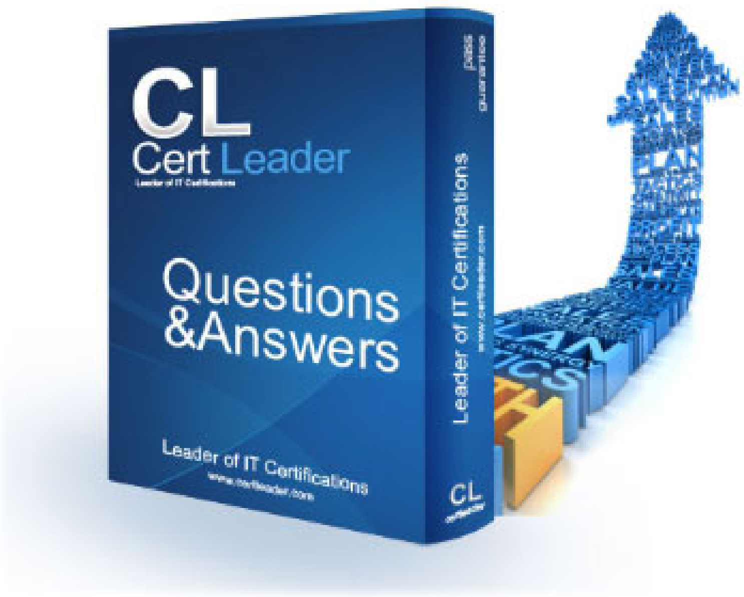
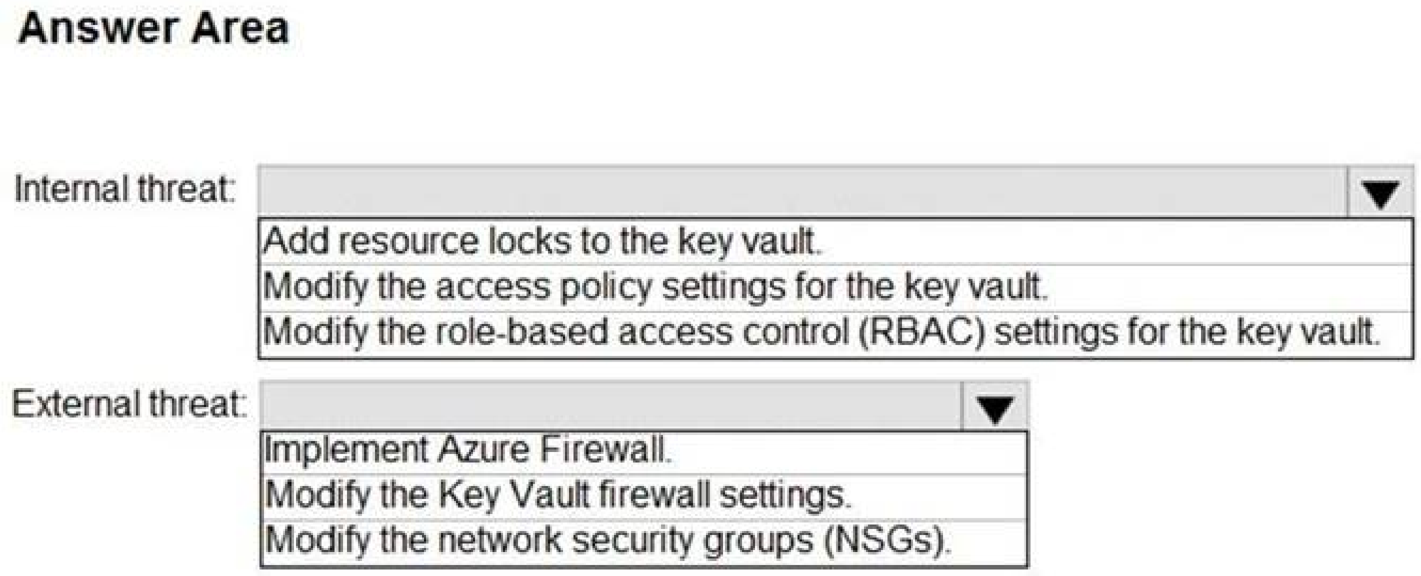
SC-200 Dumps

Microsoft Security Operations Analyst

https://www.certleader.com/SC-200-dumps.html



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



Answer Area

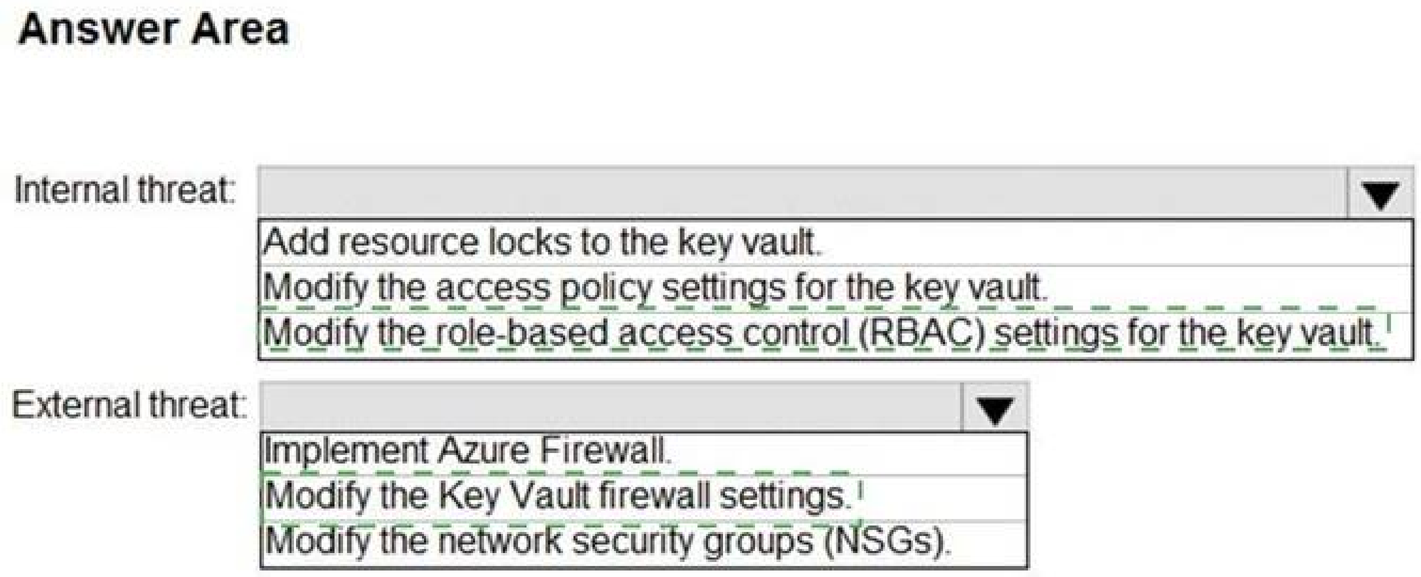
Internal threat:
- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Modify the role-based access control (RBAC) settings for the key vault.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

NEW QUESTION 2
- (Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive
B. marketing
C. security
D. sales

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb- and-teams? view=o365-worldwide

NEW QUESTION 3
- (Topic 1)
You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway

Answer: B

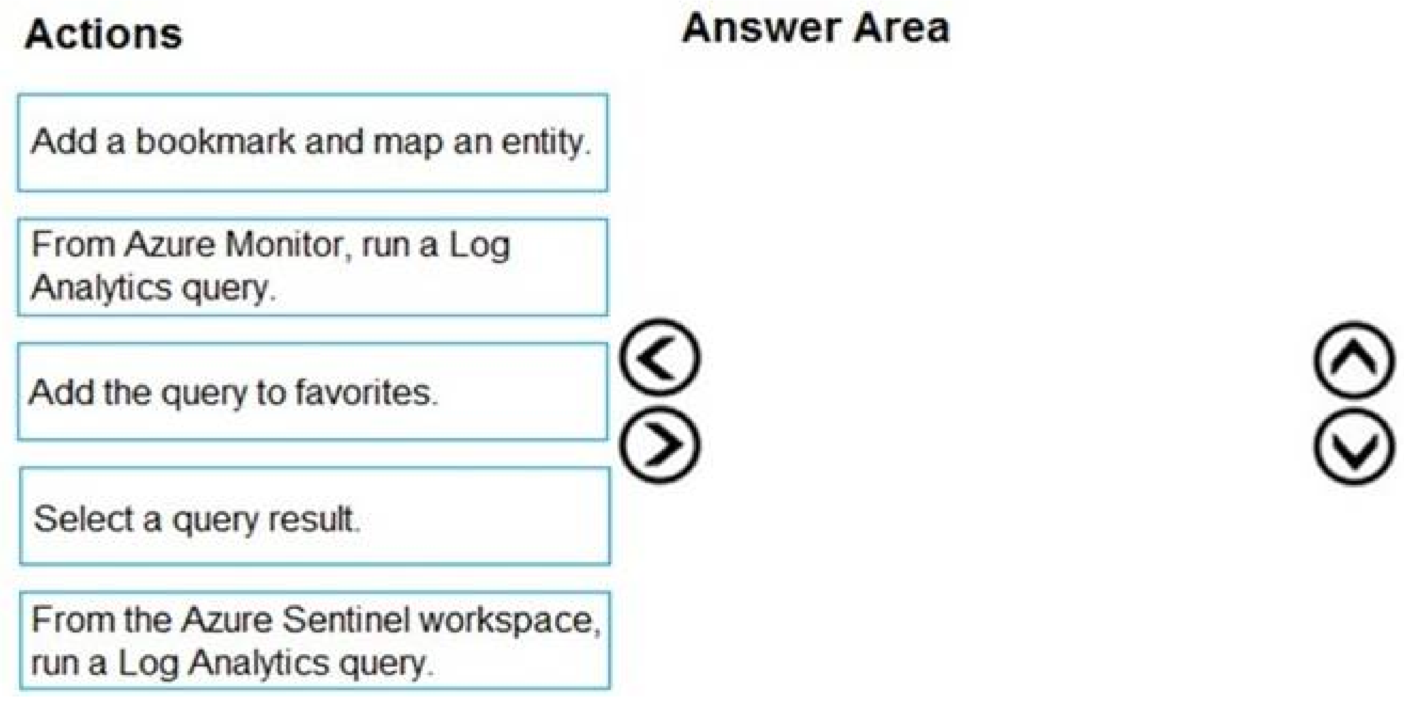
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

NEW QUESTION 4
- (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 5
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

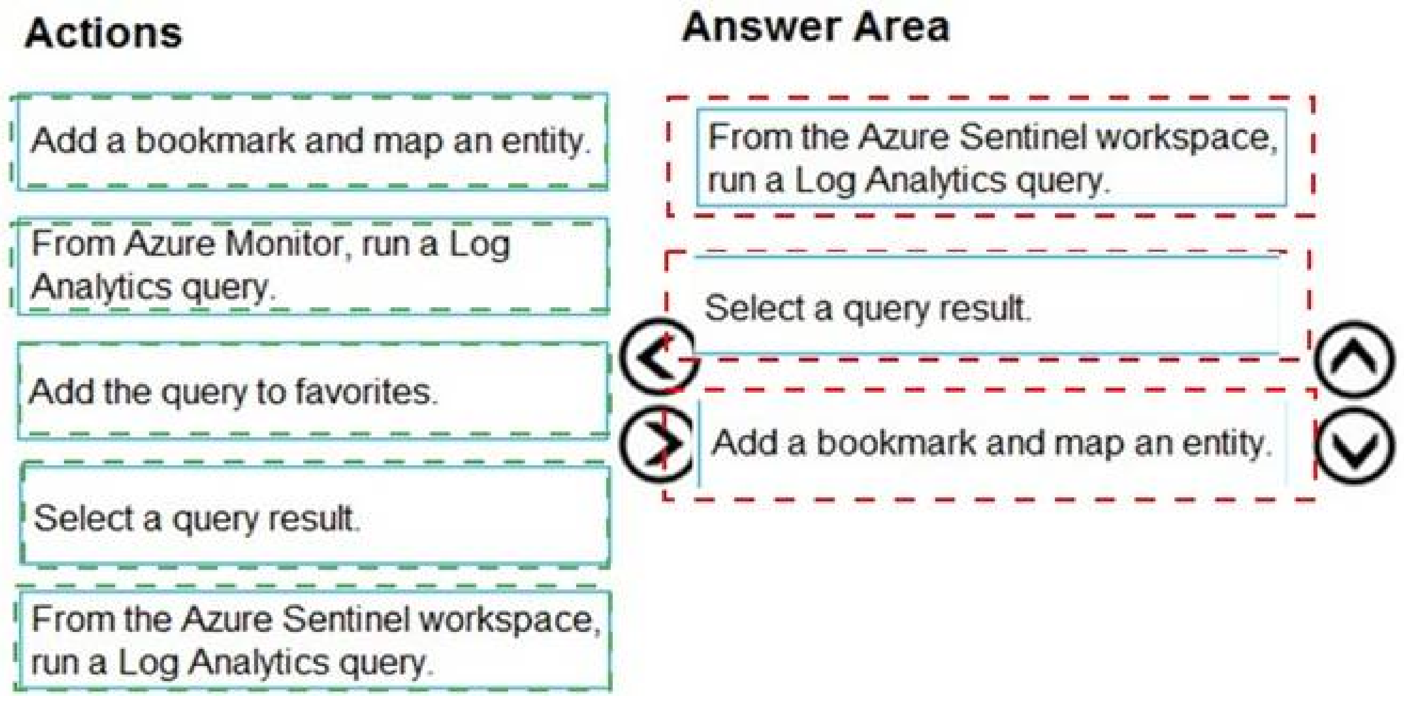
From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

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

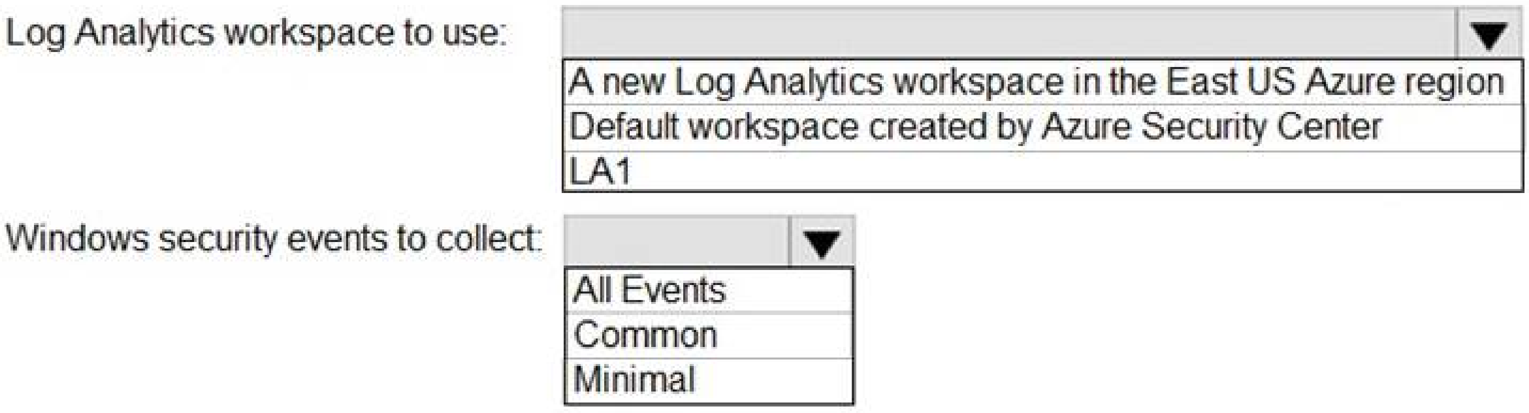
Answer Area

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

Select a query result.

Add a bookmark and map an entity.

NEW QUESTION 6
HOTSPOT - (Topic 2)
You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



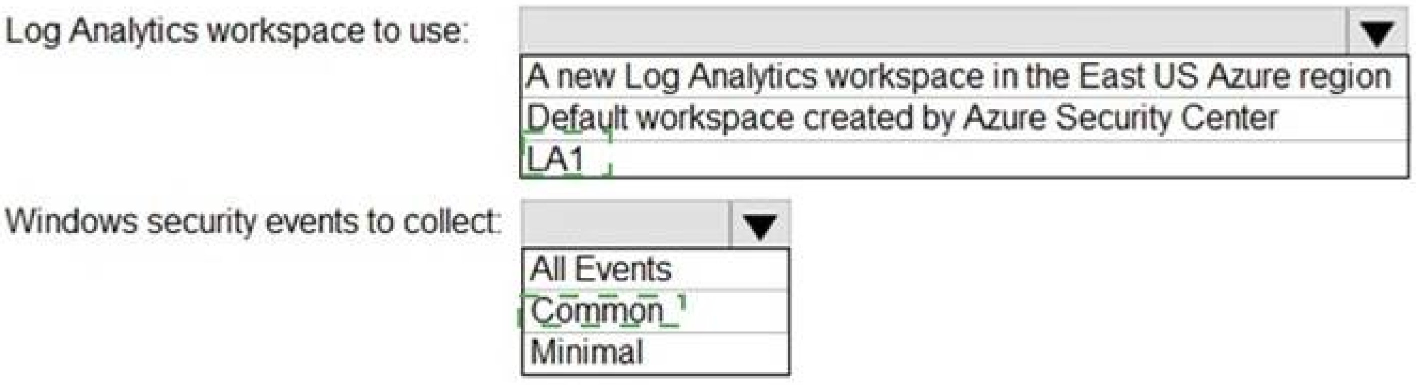
Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- LA1

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

A. Mastered
B. Not Mastered

Answer: A

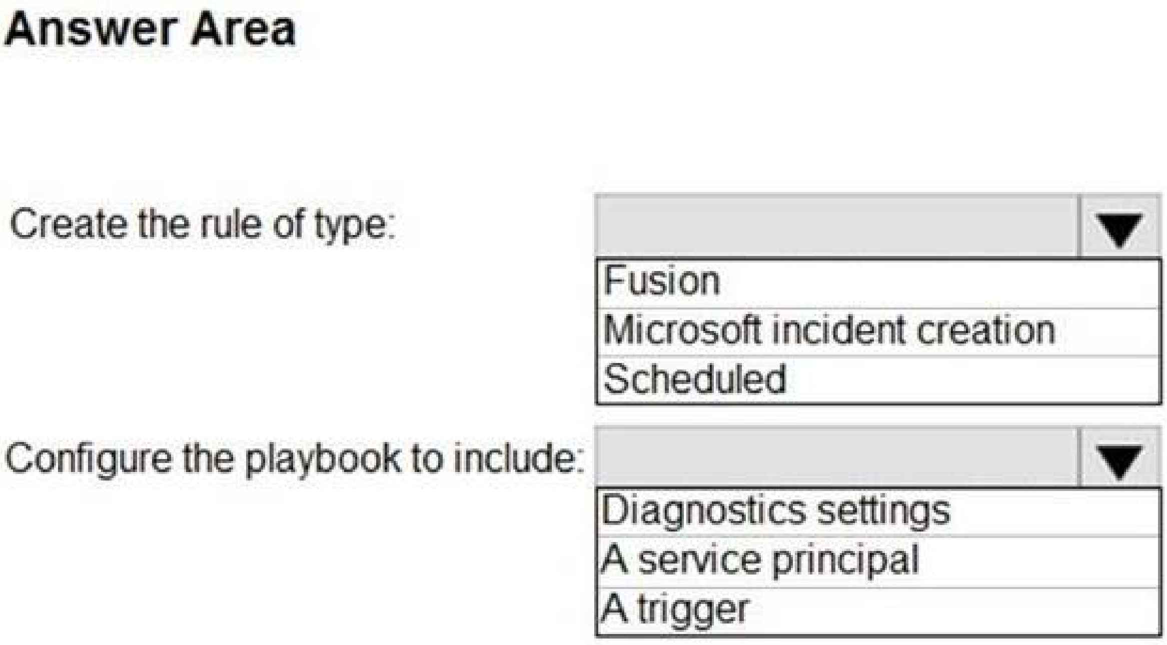
Explanation:



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

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

NEW QUESTION 7
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

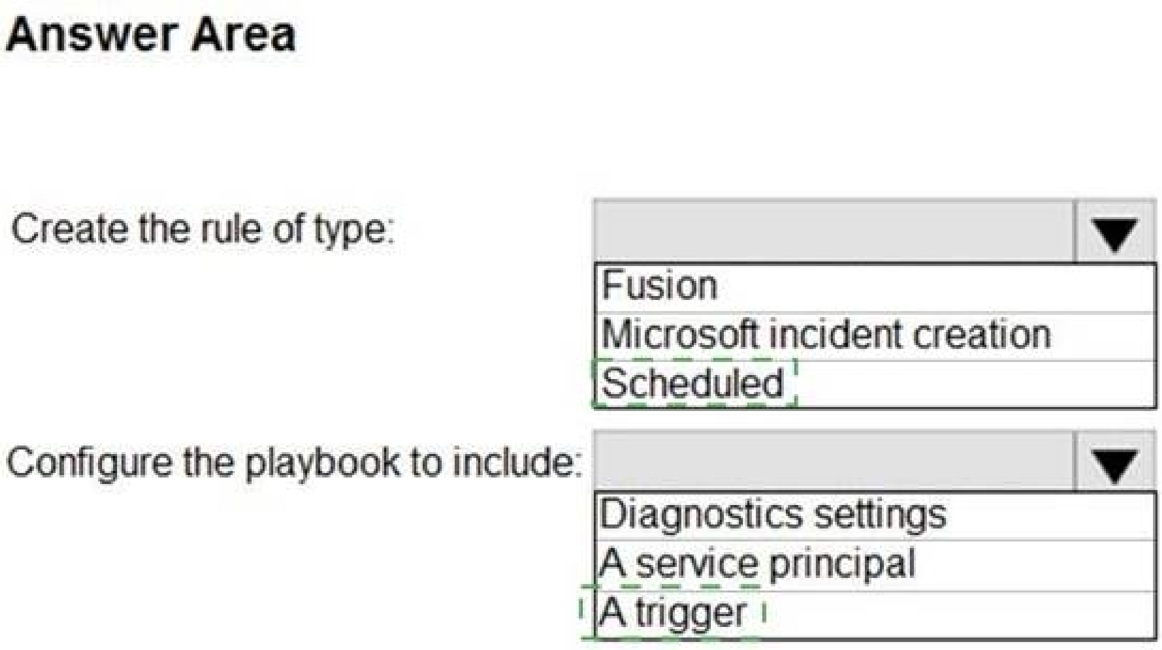
Create the rule of type:
- Fusion
- Microsoft incident creation
- Scheduled

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

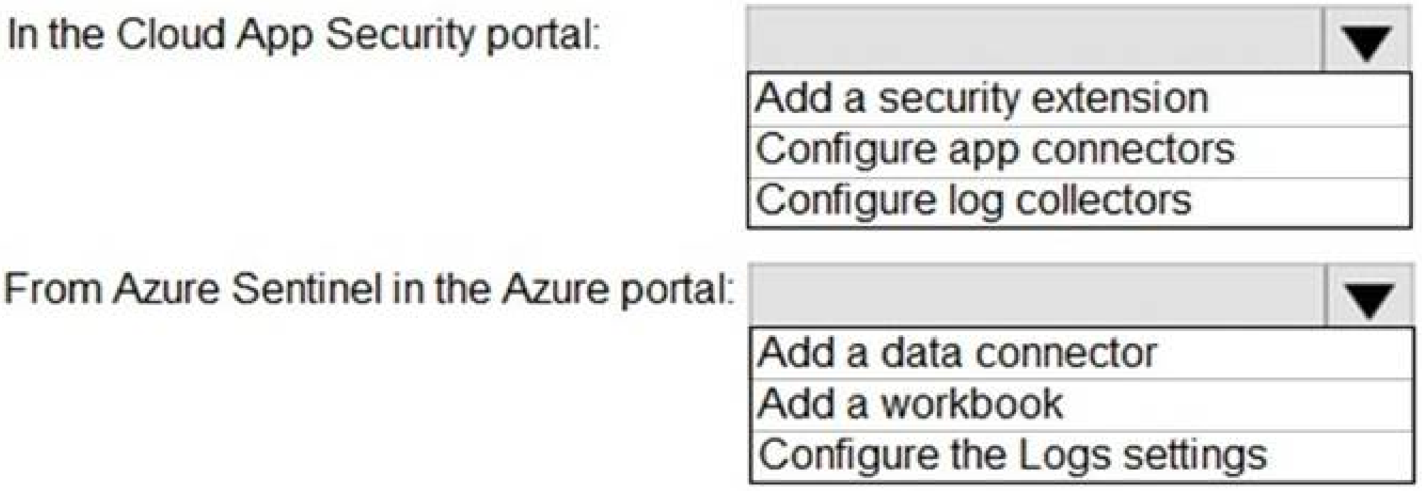


Answer Area

Create the rule of type:
Fusion
Microsoft incident creation
[✓ Scheduled]

Configure the playbook to include:
Diagnostics settings
A service principal
[✓ A trigger]

NEW QUESTION 8
HOTSPOT - (Topic 2)
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



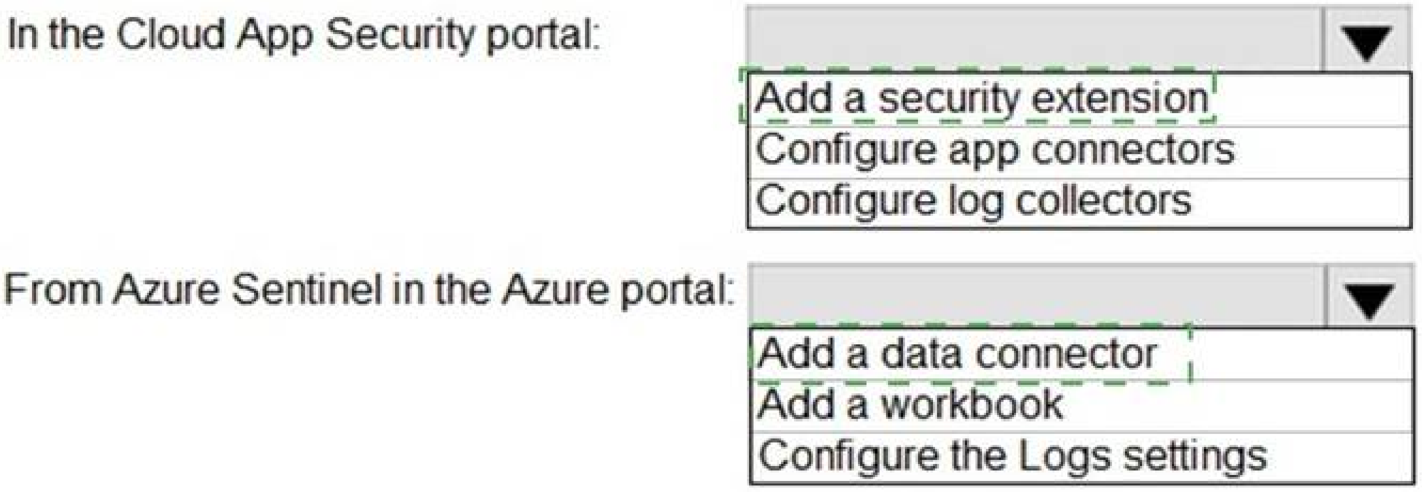
In the Cloud App Security portal:
Add a security extension
Configure app connectors
Configure log collectors

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

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

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

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

Answer: CD

Explanation:
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

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

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

Answer: C

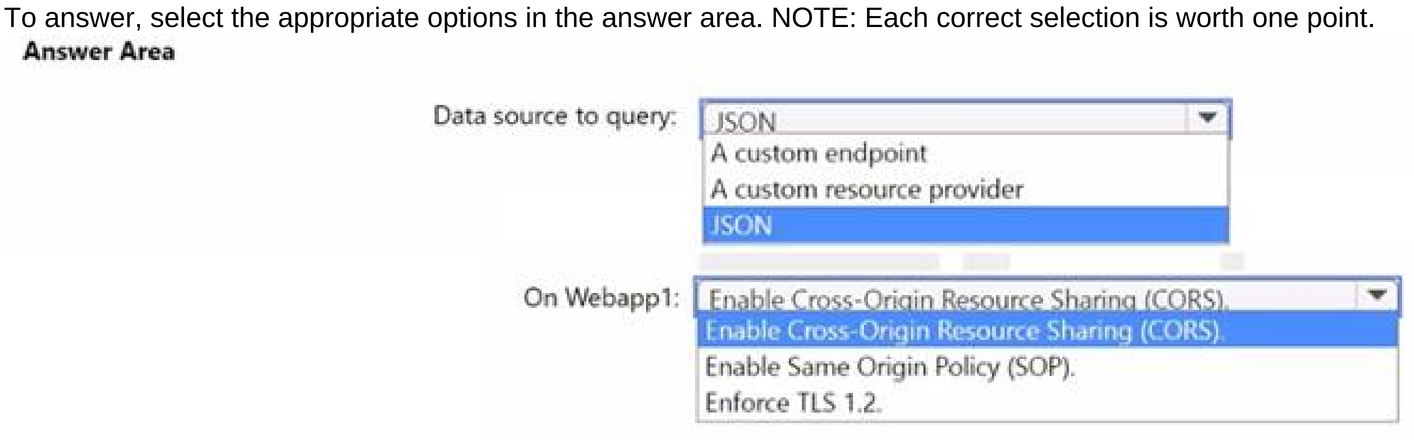
NEW QUESTION 10
- (Topic 2)
You need to implement the Azure Information Protection requirements. What should you configure first?

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

Answer: D

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

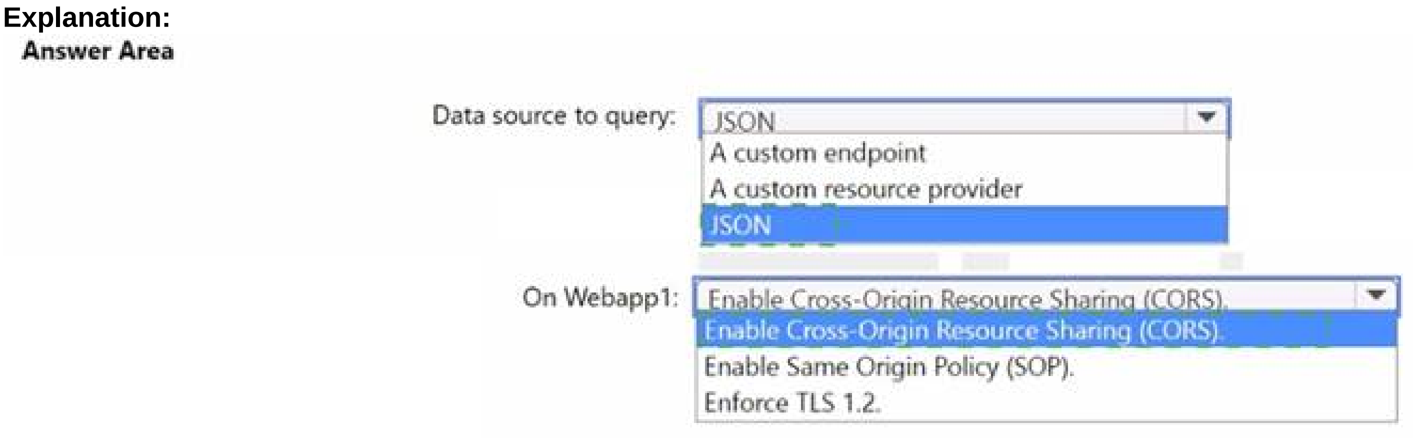
NEW QUESTION 14
HOTSPOT - (Topic 3)
You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


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:

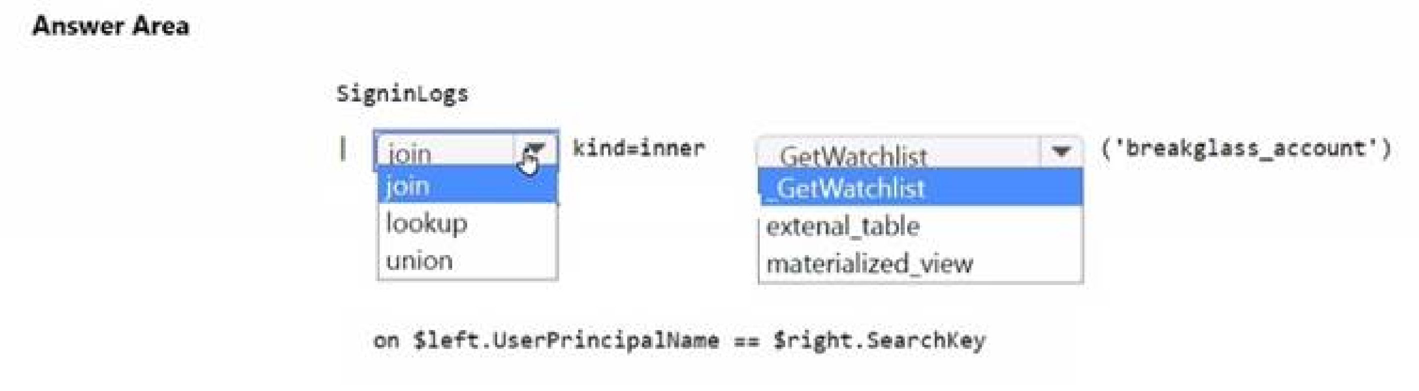

Answer Area
Data source to query:
JSON
A custom endpoint
A custom resource provider
JSON
On Webapp1:
Enable Cross-Origin Resource Sharing (CORS).
Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

NEW QUESTION 17
- (Topic 3)
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

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

Answer: D

NEW QUESTION 19
HOTSPOT - (Topic 3)
You need to implement the Microsoft Sentinel NRT rule for monitoring the designated break glass account. The solution must meet the Microsoft Sentinel requirements.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



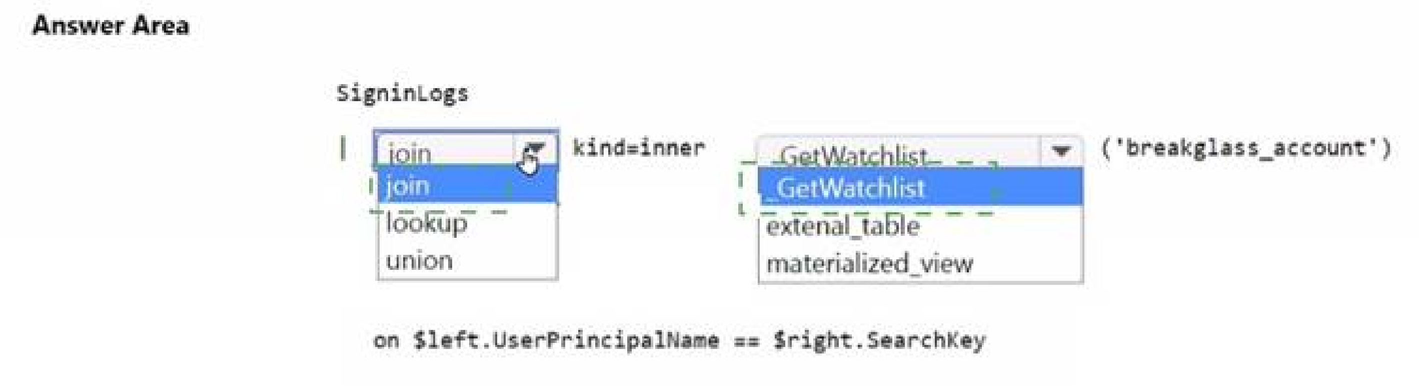
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 21
- (Topic 3)
You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.
What should you create first?

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

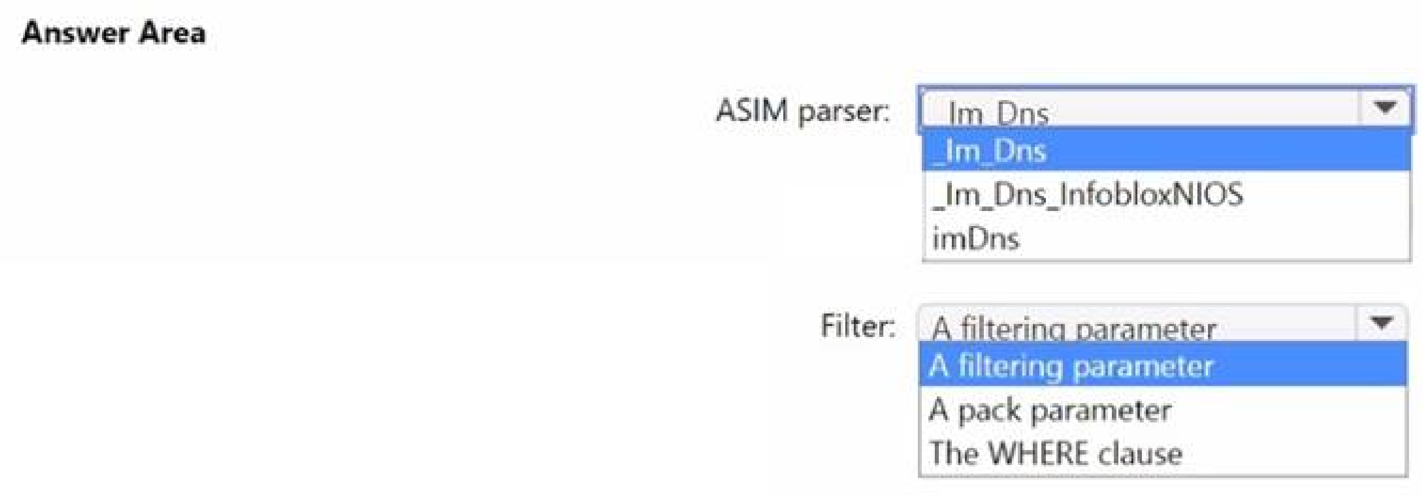
Answer: A

NEW QUESTION 25
- (Topic 3)
You need to implement the Defender for Cloud requirements. Which subscription-level role should you assign to Group1?

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

Answer: B

NEW QUESTION 26
HOTSPOT - (Topic 3)
You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

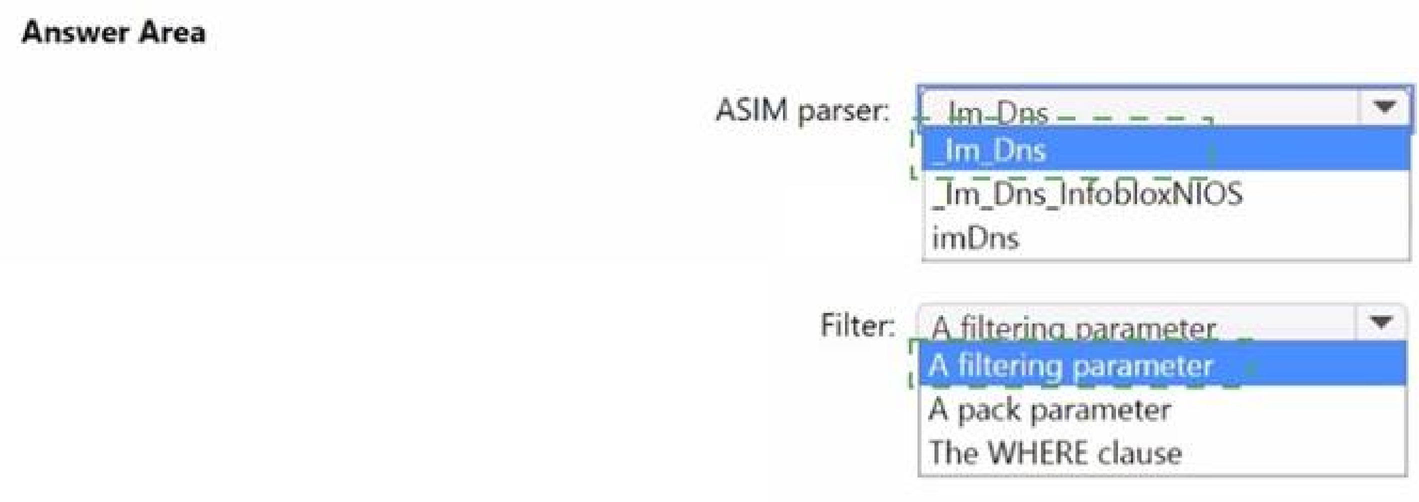
ASIM parser: Im_Dns

Filter: A filtering parameter

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

ASIM parser: _Im_Dns
- _Im_Dns
- _Im_Dns_InfobloxNIOS
- imDns

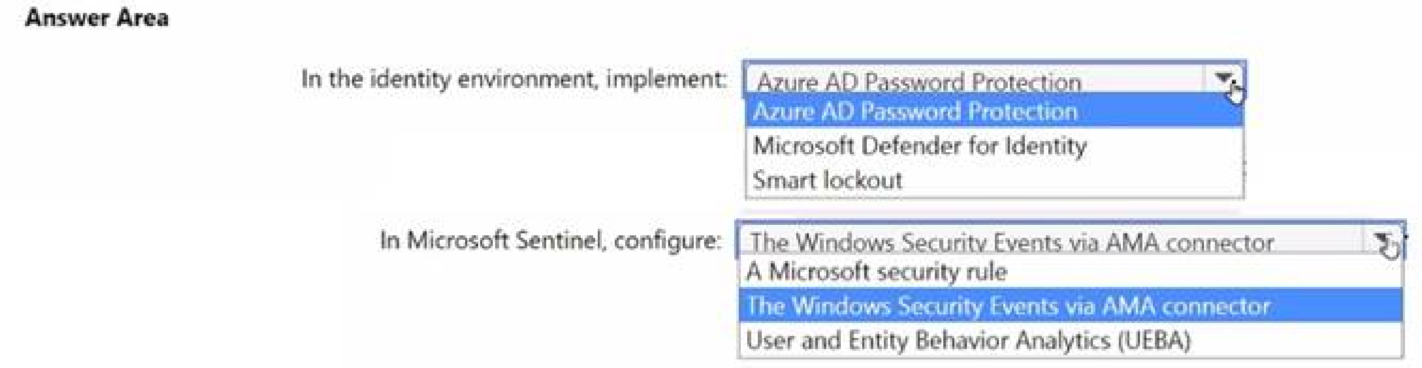
Filter: A filtering parameter
- A filtering parameter
- A pack parameter
- The WHERE clause

NEW QUESTION 27

HOTSPOT - (Topic 3)

You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.

