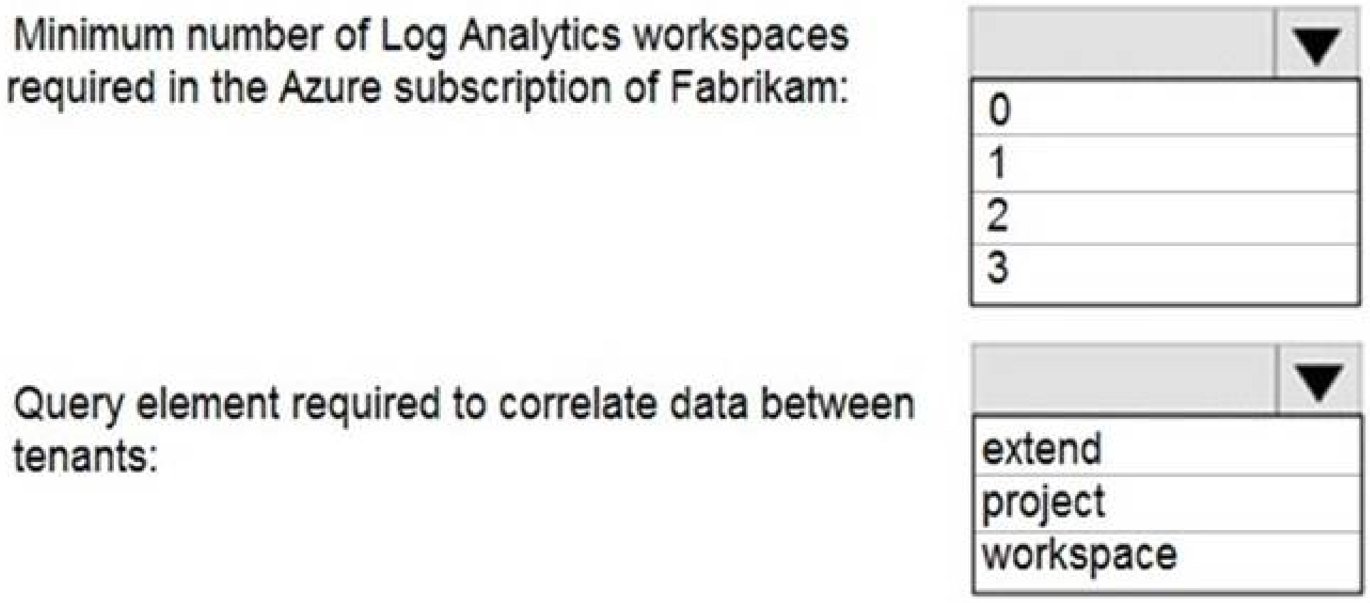
Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

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

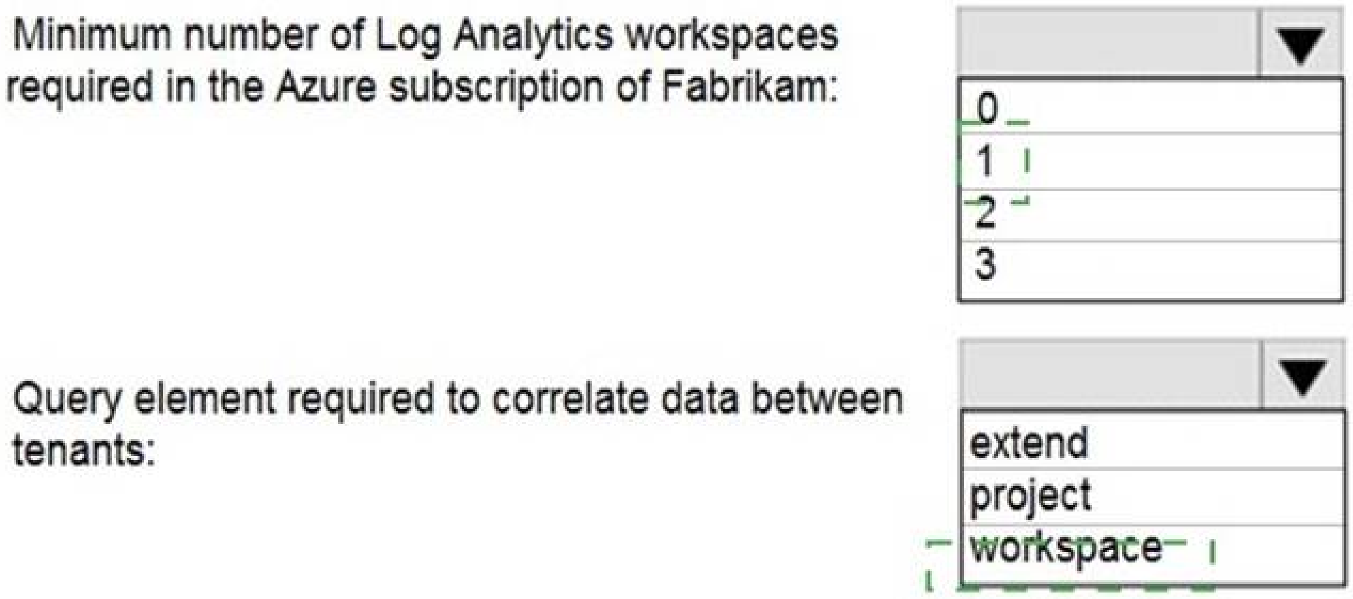
Query element required to correlate data between tenants:

- 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
- (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

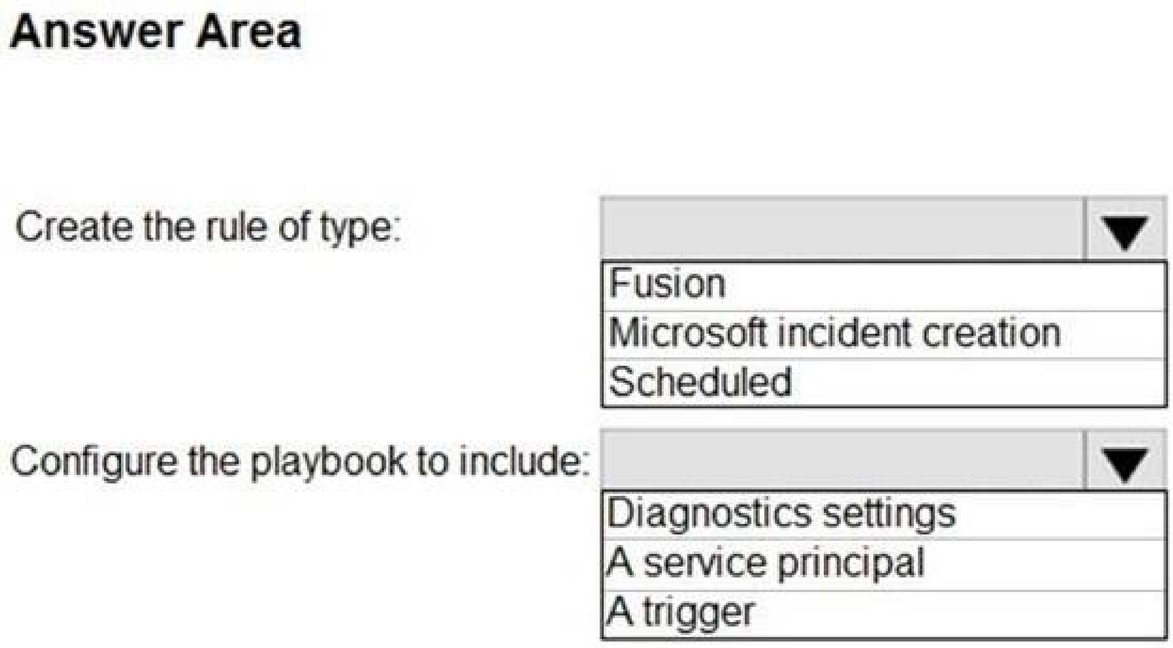
NEW QUESTION 3
- (Topic 2)
You need to restrict cloud apps running on CUENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. the Cloud Discovery settings in Microsoft Defender for Cloud Apps
B. the Onboarding settings from Device management in Settings in Microsoft 365 Defender portal
C. Microsoft Defender for Cloud Apps anomaly detection policies
D. Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal

Answer: AD

NEW QUESTION 4

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



Answer Area

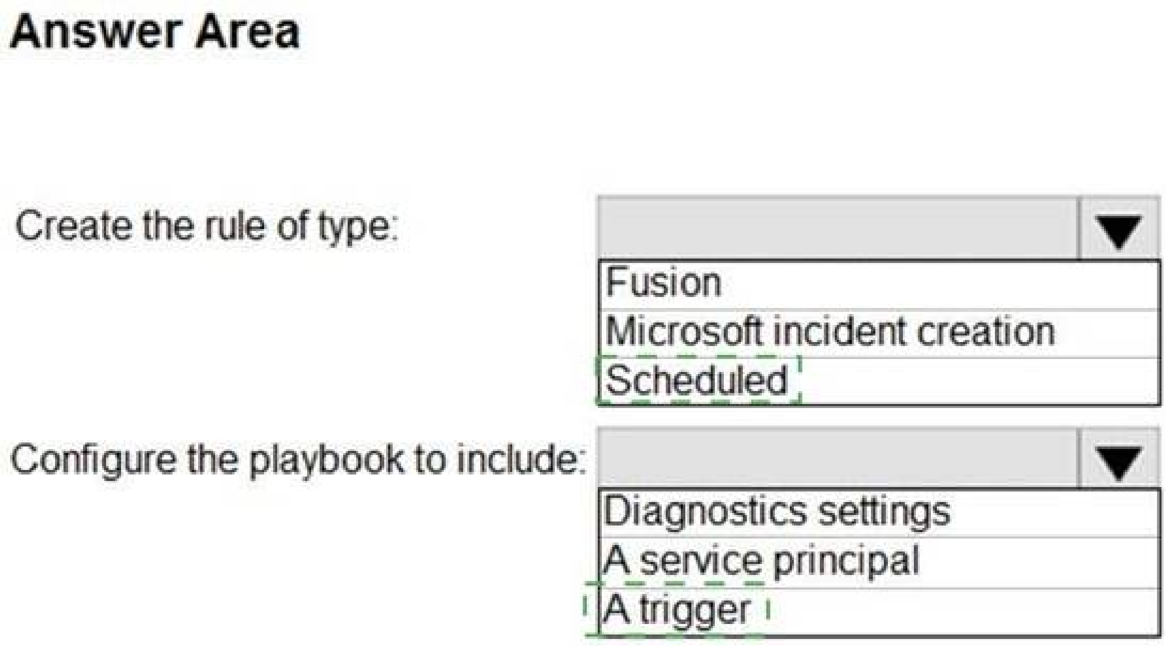
Create the rule of type:
- Fusion
- Microsoft incident creation
- Scheduled

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

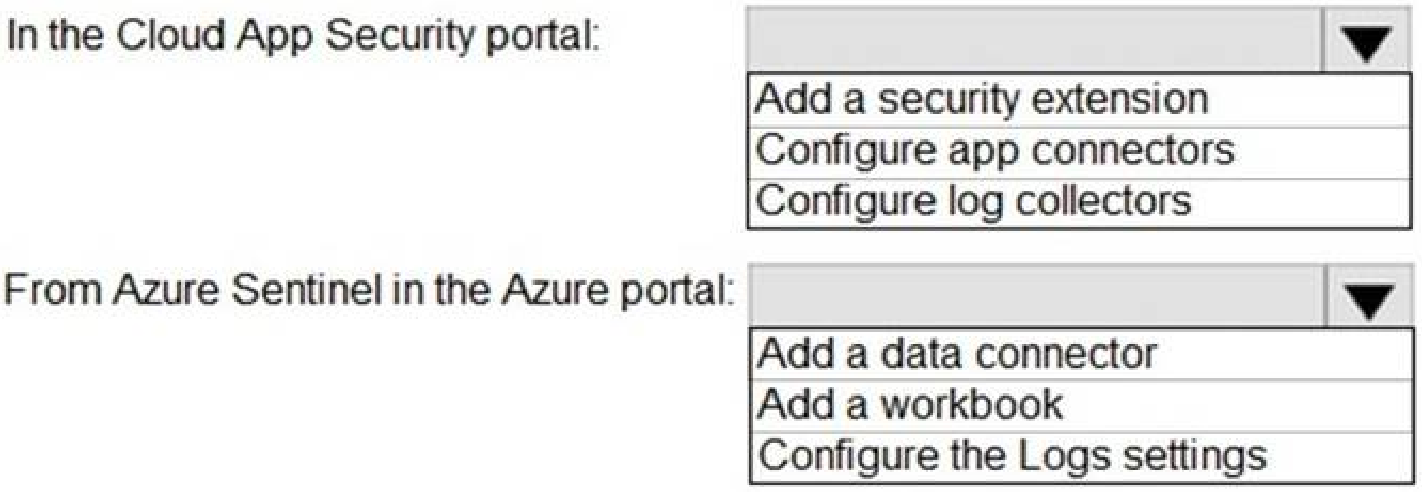
Configure the playbook to include:
- Diagnostics settings
- A service principal
- A trigger

NEW QUESTION 5
- (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 6
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

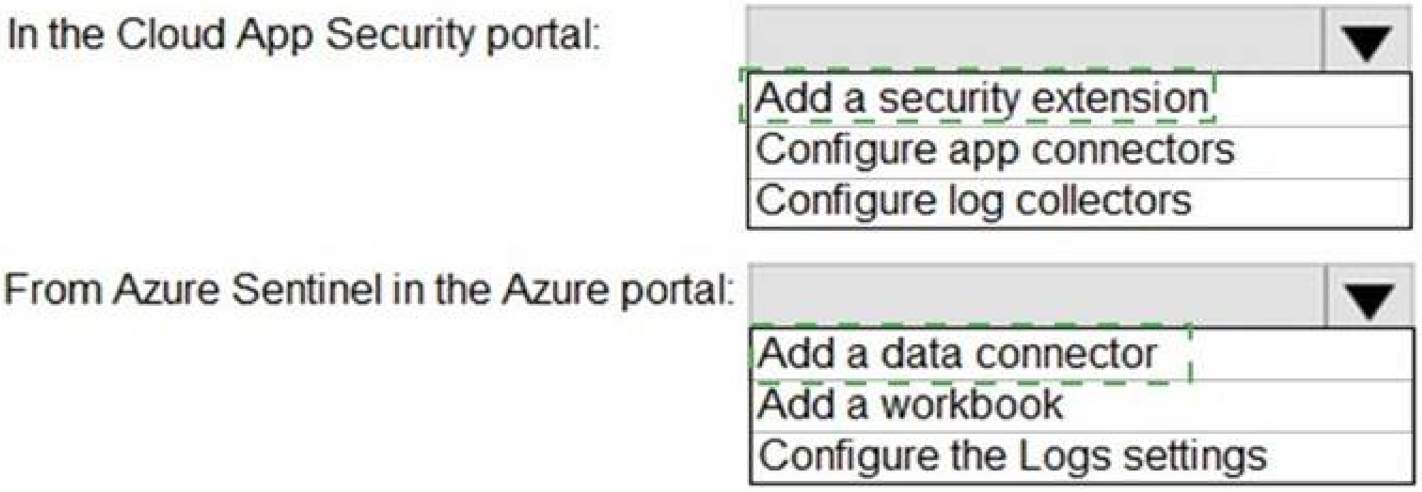
From Azure Sentinel in the Azure portal:

- Add a data connector
- Add a workbook
- Configure the Logs settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:



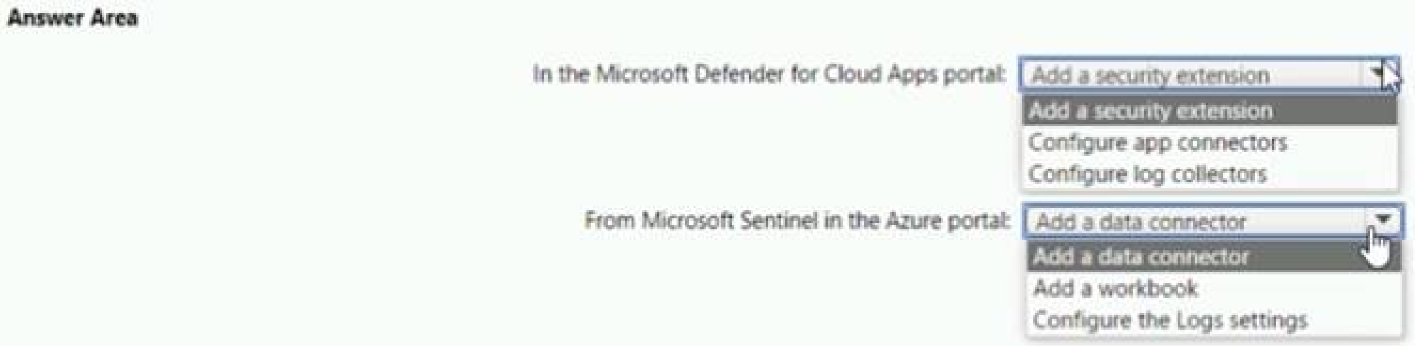
In the Cloud App Security portal:

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



Answer Area

In the Microsoft Defender for Cloud Apps portal: Add a security extension

- Add a security extension
- Configure app connectors
- Configure log collectors

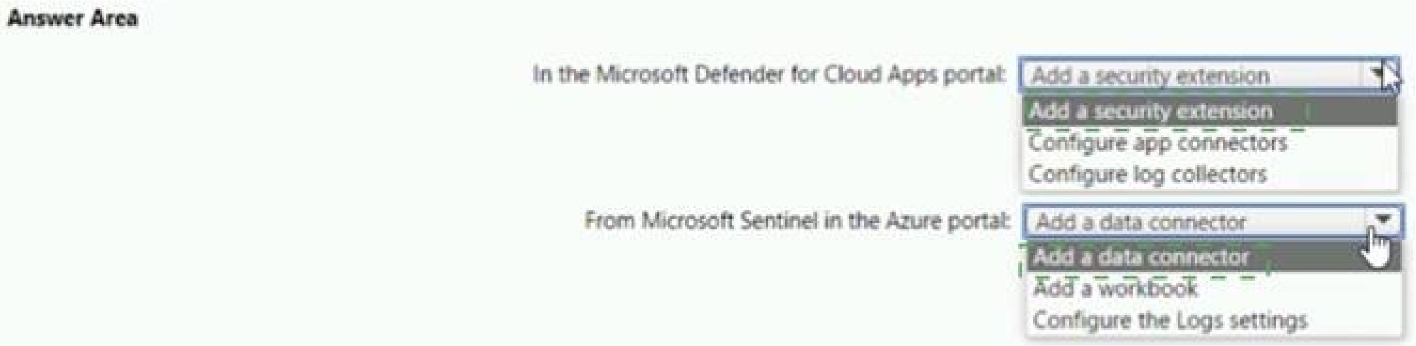
From Microsoft Sentinel in the Azure portal: Add a data connector

- Add a data connector
- Add a workbook
- Configure the Logs settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

In the Microsoft Defender for Cloud Apps portal: Add a security extension

- Add a security extension
- Configure app connectors
- Configure log collectors

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

- Add a data connector
- Add a workbook
- Configure the Logs settings

NEW QUESTION 8
- (Topic 2)
You need to 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

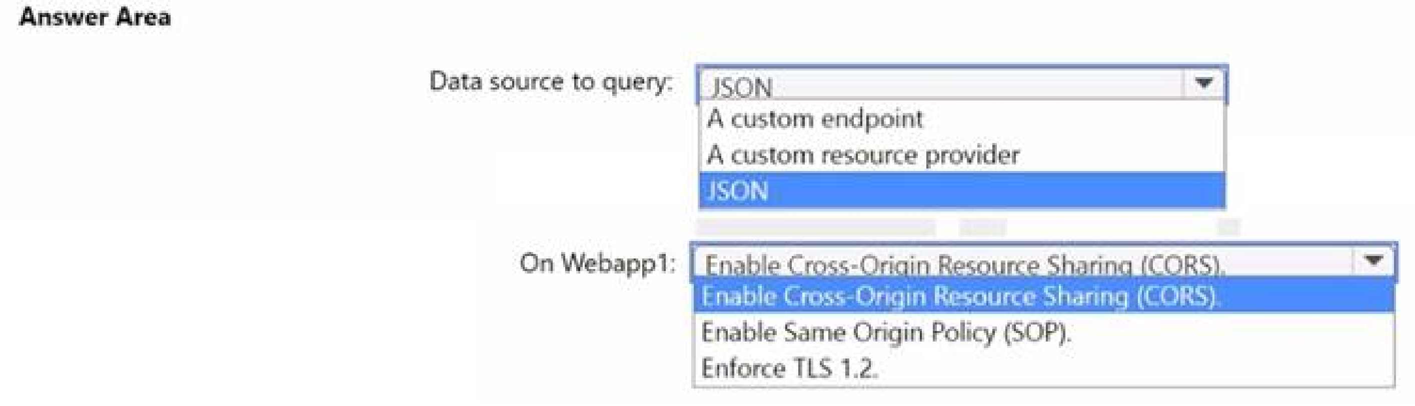
NEW QUESTION 9
- (Topic 2)
You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

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



Answer Area

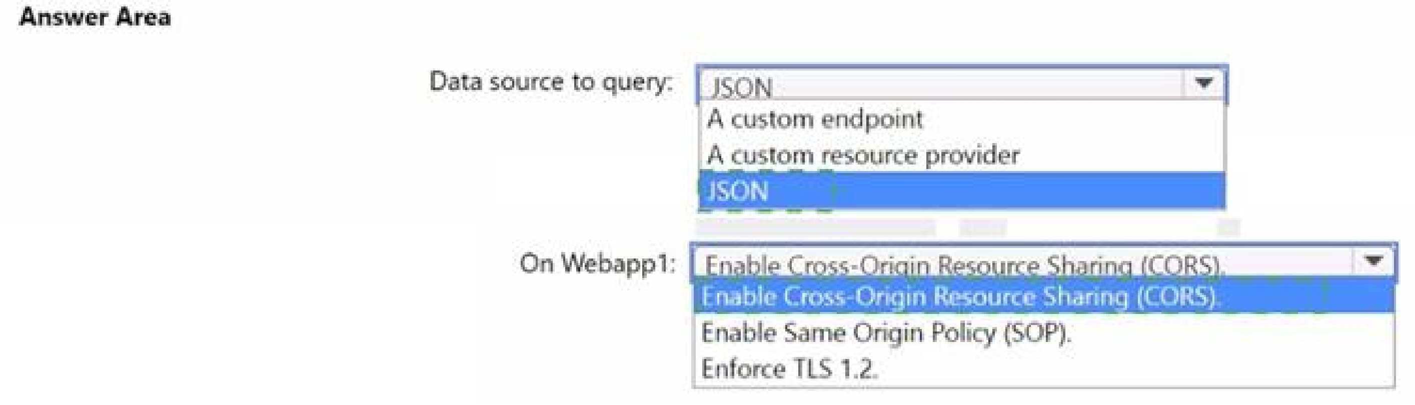
Data source to query: JSON
A custom endpoint
A custom resource provider
JSON

On Webapp1: Enable Cross-Origin Resource Sharing (CORS).
Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

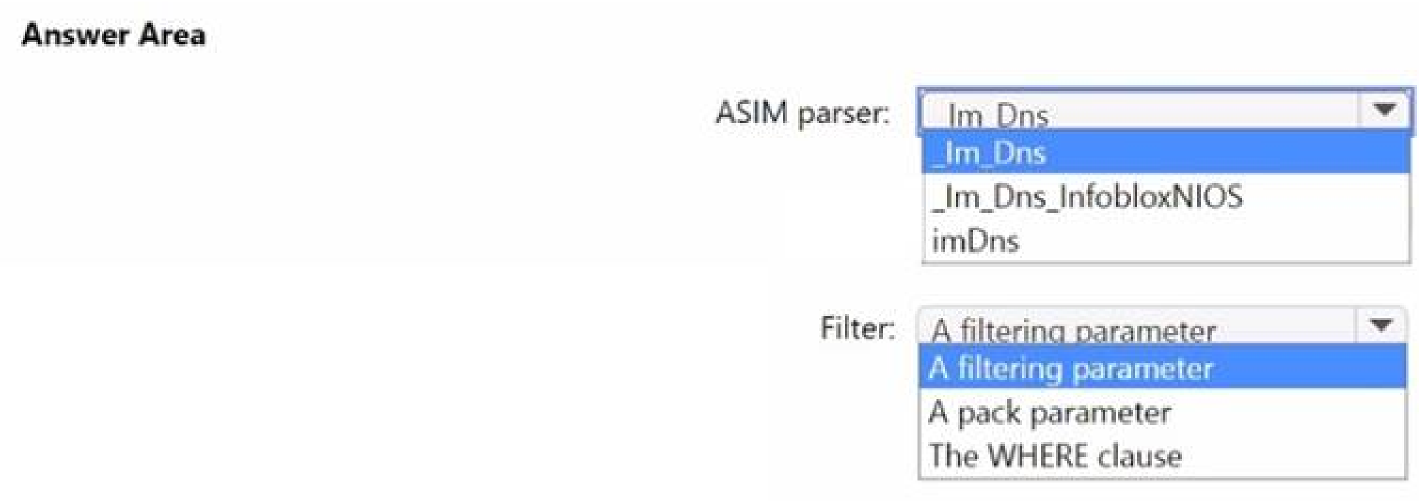
On Webapp1: Enable Cross-Origin Resource Sharing (CORS).
Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

NEW QUESTION 10
- (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 14
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

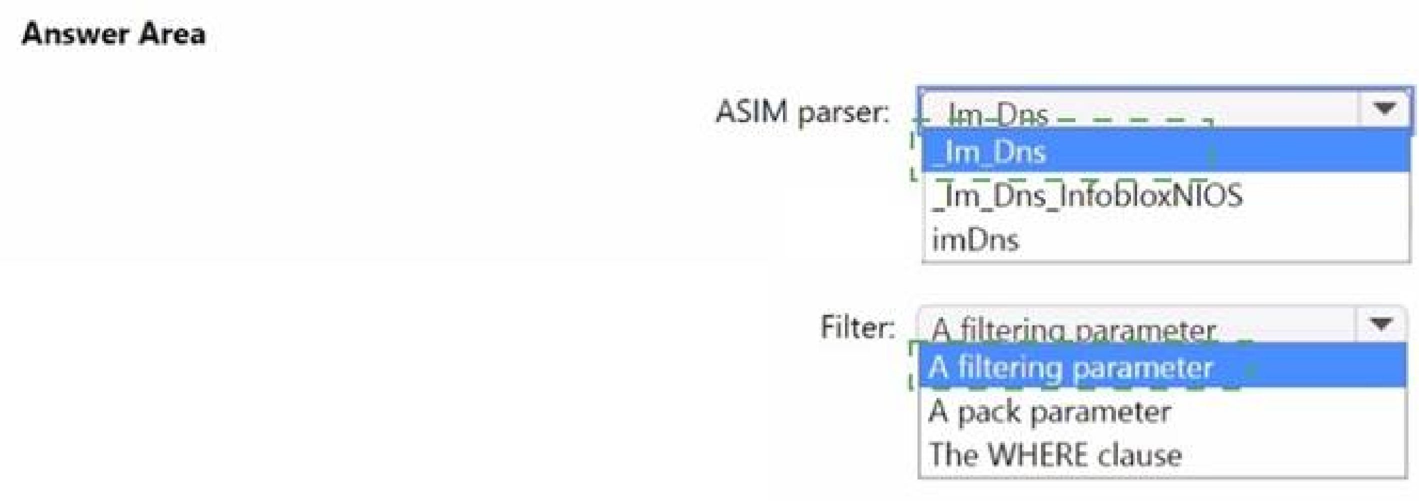
ASIM parser: _Im_Dns
- _Im_Dns
- _Im_Dns_InfobloxNIOS
- imDns

Filter: A filtering parameter
- A filtering parameter
- A pack parameter
- The WHERE clause

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

ASIM parser: _Im_Dns
- _Im_Dns
- _Im_Dns_InfobloxNIOS
- imDns

Filter: A filtering parameter
- A filtering parameter
- A pack parameter
- The WHERE clause

NEW QUESTION 15
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

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

Answer: D

NEW QUESTION 17
- (Topic 3)
You need to ensure that the configuration of HuntingQuery1 meets the Microsoft Sentinel requirements.
What should you do?

