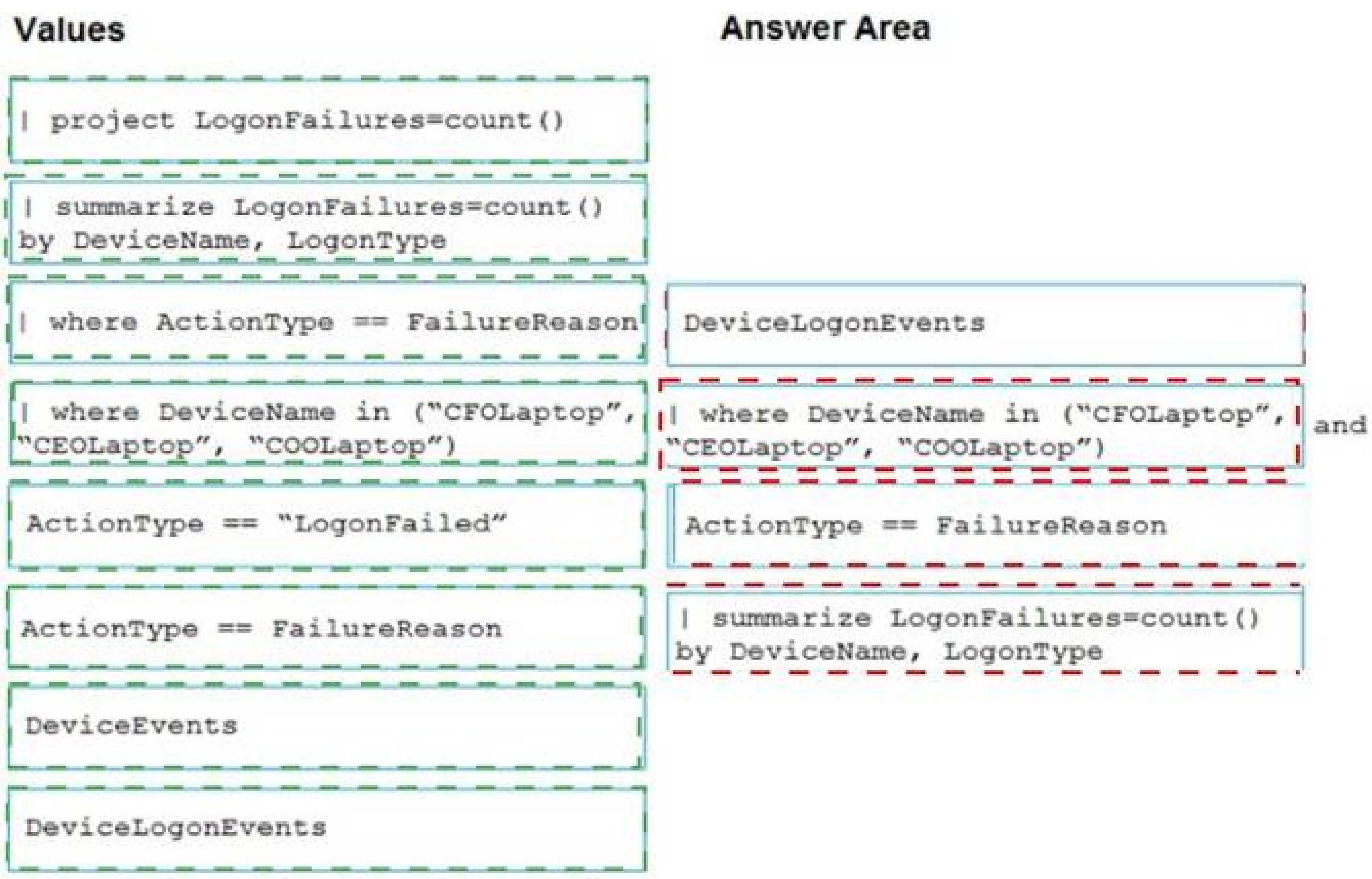
Answer Area

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
```

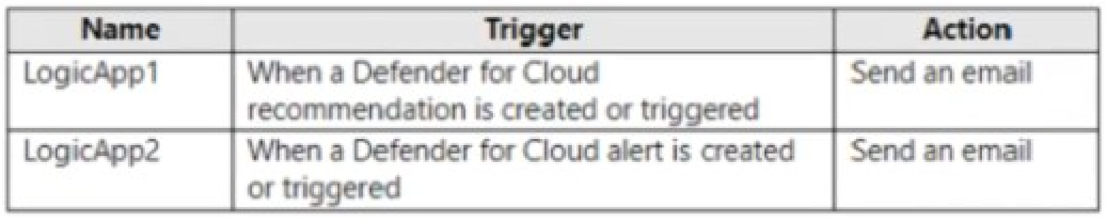
NEW QUESTION 210
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

A. a workbook
B. a hunting query
C. a watchlist
D. an analytic rule

Answer: D

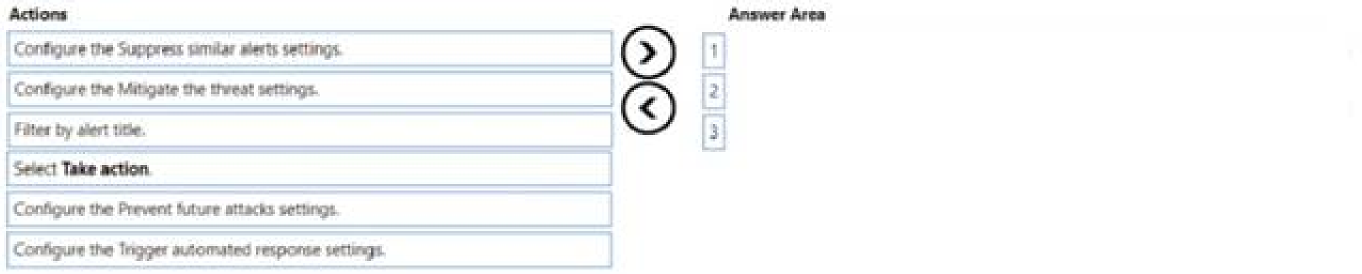
Explanation:
To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule

NEW QUESTION 214
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").

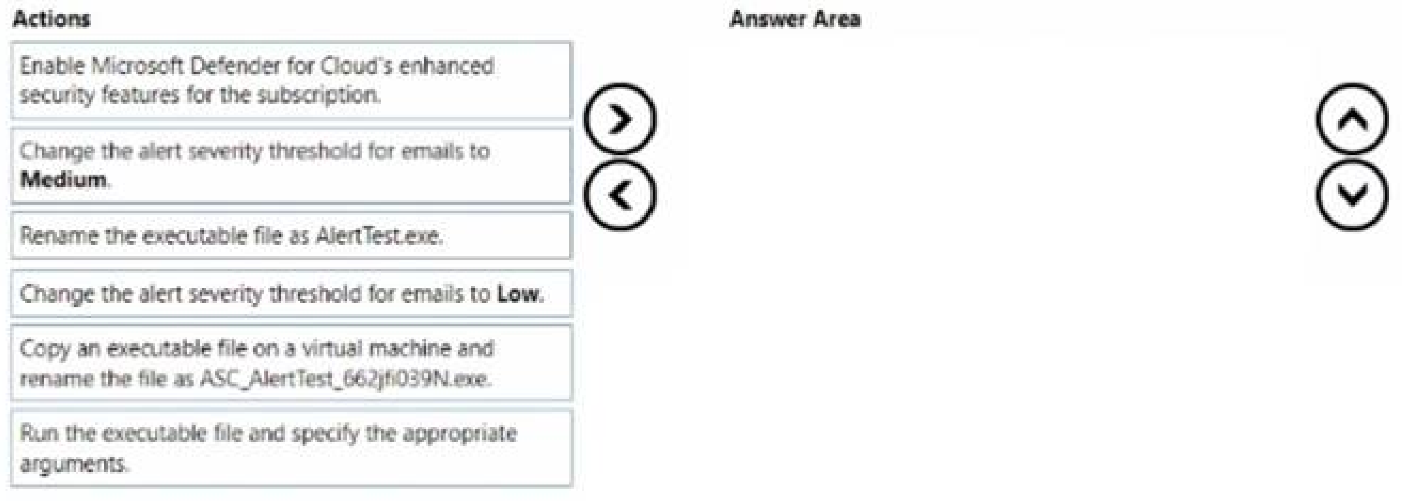
NEW QUESTION 219
- (Topic 4)
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual 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 222
DRAG DROP - (Topic 4)
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



Actions

Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

Change the alert severity threshold for emails to **Medium**.