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



Answer Area

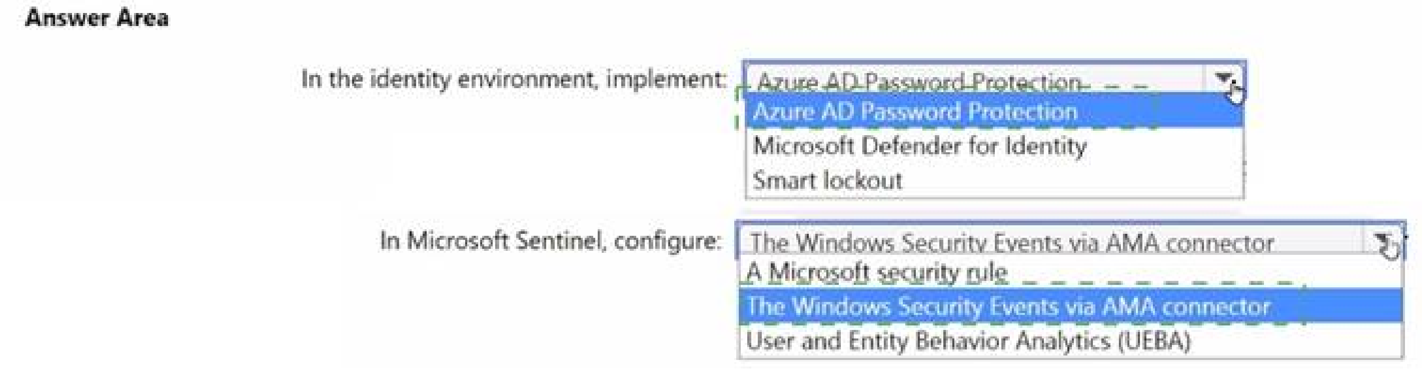
In the identity environment, implement: Azure AD Password Protection
- Azure AD Password Protection
- Microsoft Defender for Identity
- Smart lockout

In Microsoft Sentinel, configure: The Windows Security Events via AMA connector
- A Microsoft security rule
- The Windows Security Events via AMA connector
- User and Entity Behavior Analytics (UEBA)

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

In the identity environment, implement: Azure AD Password Protection
- Azure AD Password Protection
- Microsoft Defender for Identity
- Smart lockout

In Microsoft Sentinel, configure: The Windows Security Events via AMA connector
- A Microsoft security rule
- The Windows Security Events via AMA connector
- User and Entity Behavior Analytics (UEBA)

NEW QUESTION 32

- (Topic 4)

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: BC

Explanation:

B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.

C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

NEW QUESTION 33

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

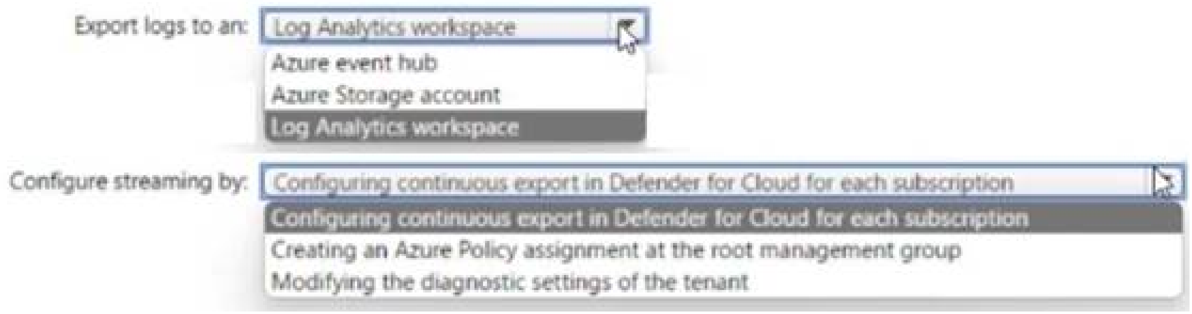
A. Security solutions
B. Security policy
C. Pricing & settings
D. Security alerts
E. Azure Defender

Answer: C

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

NEW QUESTION 36
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



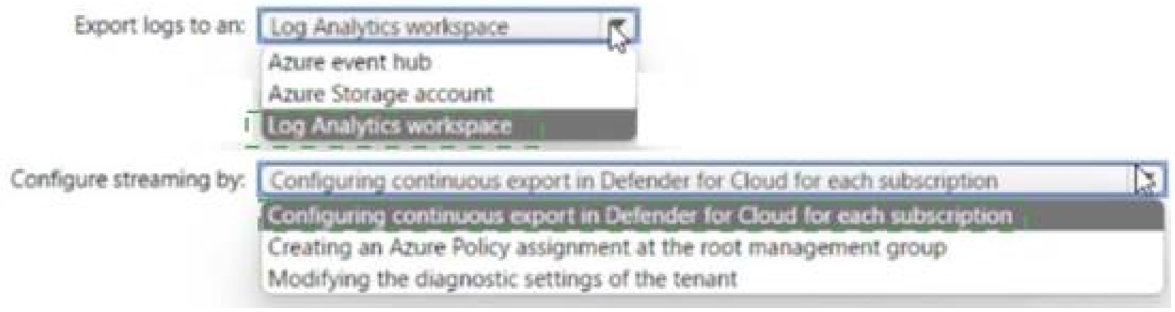
Export logs to an: Log Analytics workspace
Azure event hub
Azure Storage account
Log Analytics workspace

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 37
- (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 38
- (Topic 4)
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

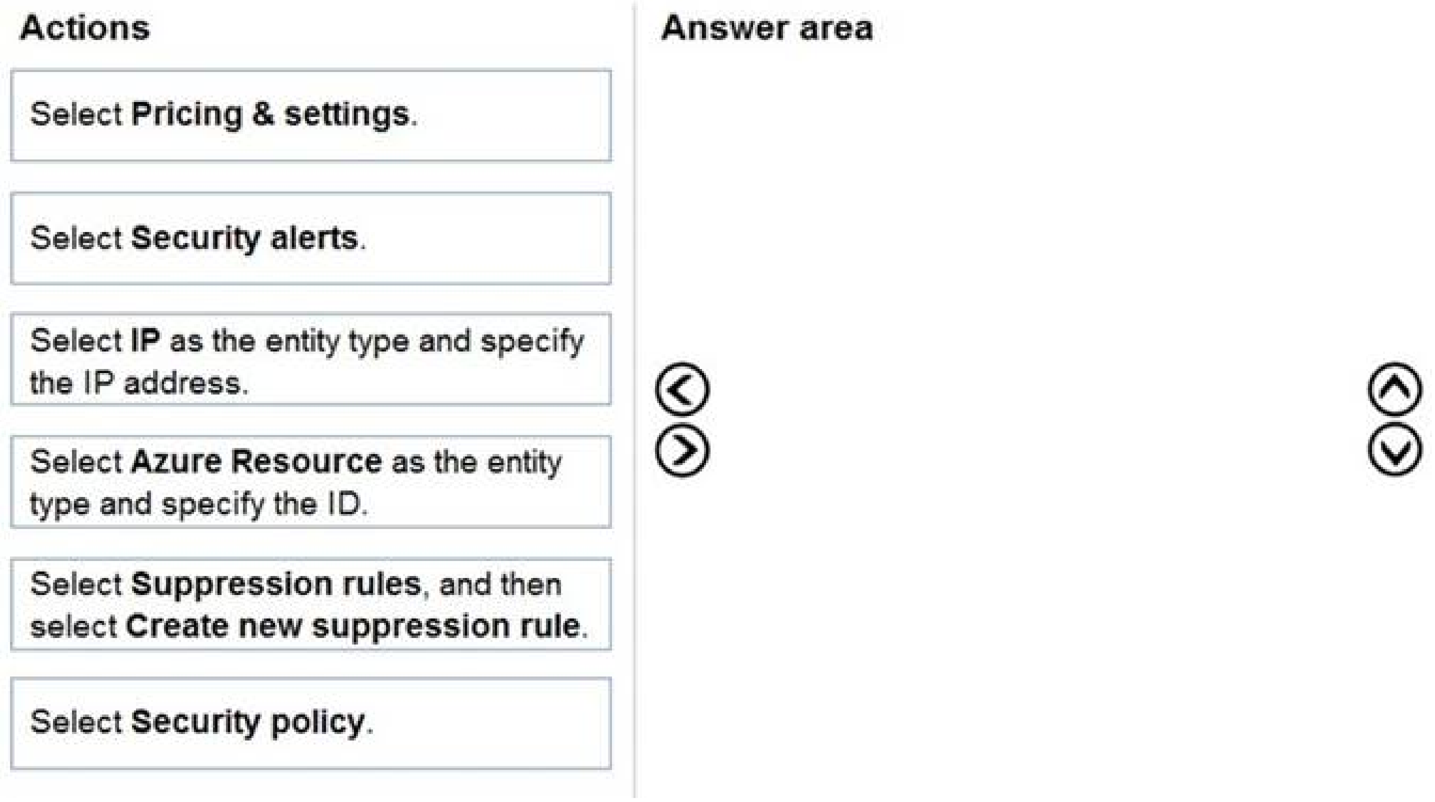
A. There are connectivity issues between the data sources and Log Analytics.
B. The number of alerts exceeded 10,000 within two minutes.

C. The rule query takes too long to run and times out.
D. Permissions to one of the data sources of the rule query were modified.

Answer: D

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

NEW QUESTION 39
DRAG DROP - (Topic 4)
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.



Actions

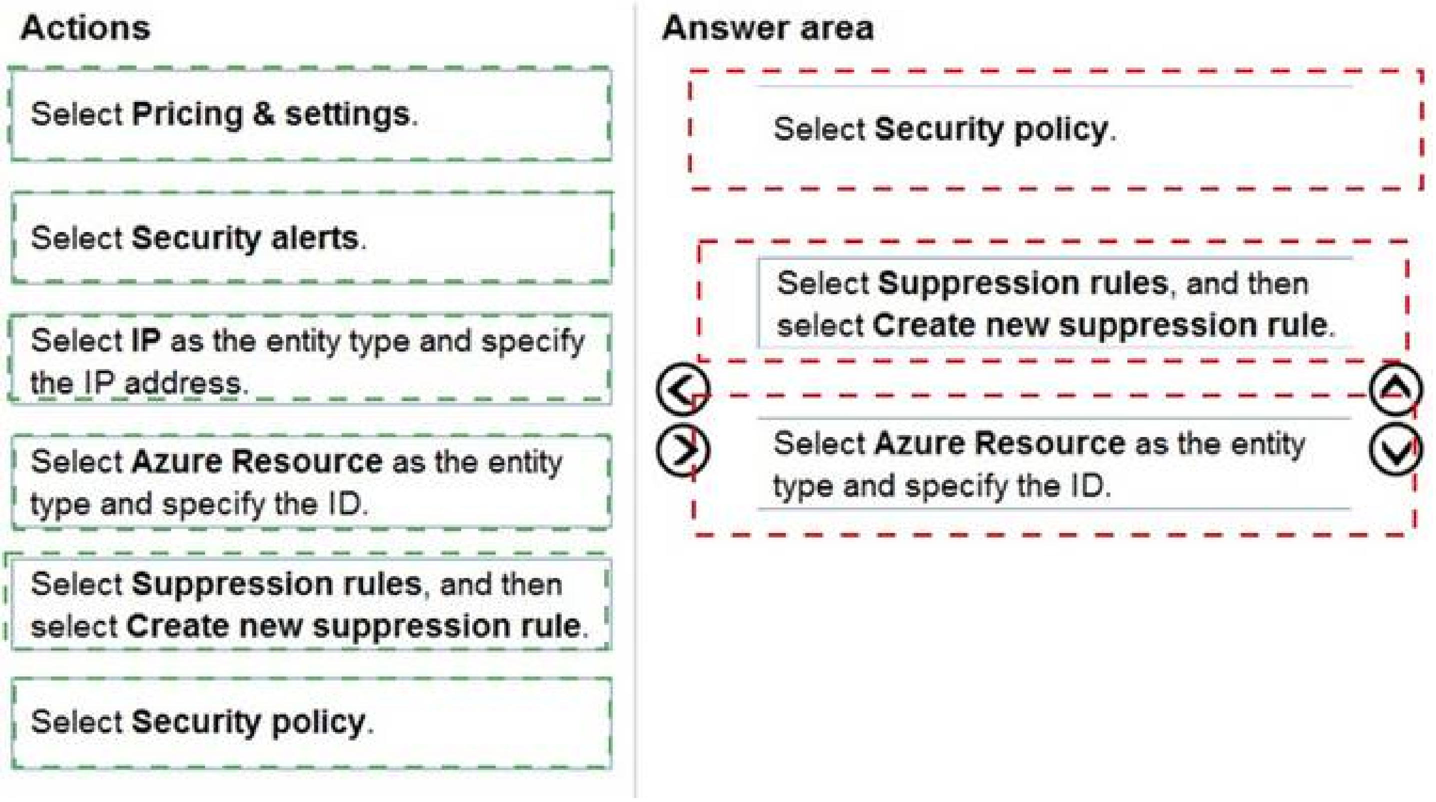
- Select **Pricing & settings**.
- Select **Security alerts**.
- Select **IP** as the entity type and specify the IP address.
- Select **Azure Resource** as the entity type and specify the ID.
- Select **Suppression rules**, and then select **Create new suppression rule**.
- Select **Security policy**.

Answer area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

- Select **Pricing & settings**.
- Select **Security alerts**.
- Select **IP** as the entity type and specify the IP address.
- Select **Azure Resource** as the entity type and specify the ID.
- Select **Suppression rules**, and then select **Create new suppression rule**.
- Select **Security policy**.

Answer area

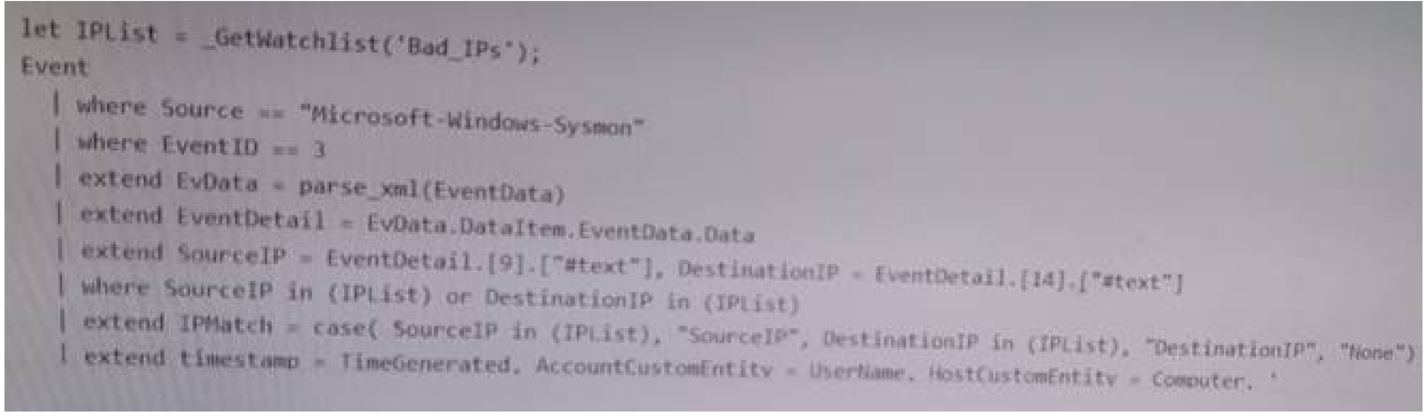
1. Select **Security policy**.
2. Select **Suppression rules**, and then select **Create new suppression rule**.
3. Select **Azure Resource** as the entity type and specify the ID.

NEW QUESTION 41
- (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?

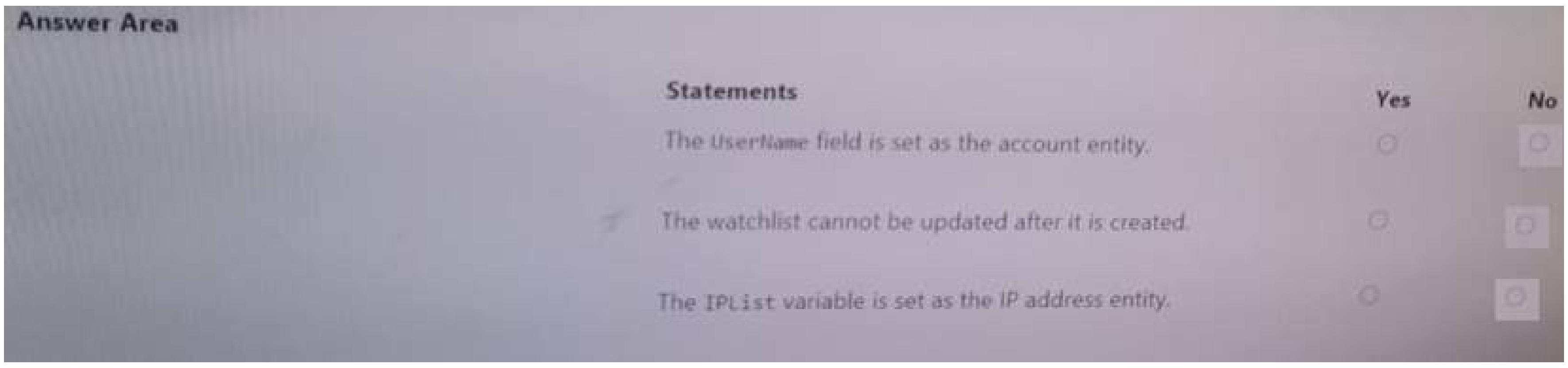
A. Modify the properties of the connector.
B. Create a Data Collection Rule (DCR).
C. Create a scheduled query rule.
D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