A. Add HuntingQuery1 to a livestream.
B. Create a watch list.
C. Create an Azure Automation rule.
D. Add HuntingQuery1 to favorites.

Answer: D

NEW QUESTION 19
- (Topic 4)
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

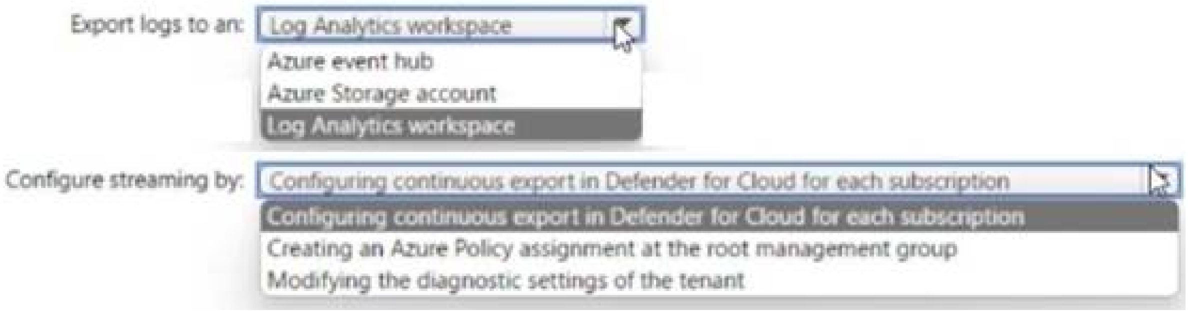
A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader

Answer: A

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

NEW QUESTION 21
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

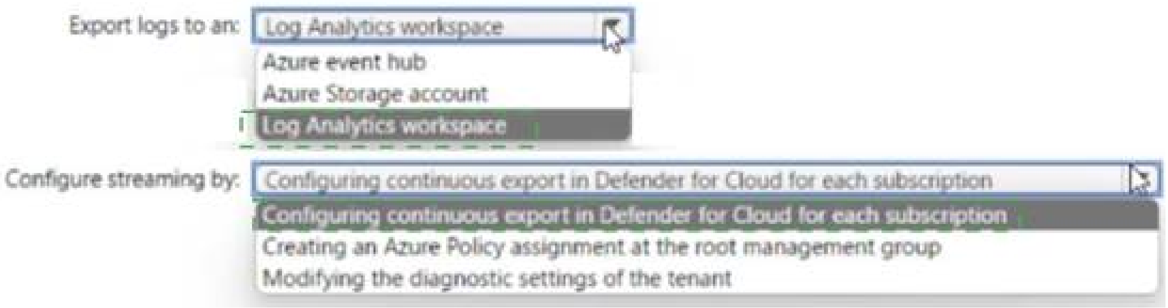
Configure streaming by: Configuring continuous export in Defender for Cloud for each subscription

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 22
- (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 23
- (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 26
- (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

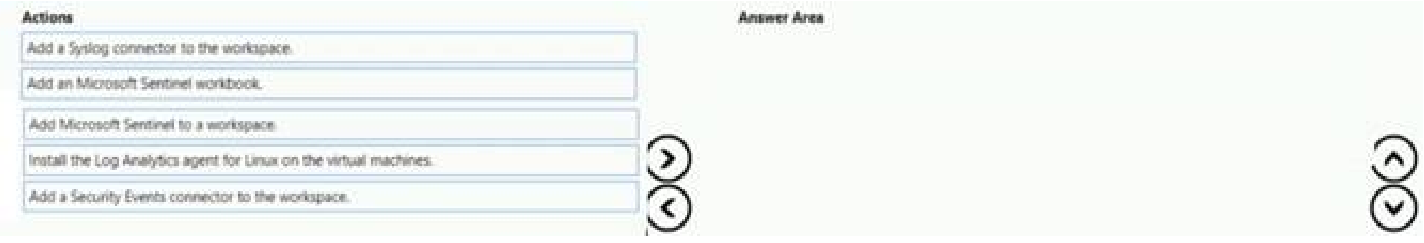
Answer: B

NEW QUESTION 27
- (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 32
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.



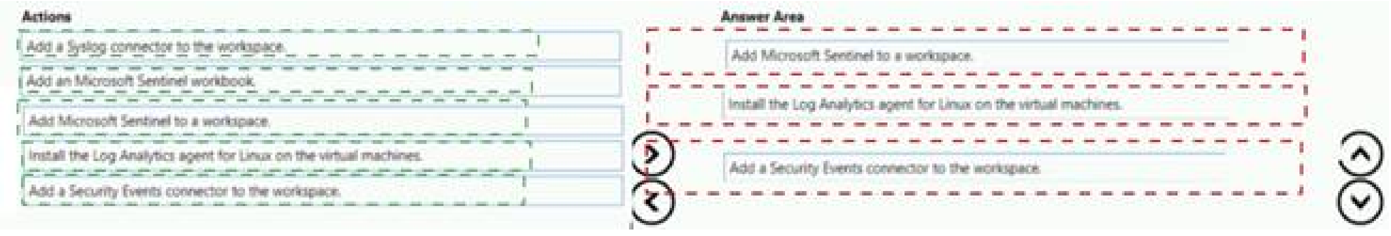
Actions
Add a Syslog connector to the workspace.
Add an Microsoft Sentinel workbook.
Add Microsoft Sentinel to a workspace.
Install the Log Analytics agent for Linux on the virtual machines.
Add a Security Events connector to the workspace.

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 37
- (Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
? Microsoft Excel macros that download scripts from untrusted websites
? Users that open executable attachments in Microsoft Outlook
? Outlook rules and forms exploits
What should you use?

A. Microsoft Defender Antivirus
B. attack surface reduction rules in Microsoft Defender for Endpoint
C. Windows Defender Firewall
D. adaptive application control in Azure Defender

Answer: B

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

NEW QUESTION 38
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a livestream from a query. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 39
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.
B. Create a JSON file based on the DNS template.
C. Create an XML file based on the DNS template.
D. Create a YAML file based on the DNS template.

Answer: A

NEW QUESTION 43
- (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 44
- (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

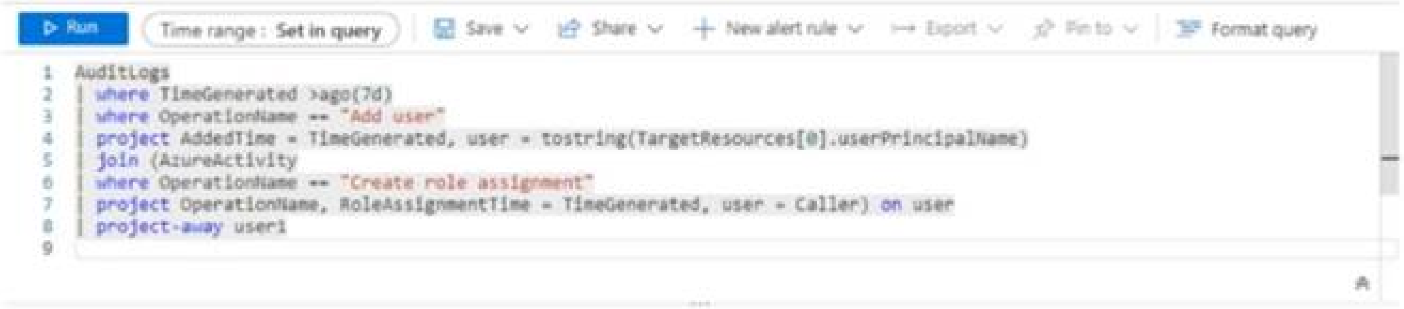
Answer: C

NEW QUESTION 45
- (Topic 4)
You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Signin Logs.
You need to ensure that failed interactive sign-ins are detected. The solution must minimize administrative effort.
What should you use?

A. a scheduled alert query
B. a UEBA activity template
C. the Activity Log data connector
D. a hunting query

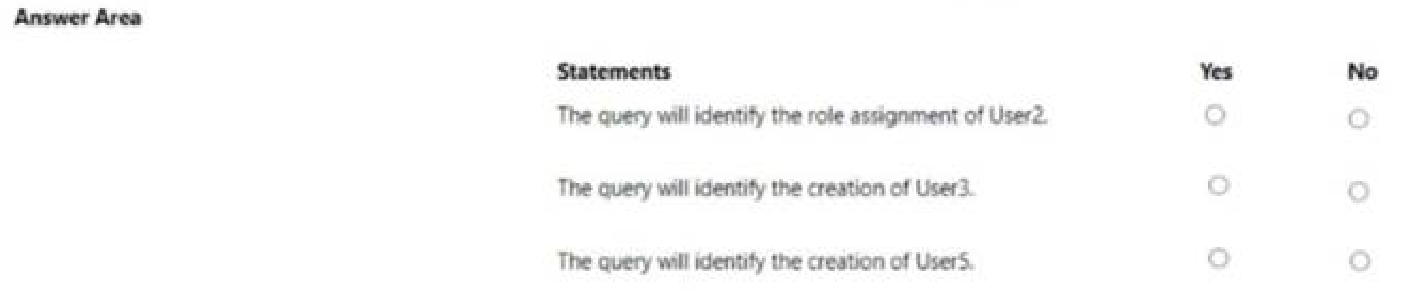
Answer: B

NEW QUESTION 48
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains two users named User! and User2. You have the hunting query shown in the following exhibit.



```
AuditLogs
| where TimeGenerated >ago(7d)
| where OperationName == "Add user"
| project AddedTime = TimeGenerated, user = tostring(TargetResources[0].userPrincipalName)
| join (AzureActivity
| where OperationName == "Create role assignment"
| project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
| project-away user1
```

The users perform the following anions:
• User1 assigns User2 the Global administrator role.
• User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
• User2 creates a new user named User4 and assigns the user the Security reader role.
• User2 creates a new user named User5 and assigns the user the Security operator role. For each of the following statements, select Yes if the statement is true. Otherwise, select
No.
NOTE: Each correct selection is worth one point.



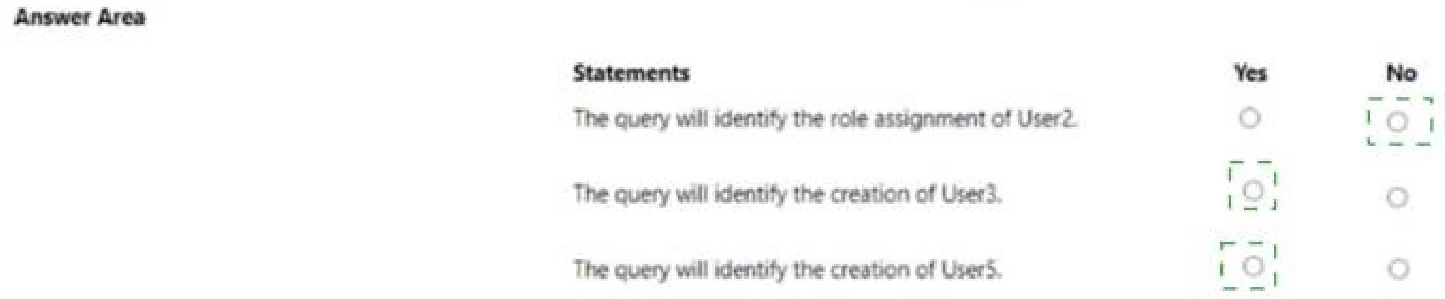
Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	[✓ ○]
The query will identify the creation of User3.	[✓ ○]	○
The query will identify the creation of User5.	[✓ ○]	○

NEW QUESTION 50
- (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 52
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

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

E. From Defender for Cloud, configure the AWS connector.

Answer: BC

NEW QUESTION 54
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.
You need to simulate an attack on the virtual machine that will generate an alert. What should you do first?

A. Run the Log Analytics Troubleshooting Tool.
B. Copy a executable and rename the file as ASC_AlerTest_662jf10N,exe
C. Modify the settings of the Microsoft Monitoring Agent.
D. Run the MMASetup executable and specify the -foo argument

Answer: B

NEW QUESTION 56
- (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.

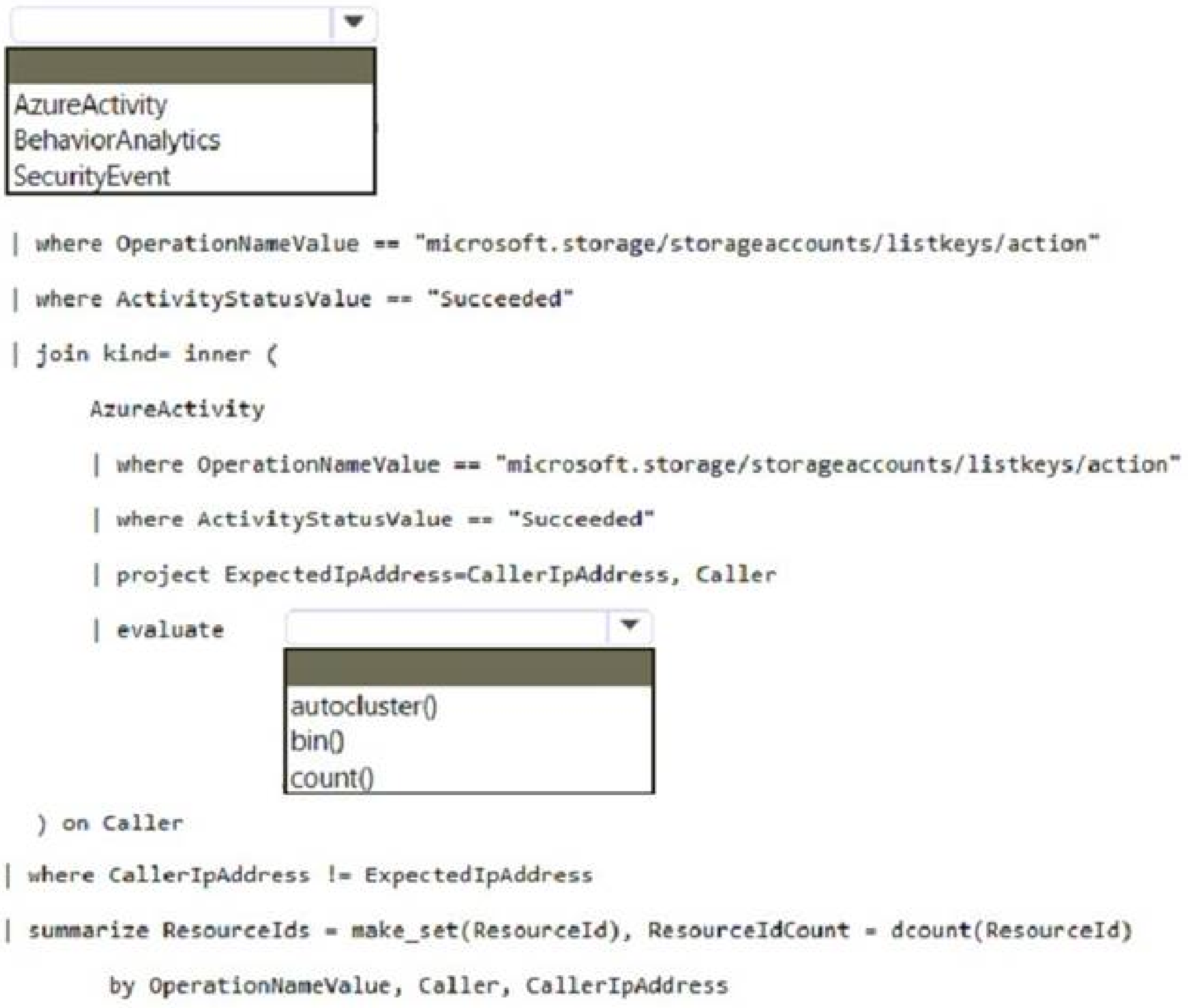
Answer: A

NEW QUESTION 60
- (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 62
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 63
- (Topic 4)
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

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

Answer: C

Explanation:

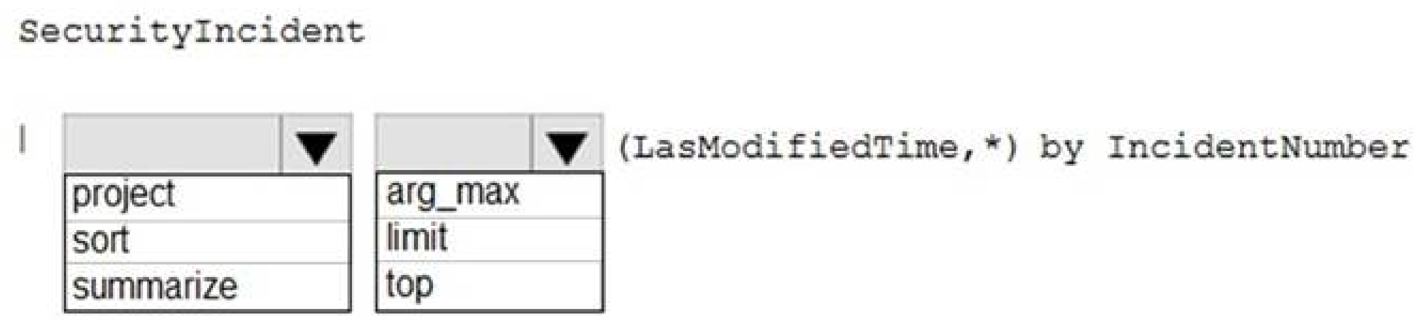
Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within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

NEW QUESTION 64
- (Topic 4)
You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

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

Answer: B

NEW QUESTION 67
HOTSPOT - (Topic 4)
You need to create a query for a workbook. The query must meet the following requirements:
? List all incidents by incident number.
? Only include the most recent log for each incident.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



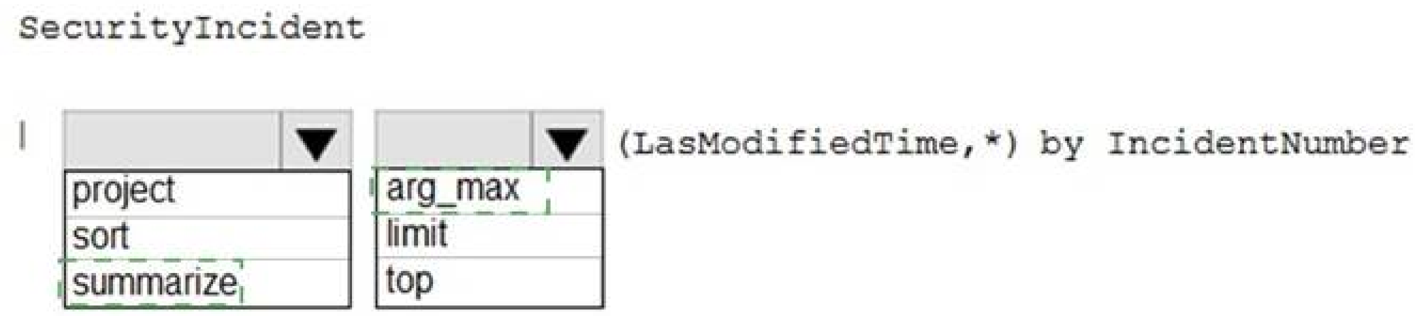
```
SecurityIncident

| [▼] [▼] (LasModifiedTime,*) by IncidentNumber
```

A. Mastered
B. Not Mastered

Answer: A

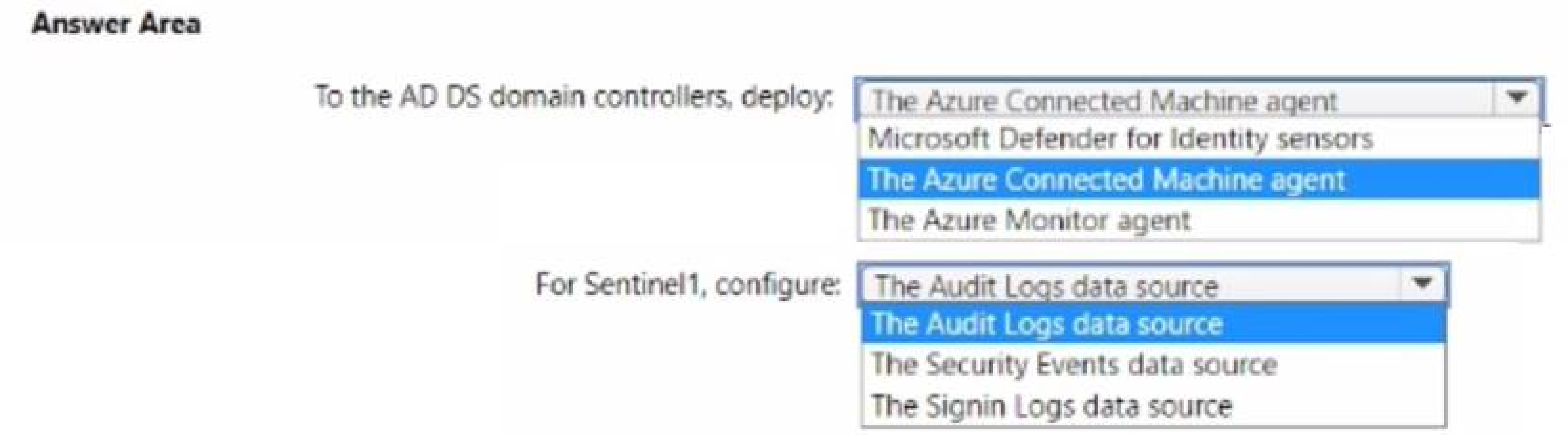
Explanation:



```
SecurityIncident

| summarize arg_max(LasModifiedTime,*) by IncidentNumber
```

NEW QUESTION 68
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

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

Microsoft Defender for Identity sensors
The Azure Connected Machine agent
The Azure Monitor agent

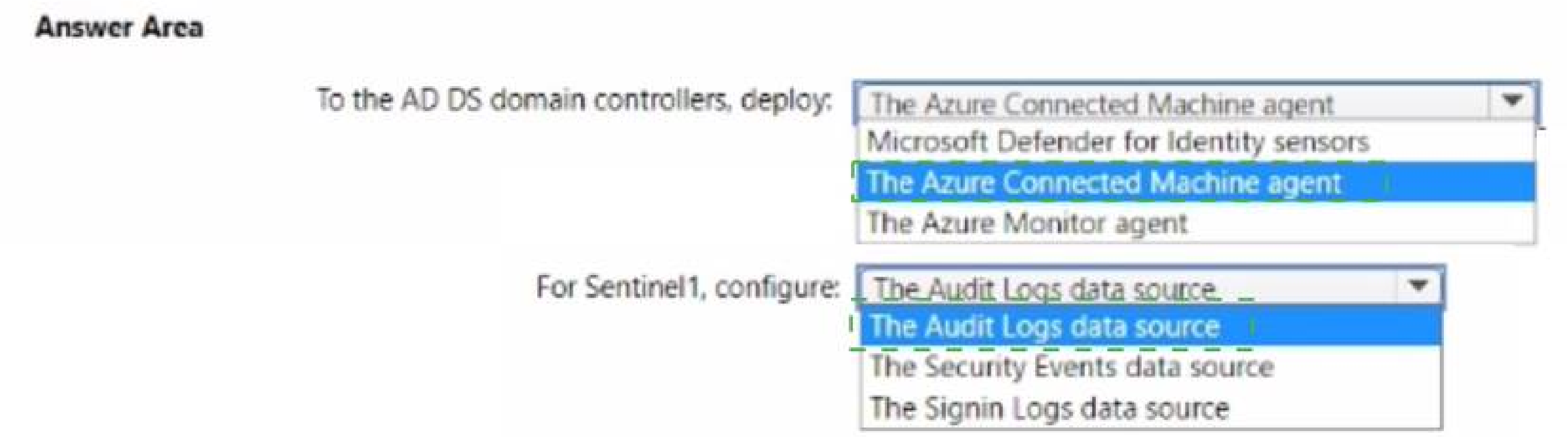
For Sentinel1, configure: The Audit Logs data source ▼

The Audit Logs data source
The Security Events data source
The Signin Logs data source

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

For Sentinel1, configure: The Audit Logs data source

- The Audit Logs data source
- The Security Events data source
- The Signin Logs data source

NEW QUESTION 70
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

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

Answer: A

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

NEW QUESTION 74
- (Topic 4)
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.
To which service should you export the alerts?