Rename the executable file as AlertTest.exe.

Change the alert severity threshold for emails to **Low**.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.

Run the executable file and specify the appropriate arguments.

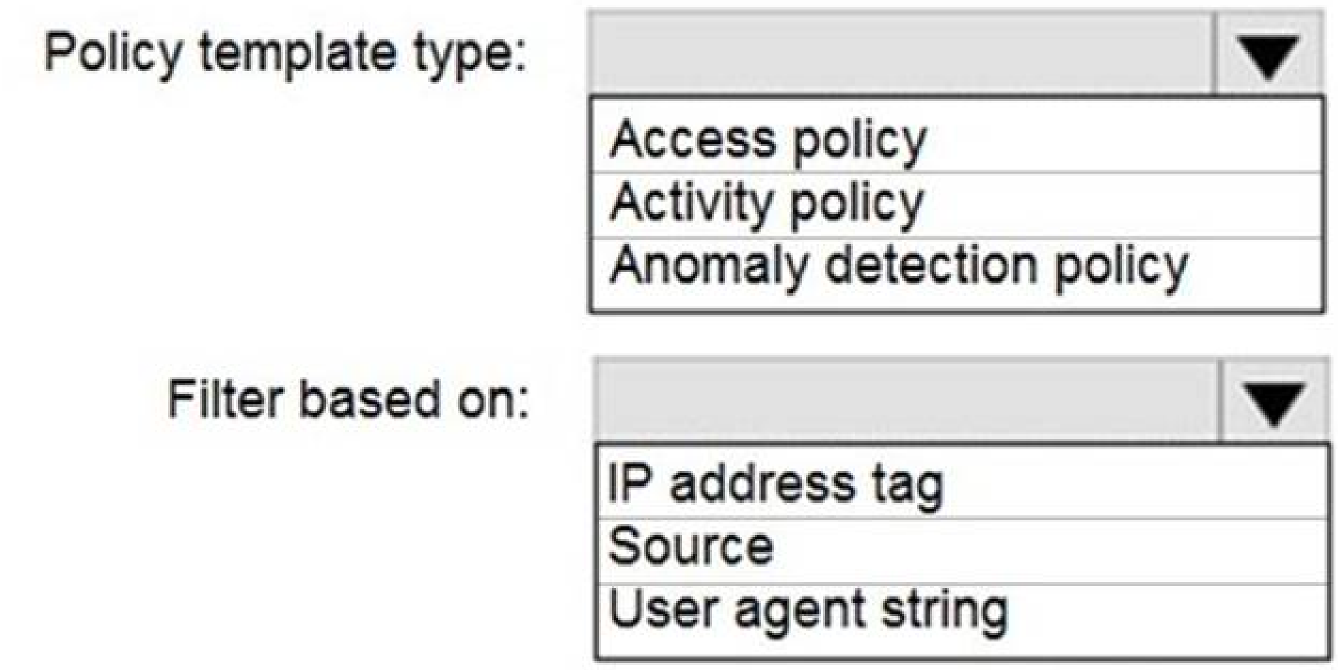
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:
? Copy an executable file on a virtual machine and rename the file as
ASC_AlertTest_662jfi039N.exe
? Run the executable file and specify the appropriate arguments
? Enable Microsoft Defender for Cloud's enhanced security features for the subscription.
These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

NEW QUESTION 226
HOTSPOT - (Topic 4)
You purchase a Microsoft 365 subscription.
You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Policy template type:

- Access policy
- Activity policy
- Anomaly detection policy

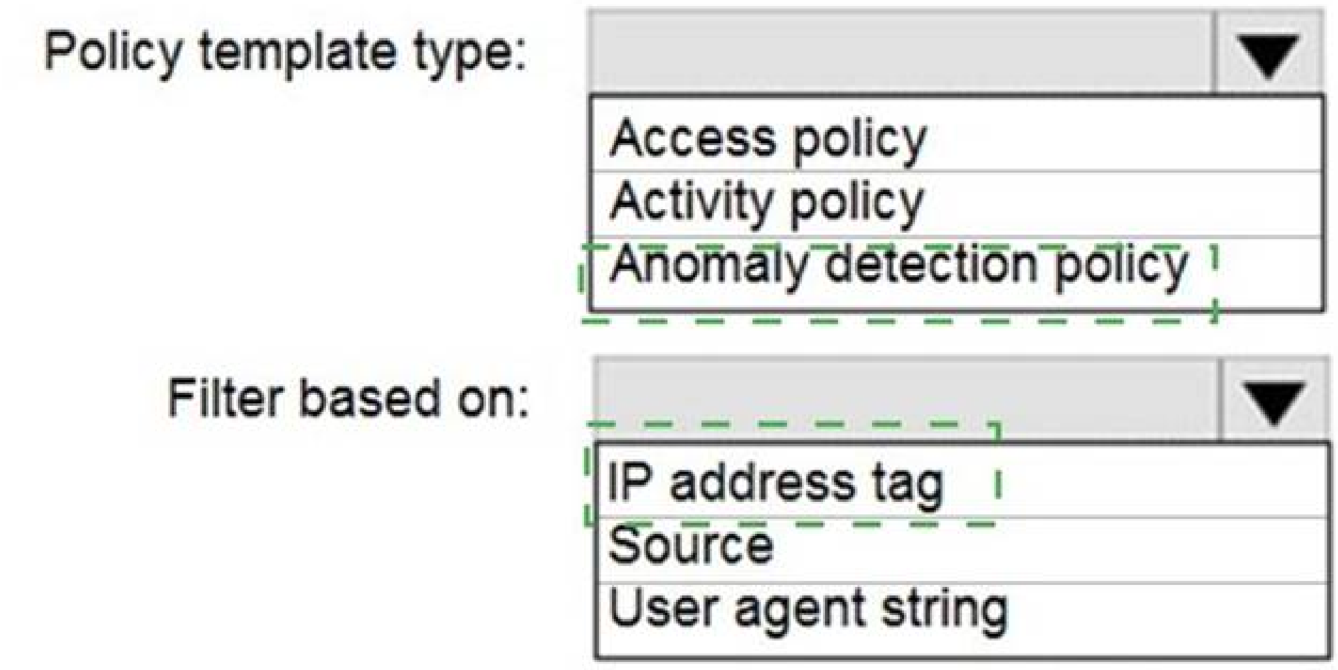
Filter based on:

- IP address tag
- Source
- User agent string

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Policy template type:

- Access policy
- Activity policy
- Anomaly detection policy

Filter based on:

- IP address tag
- Source
- User agent string

NEW QUESTION 230
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Purview. Your company has a project named Project1.
You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.
What should you do?

A. Create a records management disposition.
B. Perform a user data search.
C. Perform an audit search.
D. Perform a content search.

Answer: D

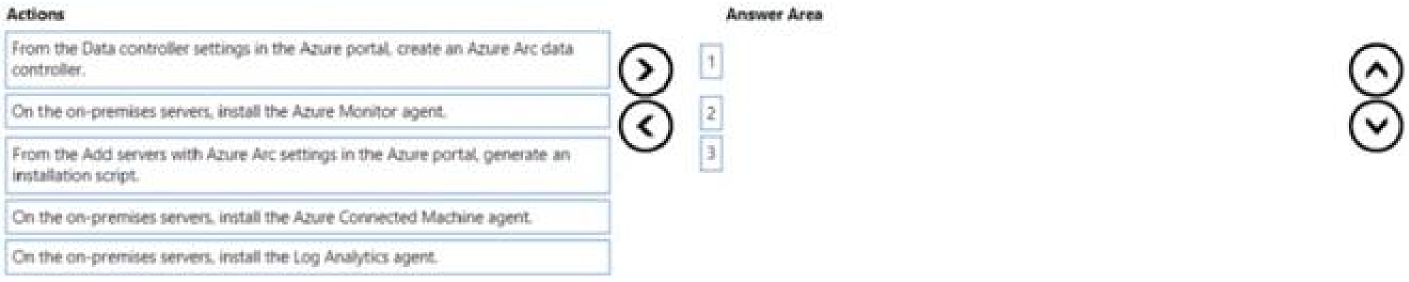
NEW QUESTION 235
- (Topic 4)
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.