NEW QUESTION 46
HOTSPOT - (Topic 4)
You have the following SQL 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, '
```



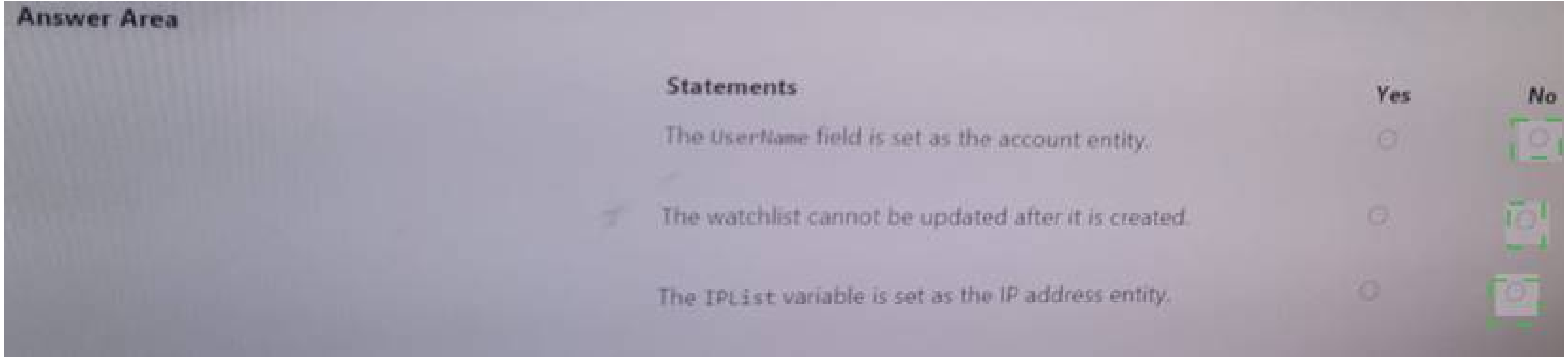
Answer Area

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

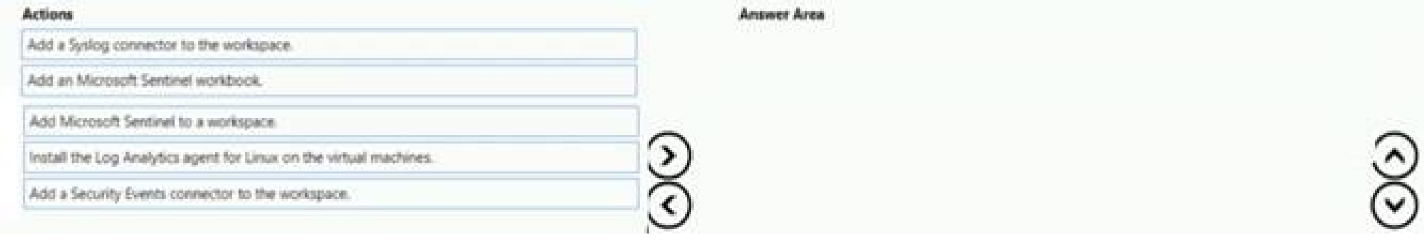
Explanation:



Answer Area

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 51
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

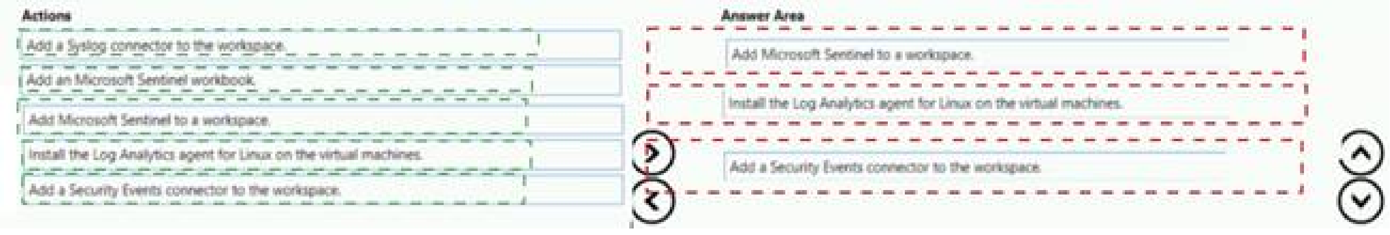
- Add a Syslog connector to the workspace.
- Add an Microsoft Sentinel workbook.
- Add Microsoft Sentinel to a workspace.
- Install the Log Analytics agent for Linux on the virtual machines.
- Add a Security Events connector to the workspace.

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.

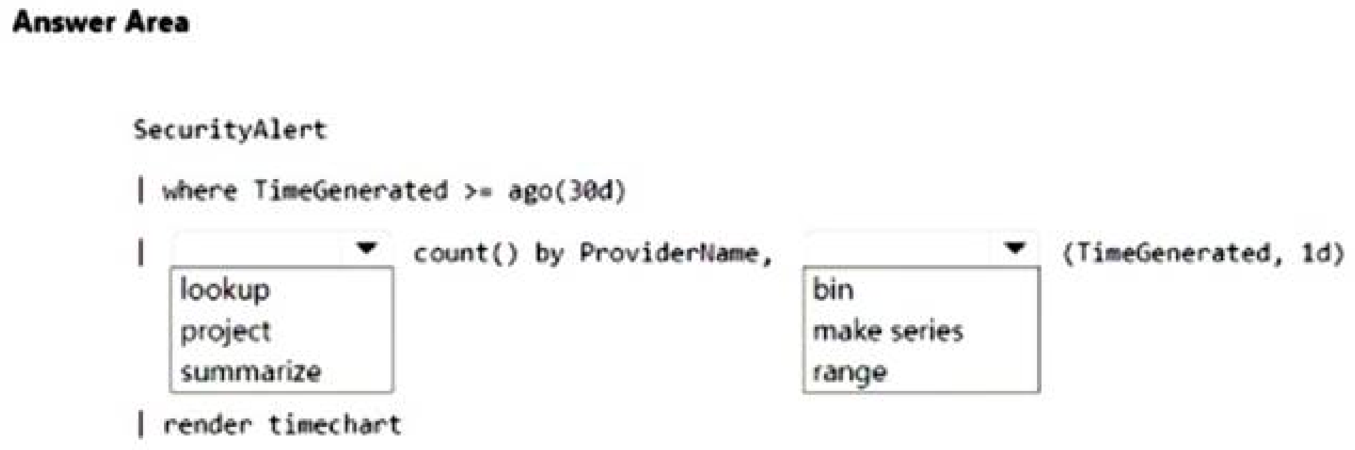
NEW QUESTION 53
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel. You detect a new threat by using a hunting query.
You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.
What should you do?

A. Create a playbook.
B. Create a watchlist.
C. Create an analytics rule.
D. Add the query to a workbook.

Answer: A

Explanation:
By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected. Reference: https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule

NEW QUESTION 57
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:
• Identify alerts that occurred during the last 30 days.
• Display the results in a timechart.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



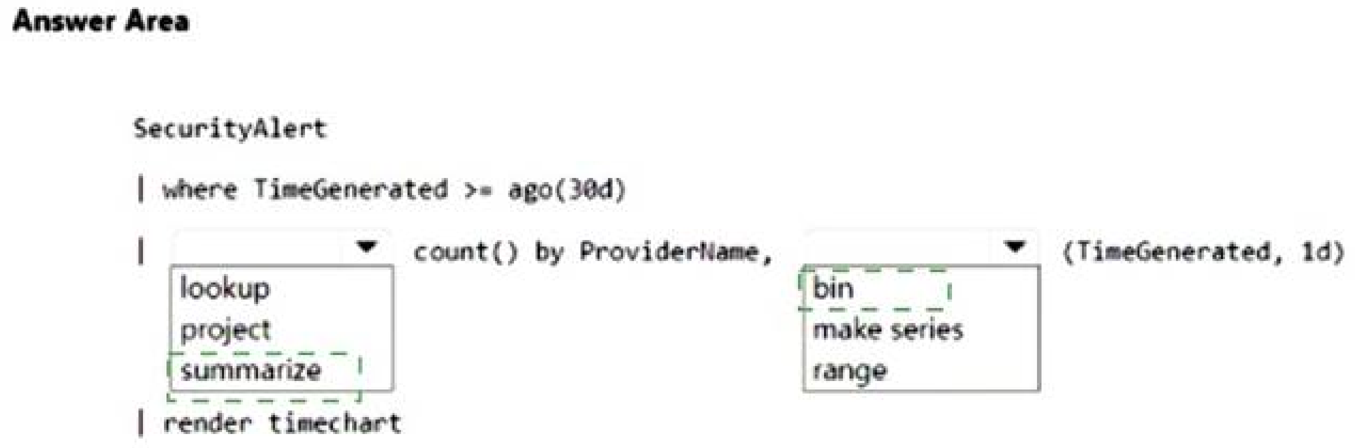
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

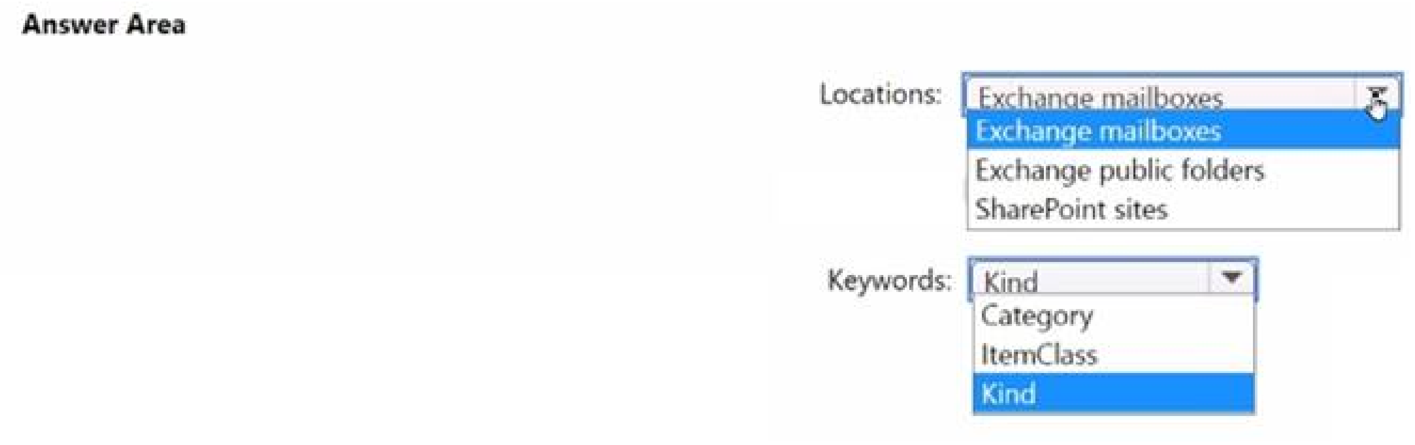
Explanation:



Answer Area

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

NEW QUESTION 59
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.
How should you configure the content search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

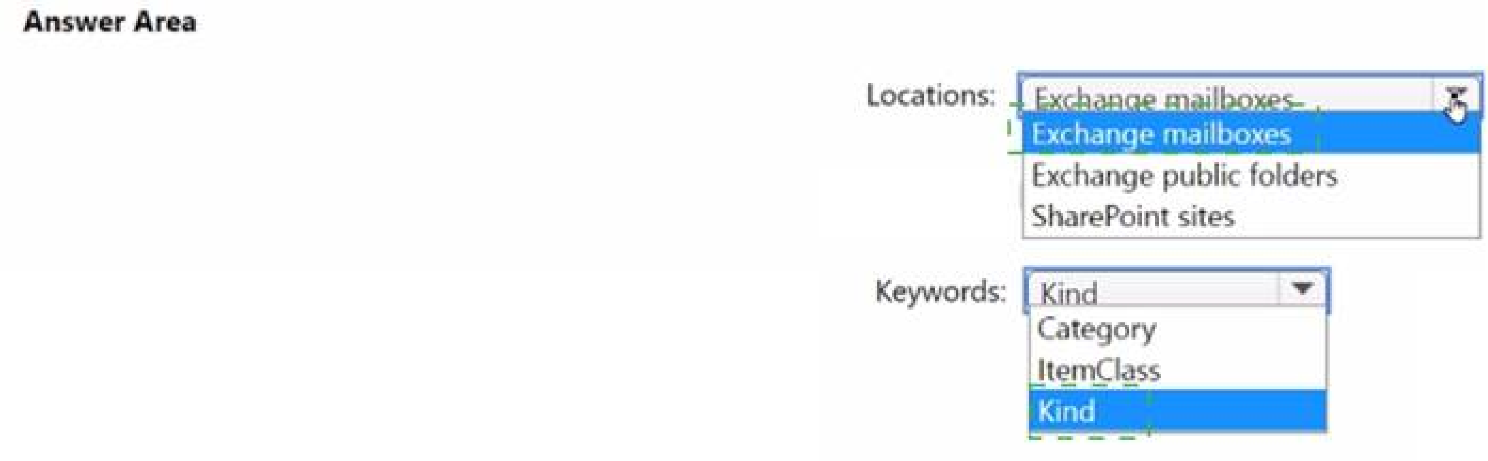
Locations: Exchange mailboxes

Keywords: Kind

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Locations: Exchange mailboxes

Keywords: Kind

NEW QUESTION 61

- (Topic 4)
You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts. What should you do?

A. Disable, and then enable the rule.
B. Add data connectors
C. Create a new machine learning analytics rule.
D. Add a hunting bookmark.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

NEW QUESTION 64

- (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 66

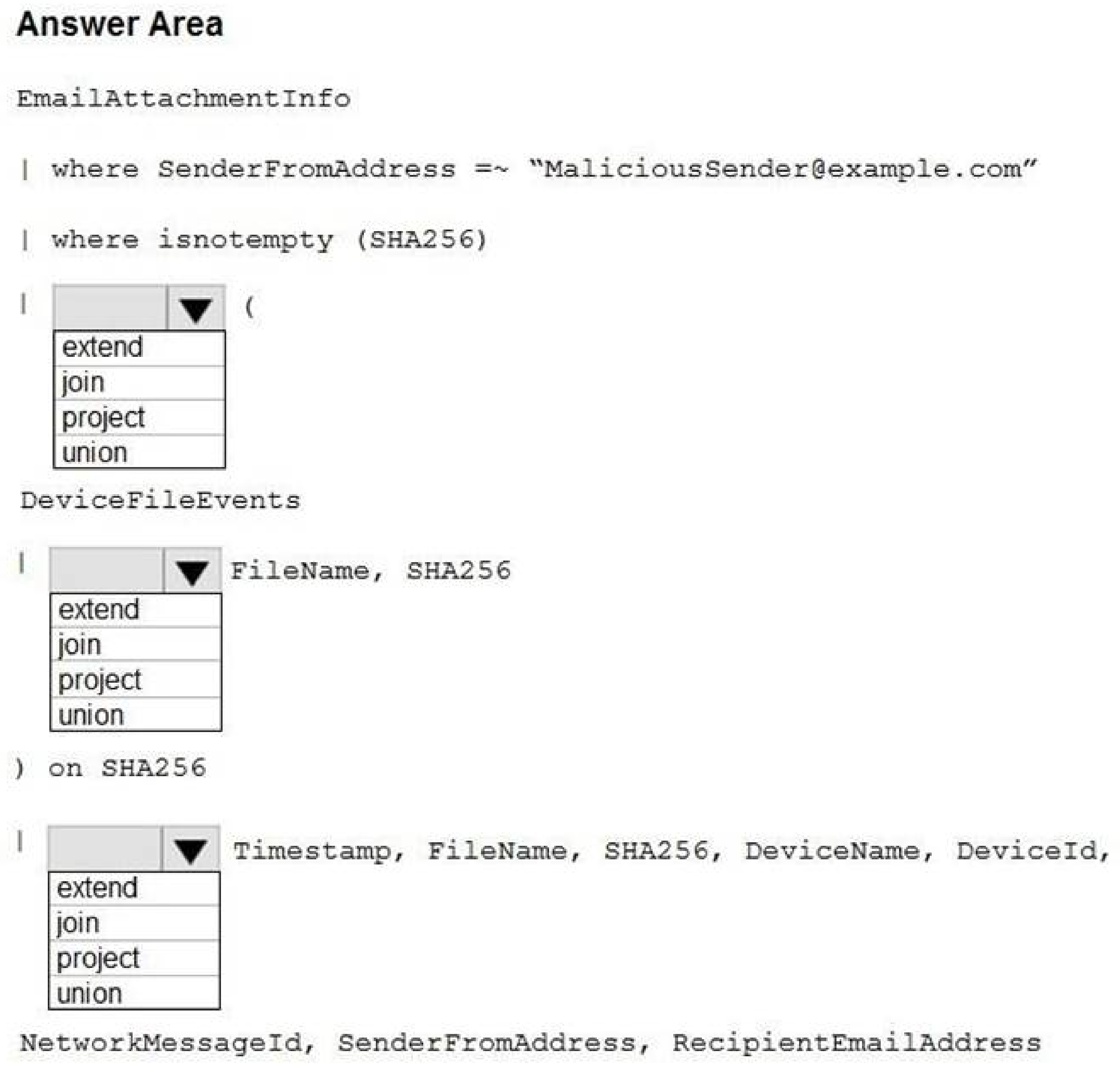
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.

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 67
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



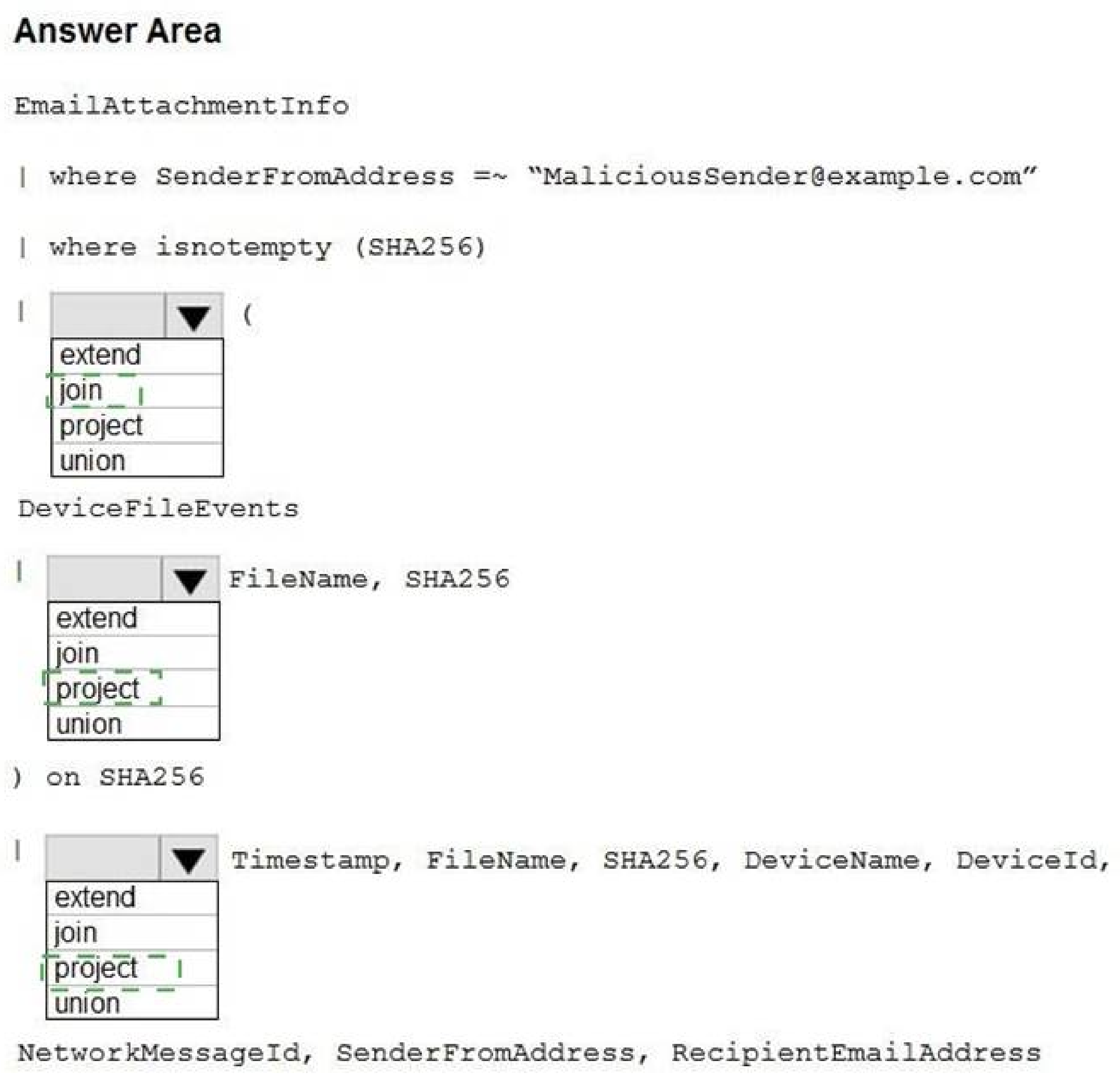
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

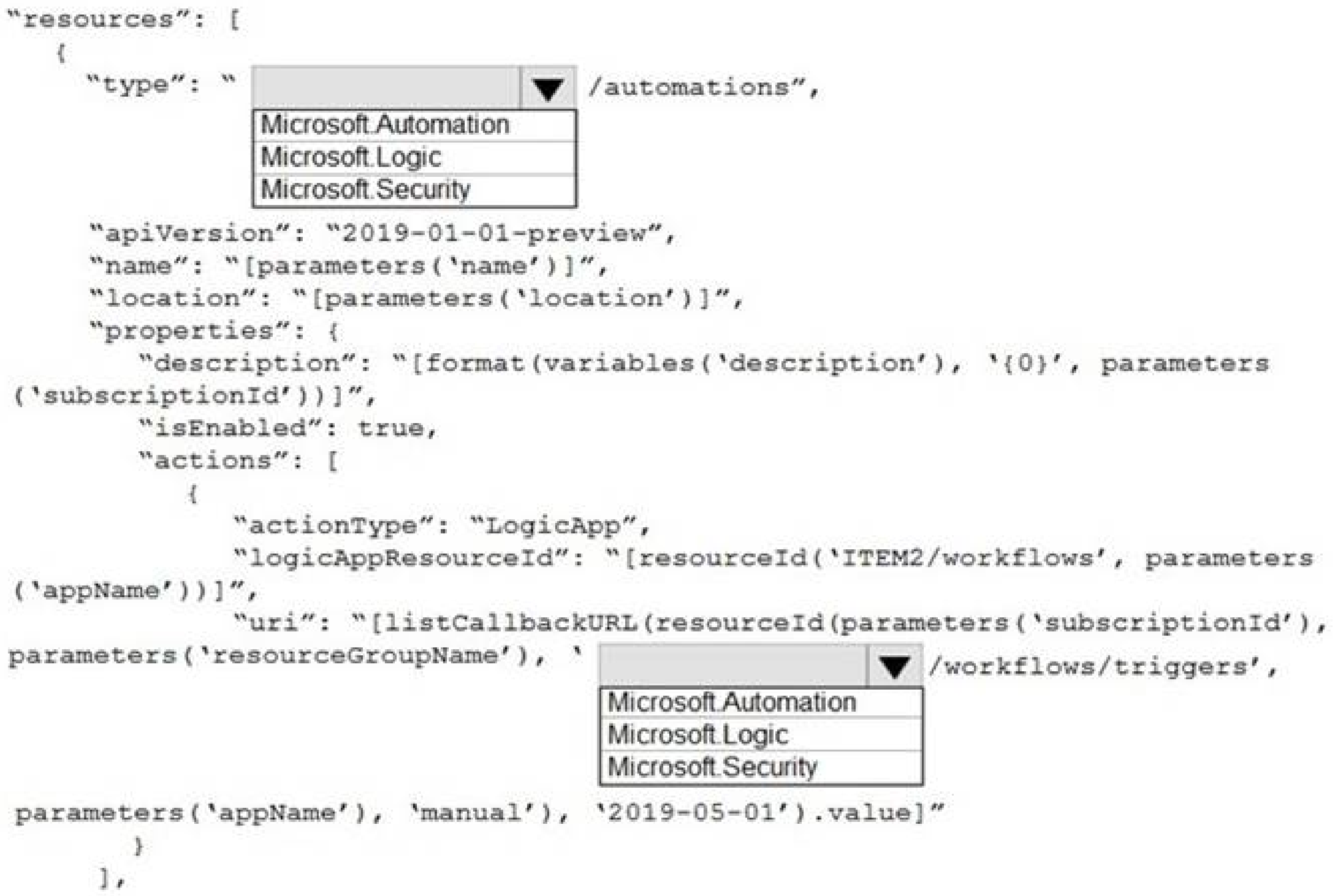
Explanation:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [ ▼ ] (
    extend
    [✓ join]
    project
    union
DeviceFileEvents

| [ ▼ ] FileName, SHA256
    extend
    join
    [✓ project]
    union
) on SHA256

| [ ▼ ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
    extend
    join
    [✓ project]
    union
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

NEW QUESTION 70
HOTSPOT - (Topic 4)
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

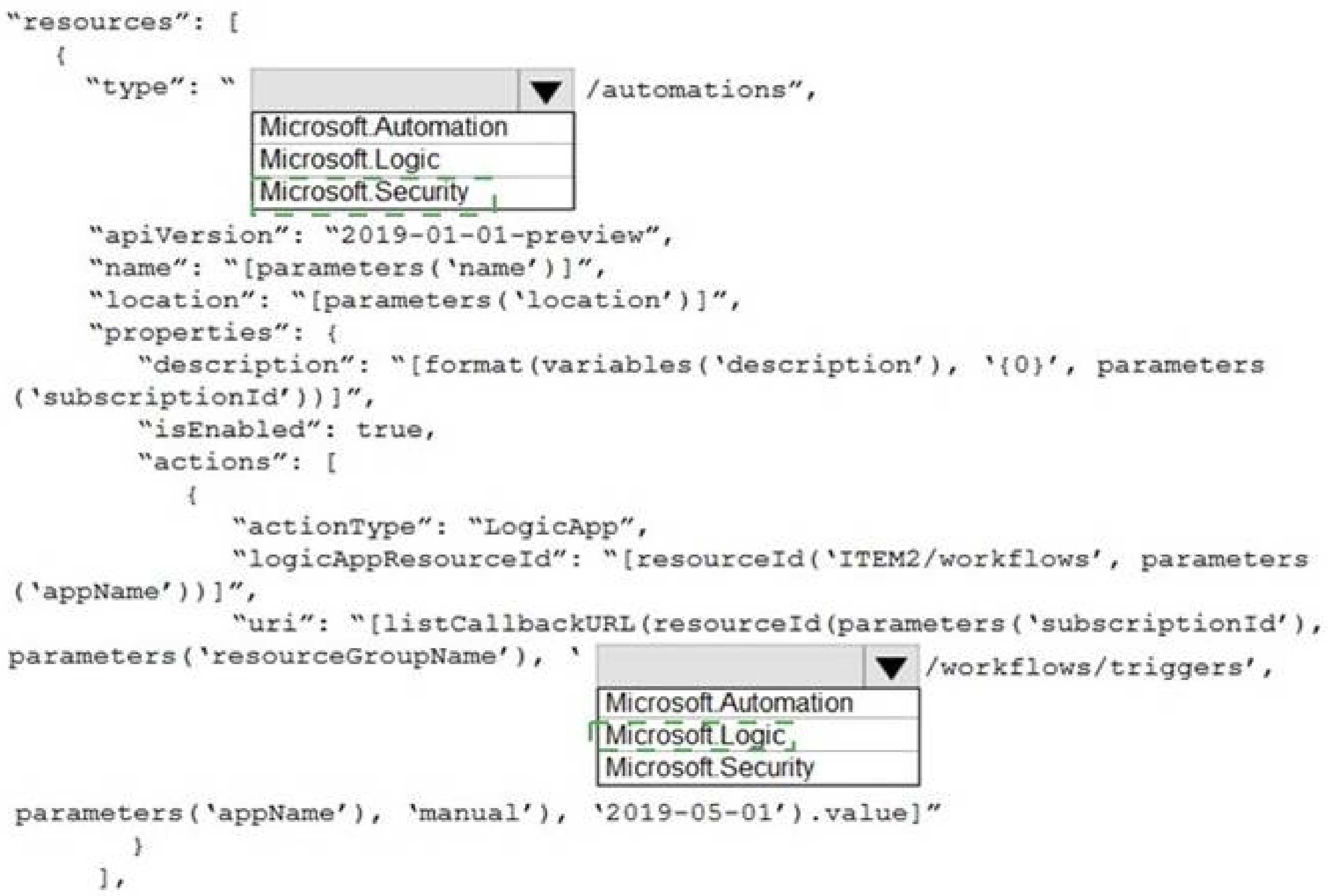