A. Azure Cosmos DB
B. Azure Event Grid
C. Azure Event Hubs
D. Azure Data Lake

Answer: C

Explanation:
Reference: https://docsmicrosoftcom/en-us/azure/security-center/continuous-export?tabs=azure-portal

NEW QUESTION 77
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 78
- (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

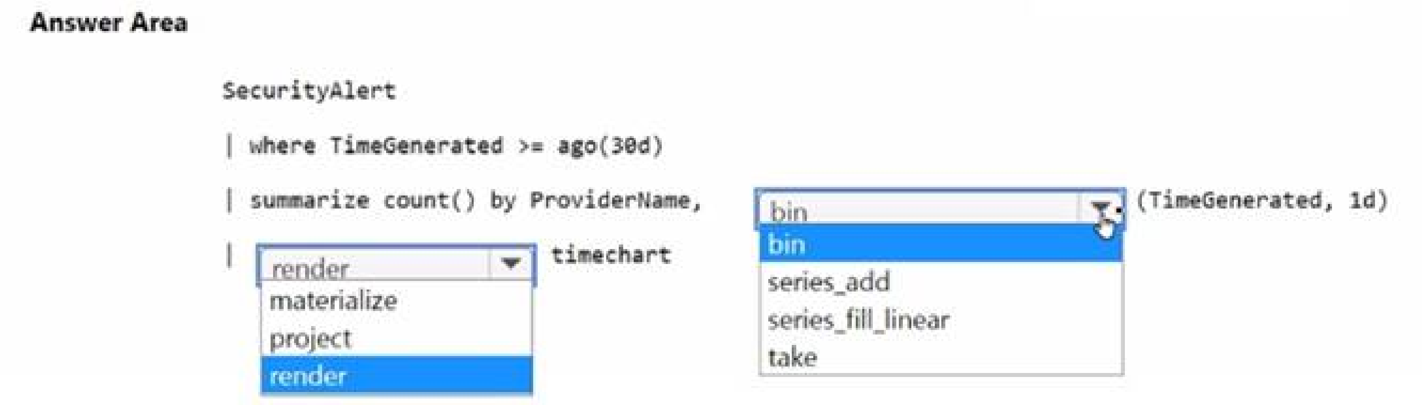
Sentinel deployment to generate alerts based on queries to LogsWest. What should you do first?

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 83
HOTSPOT - (Topic 4)
You have an Microsoft Sentinel workspace named SW1.
You plan to create a custom workbook that will include a time chart.
You need to create a query that will identify the number of security alerts per day for each provider.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



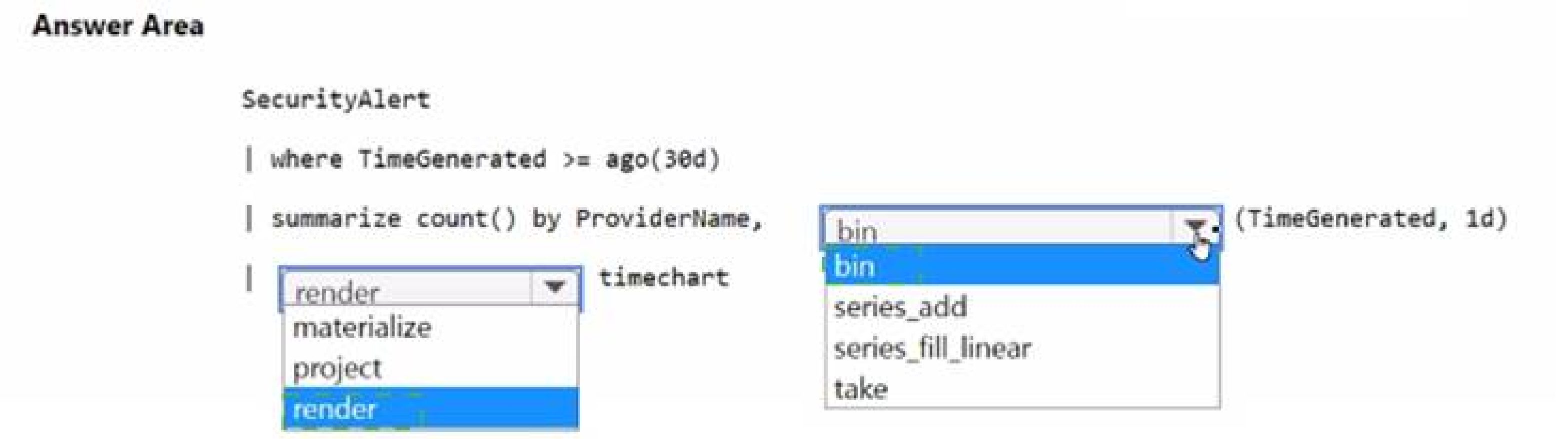
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

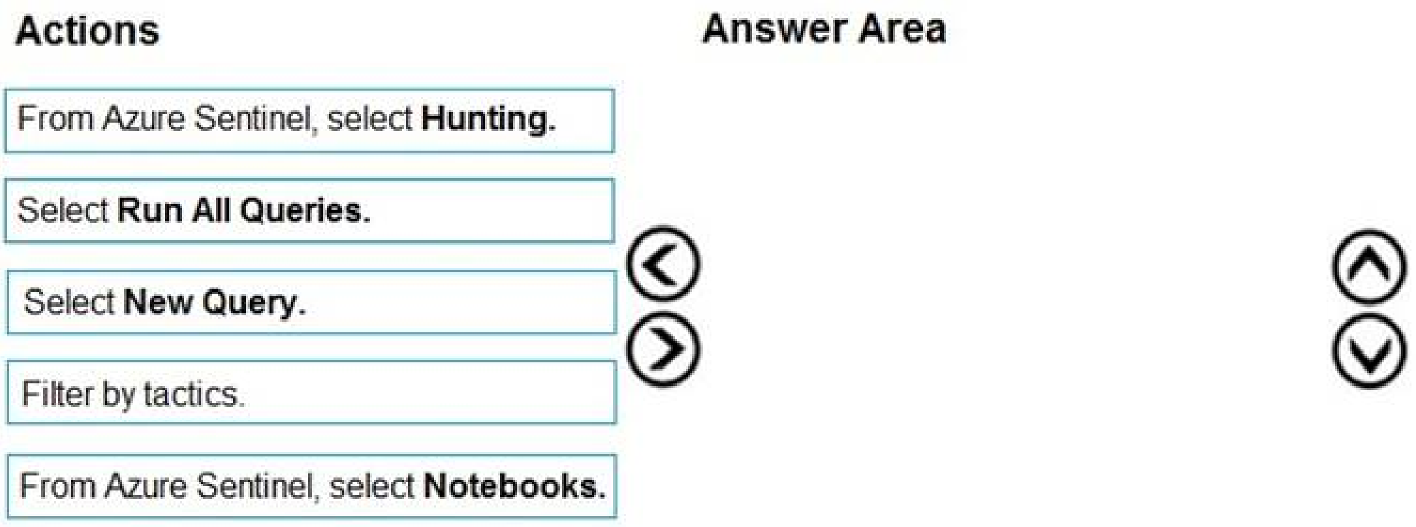
Explanation:



Answer Area

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

NEW QUESTION 85
DRAG DROP - (Topic 4)
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
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

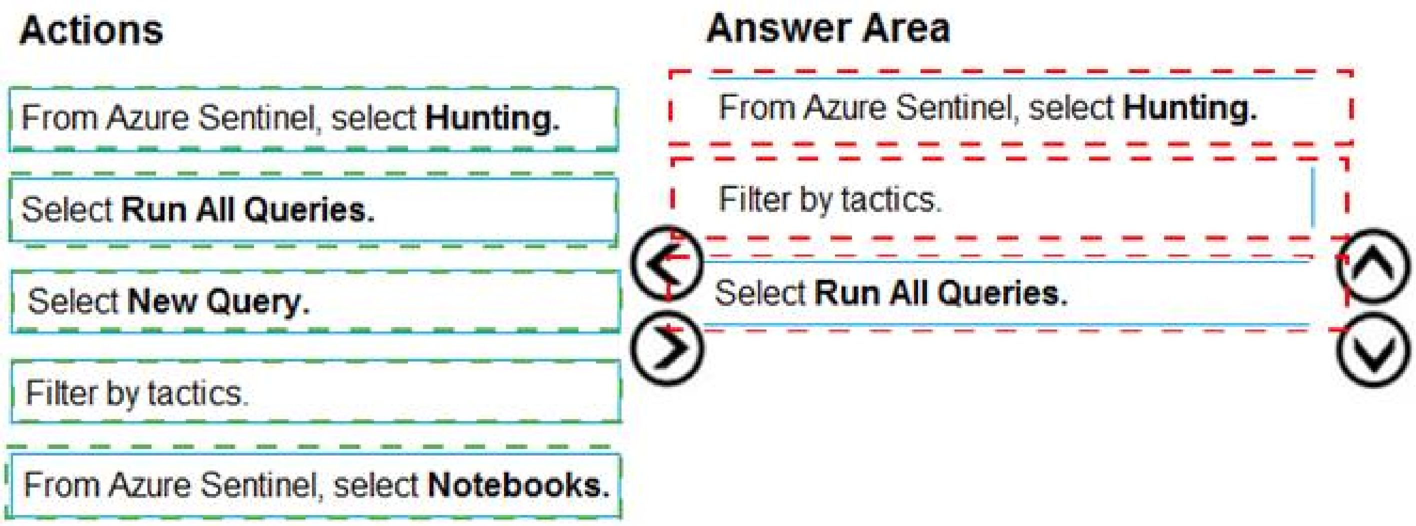
- From Azure Sentinel, select **Hunting.**
- Select **Run All Queries.**
- Select **New Query.**
- Filter by tactics.
- From Azure Sentinel, select **Notebooks.**

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

- From Azure Sentinel, select **Hunting**.
- Select **Run All Queries**.
- Select **New Query**.
- Filter by tactics.
- From Azure Sentinel, select **Notebooks**.

Answer Area

- From Azure Sentinel, select **Hunting**.
- Filter by tactics.
- Select **Run All Queries**.

NEW QUESTION 89
- (Topic 4)
You have a Microsoft Sentinel workspace.
You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.
You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.
• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort What should do?

A. Create an automation rule.
B. Create a watchlist.
C. Modify the analytics rule.
D. Add an activity template to the entity behavior.

Answer: A

Explanation:
An automation rule will allow you to specify which alerts should be suppressed, ensuring that failed sign-in alerts are generated for other accounts while minimizing administrative effort. To create an automation rule, navigate to the Automation Rules page in the Microsoft Sentinel workspace and configure the rule parameters to suppress the false positive alerts.

NEW QUESTION 93
- (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 98
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring 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 each account as a Sensitive account. Does this meet the goal?

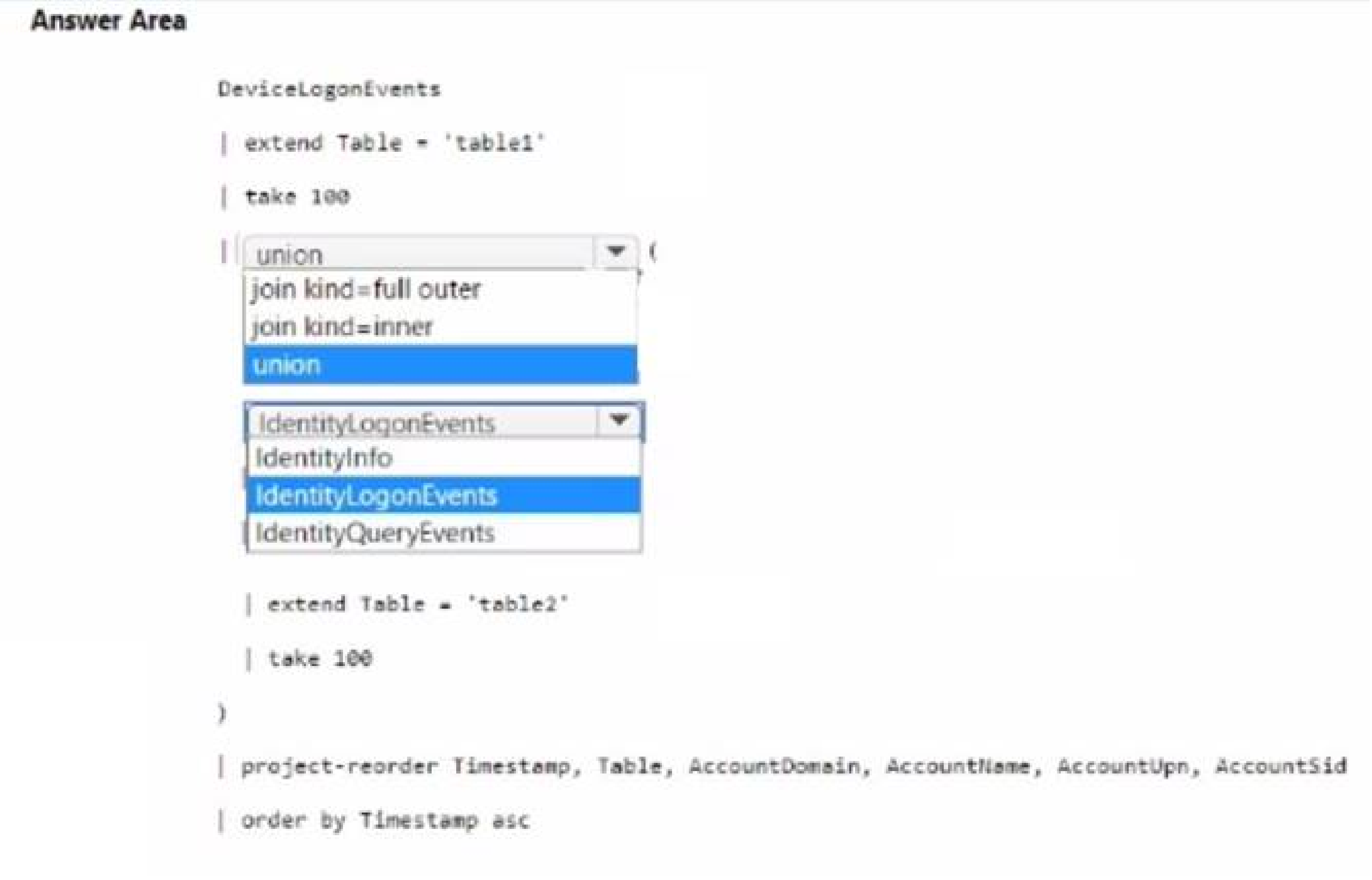
A. Yes
B. No

Answer: B

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

NEW QUESTION 99
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.