What should you create first?

A. a trigger in Azure Functions
B. an Azure logic app
C. a hunting query in Microsoft Sentinel
D. an automation rule in Microsoft Sentinel

Answer: D

NEW QUESTION 238
DRAG DROP - (Topic 4)
You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:
• Provide threat and vulnerability management.
• Support data collection rules.
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 the Data controller settings in the Azure portal, create an Azure Arc data controller.

On the on-premises servers, install the Azure Monitor agent.

From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

Answer Area

1

2

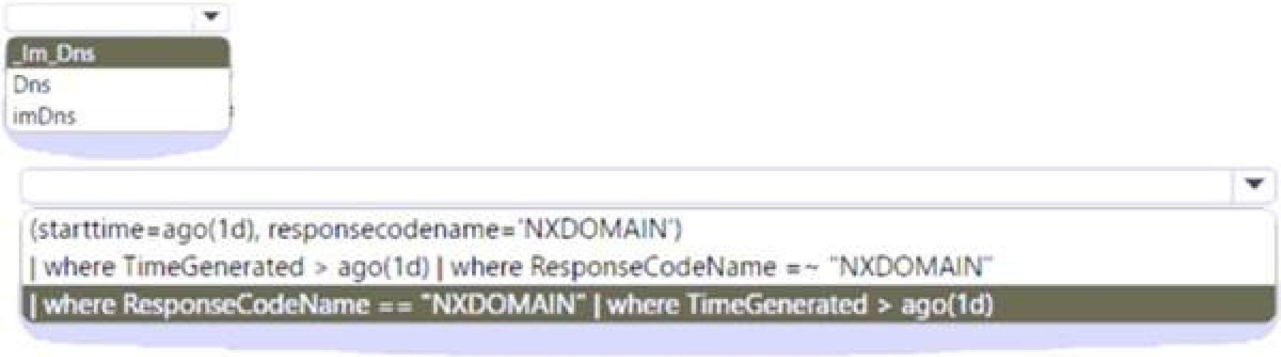
3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:
? On the on-premises servers, install the Azure Connected Machine agent.
? On the on-premises servers, install the Log Analytics agent.
? From the Data controller settings in the Azure portal, create an Azure Arc data controller.
Once these steps are completed, the on-premises servers will be able to communicate with the Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules.
Reference: https://docs.microsoft.com/en-us/azure/security-center/deploy-azure-security-center#on-premises-deployment

NEW QUESTION 241
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.
You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.



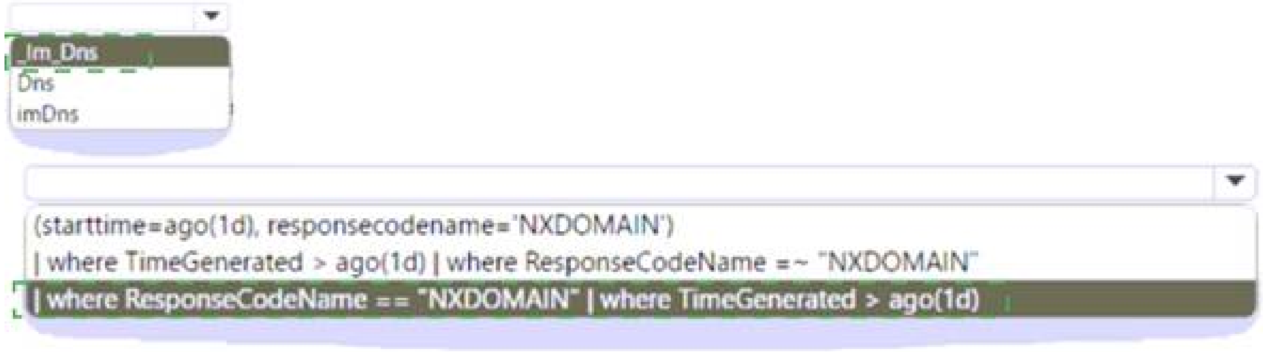
_Im_Dns
Dns
imDns

(starttime=ago(1d), responsecodename='NXDOMAIN')
| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"
| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



_Im_Dns
Dns
imDns

(starttime=ago(1d), responsecodename='NXDOMAIN')
| where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN"
| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)

NEW QUESTION 242
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

Answer: C

Explanation:
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- incidents

NEW QUESTION 243
- (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 use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the ‘Mitigate the threat’ option.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

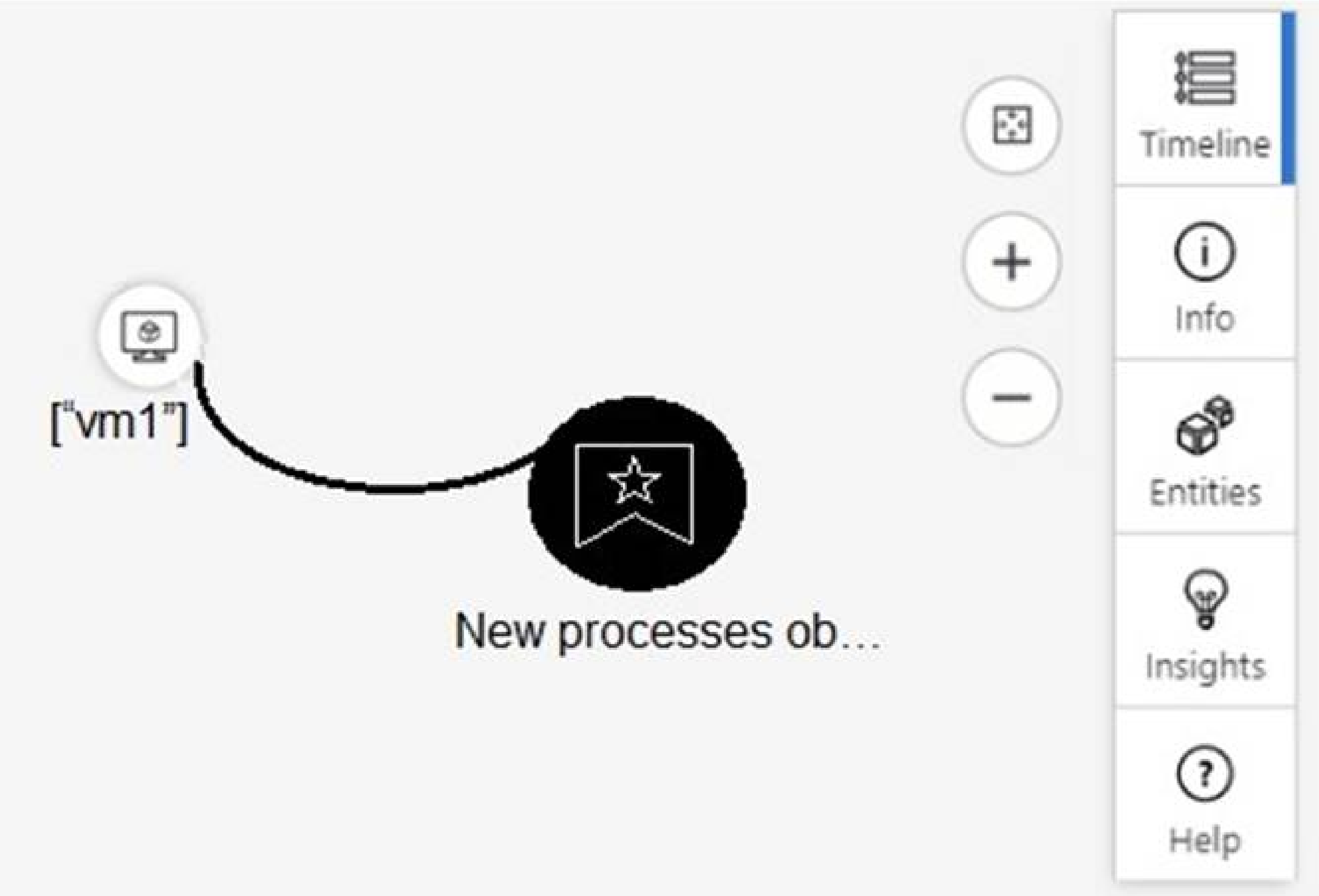
NEW QUESTION 248
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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: You add the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

A. Yes
B. No

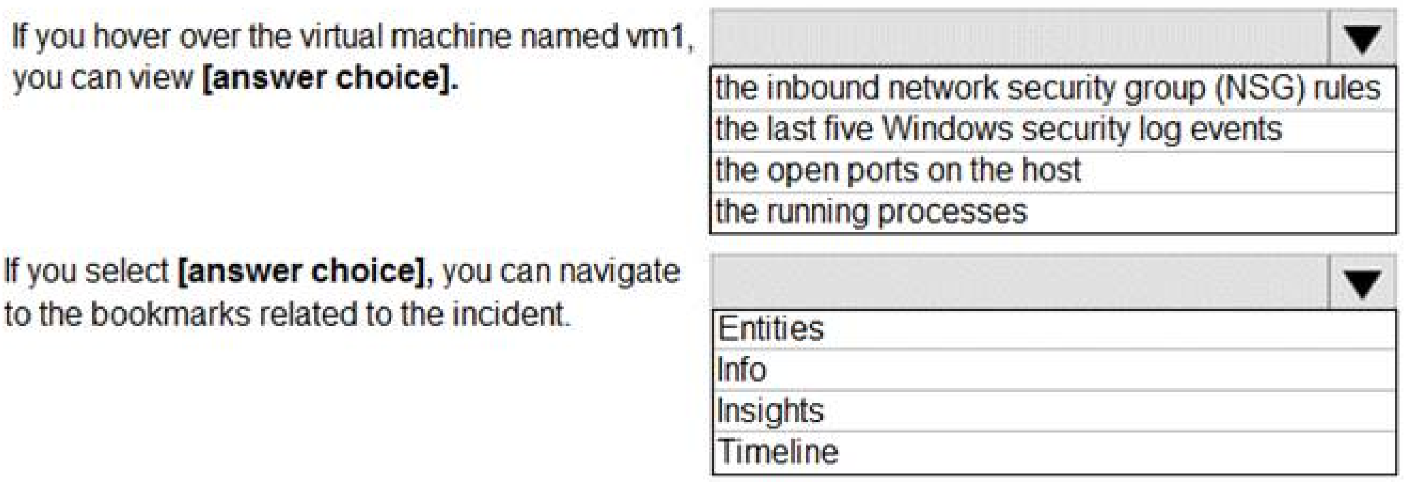
Answer: B

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

NEW QUESTION 250
HOTSPOT - (Topic 4)
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

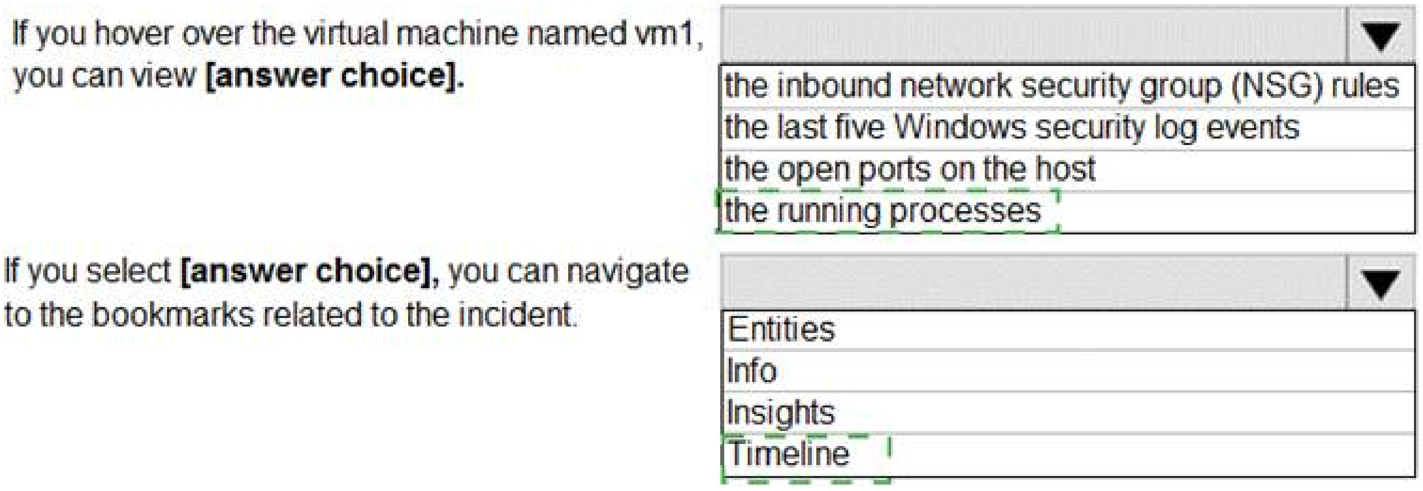
If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

A. Mastered
B. Not Mastered

Answer: A

Explanation:



If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- [✓ the running processes]

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- [✓ Timeline]

NEW QUESTION 253
- (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

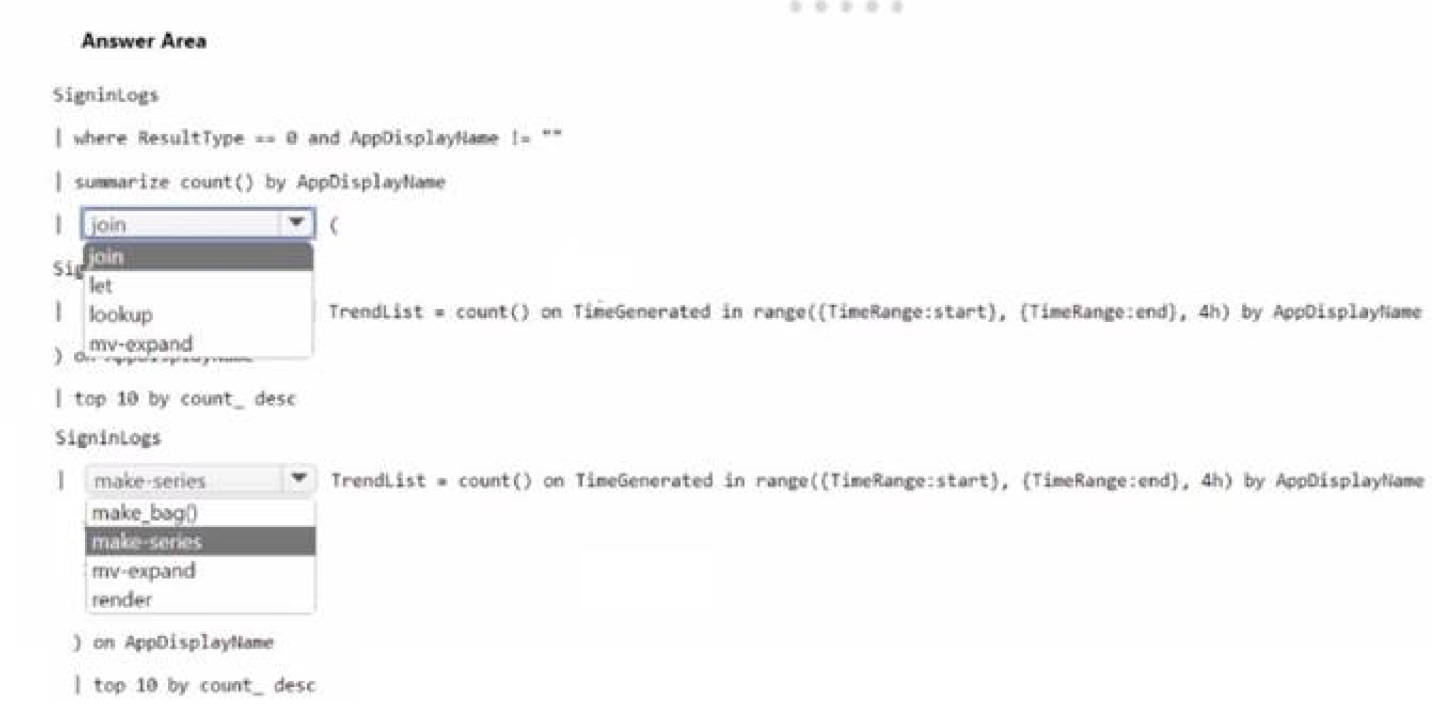
NEW QUESTION 255
- (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.