```
"resources": [
   {
    "type": " [              ▼ ] /automations",
              Microsoft.Automation
              Microsoft.Logic
              Microsoft.Security
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties":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

A. Mastered
B. Not Mastered

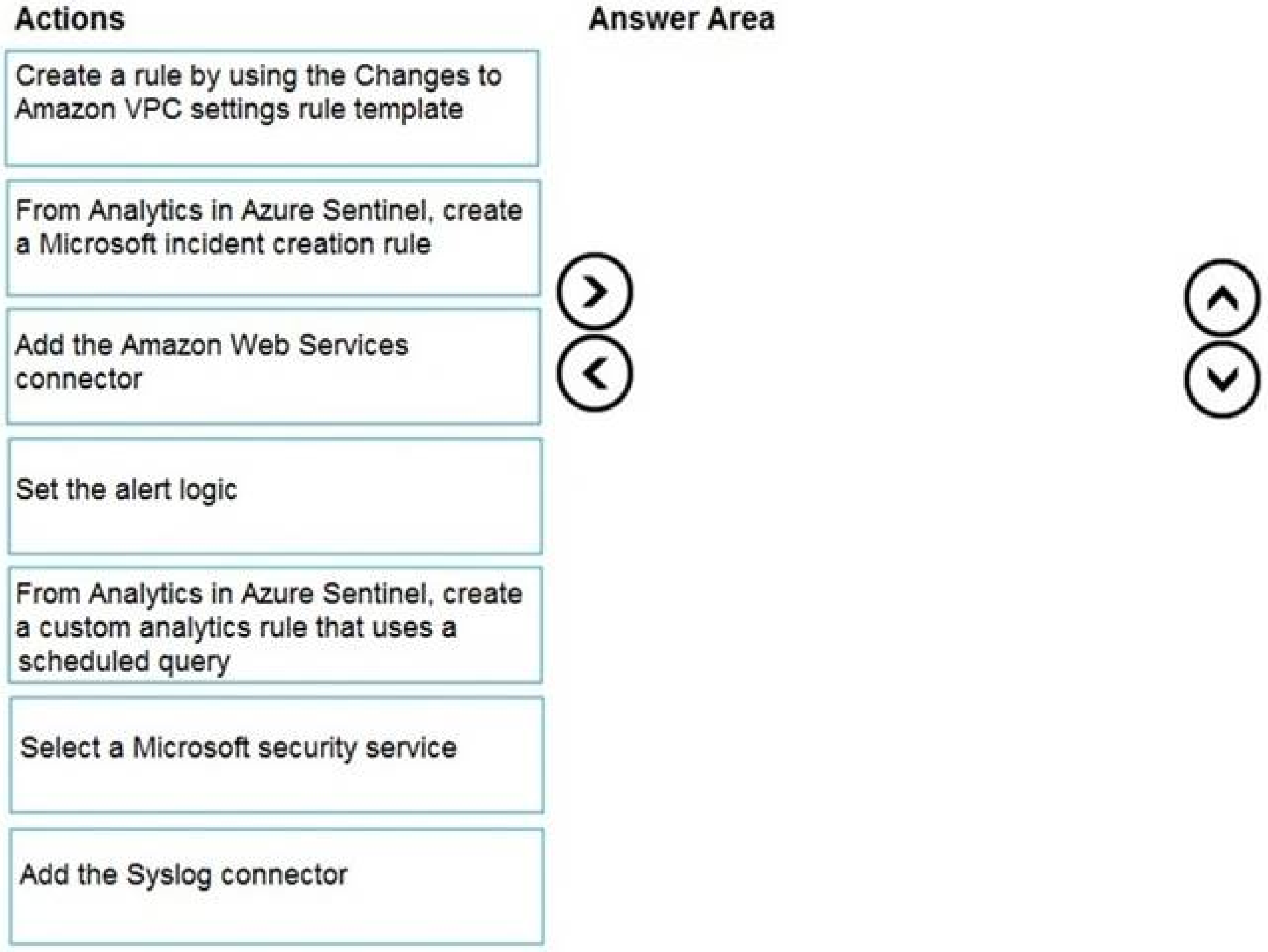
Answer: A

Explanation:



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

NEW QUESTION 75
DRAG DROP - (Topic 4)
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
a Microsoft 365 E5



Actions

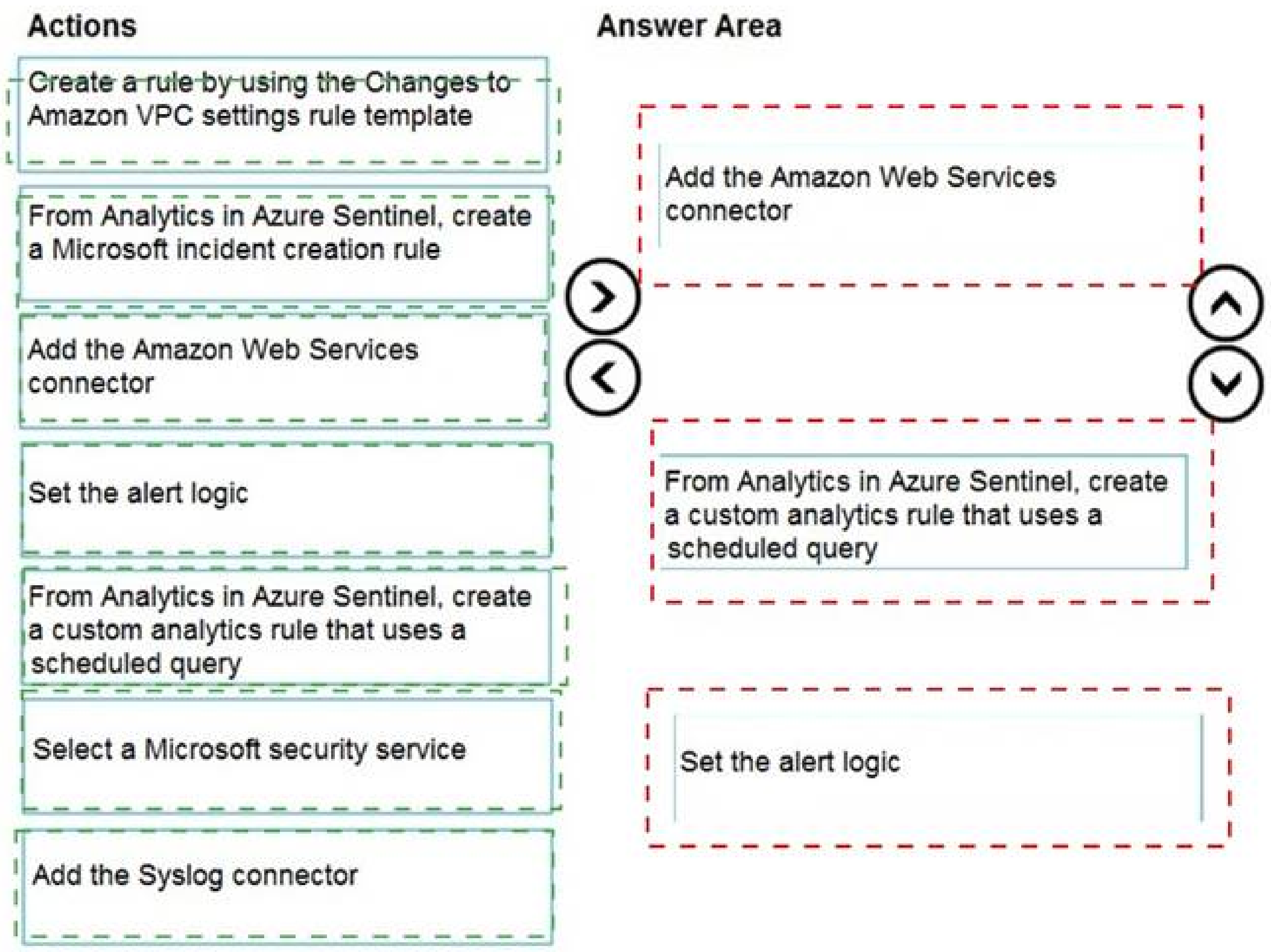
- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

~~Create a rule by using the Changes to~~ Amazon VPC settings rule template

From Analytics in Azure Sentinel, create a Microsoft incident creation rule

Add the Amazon Web Services connector

Set the alert logic

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Select a Microsoft security service

Add the Syslog connector

Answer Area

Add the Amazon Web Services connector

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Set the alert logic

NEW QUESTION 79
- (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 84
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online. You delete users from the subscription.
You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.
What should you use?

A. a file policy in Microsoft Defender for Cloud Apps
B. an access review policy
C. an alert policy in Microsoft Defender for Office 365
D. an insider risk policy

Answer: C

Explanation:
Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.
Default alert policies include:
Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

NEW QUESTION 88
- (Topic 4)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

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

Answer: D

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

NEW QUESTION 91

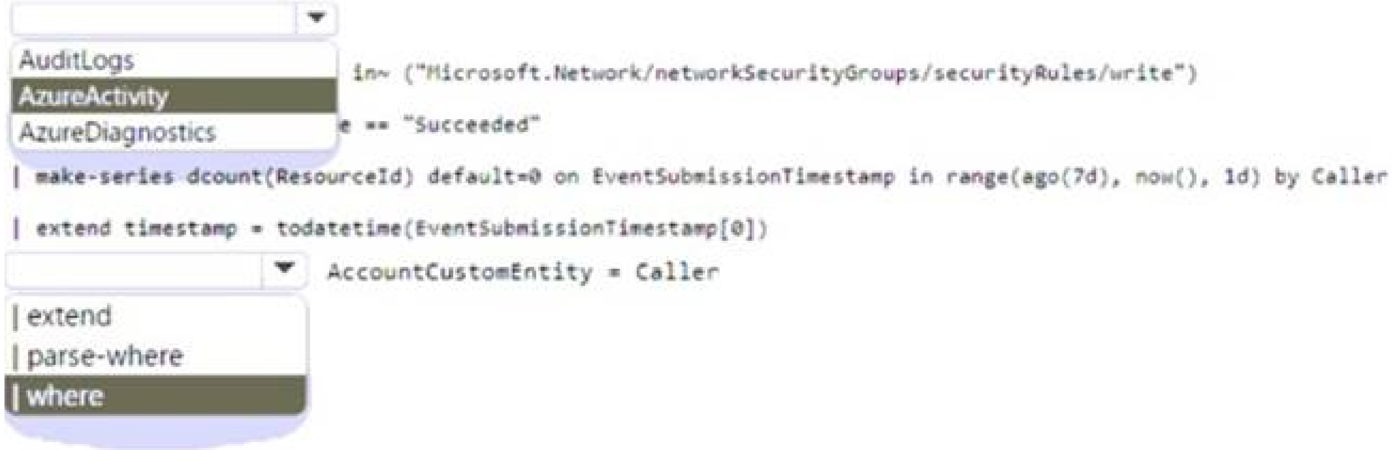
HOTSPOT - (Topic 4)

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

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

- Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
- Automatically associates the security principal with an Microsoft Sentinel entity

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

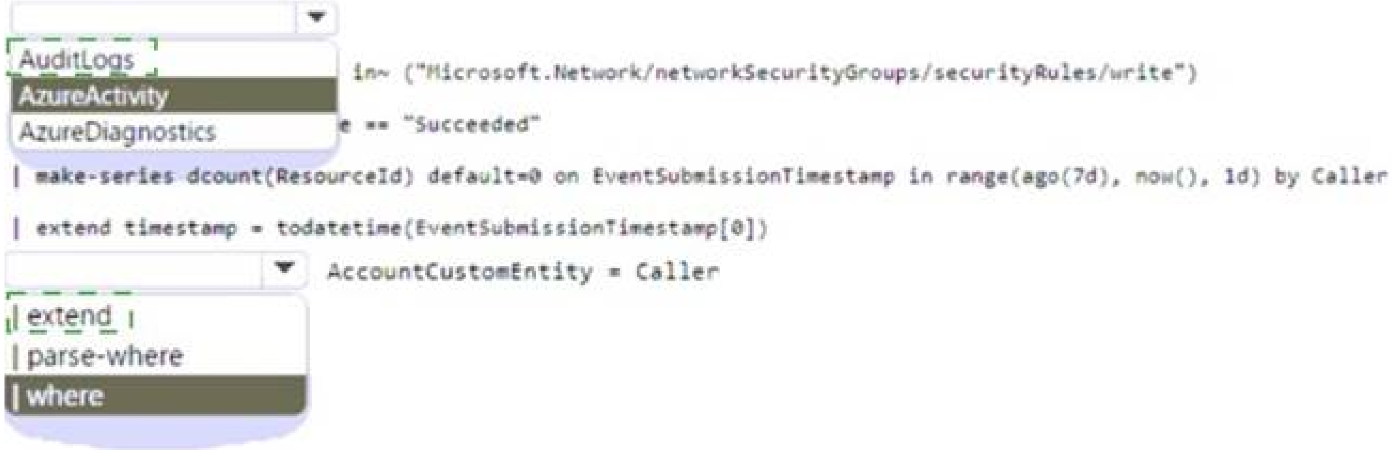


```
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

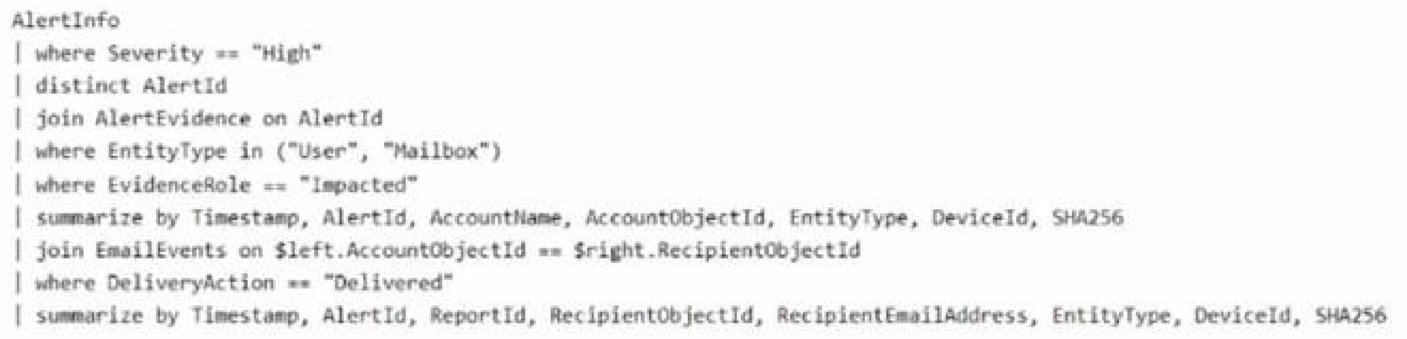