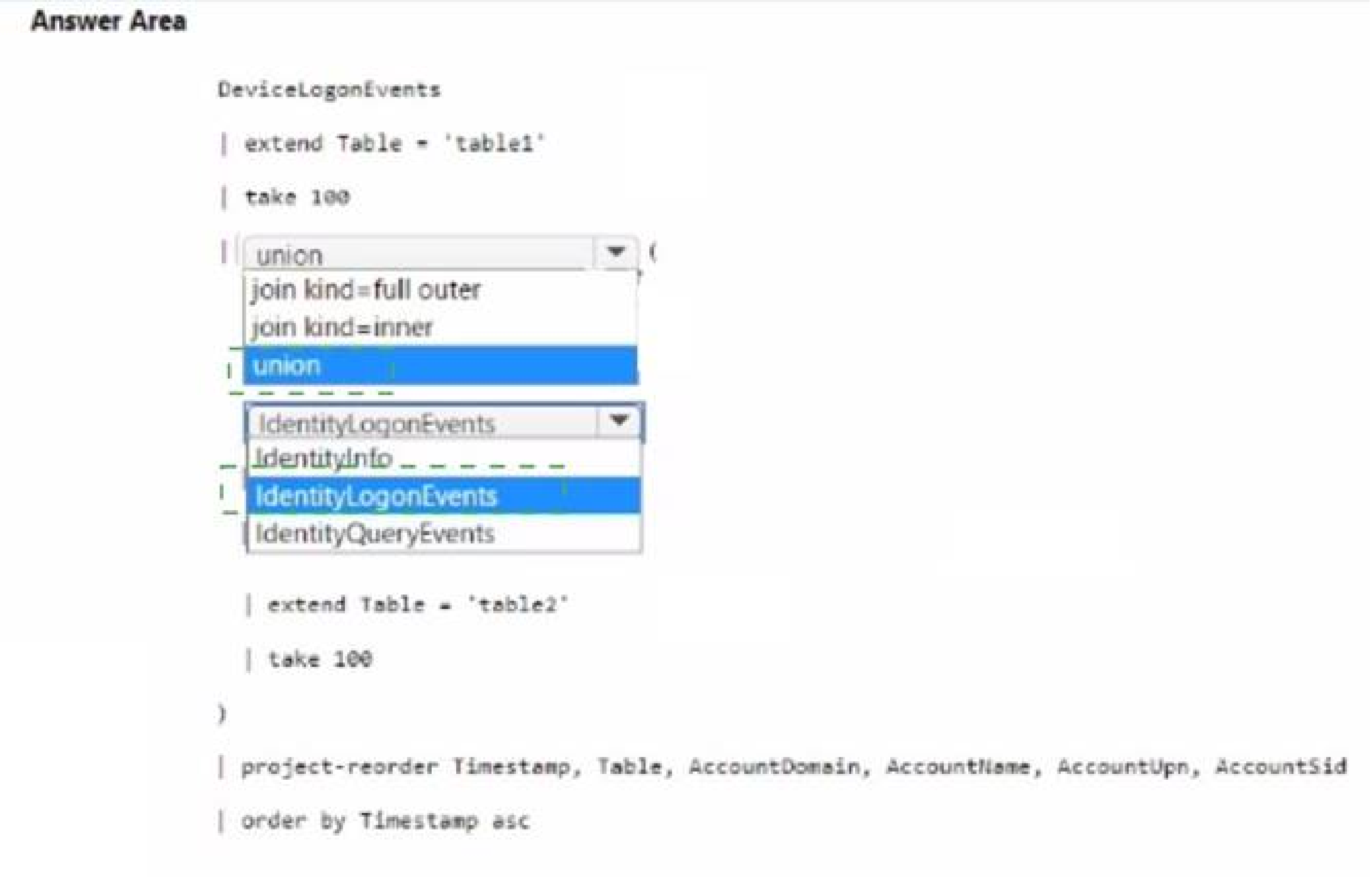
Answer Area

```
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 103

- (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 105

- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You 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

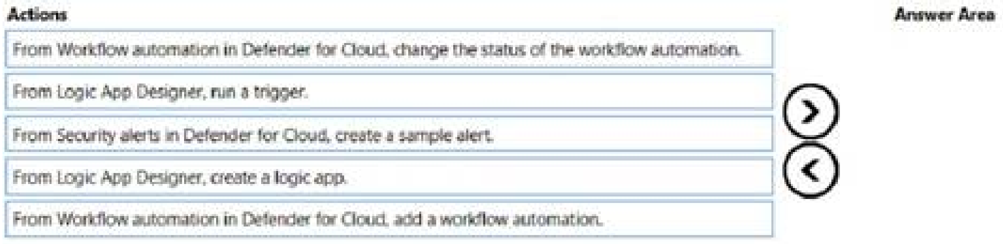
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

NEW QUESTION 109
- (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 111
DRAG DROP - (Topic 4)
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.
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 Workflow automation in Defender for Cloud, change the status of the workflow automation.

From Logic App Designer, run a trigger.

From Security alerts in Defender for Cloud, create a sample alert.

From Logic App Designer, create a logic app.

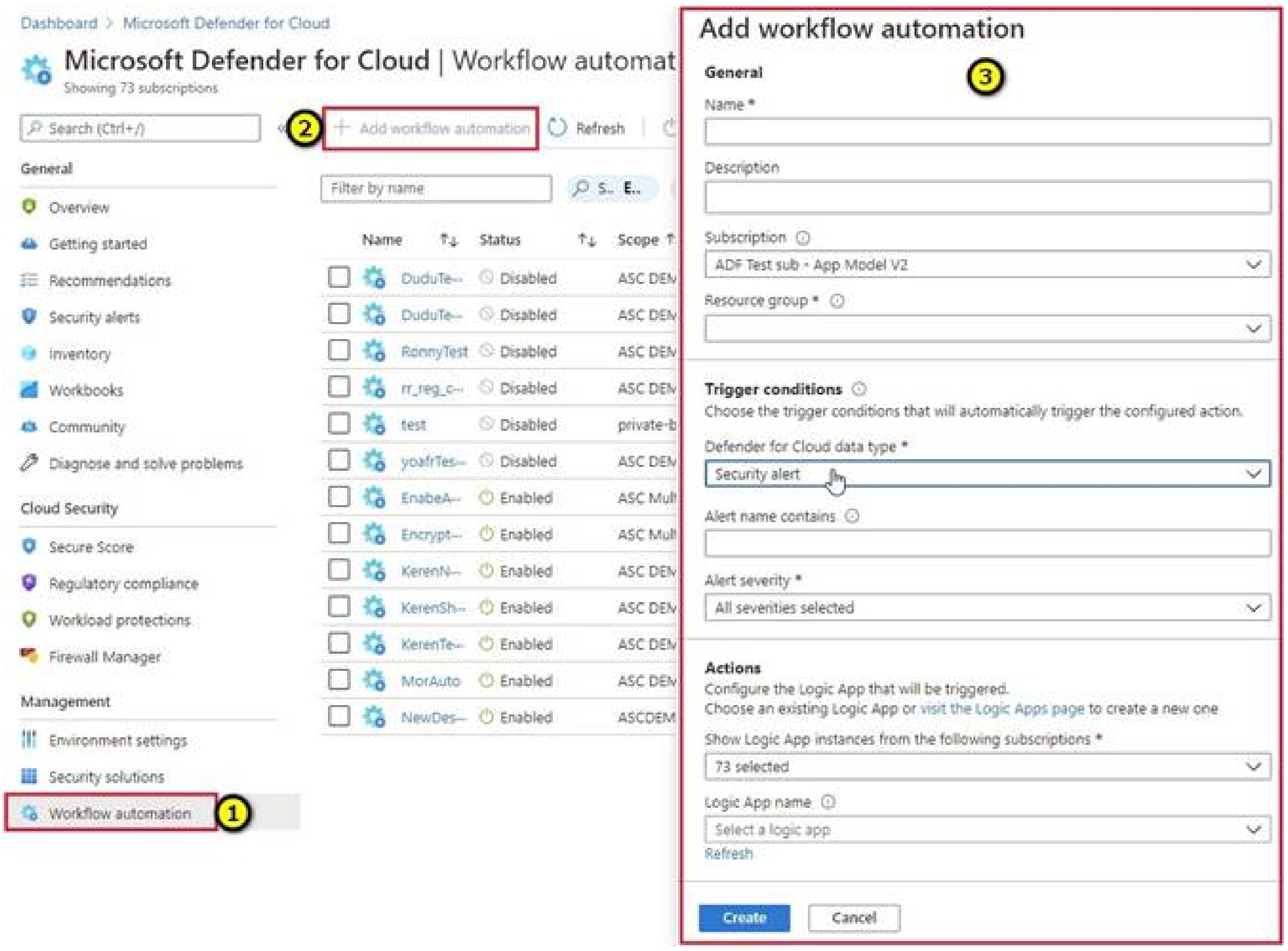
From Workflow automation in Defender for Cloud, add a workflow automation.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: From Logic App Designer, create a logic app.
Create a logic app and define when it should automatically run
* 1. From Defender for Cloud's sidebar, select Workflow automation.
* 2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Dashboard > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workflow automat

Showing 73 subscriptions

	Name	Status	Scope
□	DuduTe...	Disabled	ASC DEM
□	DuduTe...	Disabled	ASC DEM
□	RonnyTest	Disabled	ASC DEM
□	rr_reg_c...	Disabled	ASC DEM
□	test	Disabled	private-b
□	yoafrTes...	Disabled	ASC DEM
□	EnabeA...	Enabled	ASC Mul
□	Encrypt...	Enabled	ASC Mul
□	KerenN...	Enabled	ASC DEM
□	KerenSh...	Enabled	ASC DEM
□	KerenTe...	Enabled	ASC DEM
□	MorAuto	Enabled	ASC DEM
□	NewDes...	Enabled	ASCDEM

Add workflow automation

General

Name *

Description

Subscription: ADF Test sub - App Model V2

Resource group *

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Defender for Cloud data type *: Security alert

Alert name contains

Alert severity *: All severities selected

Actions

Configure the Logic App that will be triggered.

Choose an existing Logic App or visit the Logic Apps page to create a new one

Show Logic App instances from the following subscriptions *: 73 selected

Logic App name: Select a logic app

Refresh

Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

* 3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

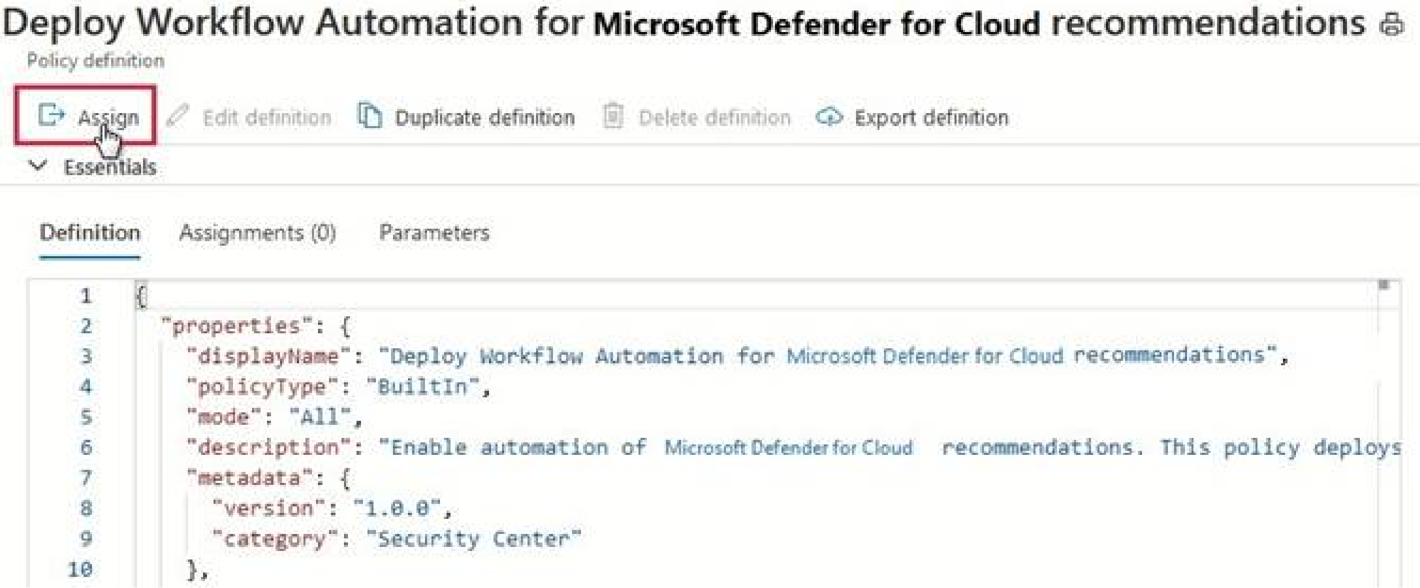
* 4. Etc.

Step 2: From Logic App Designer, run a trigger. Manually trigger a Logic App

You can also run Logic Apps manually when viewing any security alert or recommendation.

Step 3: From Workflow automation in Defender for cloud, add a workflow automation. Configure workflow automation at scale using the supplied policies

Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.



Deploy Workflow Automation for Microsoft Defender for Cloud recommendations

Policy definition

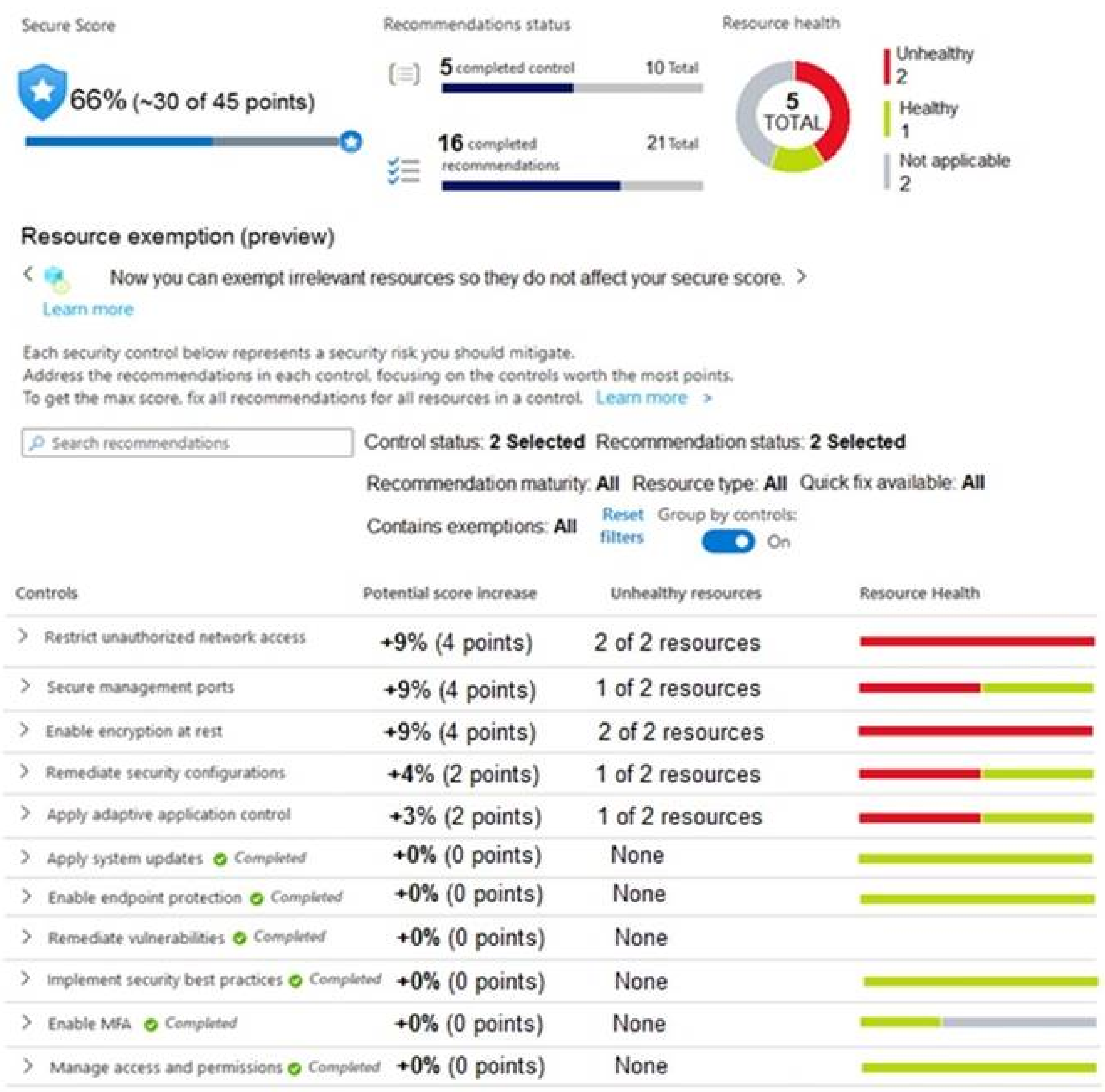
```
{
  "properties": {
    "displayName": "Deploy Workflow Automation for Microsoft Defender for Cloud recommendations",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Enable automation of Microsoft Defender for Cloud recommendations. This policy deploys
    "metadata": {
      "version": "1.0.0",
      "category": "Security Center"
    },
```

NEW QUESTION 115

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

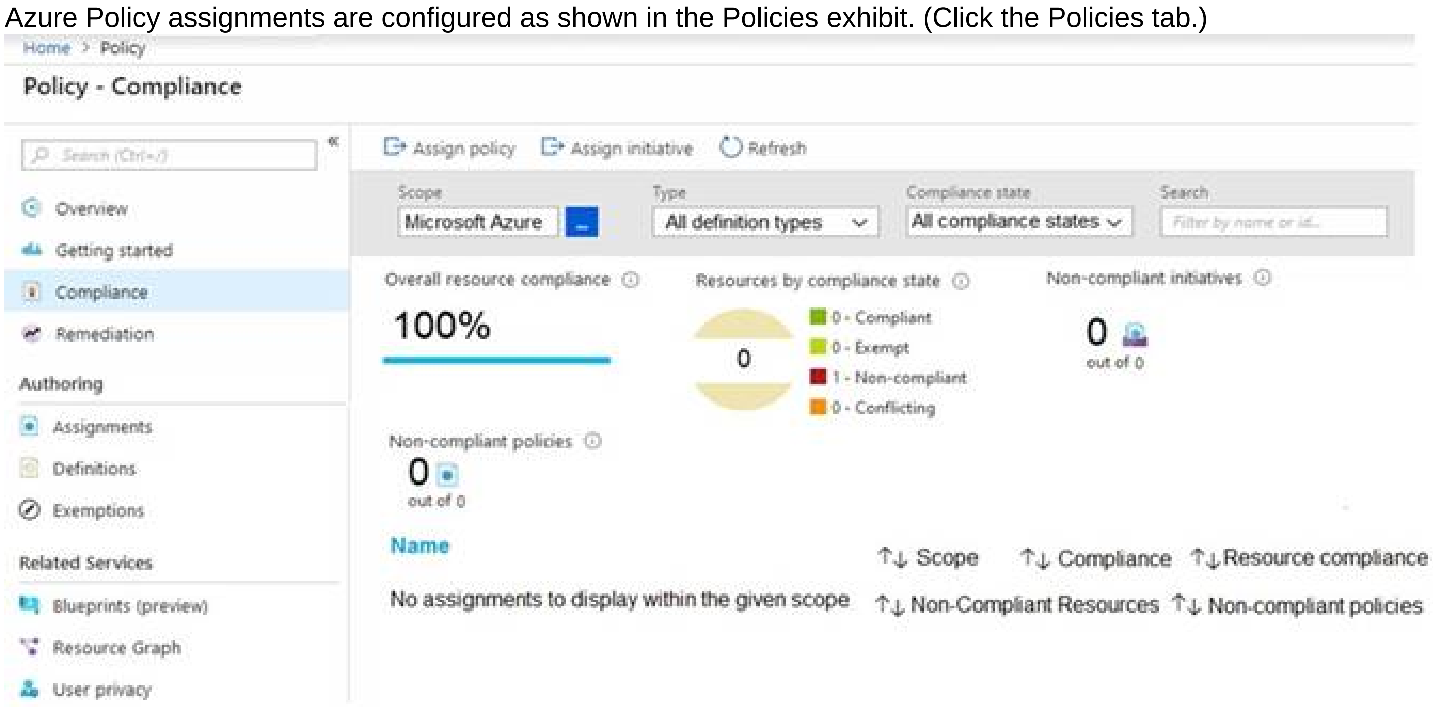
Control status: **2 Selected** Recommendation status: **2 Selected**

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

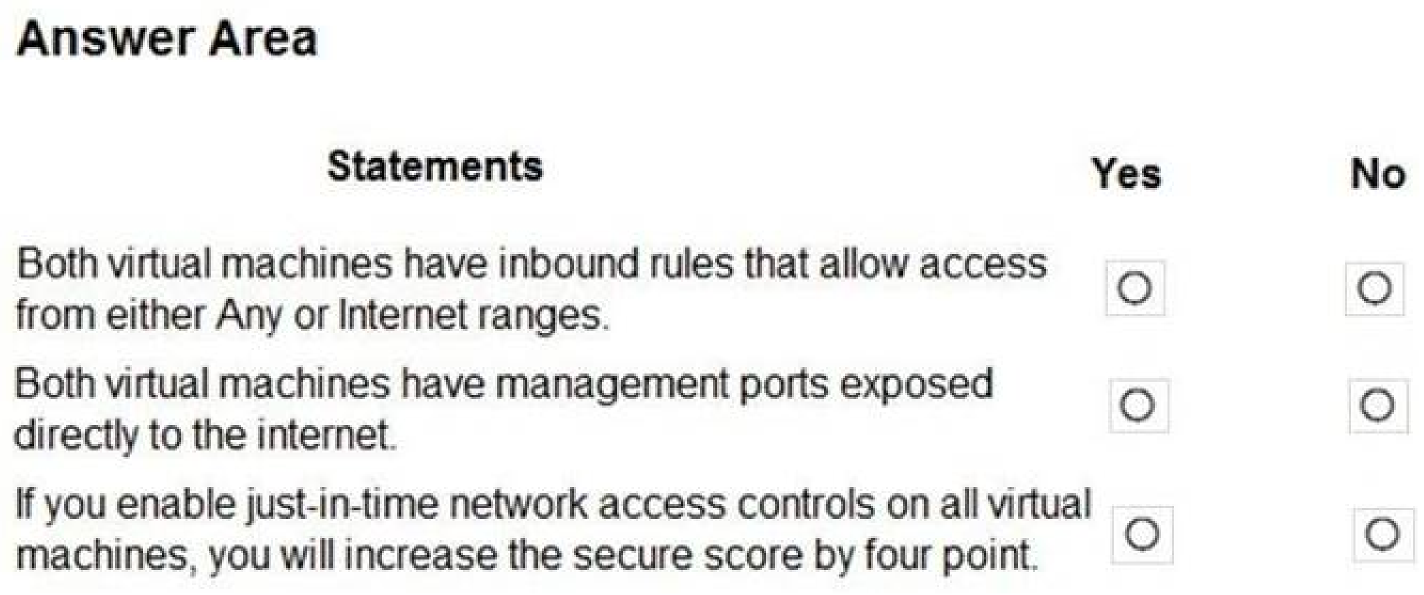
Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name ↑↓ Scope ↑↓ Compliance ↑↓ Resource compliance

No assignments to display within the given scope ↑↓ Non-Compliant Resources ↑↓ Non-compliant policies

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



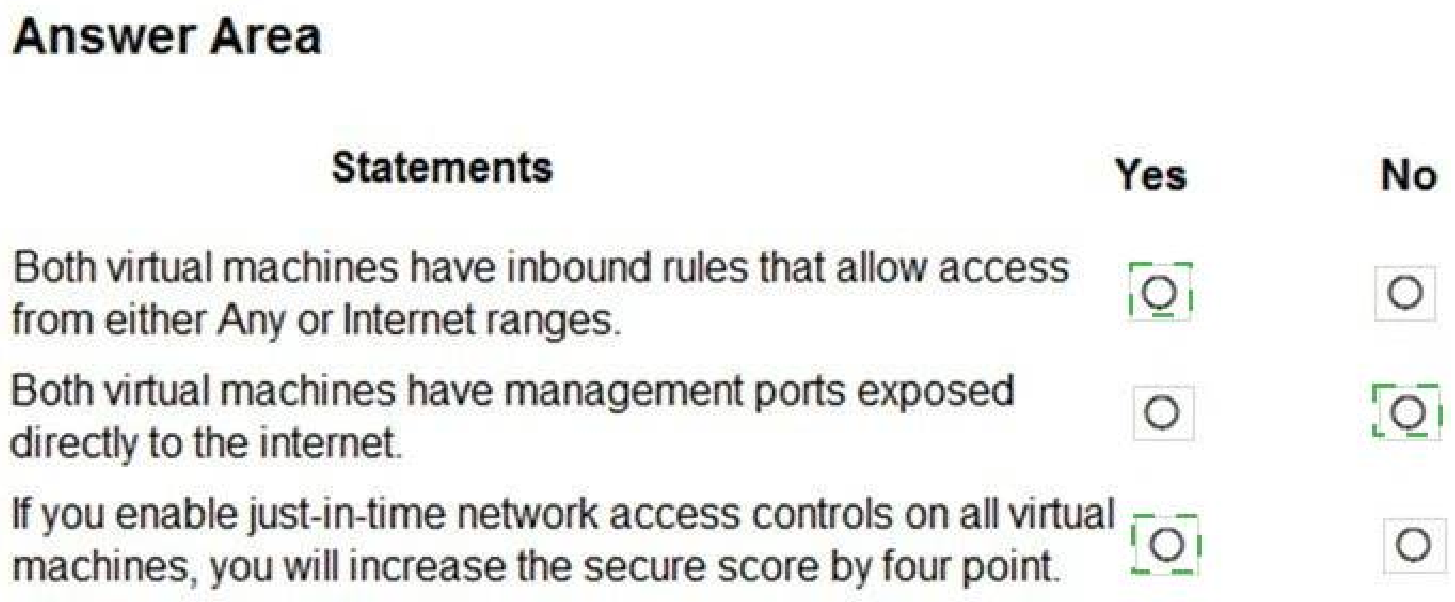
Answer Area

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

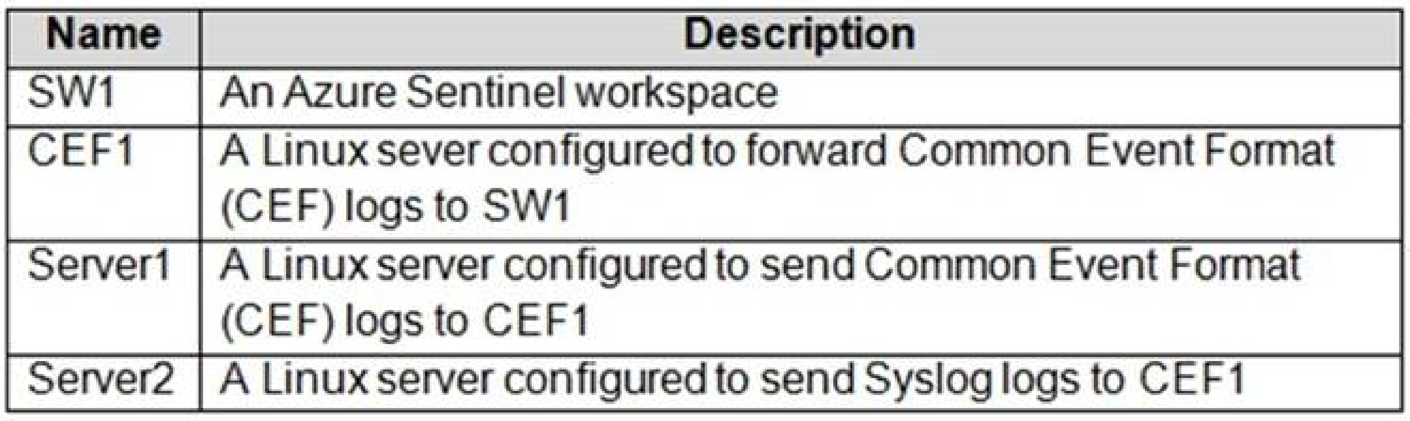
Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	[✓ ○]	○
Both virtual machines have management ports exposed directly to the internet.	○	[✓ ○]
If you enable just-in-time network access controls on all virtual machines, you will increase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

NEW QUESTION 120
- (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

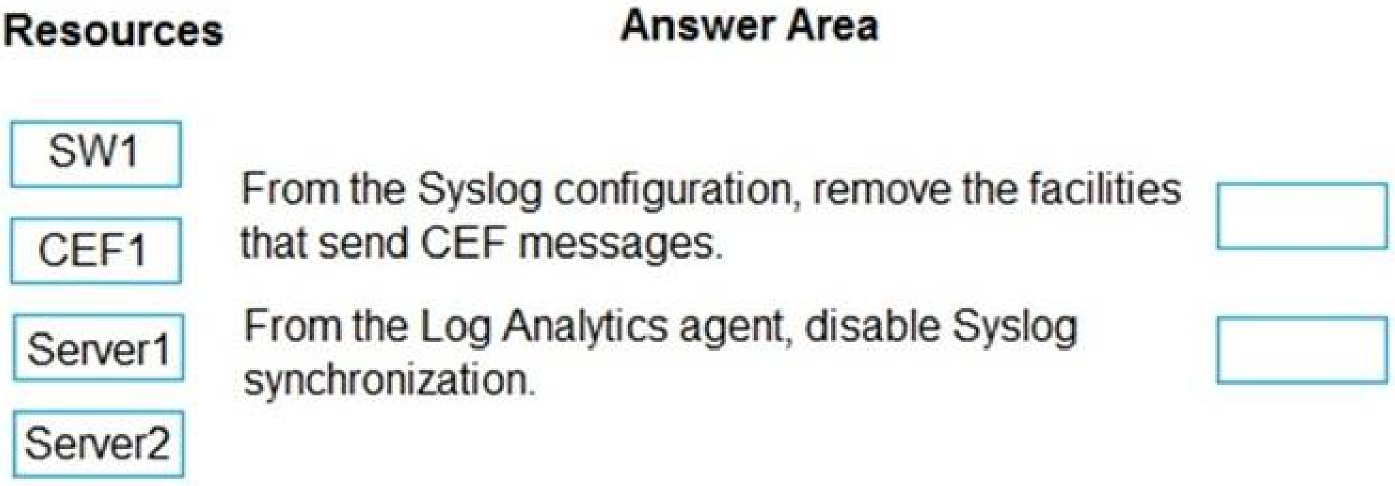
Answer: D

NEW QUESTION 121
DRAG DROP - (Topic 4)
You have the resources shown in the following table.



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

You need to prevent duplicate events from occurring in SW1.
What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Resources

SW1
CEF1
Server1
Server2

Answer Area

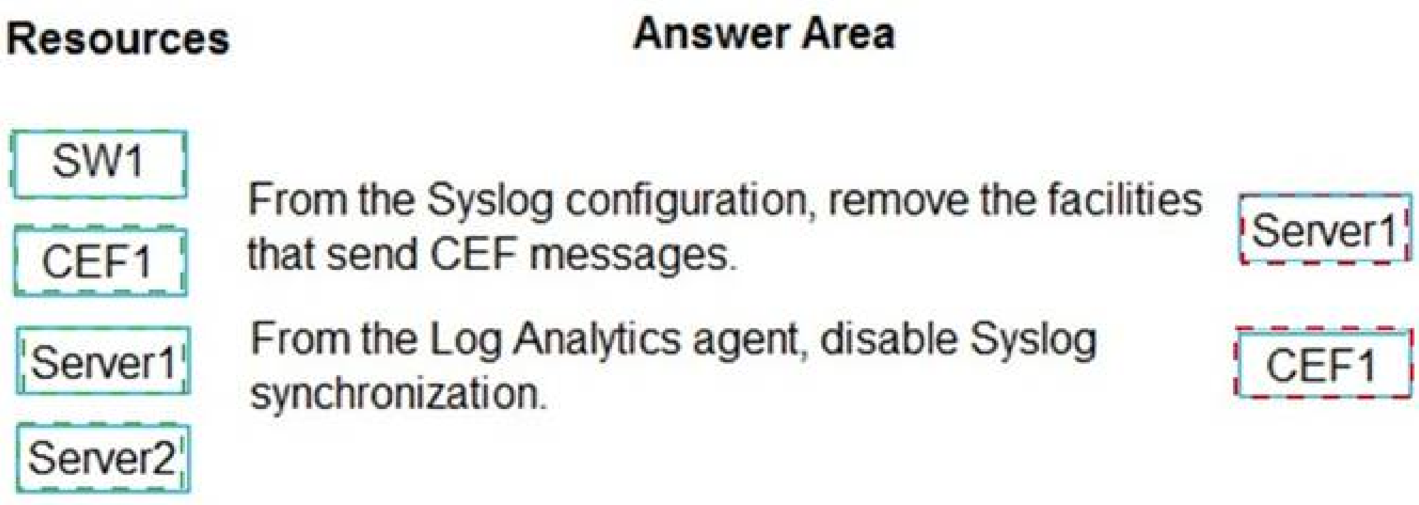
From the Syslog configuration, remove the facilities that send CEF messages. □

From the Log Analytics agent, disable Syslog synchronization. □

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Resources

SW1

CEF1

Server1

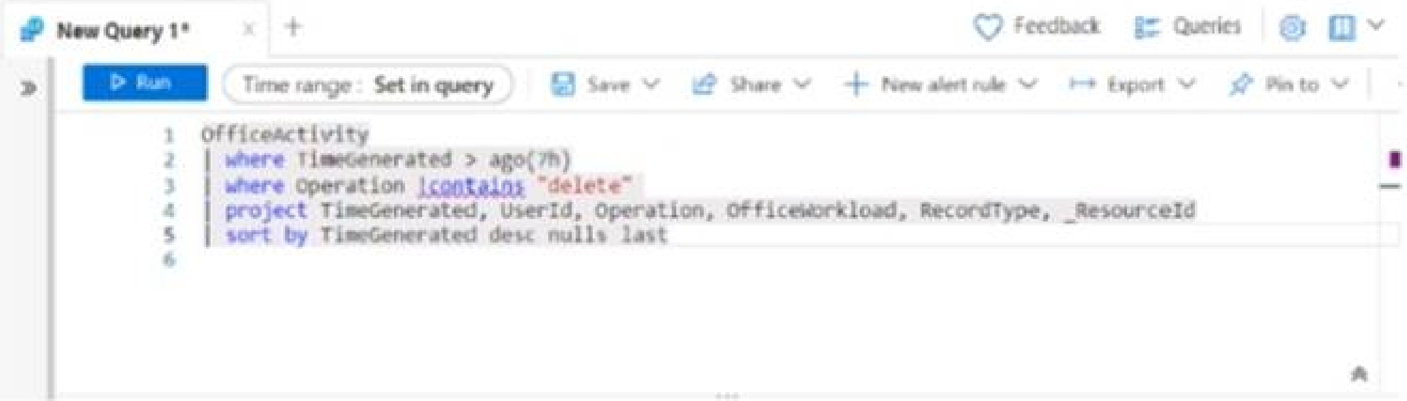
Server2

Answer Area

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

From the Log Analytics agent, disable Syslog synchronization. CEF1

NEW QUESTION 125
- (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 128
- (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 133
- (Topic 4)
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: DE

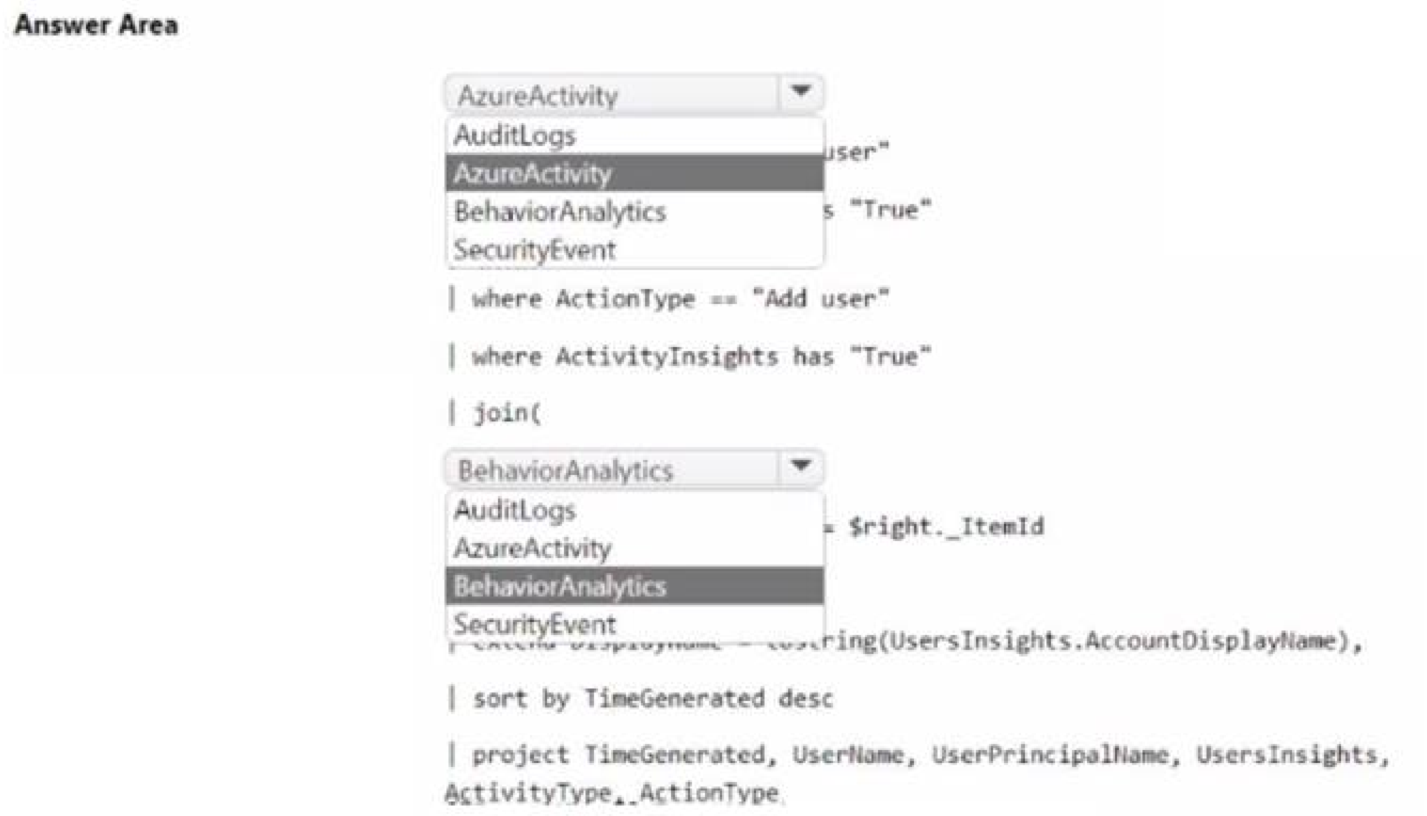
Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

NEW QUESTION 135
- (Topic 4)
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

A. the entity side panel of the Timeline card in Microsoft Sentinel
B. the investigation graph on the Incidents page of Microsoft Sentinel
C. the Timeline tab on the Incidents page of Microsoft Sentinel
D. the Alerts page in the Microsoft 365 Defender portal

Answer: A

NEW QUESTION 139
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

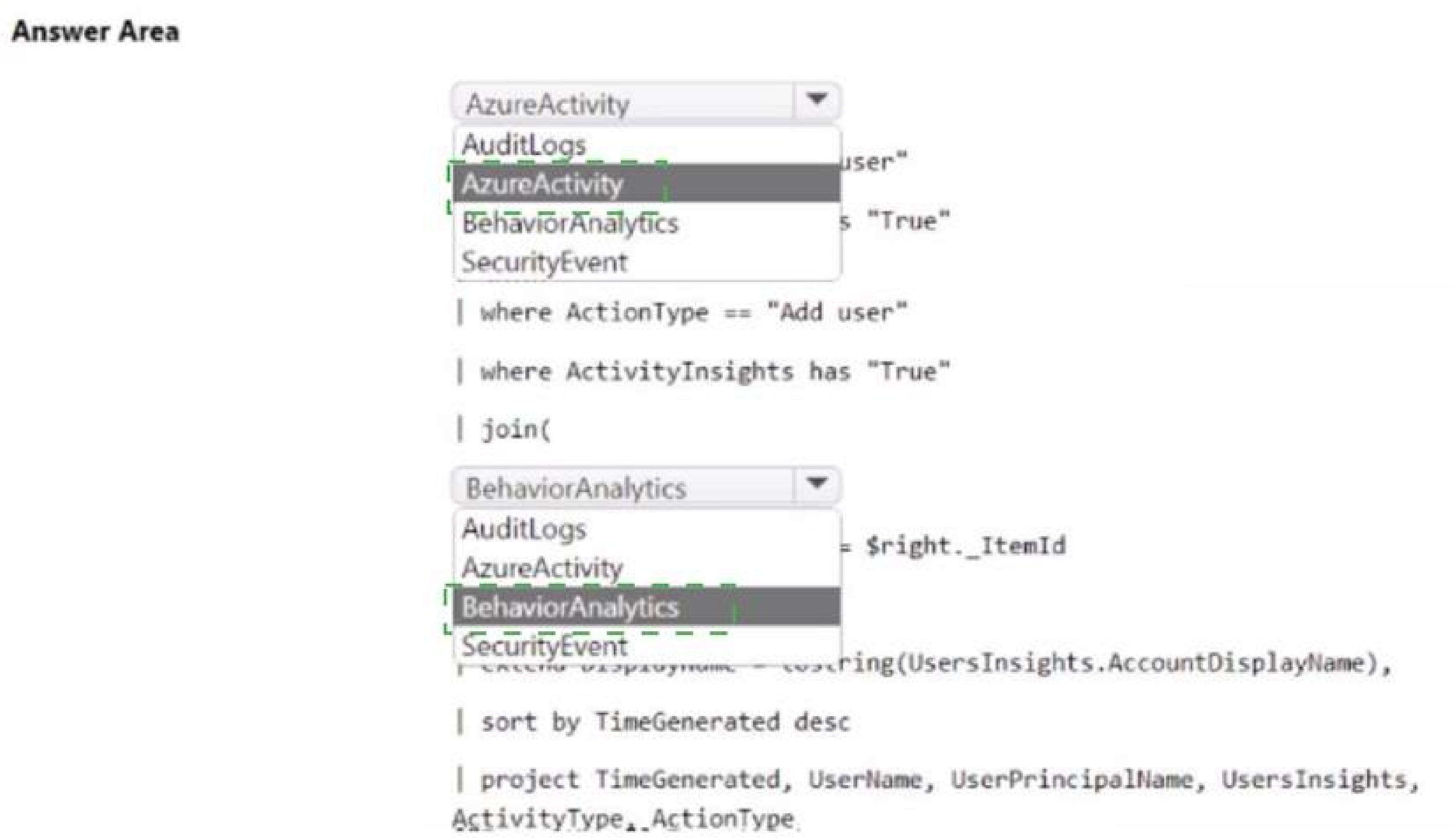
```
user"
s "True"
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
```