What should you use to create the visuals?

A. plotly
B. TensorFlow
C. msticpy
D. matplotlib

Answer: C

Explanation:
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:
Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX. Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
Visualization tools using event timelines, process trees, and geo mapping.
Advanced analyses, such as time series decomposition, anomaly detection, and clustering.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started https://msticpy.readthedocs.io/en/latest/

NEW QUESTION 256
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.

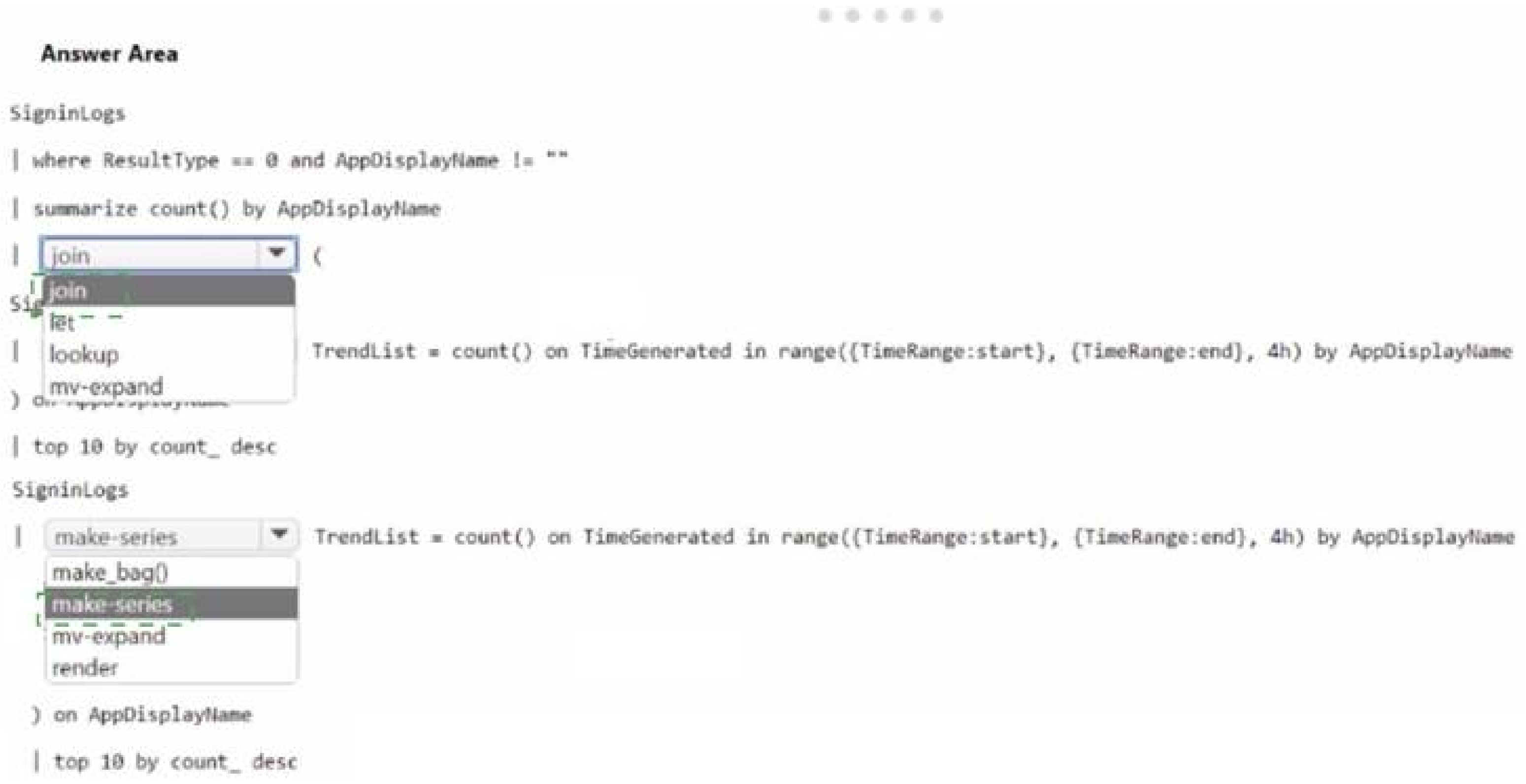

Answer Area

```
SigninLogs
| where ResultType == 0 and AppDisplayName != ""
| summarize count() by AppDisplayName
| [join ▼] (
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
```

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 257
- (Topic 4)
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

A. Playbooks
B. Analytics
C. Threat intelligence
D. Incidents

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

NEW QUESTION 260
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information- protection

NEW QUESTION 261
- (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

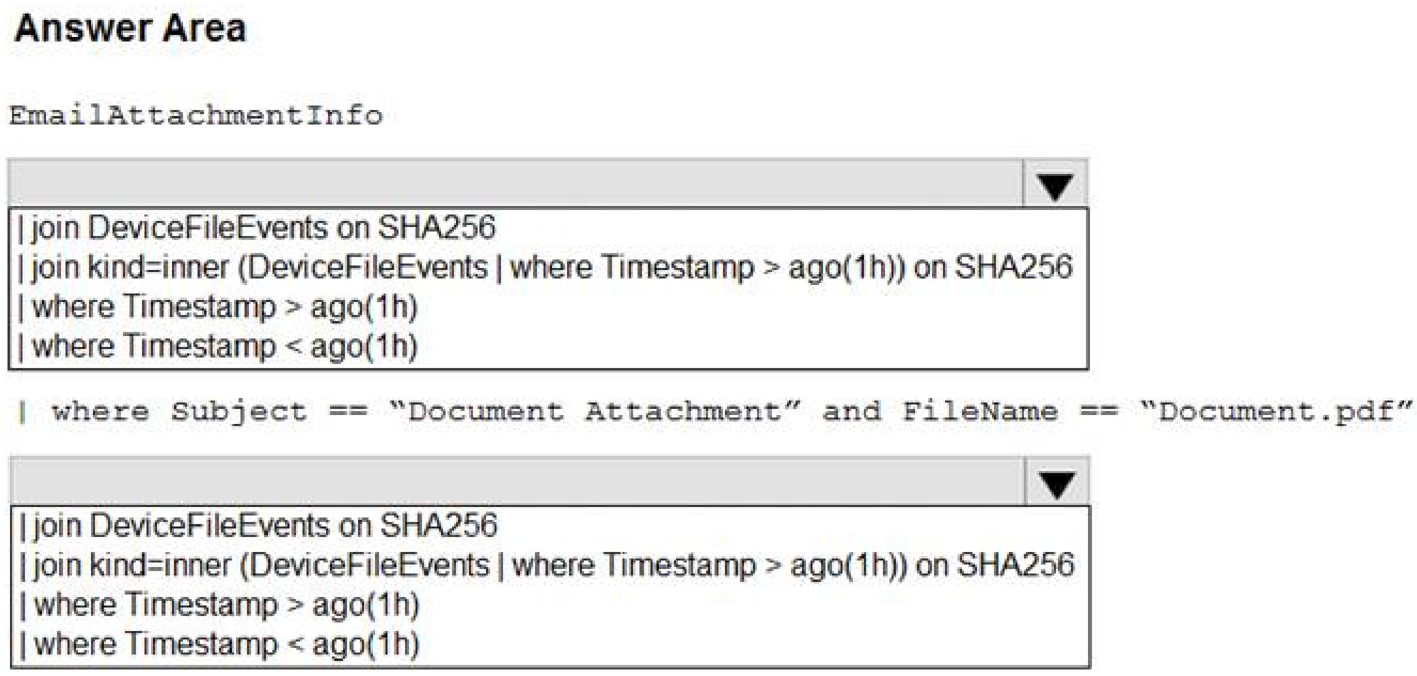
NEW QUESTION 264
- (Topic 4)
You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident. What should you do?