```
in~ ("Microsoft.Network/networkSecurityGroups/securityRules/write")
e == "Succeeded"
| make-series dcount(ResourceId) default=0 on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
| extend timestamp = todatetime(EventSubmissionTimestamp[0])
AccountCustomEntity = Caller
```

NEW QUESTION 94

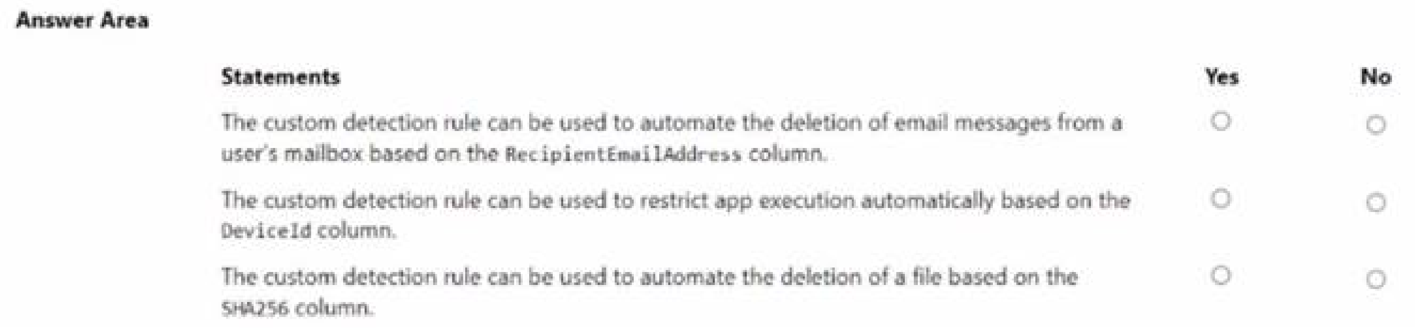
HOTSPOT - (Topic 4)

You have a custom detection rule that includes the following KQL query.



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

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



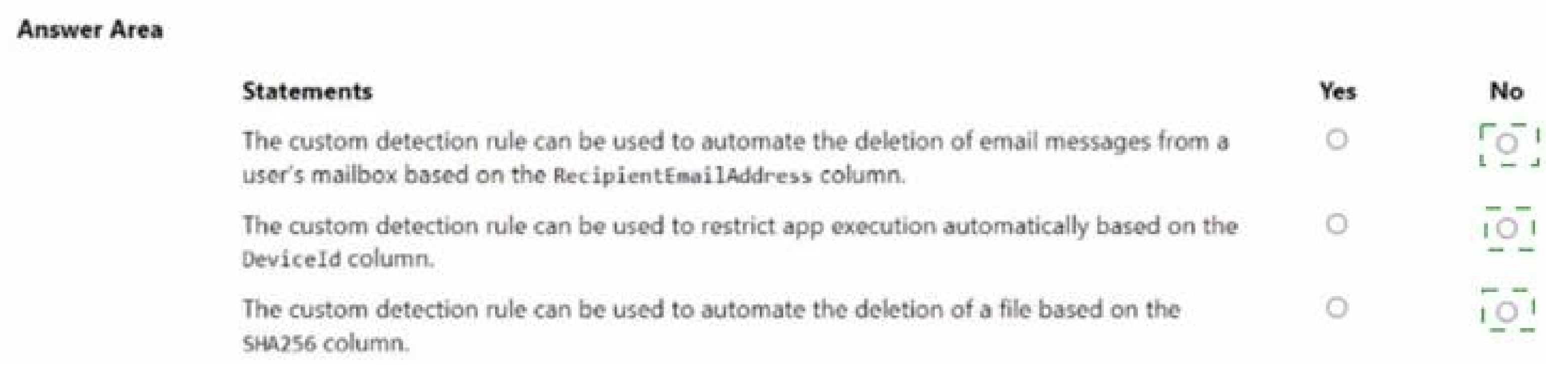
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

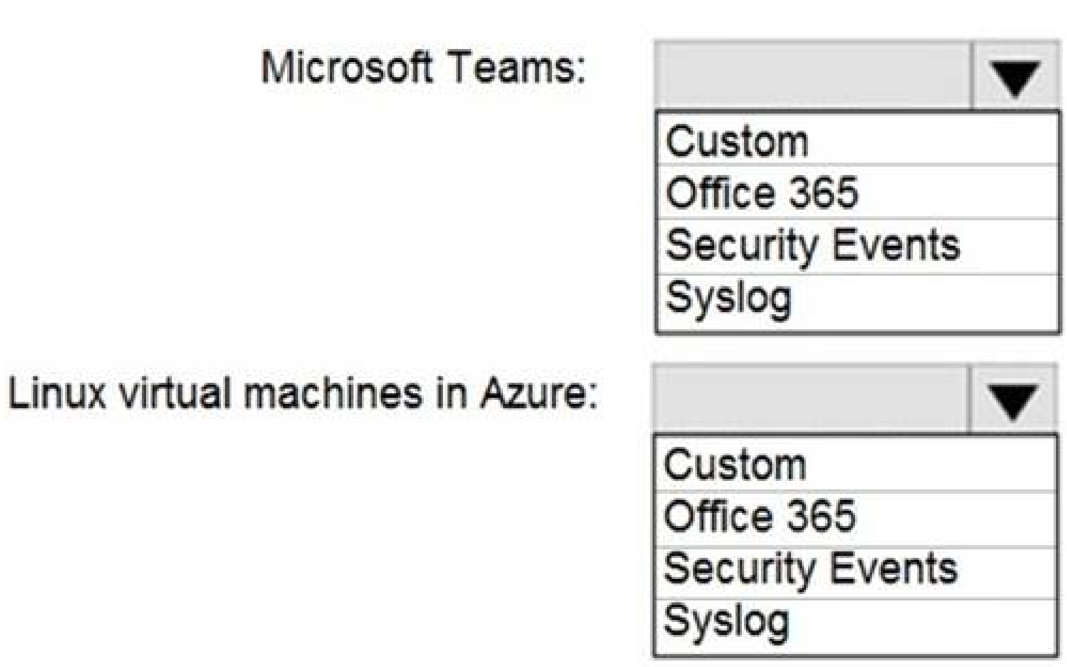
NEW QUESTION 99
- (Topic 4)
You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks
B. Azure Active Directory (Azure AD) permissions
C. role-based access control (RBAC) for the key vault
D. the access policy settings of the key vault

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

NEW QUESTION 104
HOTSPOT - (Topic 4)
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



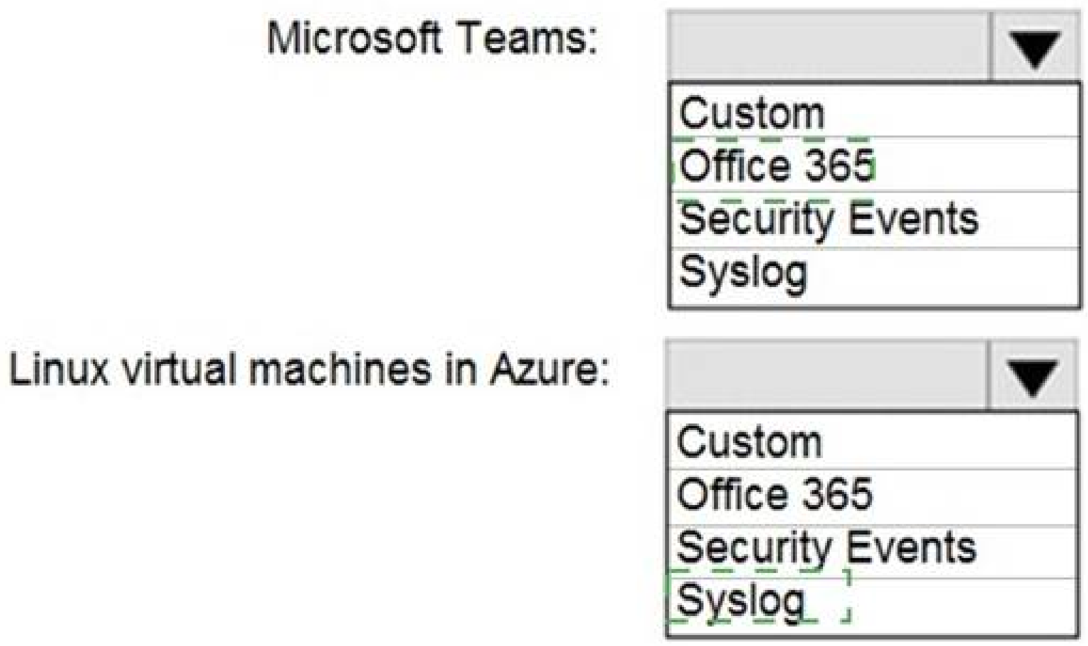
Microsoft Teams:
- Custom
- Office 365
- Security Events
- Syslog

Linux virtual machines in Azure:
- Custom
- Office 365
- Security Events
- Syslog

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Microsoft Teams:
- Custom
- [✓ Office 365]
- Security Events
- Syslog

Linux virtual machines in Azure:
- Custom
- Office 365
- Security Events
- [✓ Syslog]

NEW QUESTION 107
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspace1.
You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser. What should you create in Workspace1?

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

Answer: A

NEW QUESTION 109
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender fof Ctoud.
You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.
You need to onboard EC2-1 to Defender for Cloud. What should you install on EC2-1?

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

Answer: A

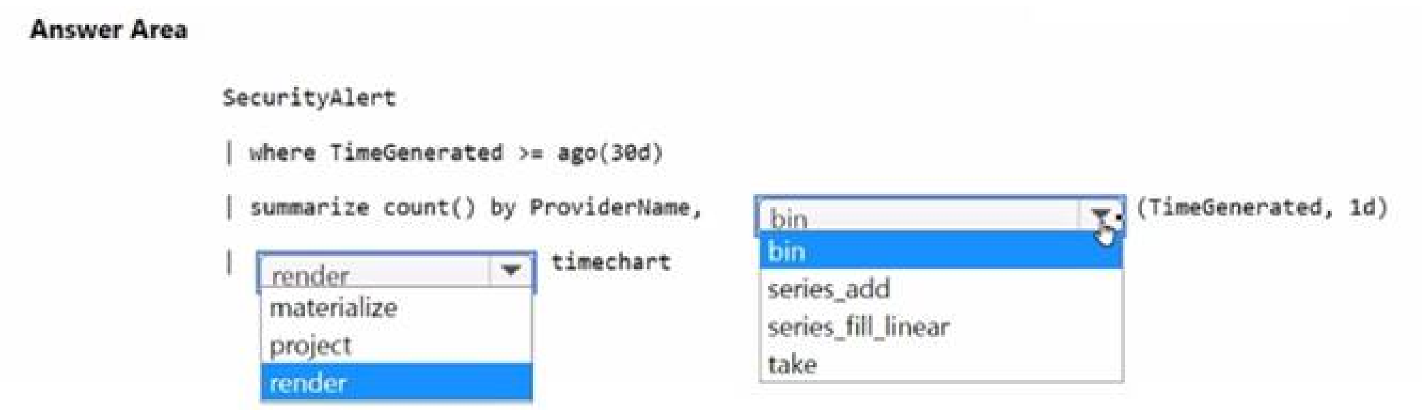
NEW QUESTION 110
- (Topic 4)
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure
Sentinel deployment to generate alerts based 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 113
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.



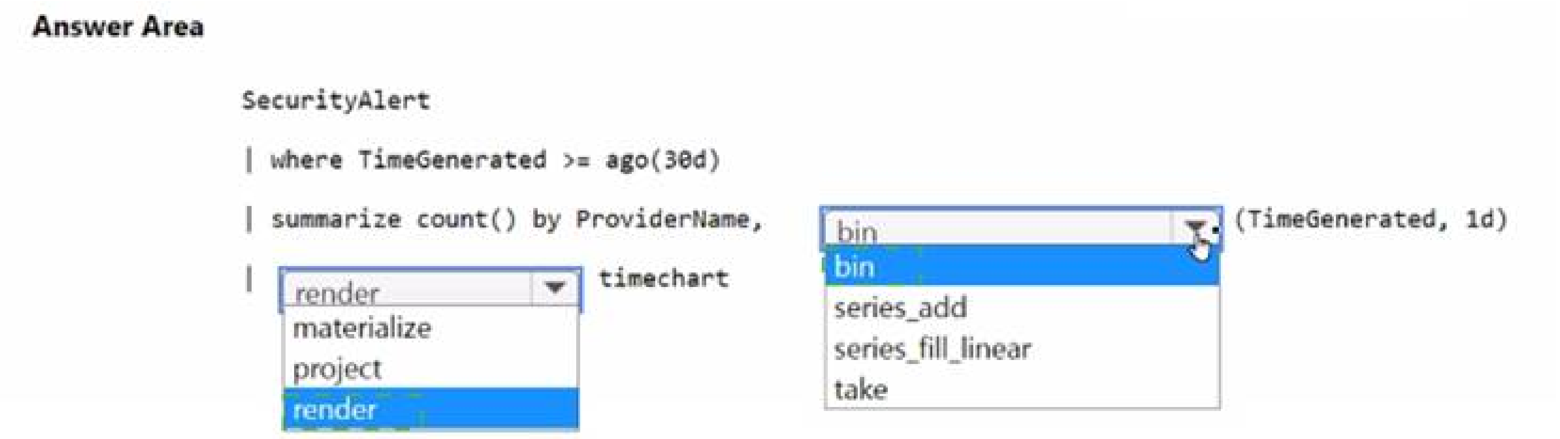
Answer Area

```
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 114
- (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 116
- (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

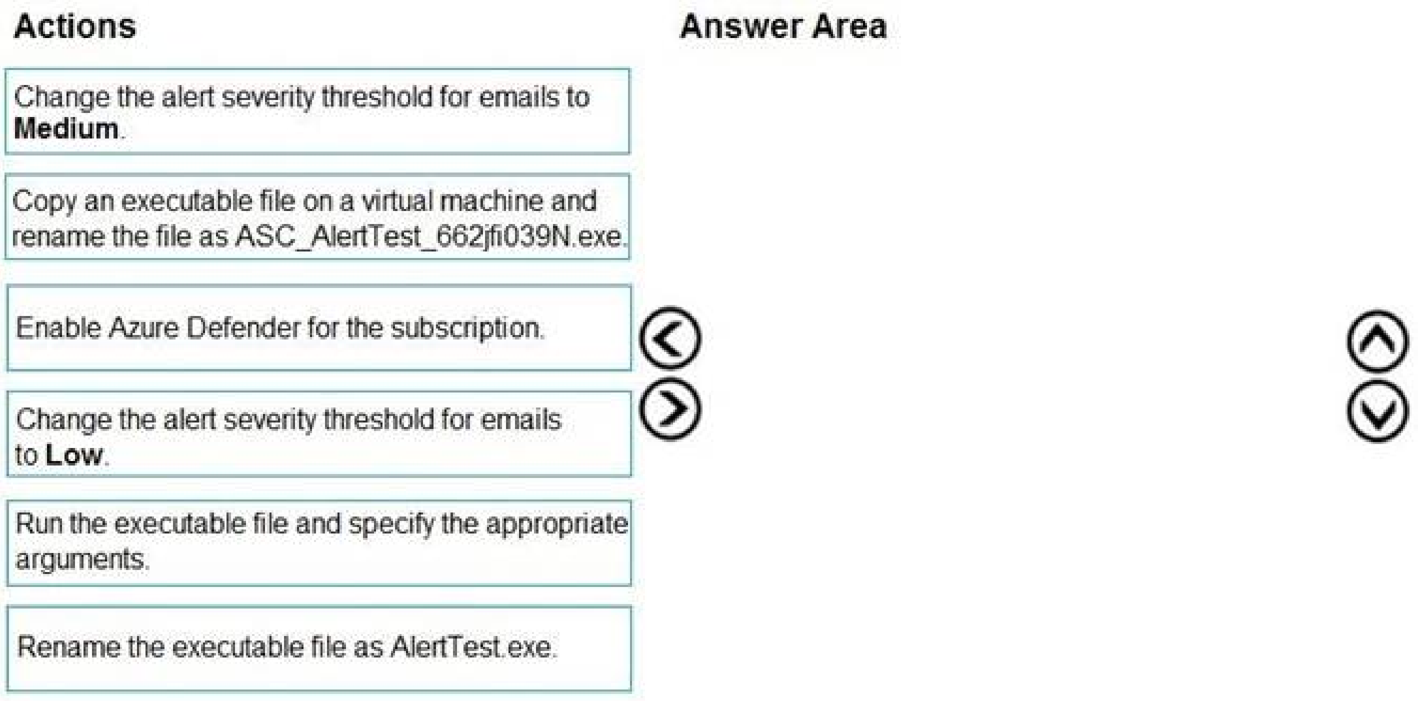
NEW QUESTION 119
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks
B. Azure Automation runbooks
C. Microsoft Sentinel automation rules
D. Microsoft Sentinel playbooks
E. Azure Functions apps

Answer: CE

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

NEW QUESTION 124
DRAG DROP - (Topic 4)
DRAG DROP
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

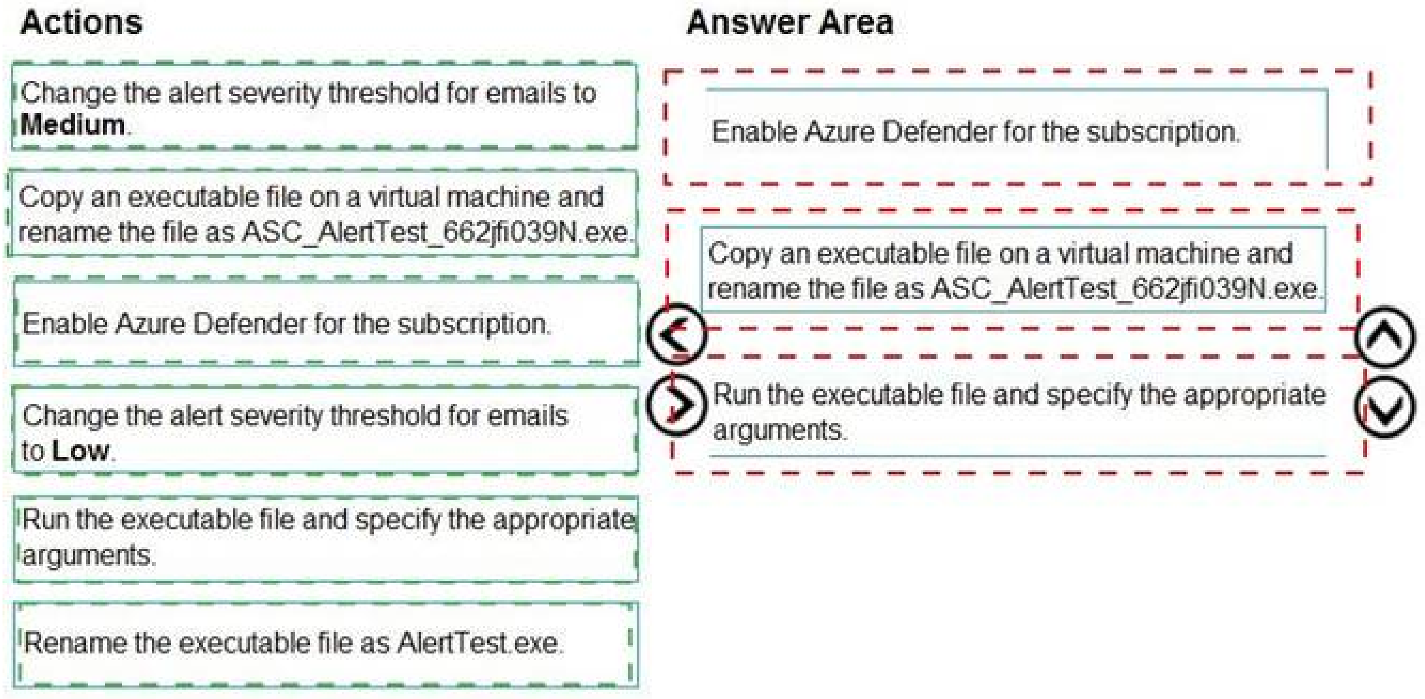
- Change the alert severity threshold for emails to **Medium**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Enable Azure Defender for the subscription.
- Change the alert severity threshold for emails to **Low**.
- Run the executable file and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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

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

Answer Area

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

NEW QUESTION 125
- (Topic 4)
You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

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

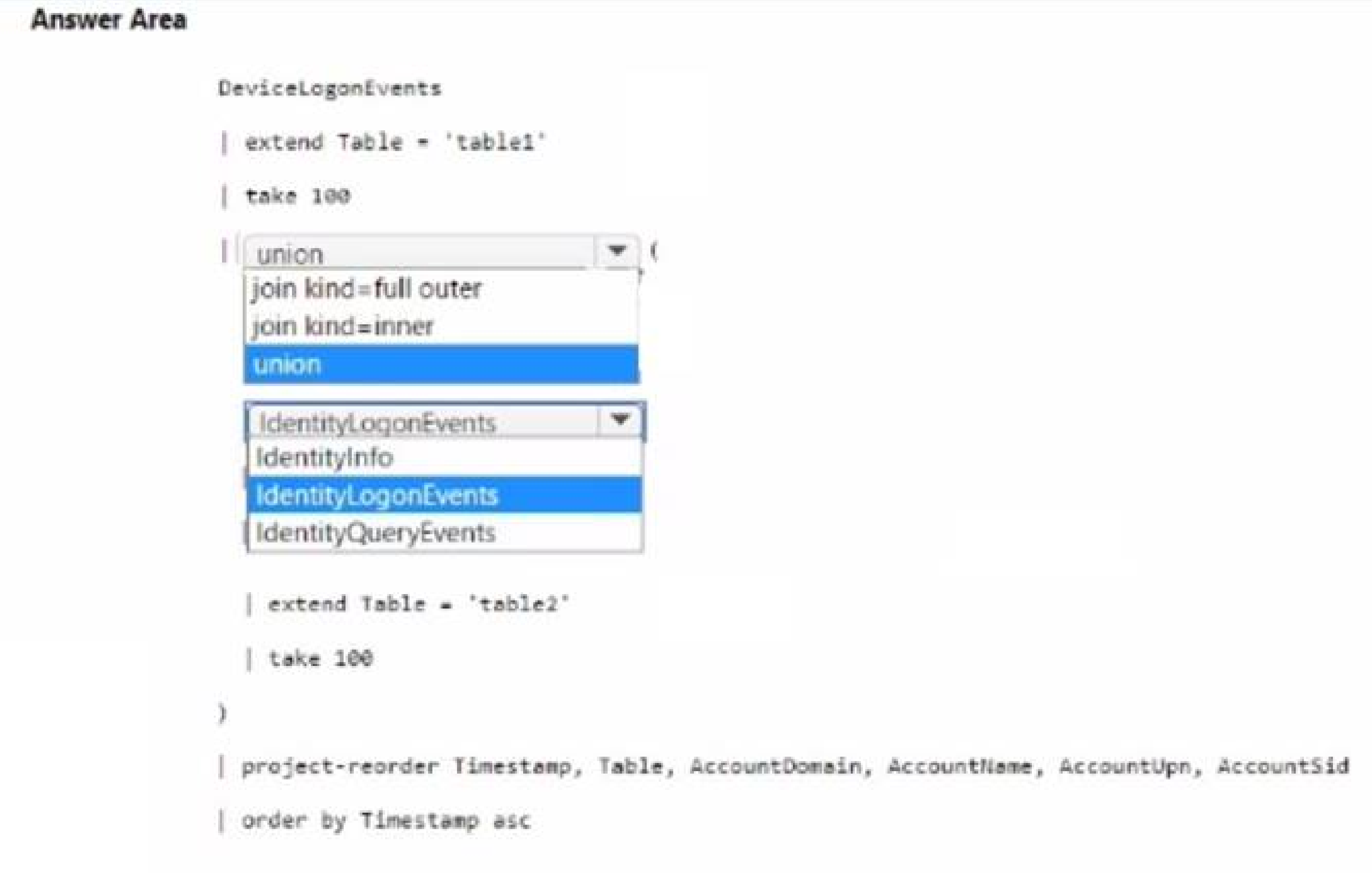
Answer: C

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

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

Answer: DE

NEW QUESTION 133
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.