```
= $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

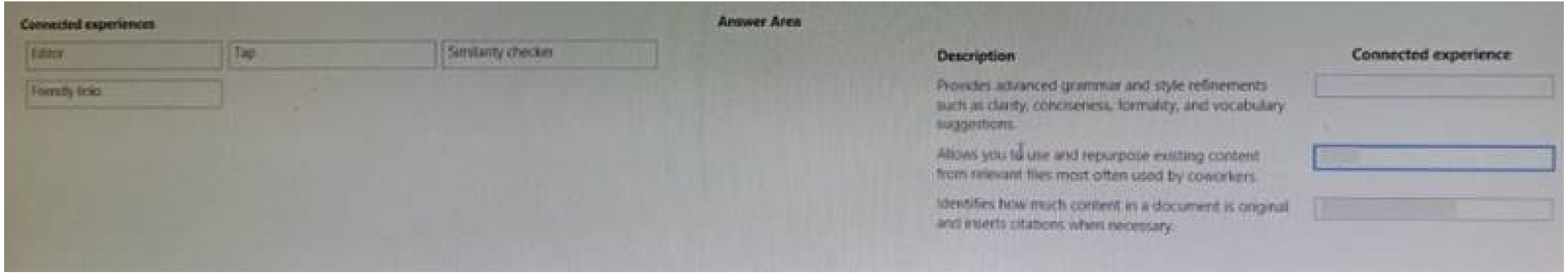
AzureActivity ▼
- AuditLogs
- AzureActivity
- BehaviorAnalytics
- SecurityEvent

```
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 140
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

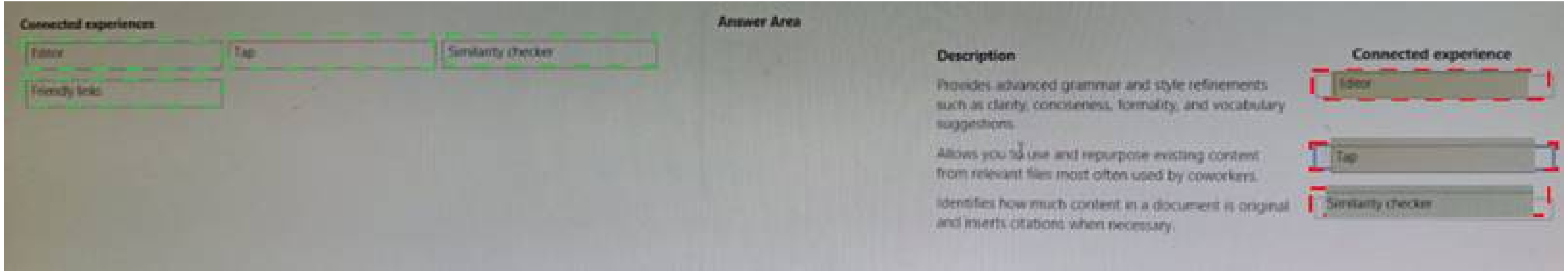
Answer Area

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:



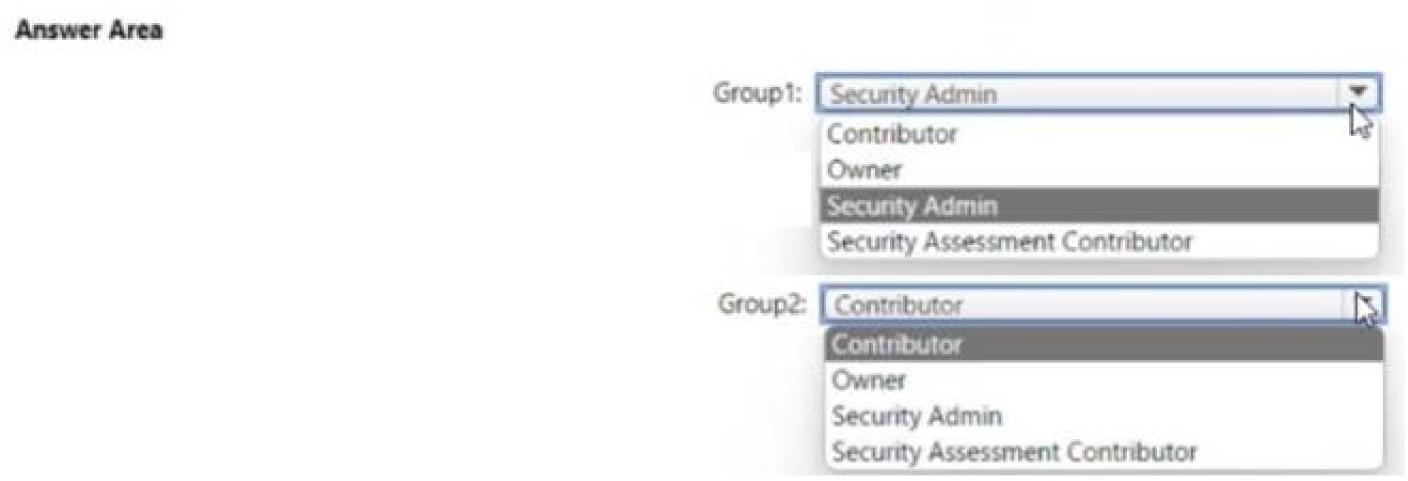
Connected experiences

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 144
HOTSPOT - (Topic 4)
You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.



Answer Area

Group1: Security Admin

Contributor
Owner
Security Admin
Security Assessment Contributor

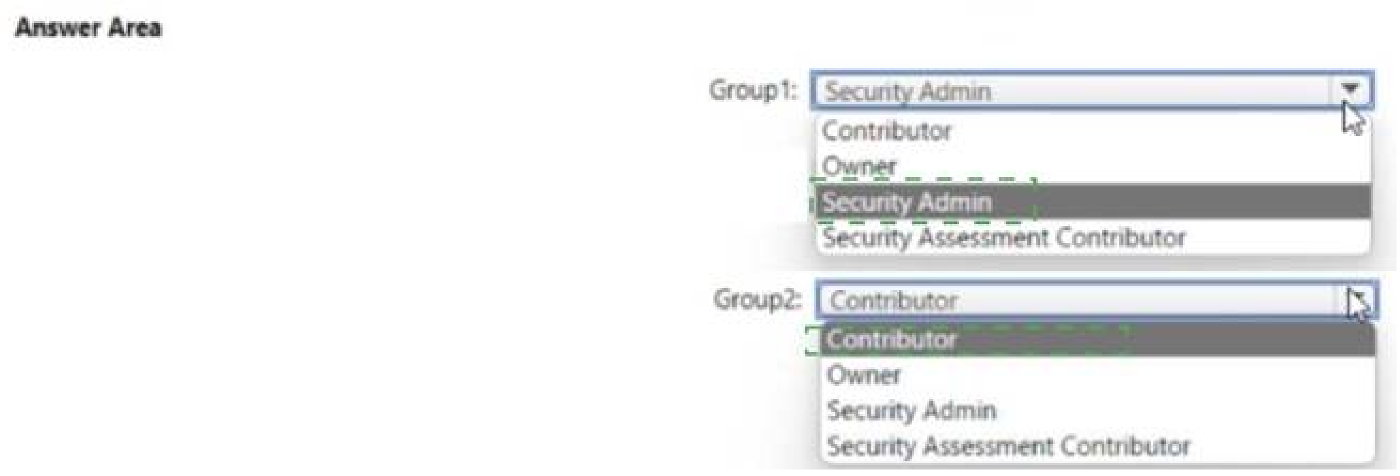
Group2: Contributor

Contributor
Owner
Security Admin
Security Assessment Contributor

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Group1: Security Admin

Contributor
Owner
Security Admin
Security Assessment Contributor

Group2: Contributor

Contributor
Owner
Security Admin
Security Assessment Contributor

NEW QUESTION 149

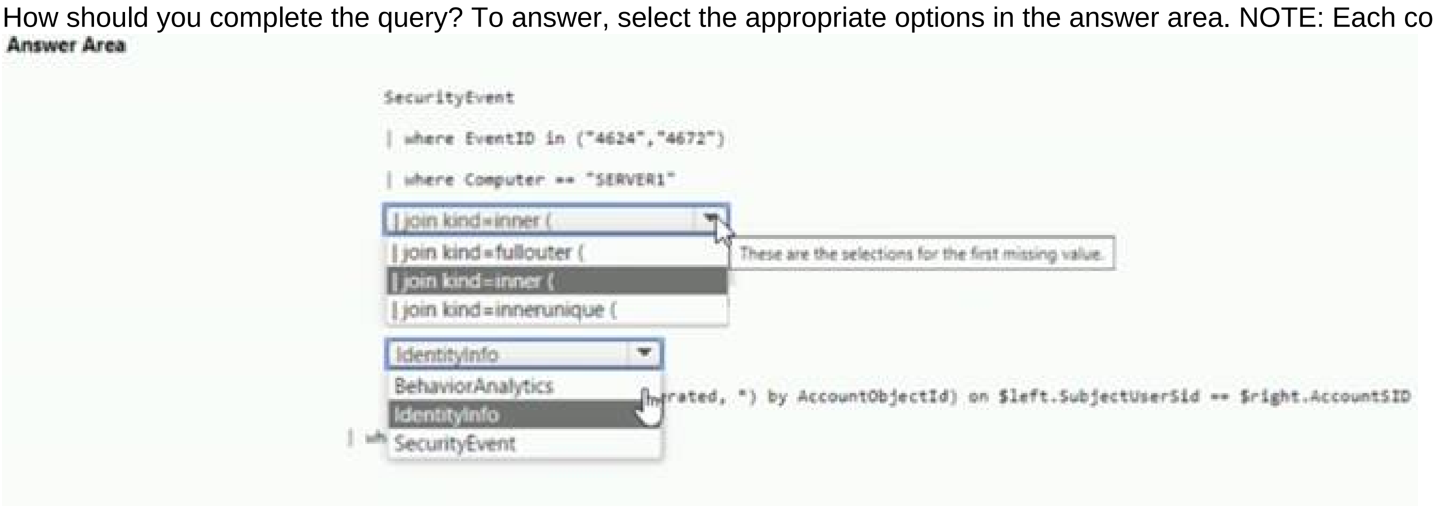
HOTSPOT - (Topic 4)

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.



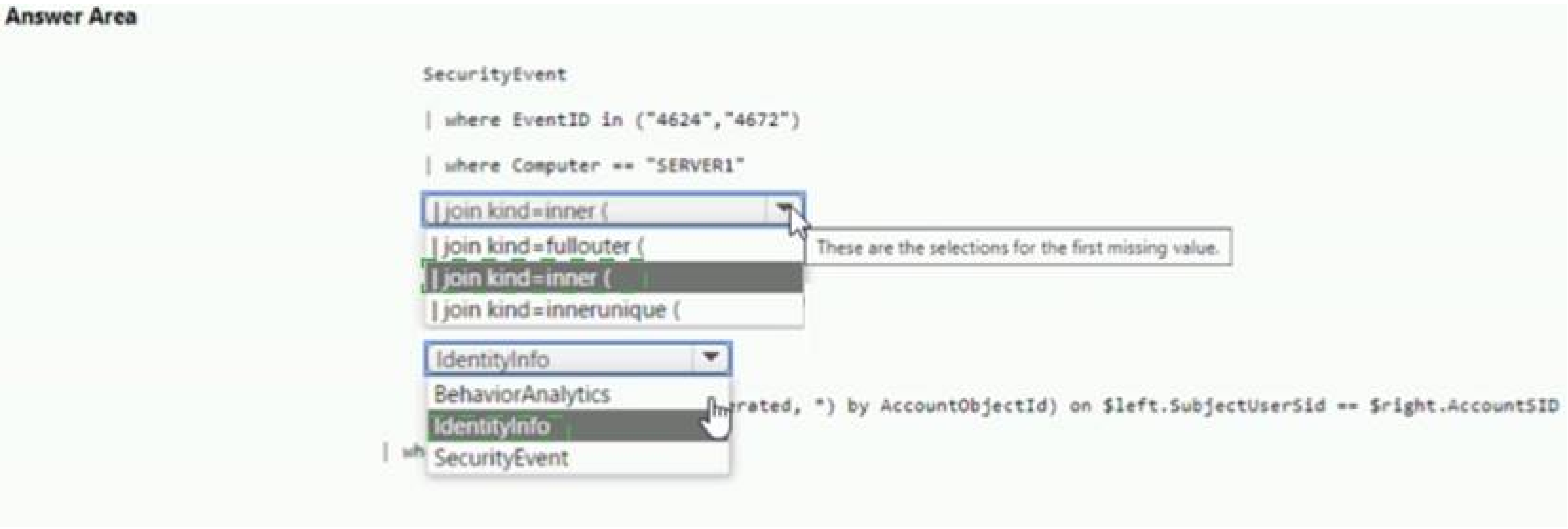
Answer Area

```
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

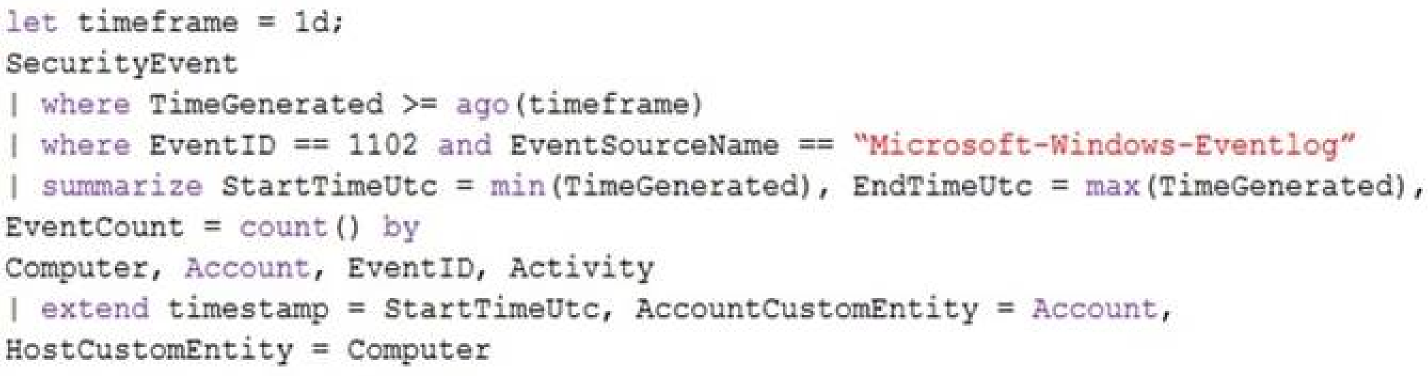
Explanation:



Answer Area

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

NEW QUESTION 153
- (Topic 4)
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.



```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete
solution.
NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address
D. computer

Answer: CD

NEW QUESTION 157
- (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

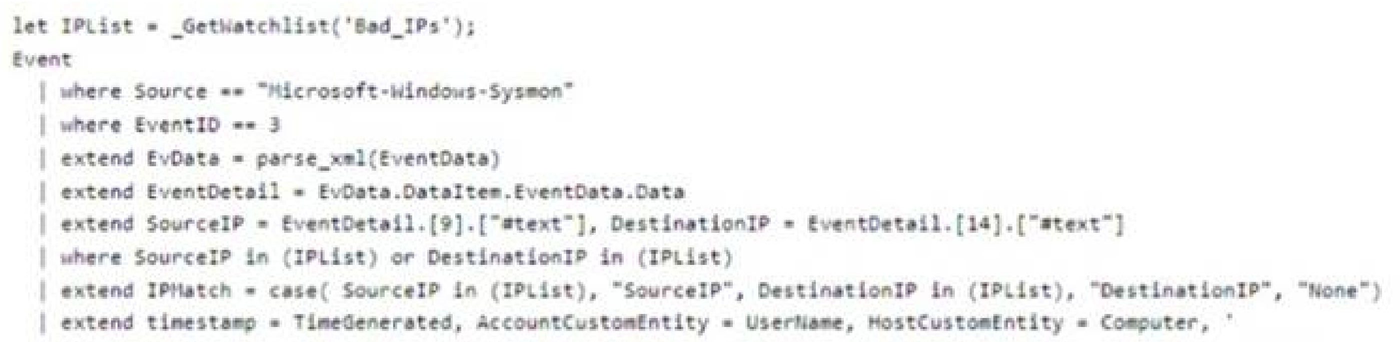
NEW QUESTION 159
- (Topic 4)
A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

A. the severity level of email notifications
B. a cloud connector
C. the Azure Defender plans
D. the integration settings for Threat detection

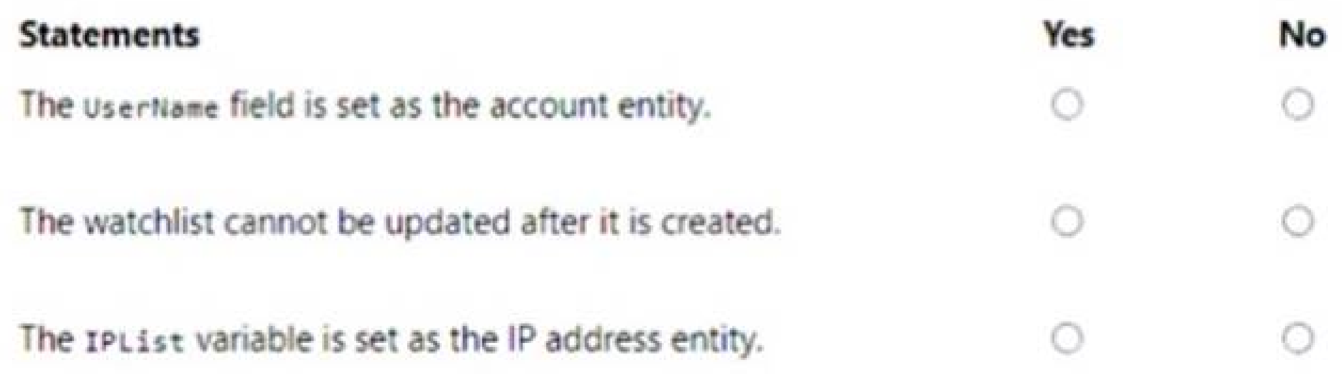
Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

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



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

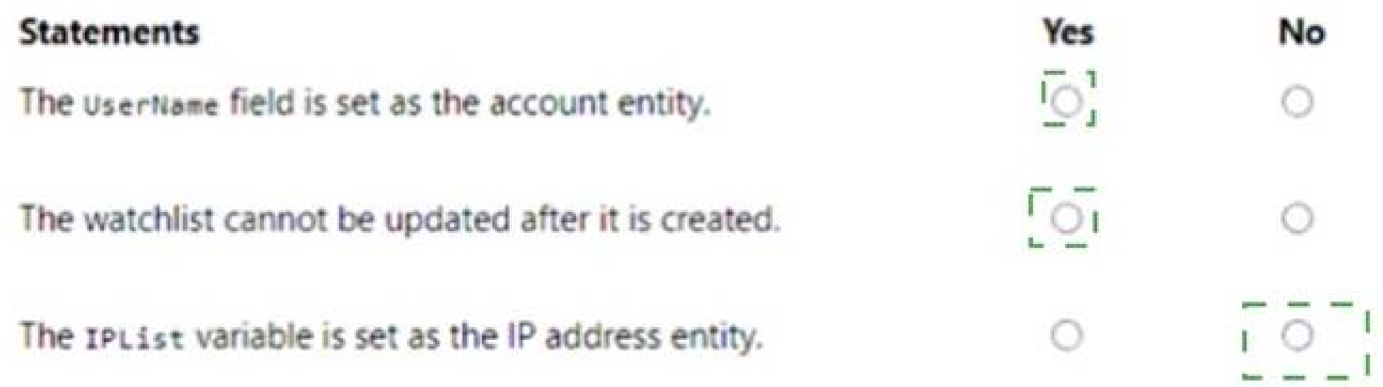


Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

A. Mastered
B. Not Mastered

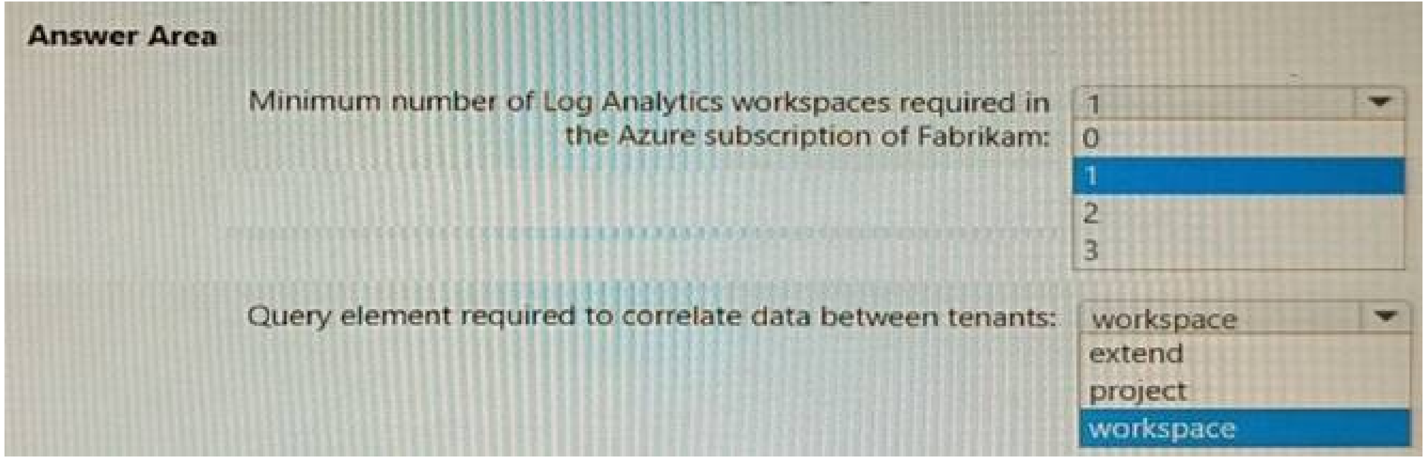
Answer: A

Explanation:



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

NEW QUESTION 168
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

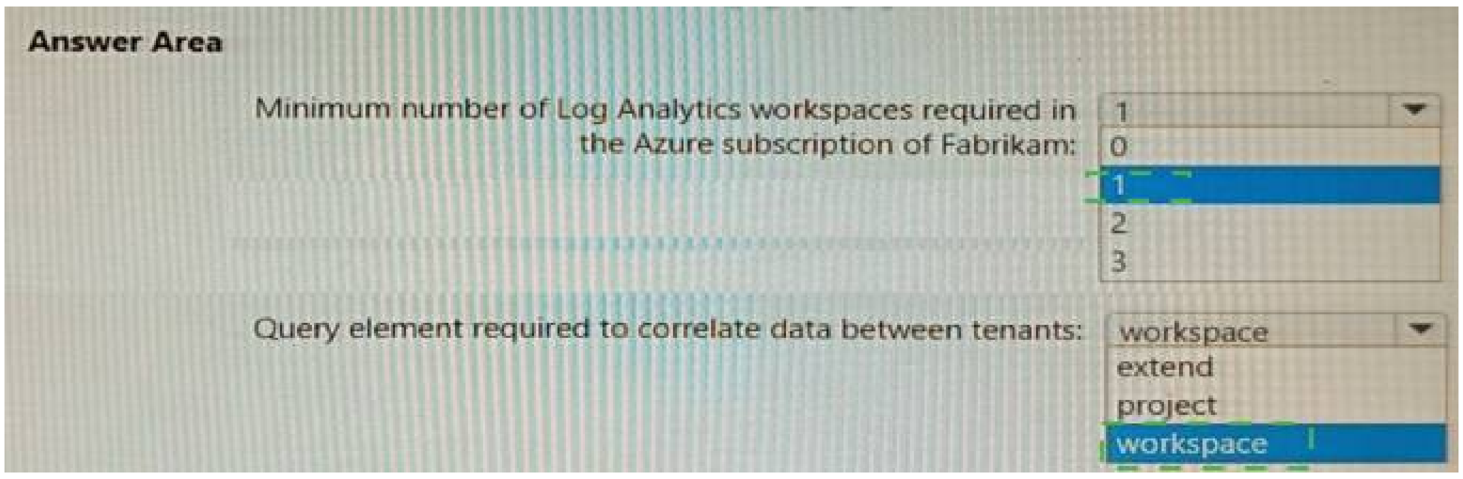
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

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
- 0
- 1
- 2
- 3

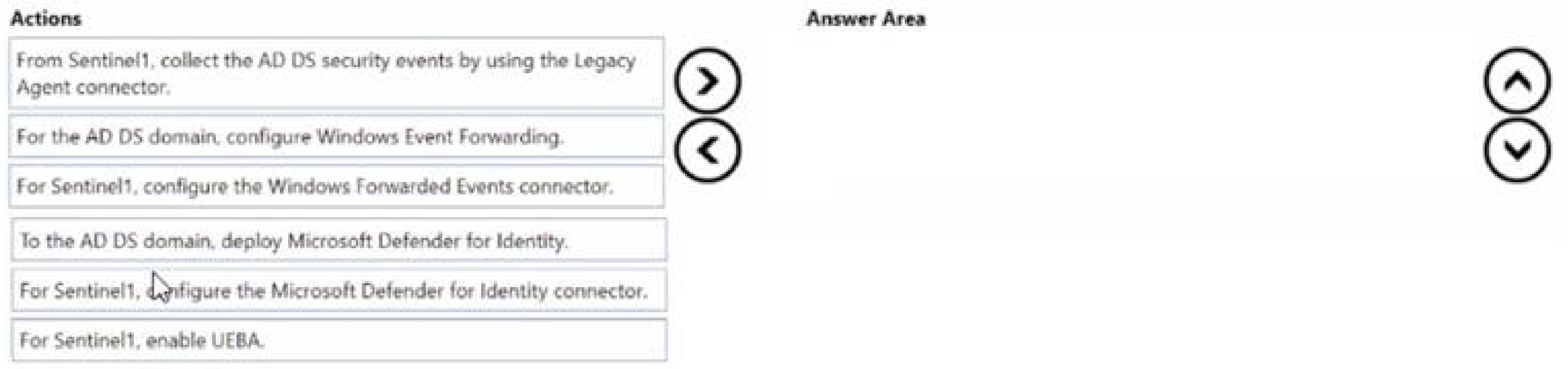
Query element required to correlate data between tenants: workspace
- extend
- project
- workspace

NEW QUESTION 170
- (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 173
DRAG DROP - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You have a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel1 and collect security events from the AD DS domain.
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.



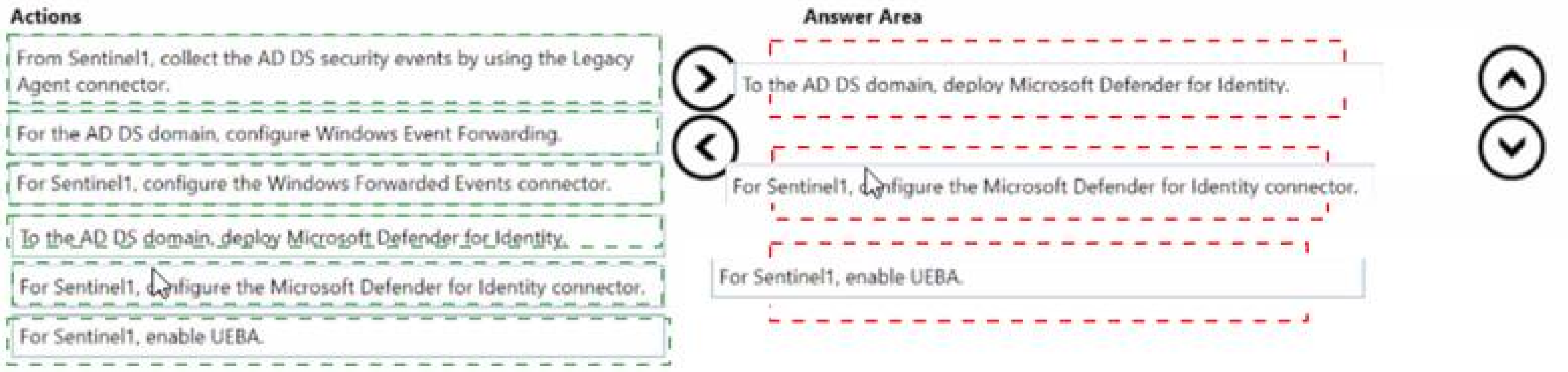
Actions
- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

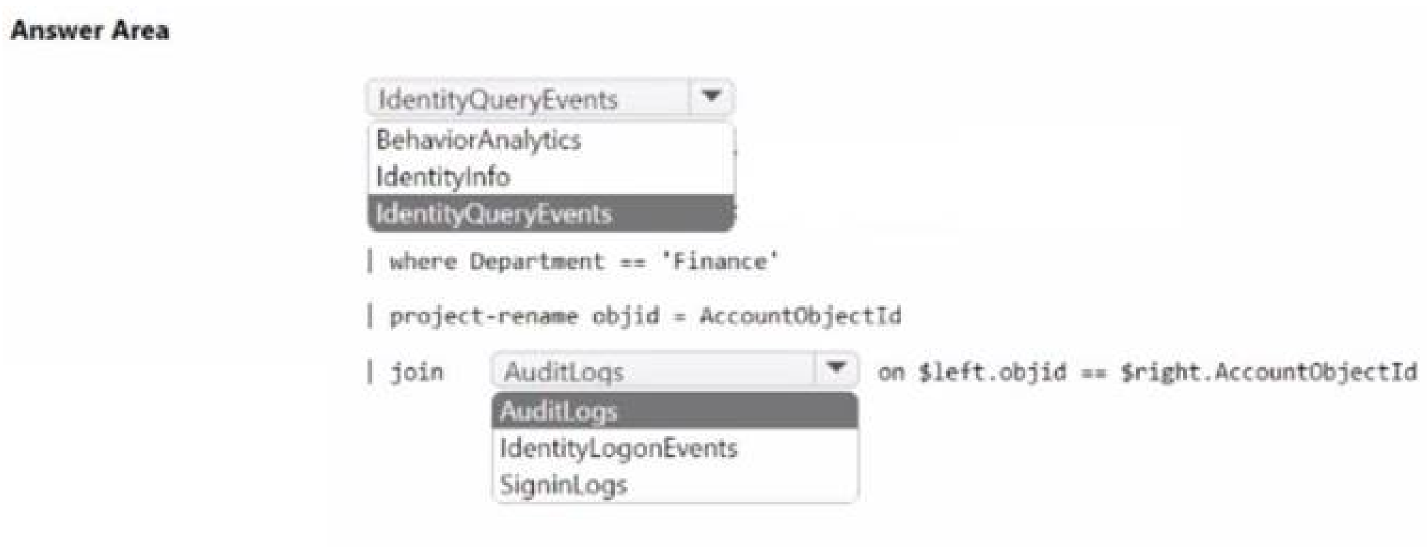
Explanation:



Actions
- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

Answer Area
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure the Microsoft Defender for Identity connector.
- For Sentinel1, enable UEBA.

NEW QUESTION 177
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.

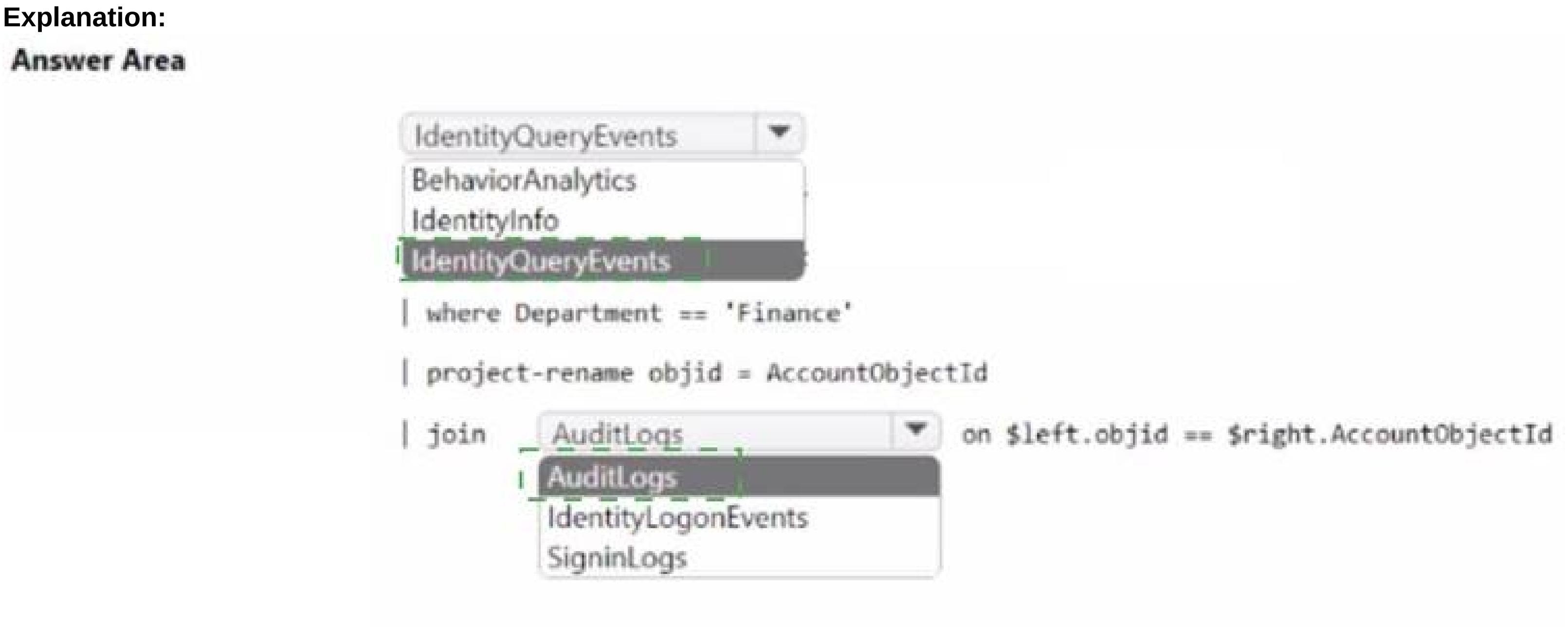


```
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join [AuditLogs] on $left.objid == $right.AccountObjectId
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

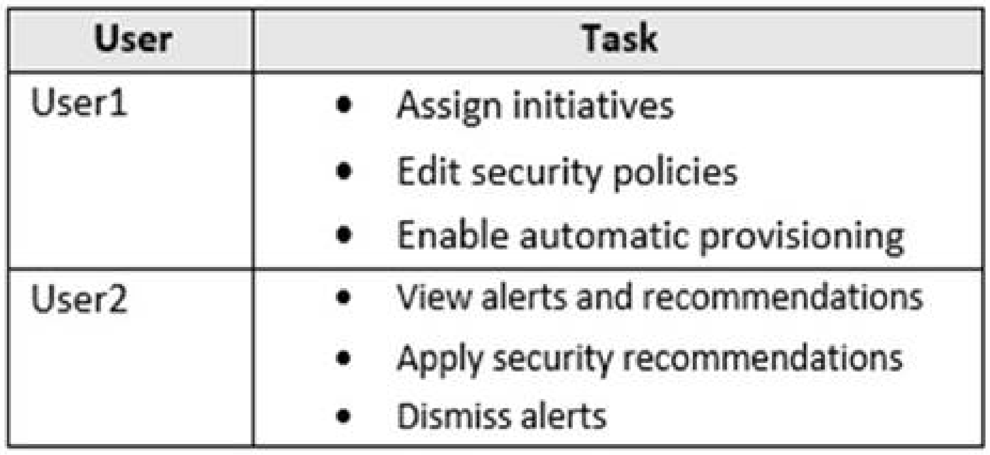
NEW QUESTION 182
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

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

Answer: D

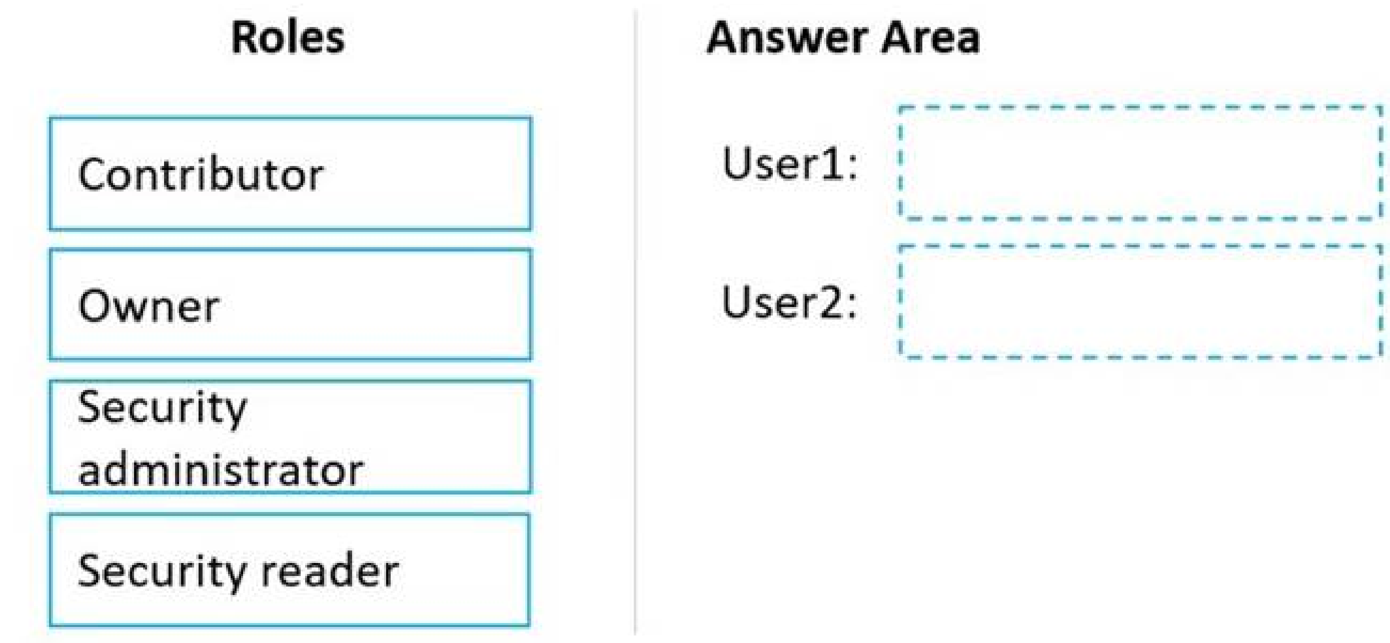
Explanation:
To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude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

NEW QUESTION 185
DRAG DROP - (Topic 4)
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.



User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.



Roles

- Contributor
- Owner
- Security administrator
- Security reader

Answer Area

User1:

User2:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Owner
Only the Owner can assign initiatives.
Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.