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 269
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:
• Only show emails sent during the last hour.
• Optimize query performance.
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

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

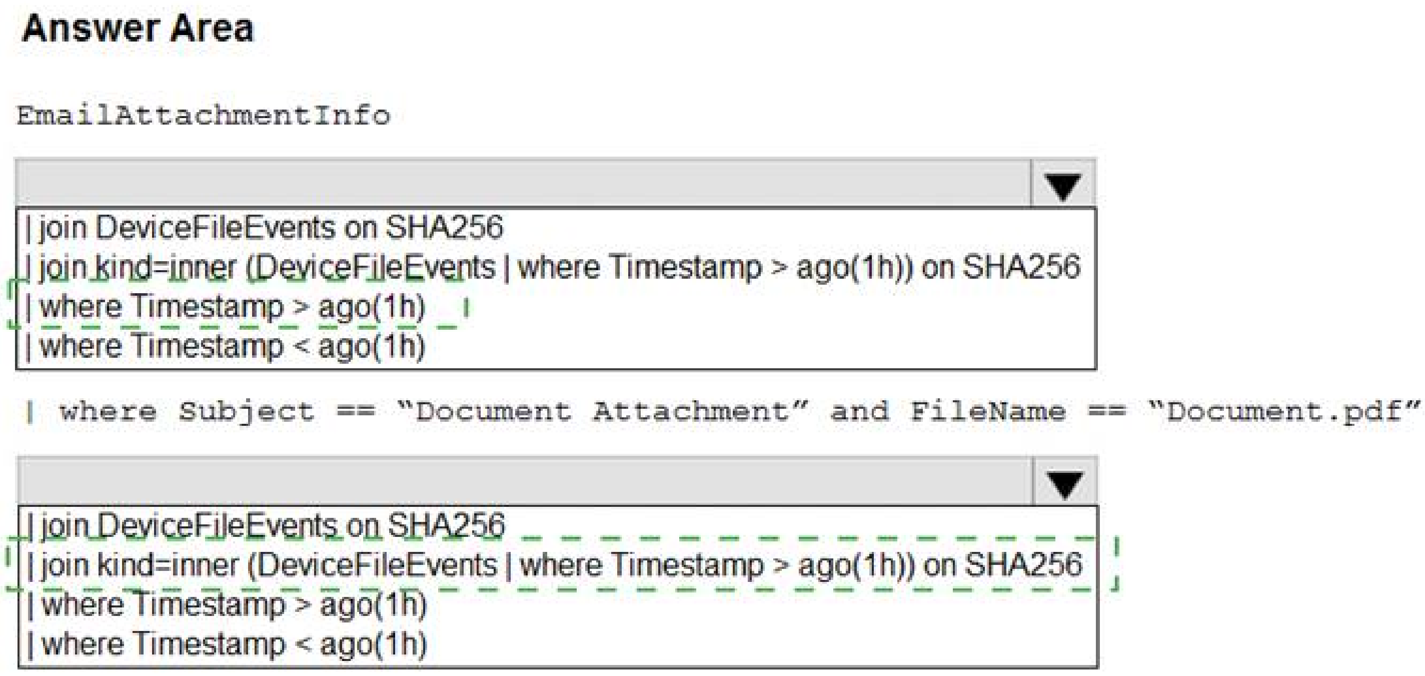
| where Subject == "Document Attachment" and FileName == "Document.pdf"

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

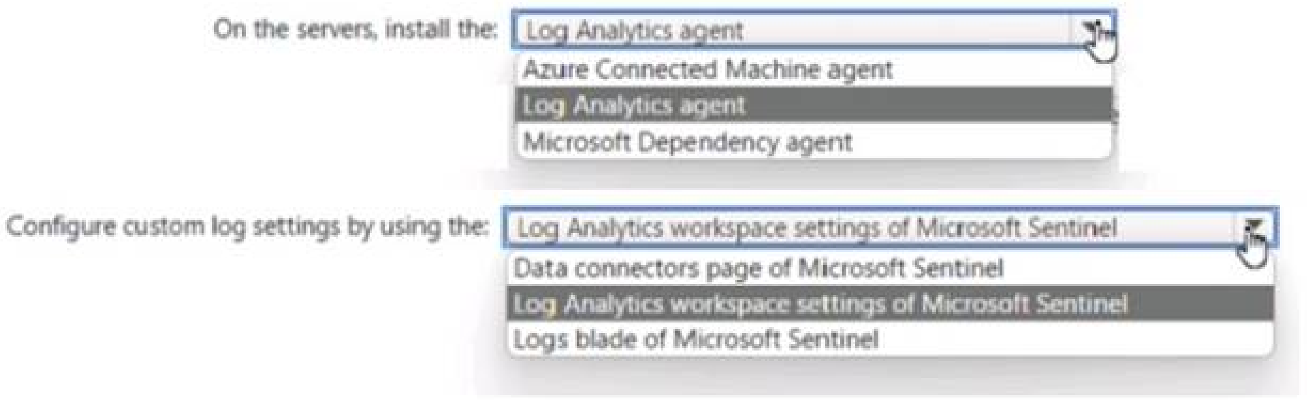
EmailAttachmentInfo

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
[✓ | where Timestamp > ago(1h)]
| where Timestamp < ago(1h)

| where Subject == "Document Attachment" and FileName == "Document.pdf"

| join DeviceFileEvents on SHA256
[✓ | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256]
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

NEW QUESTION 270
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.

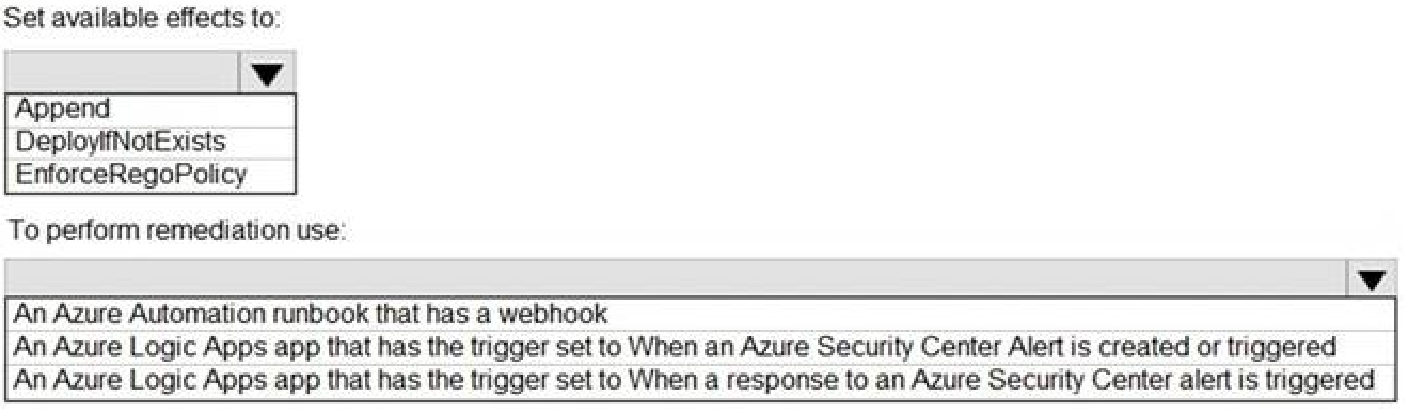
NEW QUESTION 271
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a custom report that will visualise sign-in information over time.
What should you create first?

A. a workbook
B. a hunting query
C. a notebook
D. a playbook

Answer: A

Explanation:
A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview

NEW QUESTION 275
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.



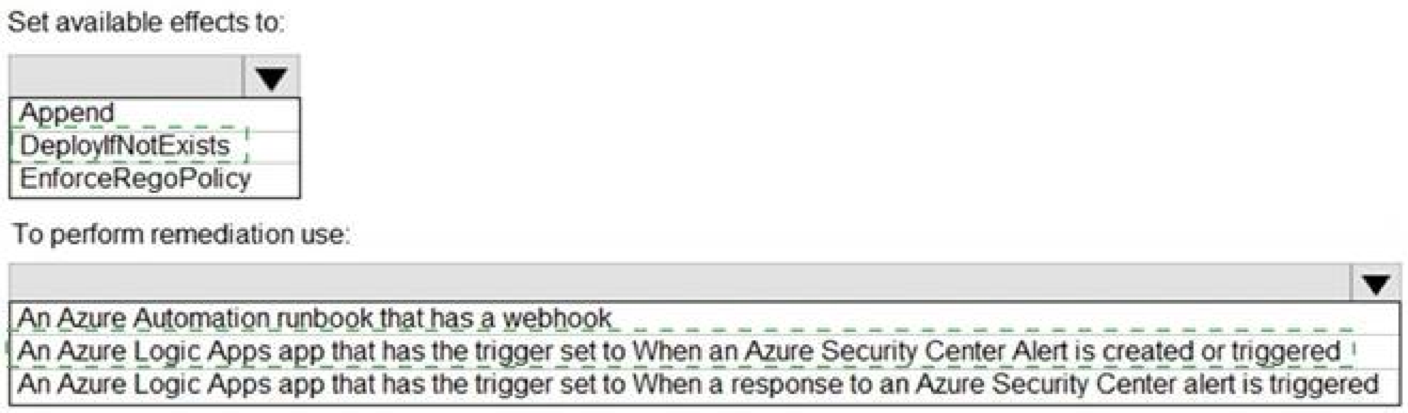
Set available effects to:
- Append
- DeployIfNotExists
- EnforceRegoPolicy

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 277

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace named sws1.

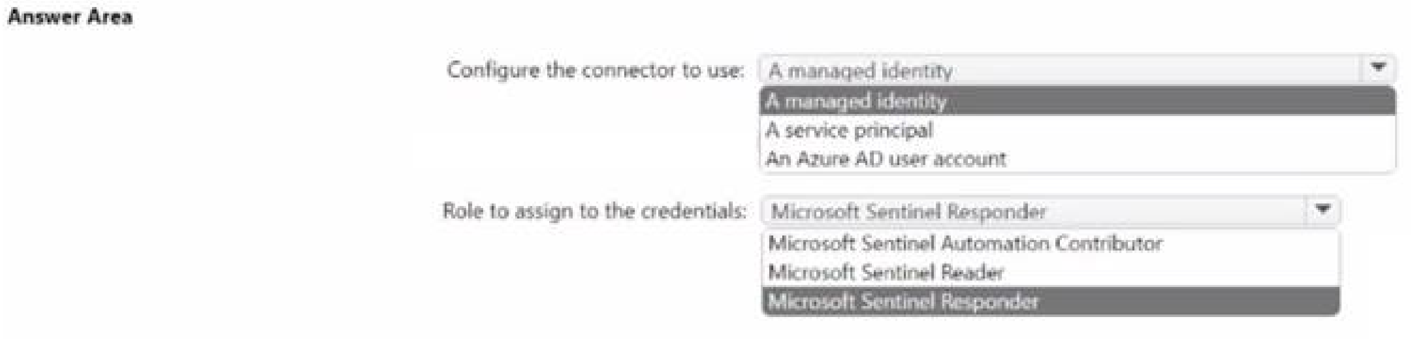
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

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

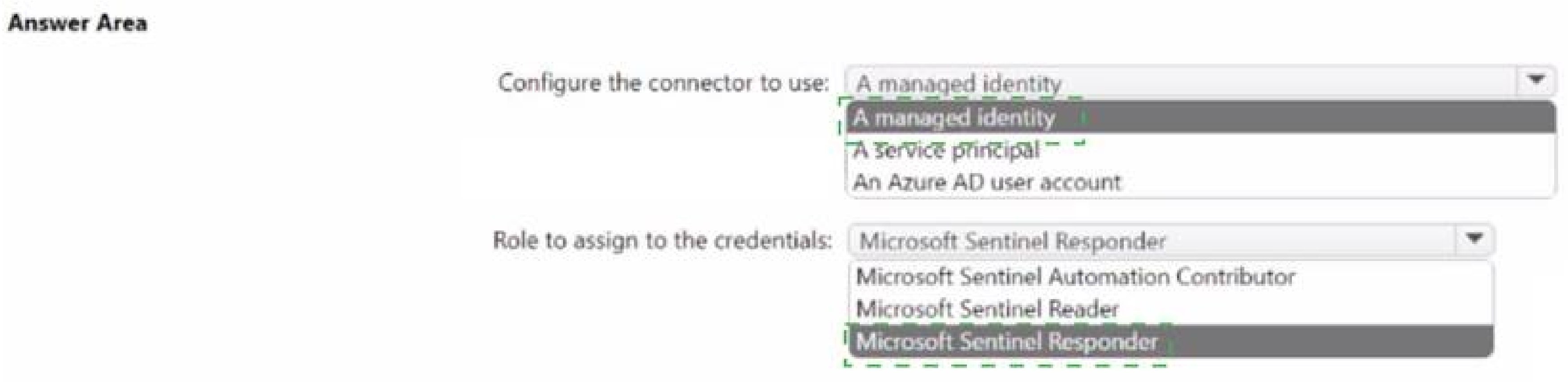
Microsoft Sentinel Automation Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

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

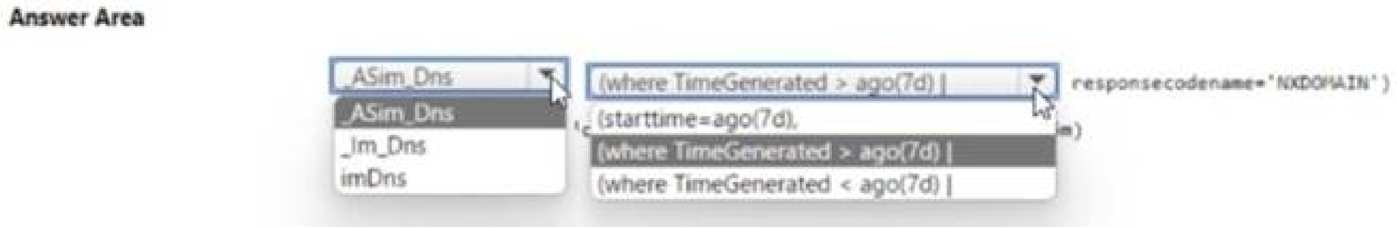
Role to assign to the credentials: Microsoft Sentinel Responder

Microsoft Sentinel Automation Contributor
Microsoft Sentinel Reader
Microsoft Sentinel Responder

NEW QUESTION 282

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 | (where TimeGenerated > ago(7d) | responsecodename='NXDOMAIN')

_ASim_Dns
_Im_Dns
imDns

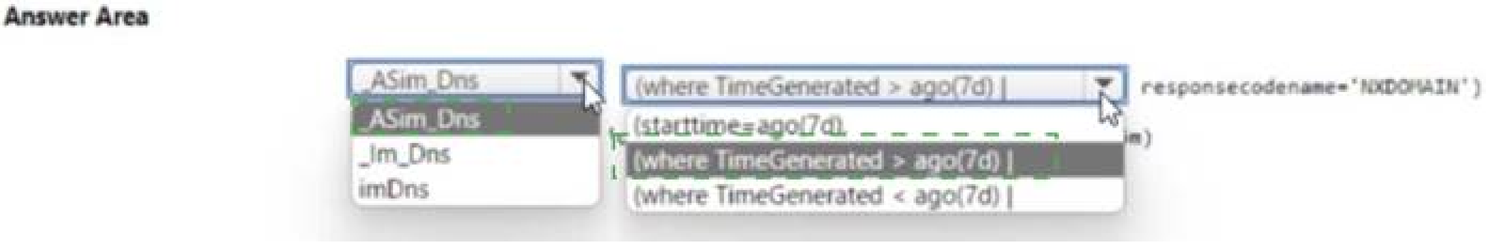
(starttime=ago(7d),
(where TimeGenerated > ago(7d) |
(where TimeGenerated < ago(7d) |

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Answer Area

_ASim_Dns | (where TimeGenerated > ago(7d) | responsecodename='NXDOMAIN')

_ASim_Dns
_Im_Dns
imDns

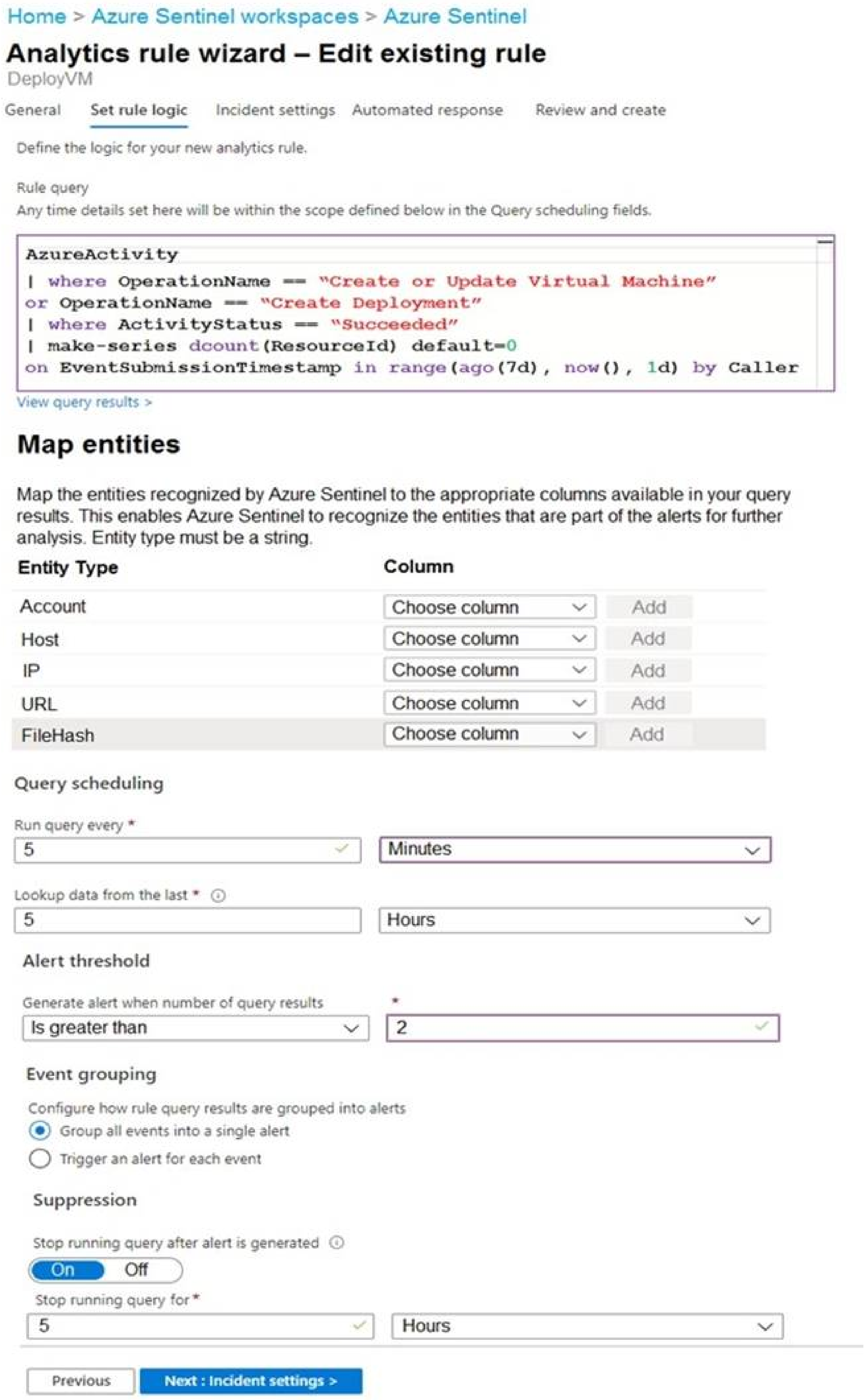
(starttime=ago(7d),
(where TimeGenerated > ago(7d) |
(where TimeGenerated < ago(7d) |

NEW QUESTION 286

HOTSPOT - (Topic 4)

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.



Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