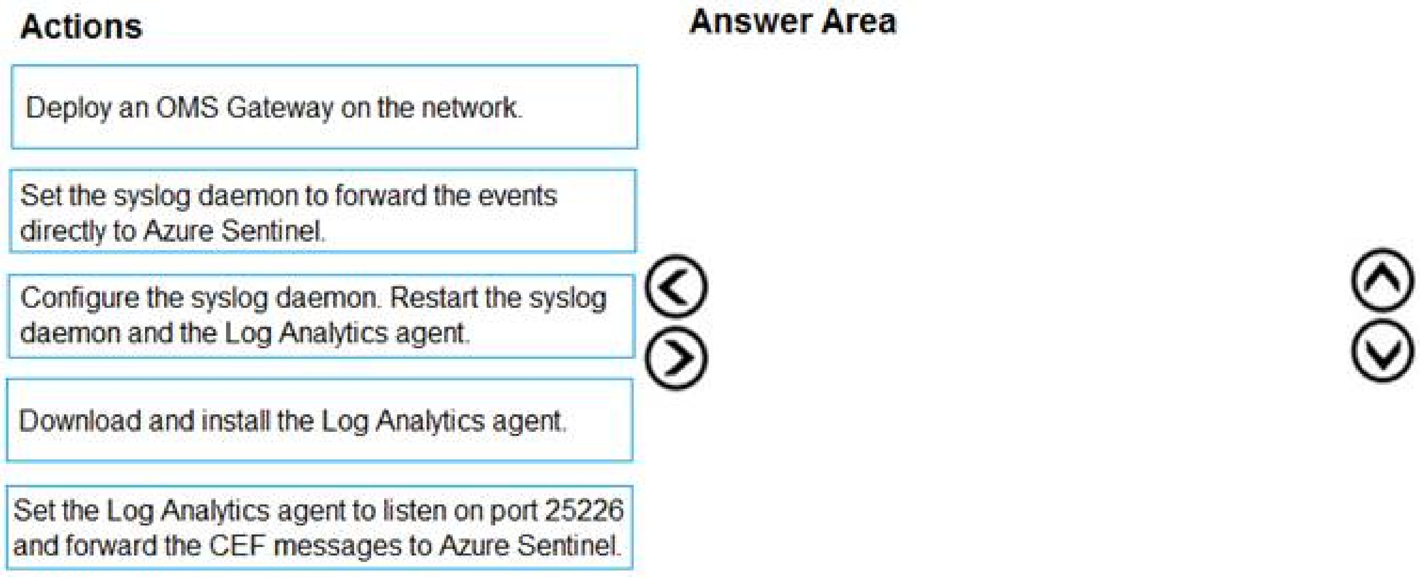
NEW QUESTION 190
- (Topic 4)
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual 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 193
DRAG DROP - (Topic 4)
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.



Actions

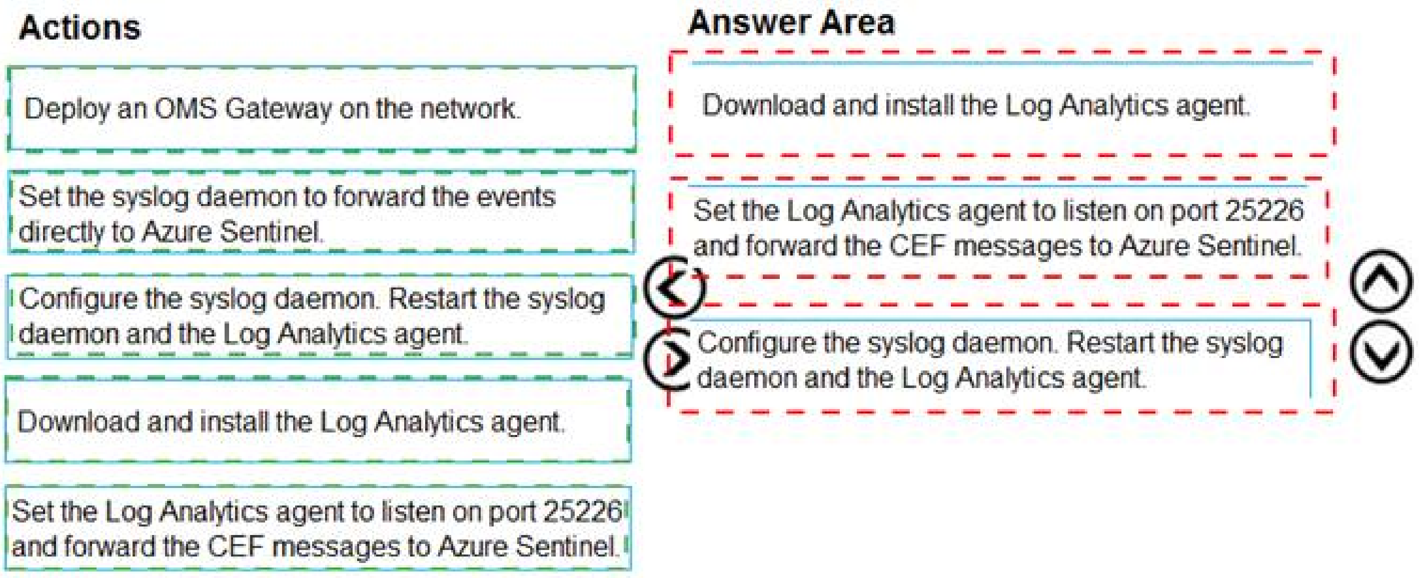
- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.
- Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
- Download and install the Log Analytics agent.
- Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

NEW QUESTION 194
- (Topic 4)
Your company uses Microsoft Sentinel
A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

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

Answer: A

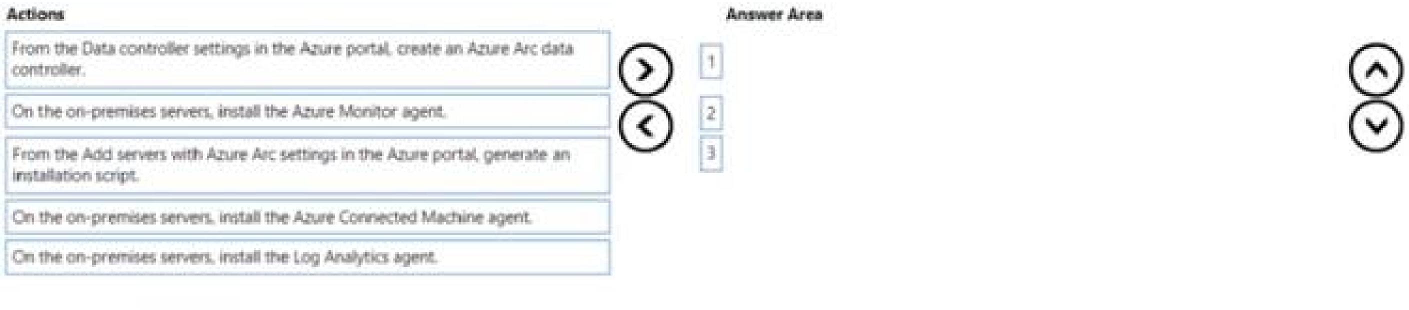
Explanation:
The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac

NEW QUESTION 197
- (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 200
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

A. Mastered
B. Not Mastered

Answer: A

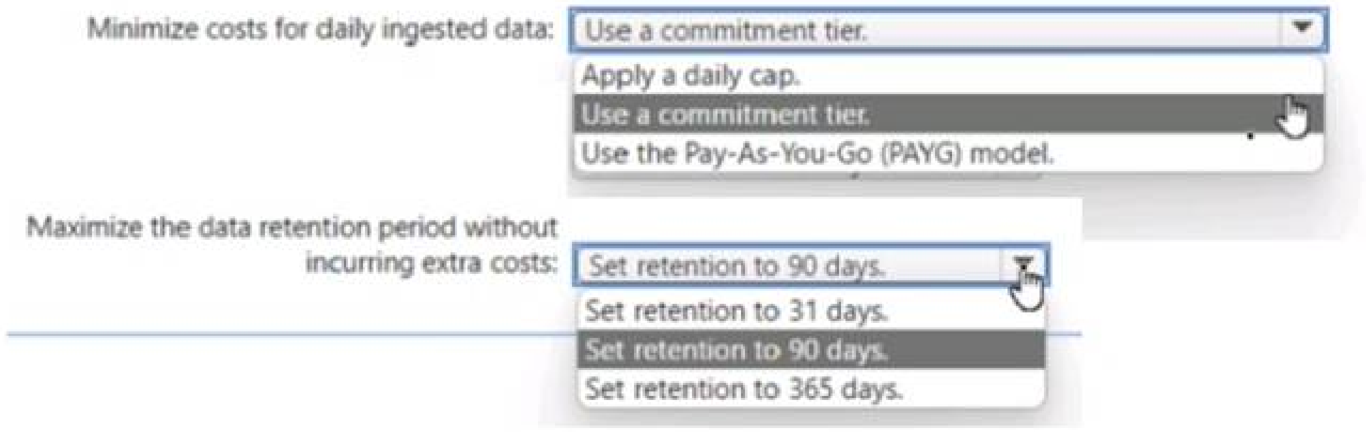
Explanation:
To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:
? On the on-premises servers, install the Azure Connected Machine agent.
? On the on-premises servers, install the Log Analytics agent.
? From the Data controller 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 201
- (Topic 4)
You create a custom analytics rule to detect threats in Azure Sentinel. You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.
B. The target workspace was deleted.
C. Permissions to the data sources of the rule query were modified.
D. There are connectivity issues between the data sources and Log Analytics

Answer: AD

NEW QUESTION 205
HOTSPOT - (Topic 4)
You have an Azure subscription.
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.
You need to configure storage for the workspace. The solution must meet the following requirements:
• Minimize costs for daily ingested data.
• Maximize the data retention period without incurring extra costs.
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



Minimize costs for daily ingested data: Use a commitment tier.

Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

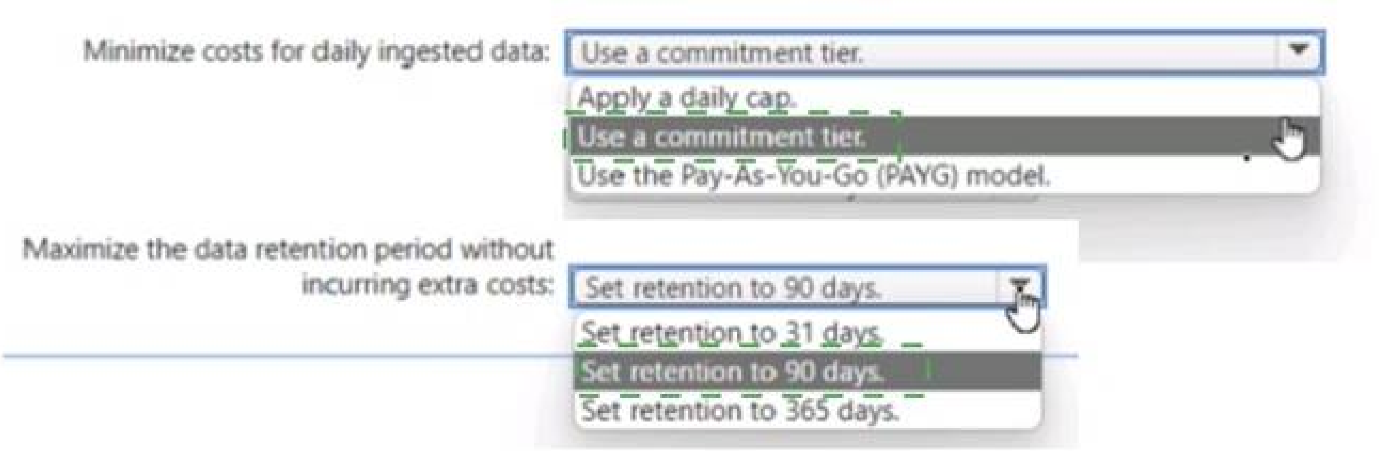
Maximize the data retention period without incurring extra costs: Set retention to 90 days.

Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

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

NEW QUESTION 208
- (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

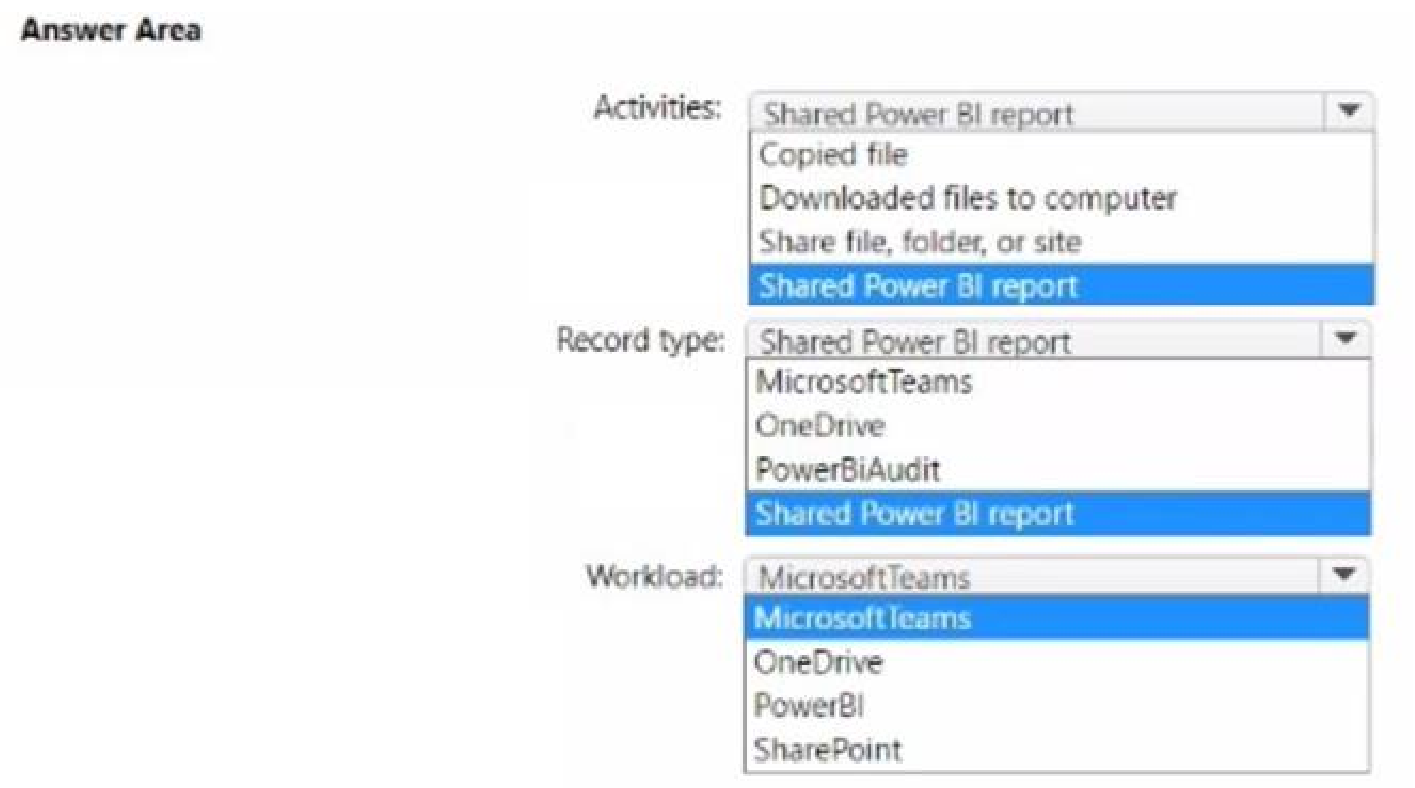
NEW QUESTION 212
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 213
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.
User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.
You need to identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Activities: Shared Power BI report ▾
- Copied file
- Downloaded files to computer
- Share file, folder, or site
- Shared Power BI report

Record type: Shared Power BI report ▾
- MicrosoftTeams
- OneDrive
- PowerBiAudit
- Shared Power BI report

Workload: MicrosoftTeams ▾
- MicrosoftTeams
- OneDrive
- PowerBI
- SharePoint

A. Mastered
B. Not Mastered

Answer: A

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

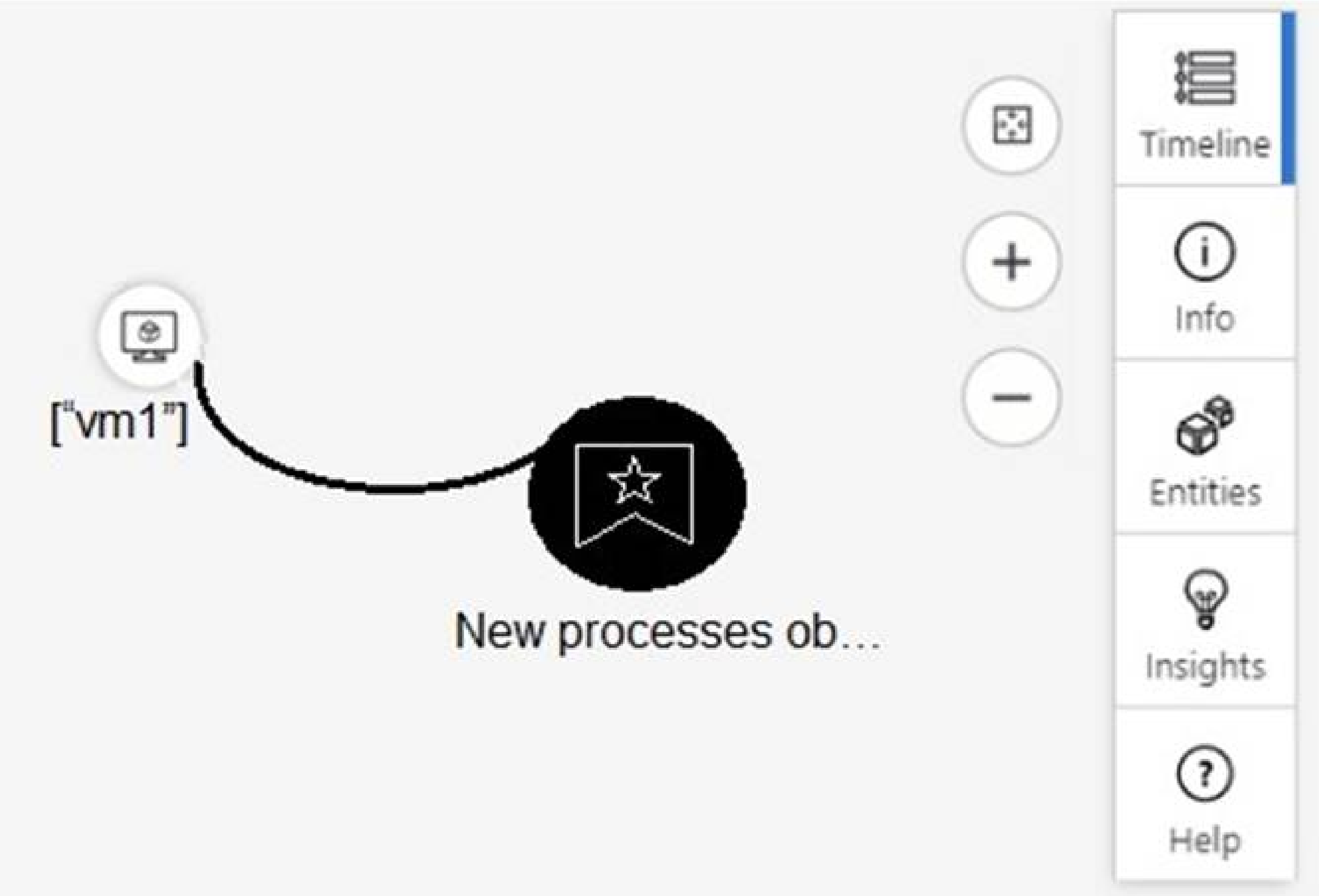
NEW QUESTION 217
- (Topic 4)
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company’s accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

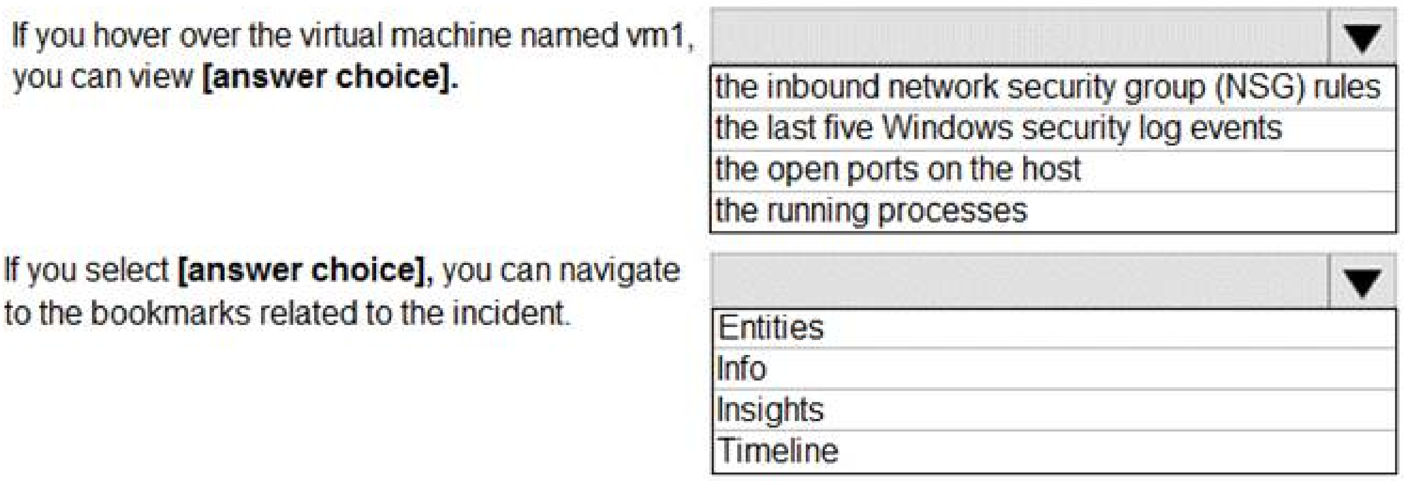
Answer: BCE

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

NEW QUESTION 219
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

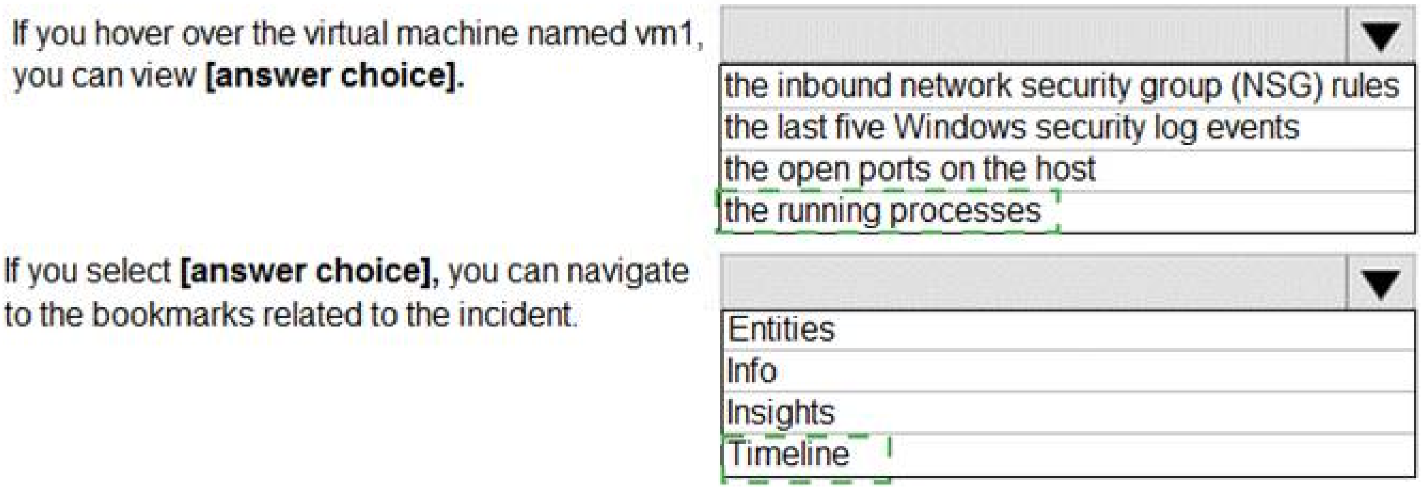
If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- 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 221
- (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