General | Set rule logic | Incident settings | Automated response | Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every * 5 Minutes

Lookup data from the last * 5 Hours

Alert threshold

Generate alert when number of query results * Is greater than 2

Event grouping

Configure how rule query results are grouped into alerts

● Group all events into a single alert

○ Trigger an alert for each event

Suppression

Stop running query after alert is generated: On | Off

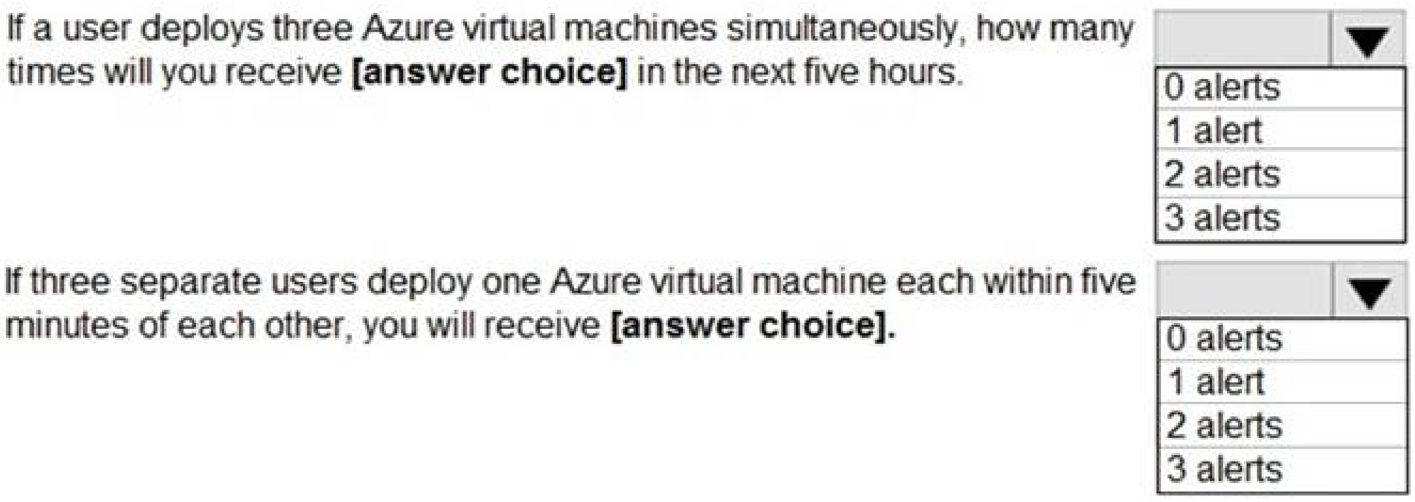
Stop running query for * 5 Hours

Previous | Next : Incident settings >

You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice].**

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated

NEW QUESTION 290
- (Topic 4)
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add a tag to the device group.
B. Add the device users to the admin role.
C. Add a tag to the machines.
D. Create a new device group that has a rank of 1.
E. Create a new admin role.
F. Create a new device group that has a rank of 4.

Answer: ACD

Explanation:
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints- environment/4-manage-access

NEW QUESTION 294
- (Topic 4)
You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription
B. the Contributor for the subscription
C. the Contributor role for RG1
D. the Owner role for RG1

Answer: C

NEW QUESTION 295
- (Topic 4)
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.
B. Configure the Diagnostics settings in Azure AD to stream to an event hub.
C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.
D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview- monitoring

NEW QUESTION 298
......