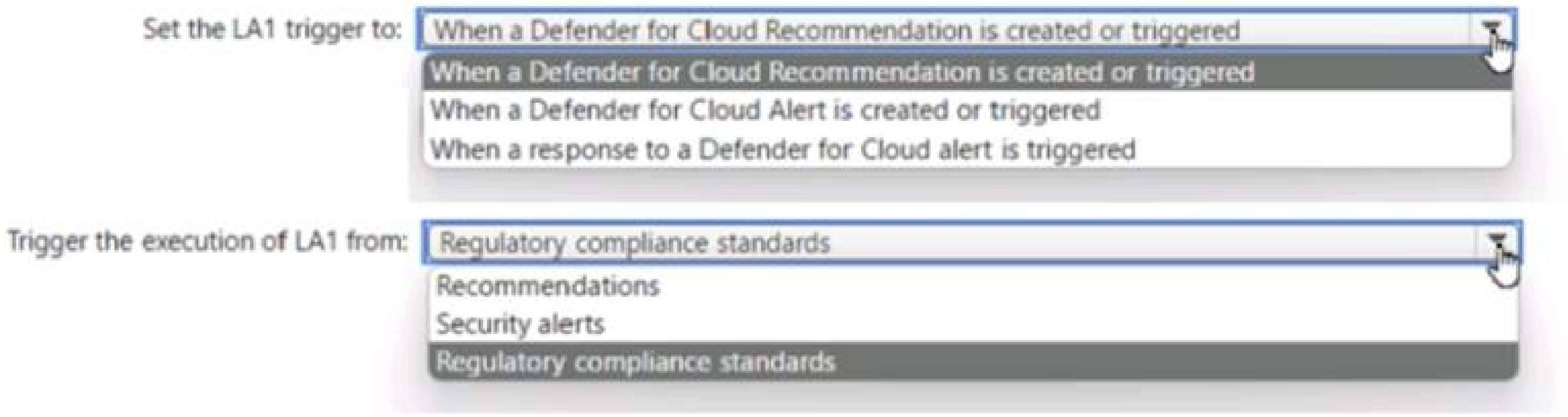
NEW QUESTION 226
- (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize 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 231
HOTSPOT - (Topic 4)
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.
You need to test LA1 in Defender for Cloud.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

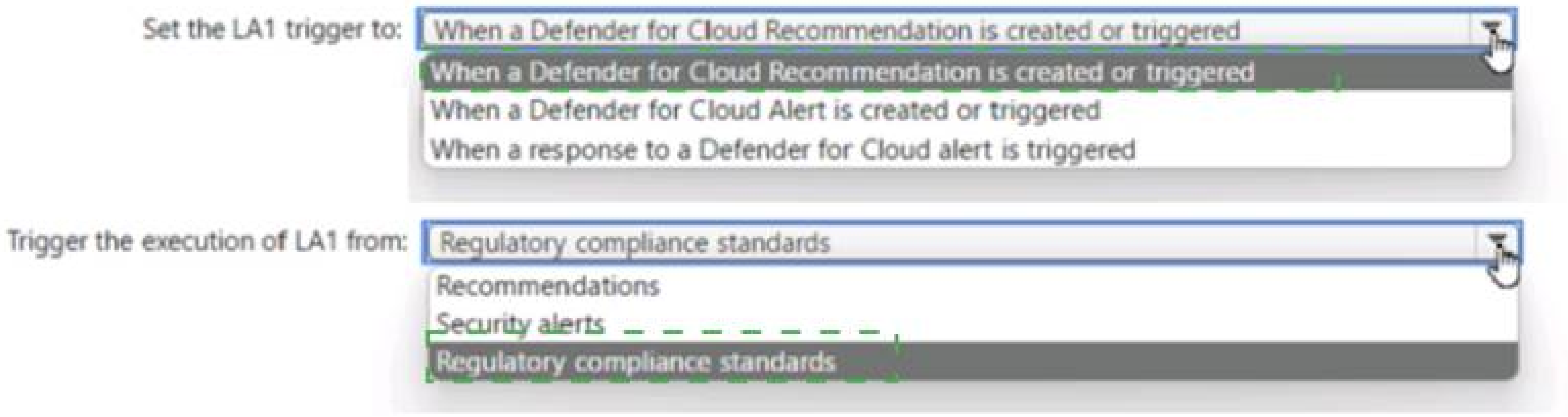

Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Recommendation is created or triggered
When a Defender for Cloud Alert is created or triggered
When a response to a Defender for Cloud alert is triggered

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:


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

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

NEW QUESTION 234
- (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 Regulatory compliance, you download the report.
Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

NEW QUESTION 239
- (Topic 4)
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.
B. Create an Azure logic appthat has a manual trigger
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic appthat has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Answer: AC

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

NEW QUESTION 241
- (Topic 4)
You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.
You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

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

Answer: B

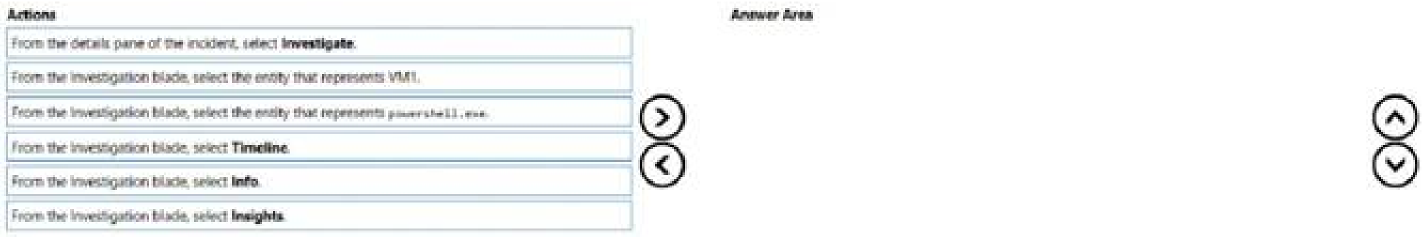
NEW QUESTION 245
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 250
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
? The modification of local group memberships
? The purging of event logs
Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

From the details pane of the incident, select **Investigate**.

From the investigation blade, select the entity that represents VM1.

From the investigation blade, select the entity that represents `powershell.exe`.

From the investigation blade, select **Timeline**.

From the investigation blade, select **Info**.

From the investigation blade, select **Insights**.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

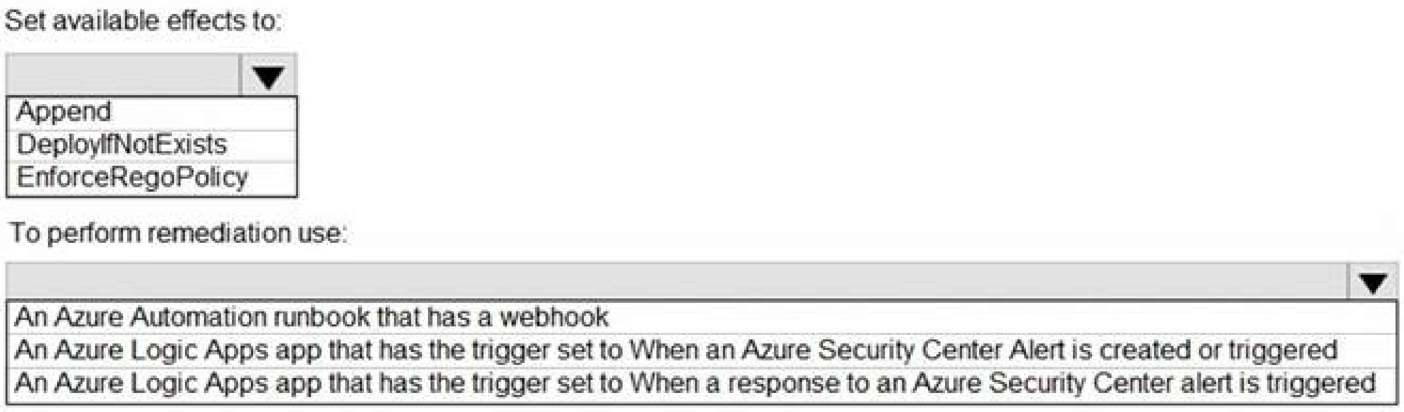
NEW QUESTION 255
- (Topic 4)
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

A. built-in queries
B. livestream
C. notebooks
D. bookmarks

Answer: C

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

NEW QUESTION 257
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

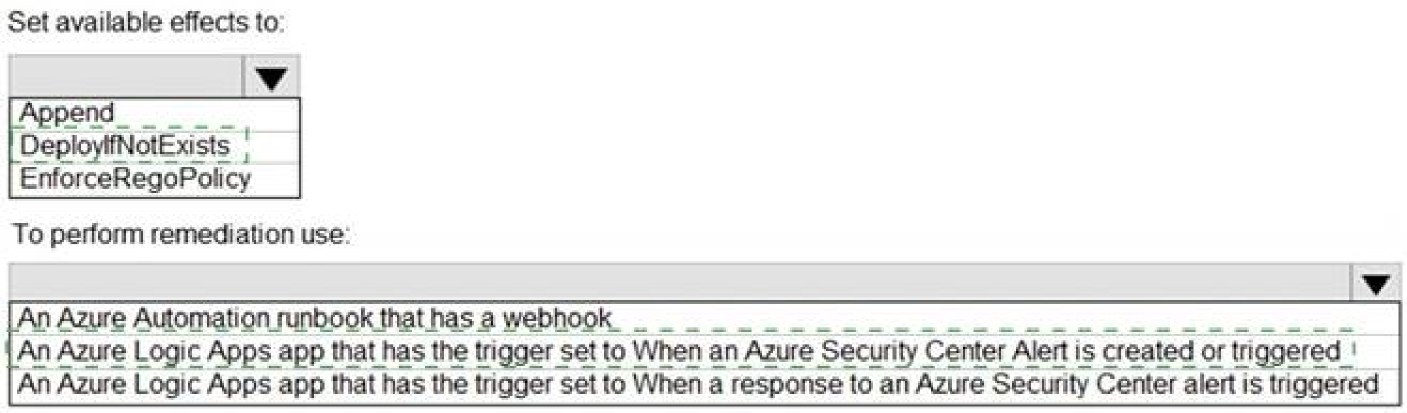
To perform remediation use:

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:



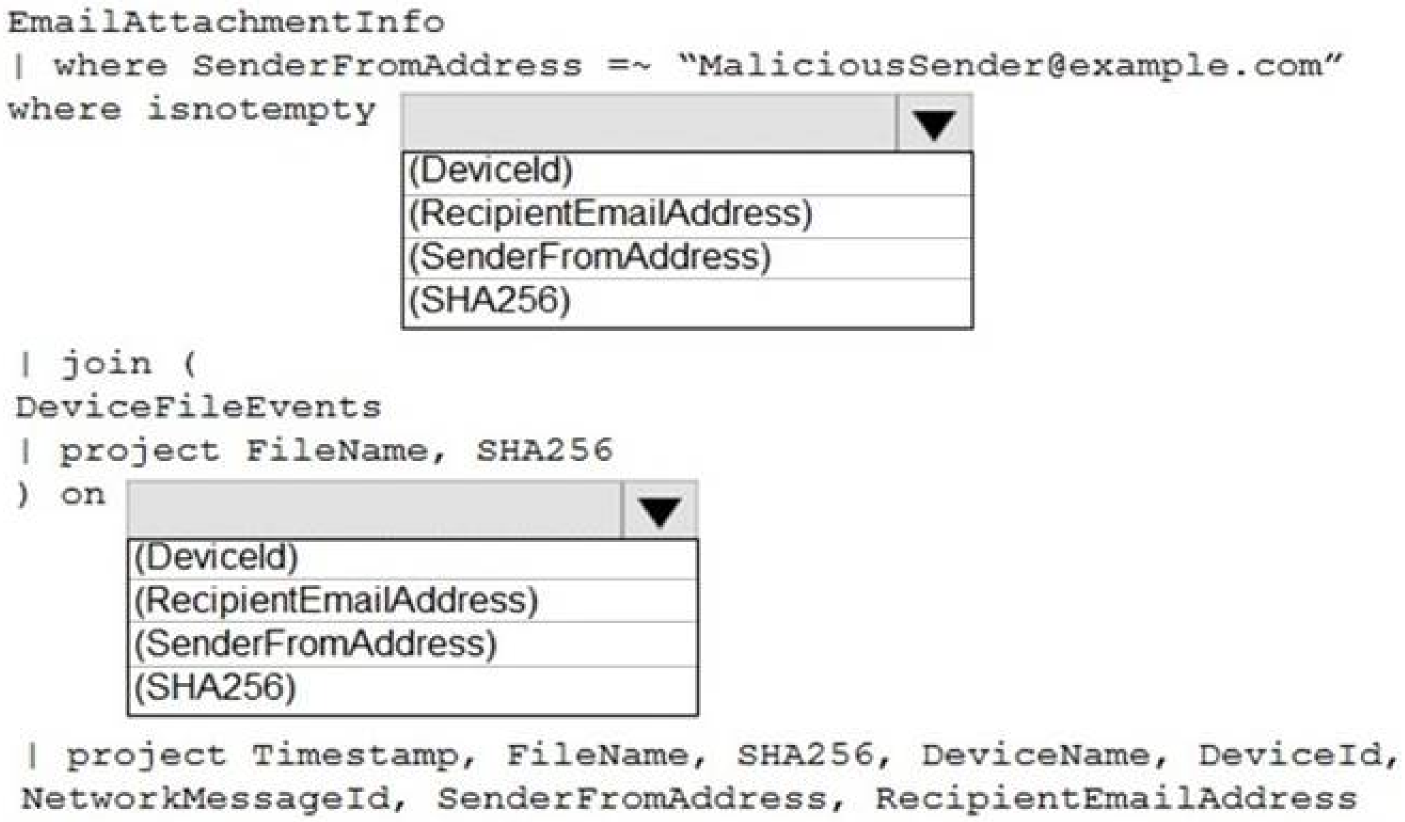
Set available effects to:

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 260
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on
```

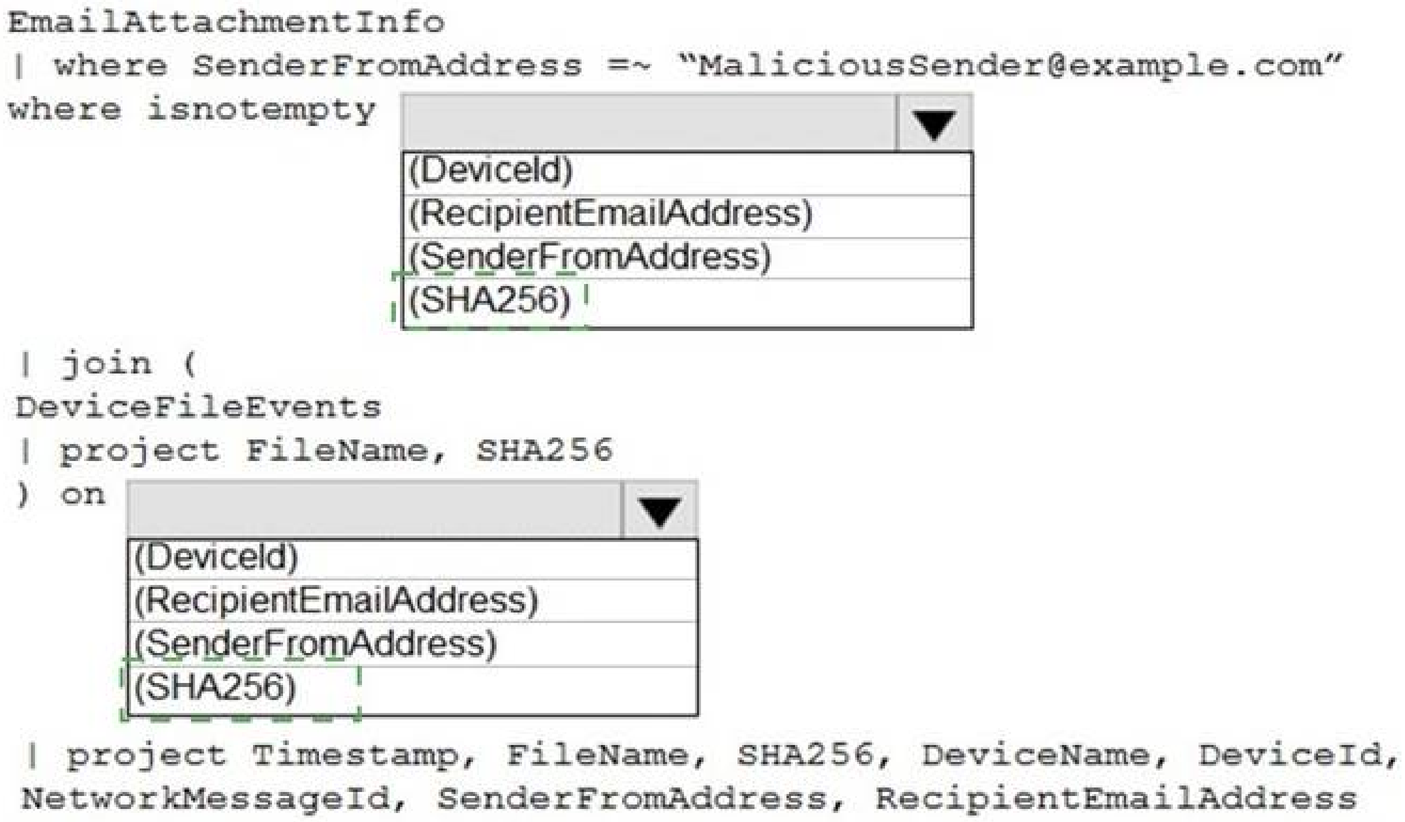
(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
[✓ (SHA256)]

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
[✓ (SHA256)]

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

NEW QUESTION 263
- (Topic 4)
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. What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.
B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.
C. From Regulatory compliance, download the report.
D. From Recommendations, download the CSV report.

Answer: B

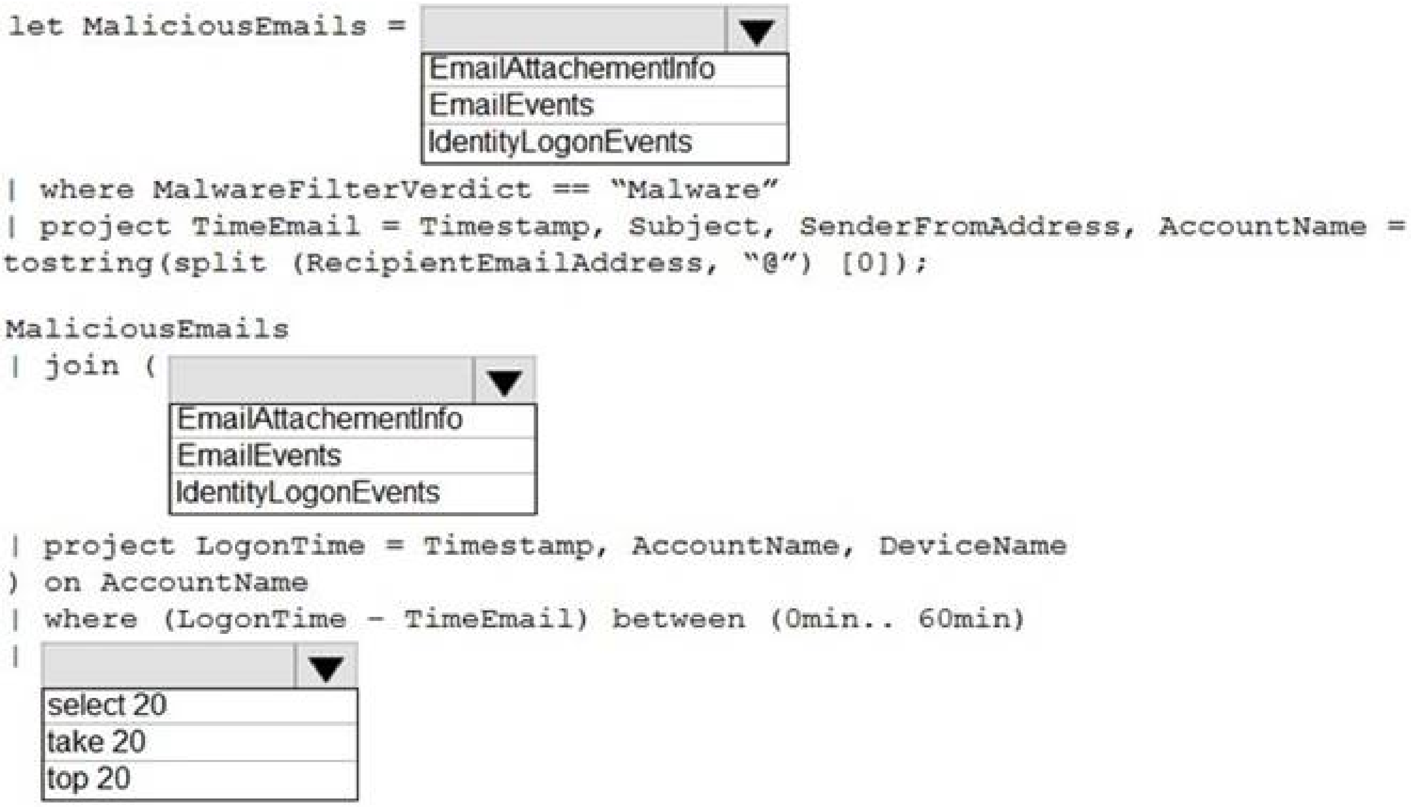
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and- responding-alerts

NEW QUESTION 268
- (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 269
HOTSPOT - (Topic 4)
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
How should you complete the query? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point.



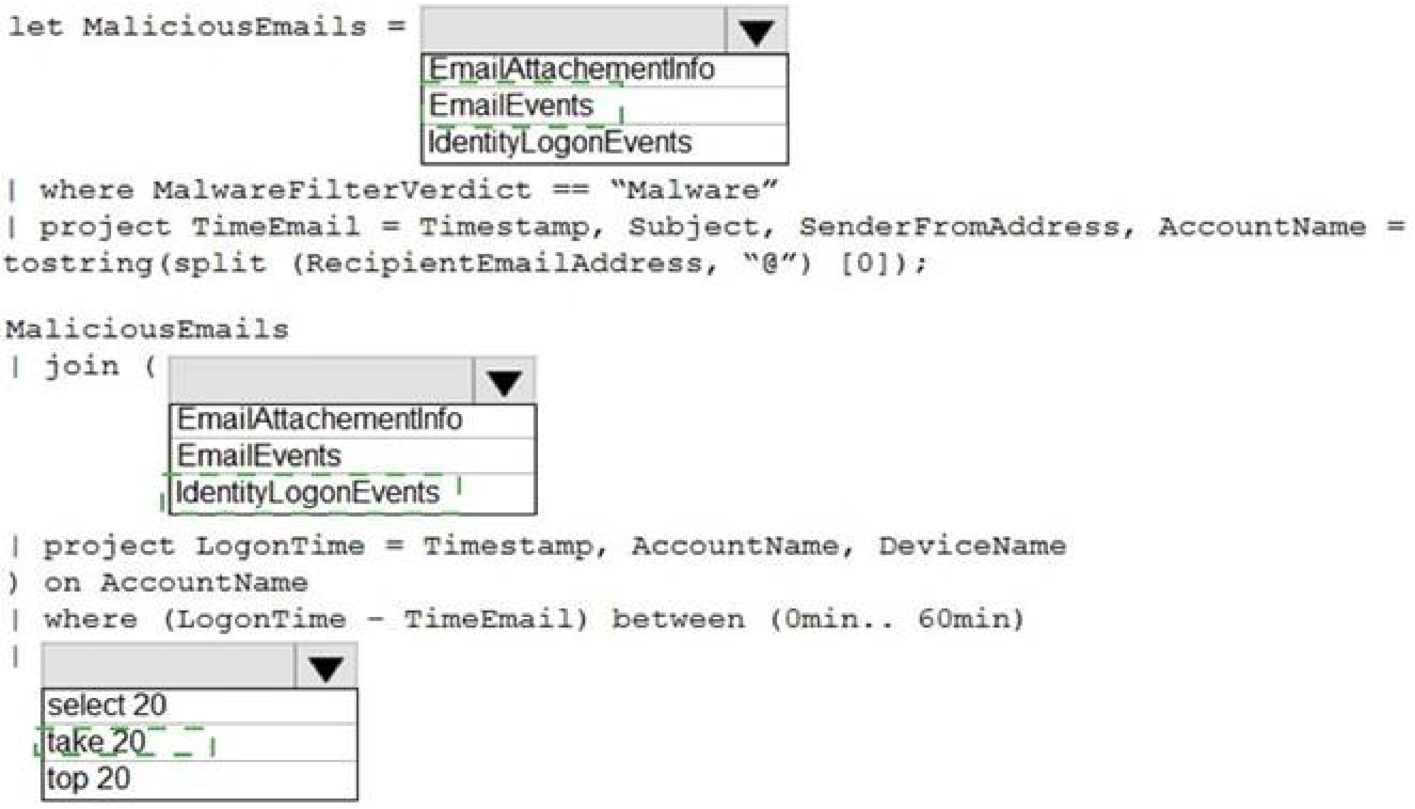
```
let MaliciousEmails = [▼ EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [▼ EmailAttachementInfo | EmailEvents | IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [▼ select 20 | take 20 | top 20]
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:



```
let MaliciousEmails =
    EmailAttachementInfo
    [✓ EmailEvents]
    IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
    EmailAttachementInfo
    EmailEvents
    [✓ IdentityLogonEvents]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
    select 20
    [✓ take 20]
    top 20
```

NEW QUESTION 274

......