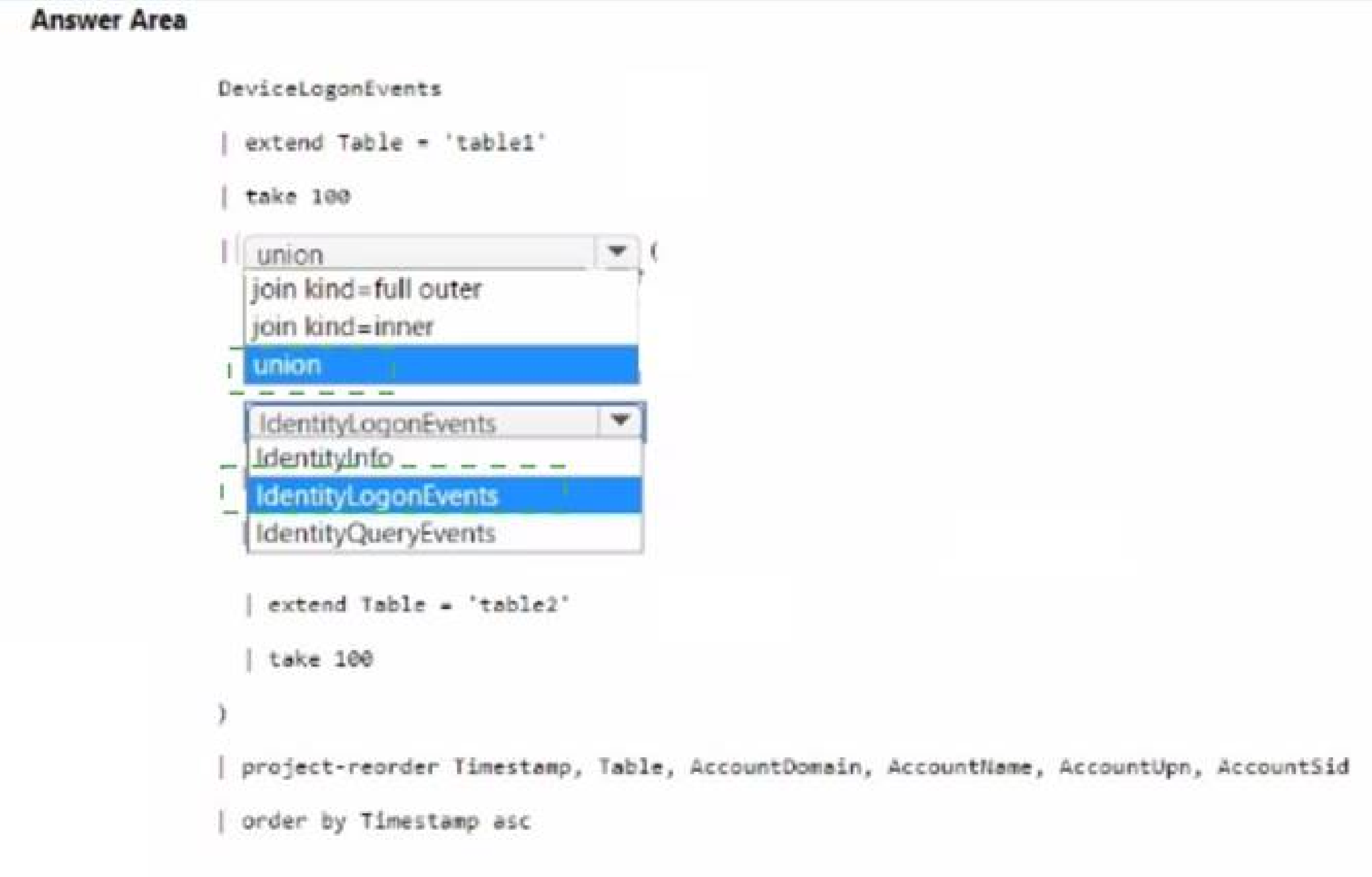
Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

A. Mastered
B. Not Mastered

Answer: A

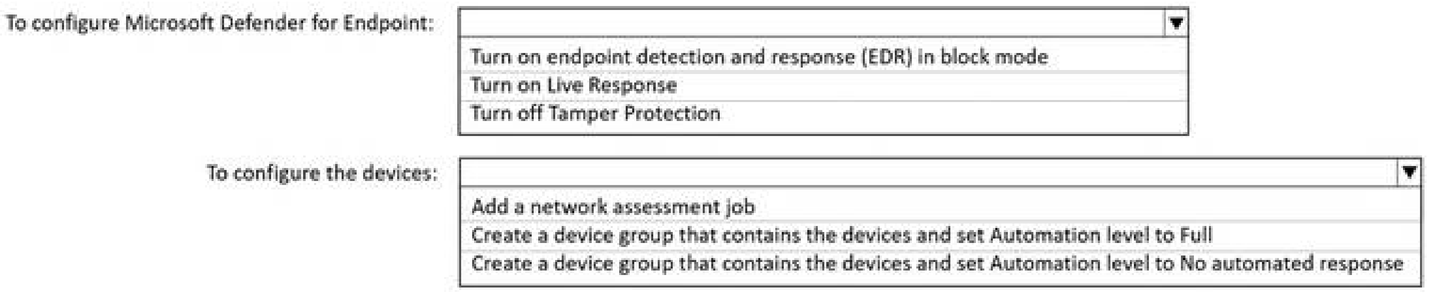
Explanation:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

NEW QUESTION 134
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled
in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



To configure Microsoft Defender for Endpoint:
- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:
- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

NEW QUESTION 138
- (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

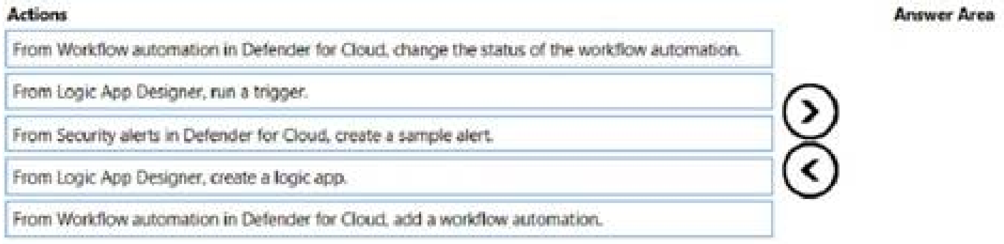
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location- condition

NEW QUESTION 140
- (Topic 4)
You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

A. Run antivirus scan
B. Initiate Automated Investigation
C. Collect investigation package
D. Initiate Live Response Session

Answer: D

NEW QUESTION 144
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.



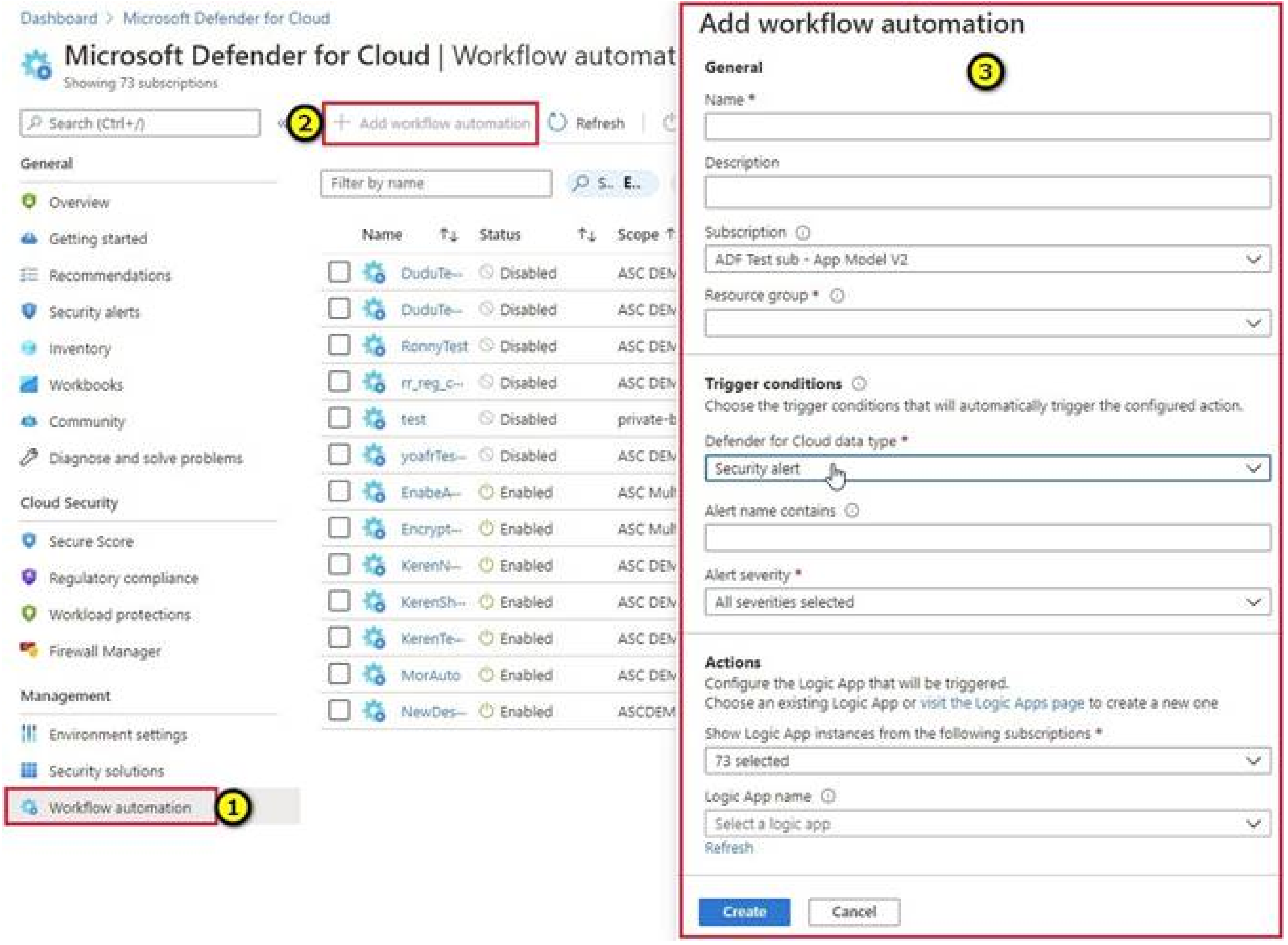
Actions
- From Workflow automation in Defender for Cloud, change the status of the workflow automation.
- From Logic App Designer, run a trigger.
- From Security alerts in Defender for Cloud, create a sample alert.
- From Logic App Designer, create a logic app.
- From Workflow automation in Defender 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 DEN
☐	DuduTe--	Disabled	ASC DEN
☐	RonnyTest	Disabled	ASC DEN
☐	rr_reg_c--	Disabled	ASC DEN
☐	test	Disabled	private-b
☐	yoafrTes--	Disabled	ASC DEN
☐	EnabeA--	Enabled	ASC Mul
☐	Encrypt--	Enabled	ASC Mul
☐	KerenN--	Enabled	ASC DEN
☐	KerenSh--	Enabled	ASC DEN
☐	KerenTe--	Enabled	ASC DEN
☐	MorAuto	Enabled	ASC DEN
☐	NewDes--	Enabled	ASCDEM

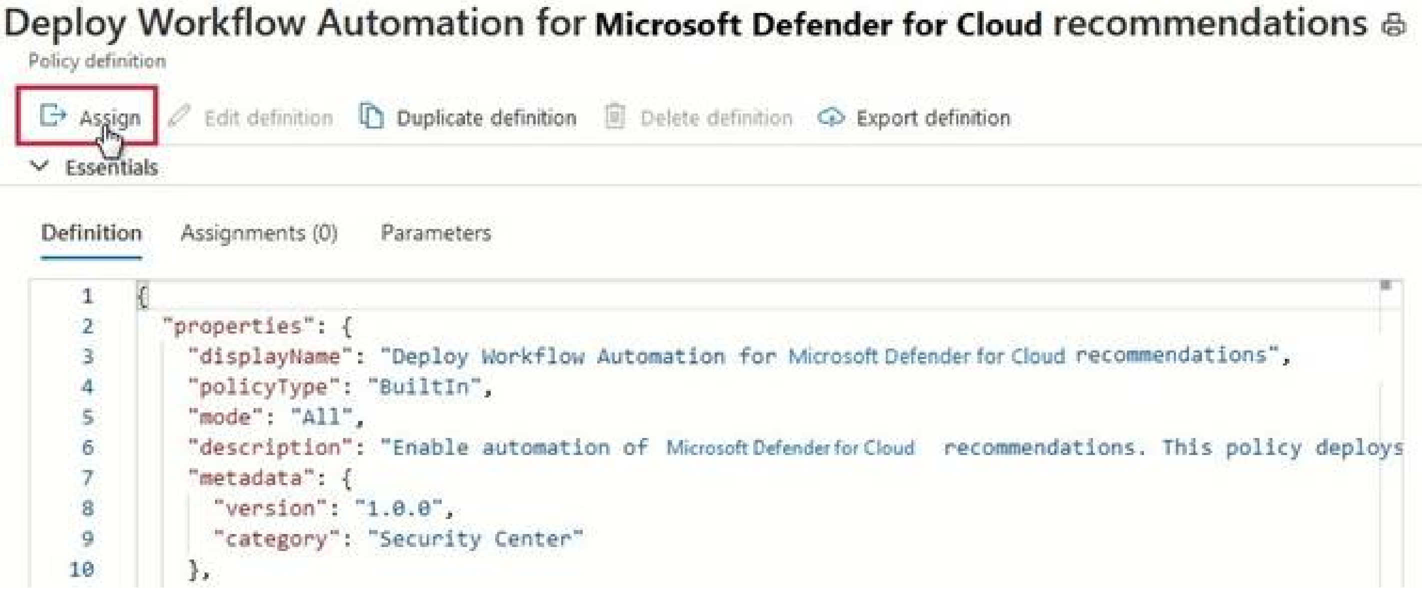
Add workflow automation

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 146
- (Topic 4)
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

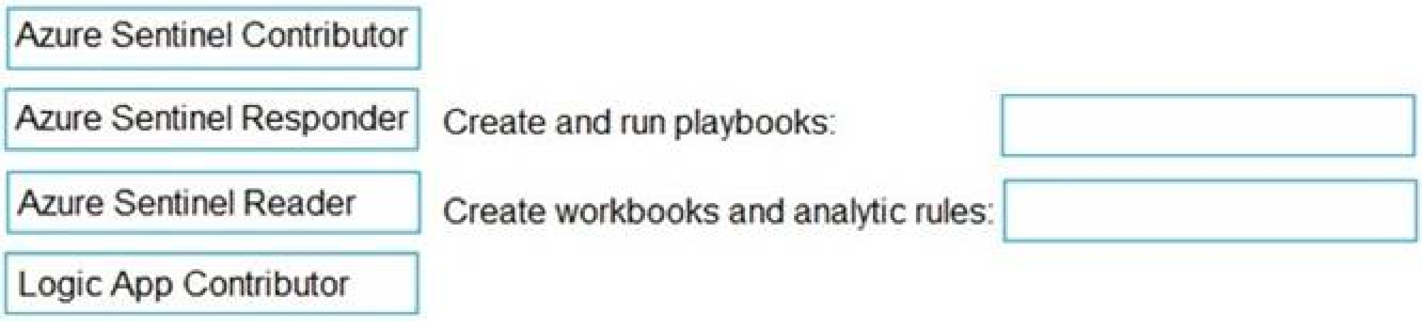
A. the Incidents blade of the Microsoft 365 Defender portal
B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center
C. Activity explorer in the Microsoft 365 compliance center
D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Answer: C

Explanation:
Labeling activities are available in Activity explorer. For example:
Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.
It is captured at the time of save in Office native applications and web applications. It is captured at the time of occurrence in Azure Information protection add-ins.
Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification- activity-explorer-available-events?view=o365-worldwide

NEW QUESTION 147
DRAG DROP - (Topic 4)
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups. You need to delegate the following tasks:
? Create and run playbooks
? Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



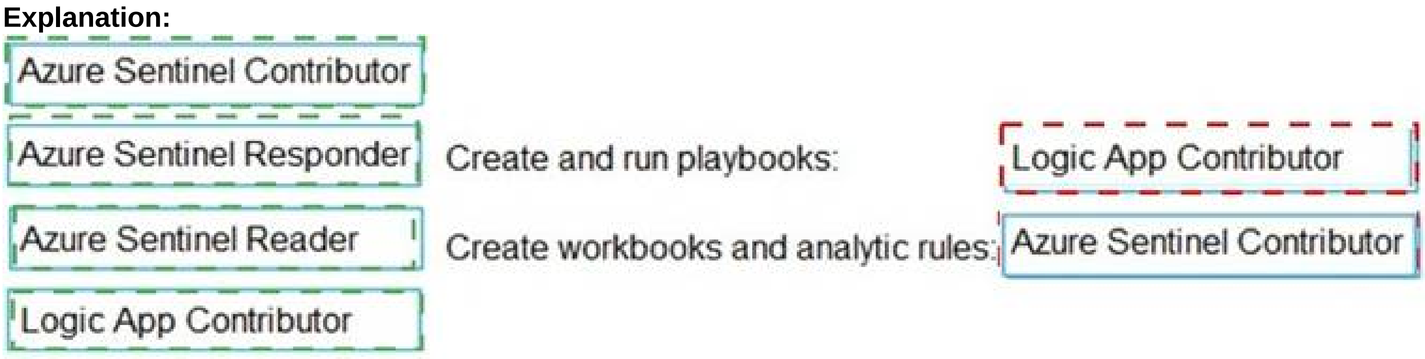
Azure Sentinel Contributor
Azure Sentinel Responder
Azure Sentinel Reader
Logic App Contributor

Create and run playbooks:
Create workbooks and analytic rules:

A. Mastered
B. Not Mastered

Answer: A

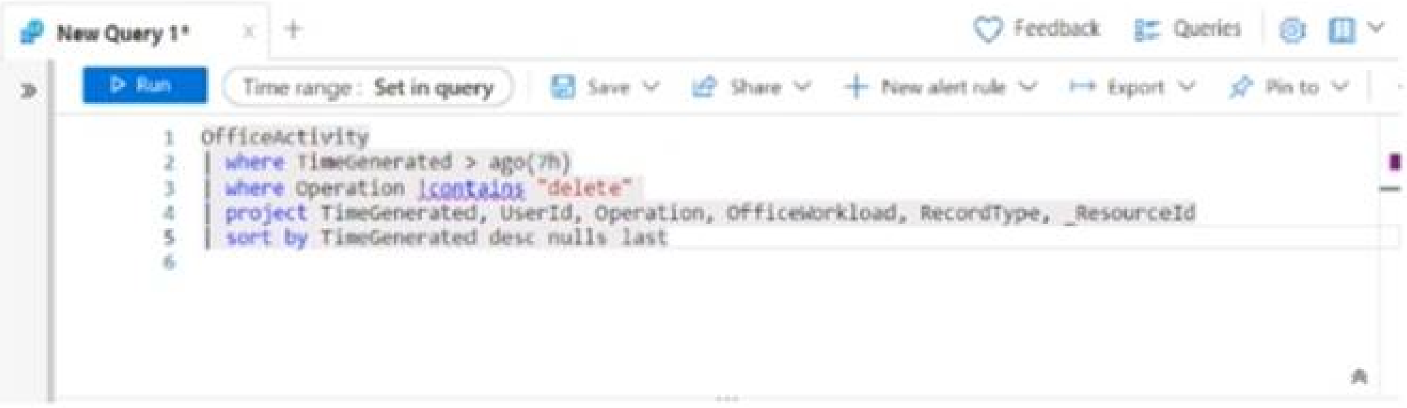
Explanation:



Azure Sentinel Contributor
Azure Sentinel Responder
Azure Sentinel Reader
Logic App Contributor

Create and run playbooks: Logic App Contributor
Create workbooks and analytic rules: Azure Sentinel Contributor

NEW QUESTION 148
- (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
```

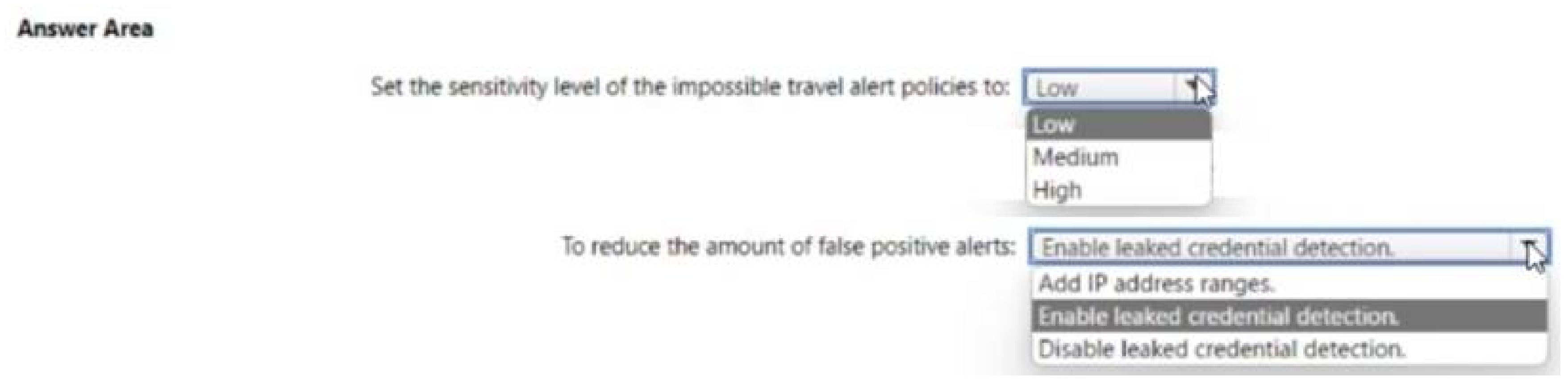
You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

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 149
HOTSPOT - (Topic 4)
You need to meet the Microsoft Defender for Cloud Apps requirements
What should you do? To answer. select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.


Answer Area

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

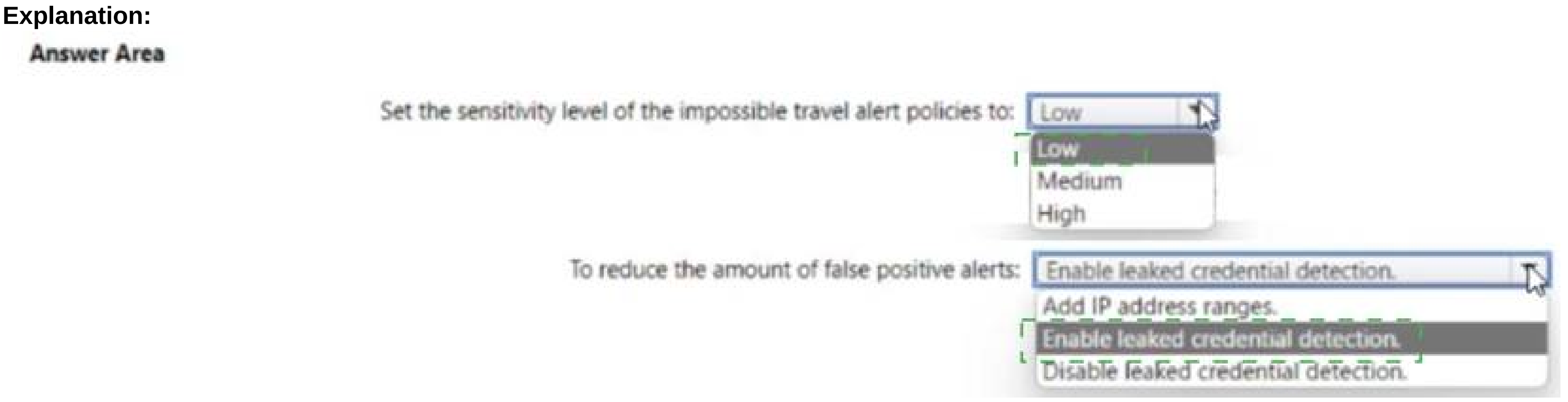
To reduce the amount of false positive alerts: Enable leaked credential detection.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

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

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

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

NEW QUESTION 154
- (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 156
- (Topic 4)
You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.
You need to create a query that will be used to display the time chart. What should you include in the query?

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

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

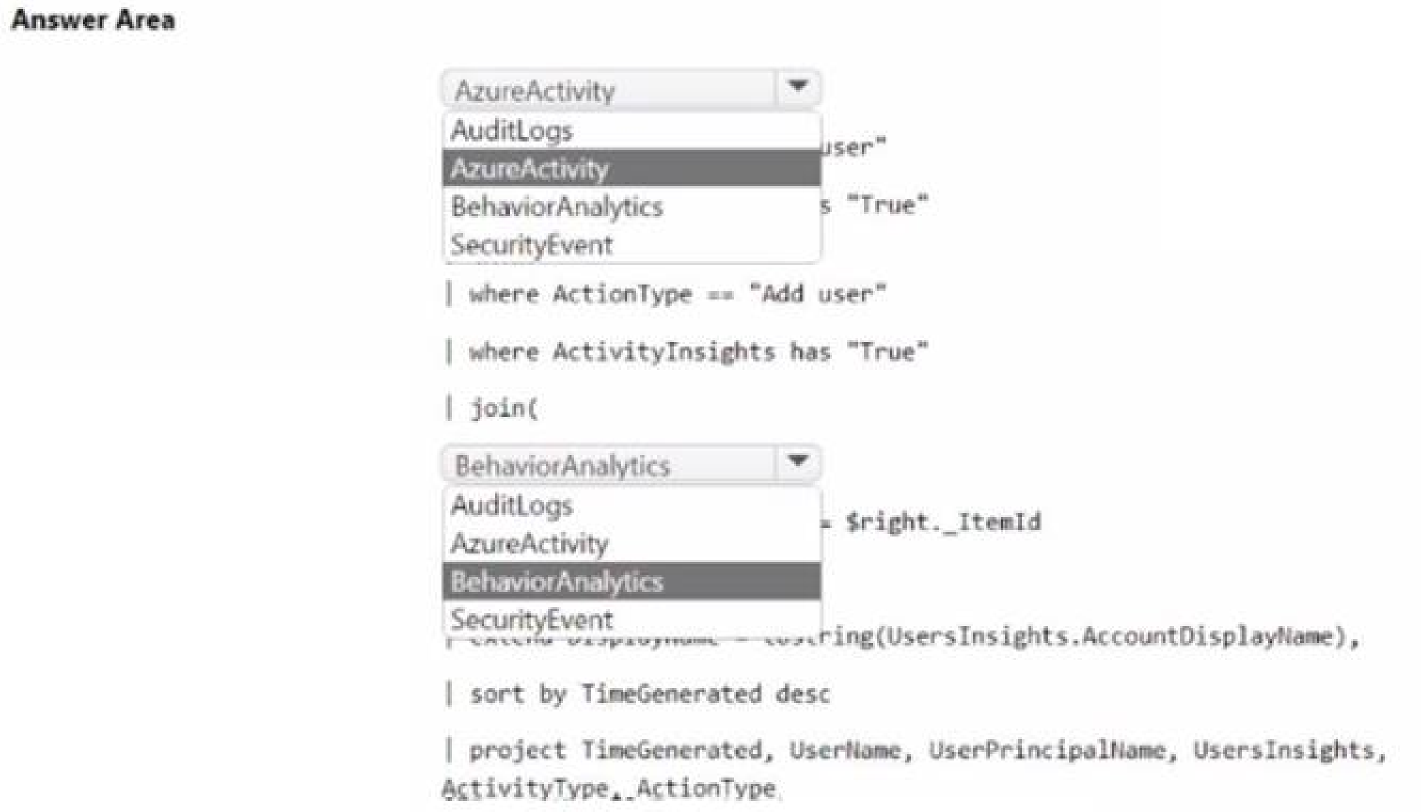
NEW QUESTION 161
- (Topic 4)
You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: C

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

NEW QUESTION 165
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

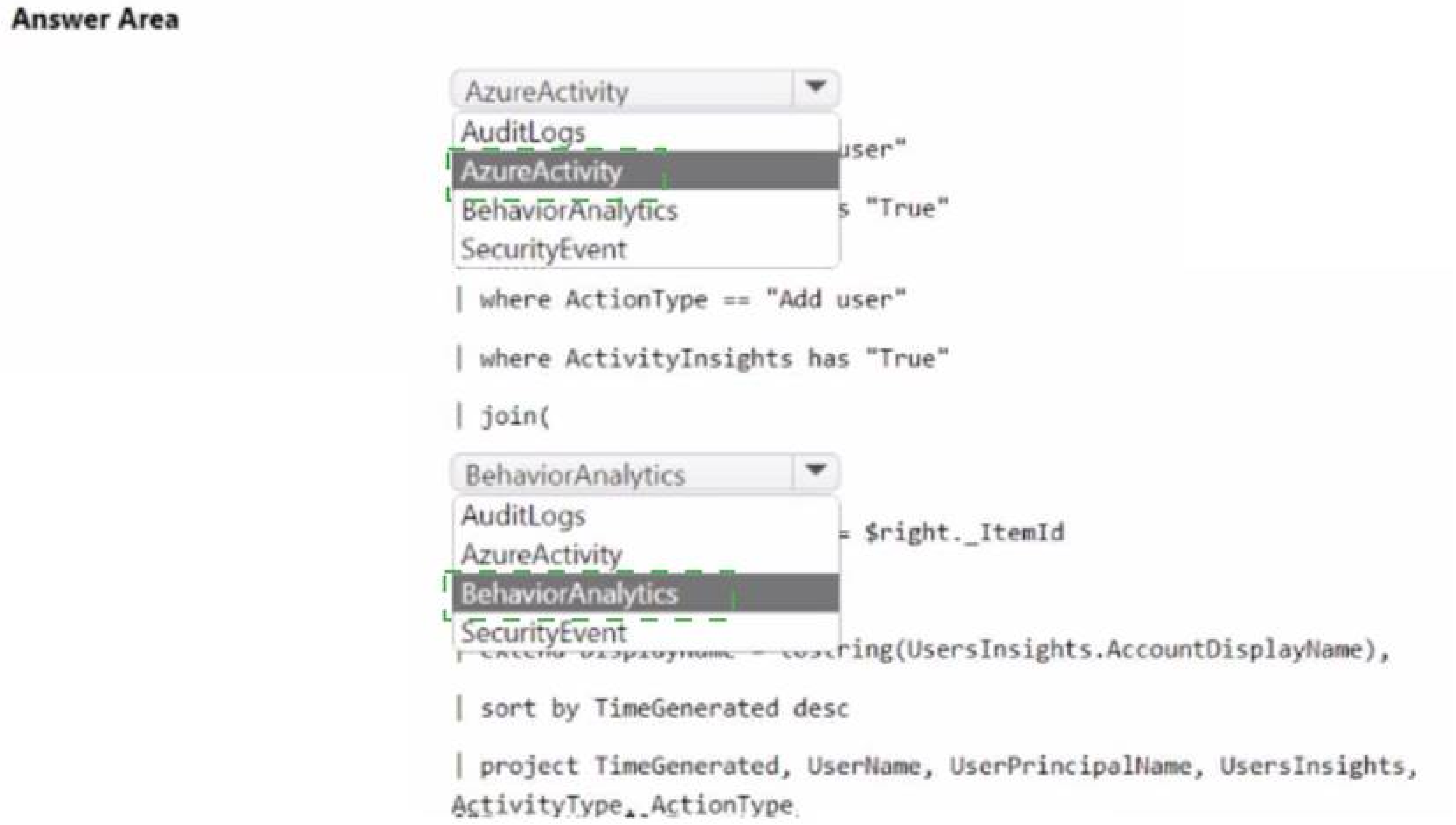
```
user"
s "True"
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
```

```
= $right._ItemId
ring(UsersInsights.AccountDisplayName),
| sort by TimeGenerated desc
| project TimeGenerated, UserName, UserPrincipalName, UsersInsights,
ActivityType, ActionType
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

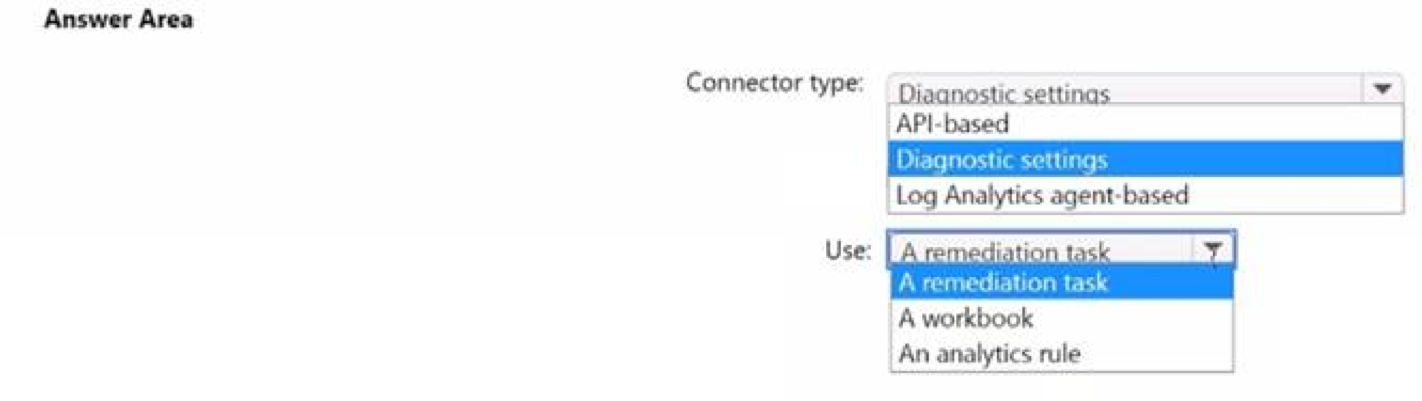

Answer Area

```
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
```

NEW QUESTION 166
HOTSPOT - (Topic 4)
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer Area

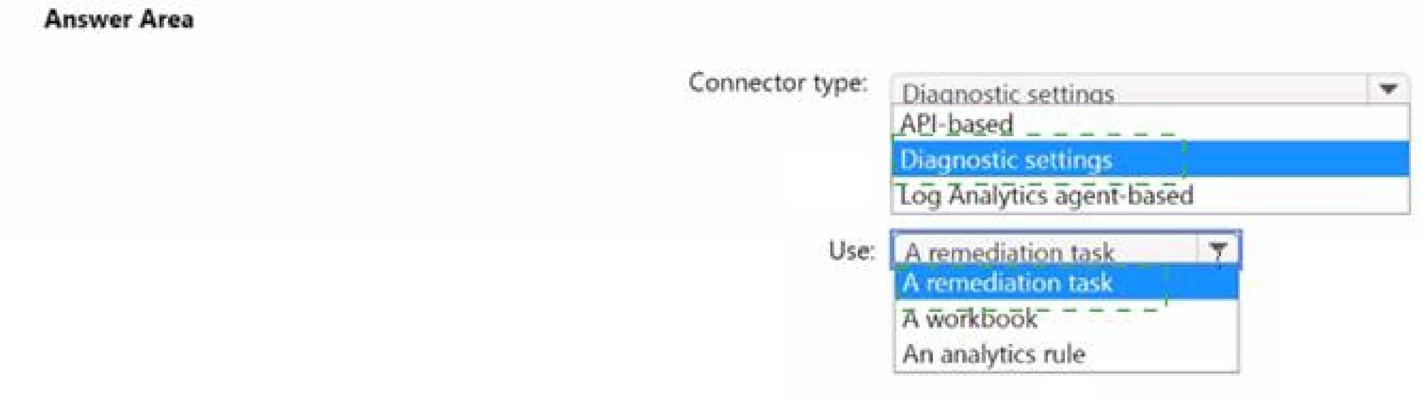
Connector type: Diagnostic settings

Use: A remediation task

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Connector type: Diagnostic settings

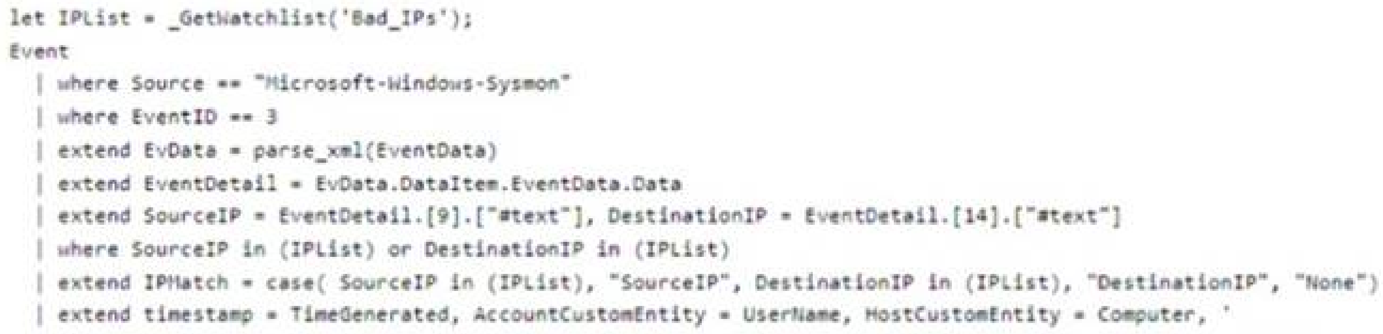
Use: A remediation task

NEW QUESTION 169
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to create a query that will link the Alertlnfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.
Which operator should you use?

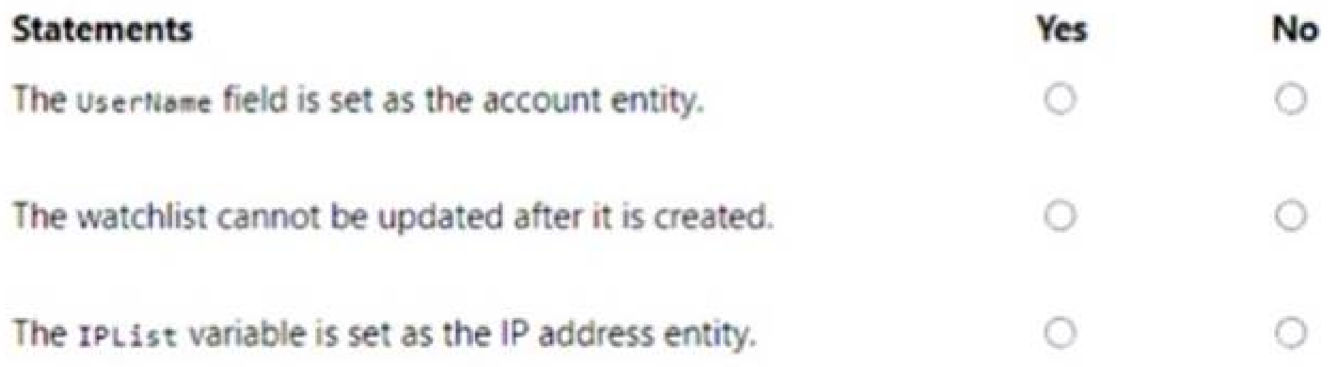
A. join kind = inner
B. evaluate hin
C. Remote =
D. search *
E. union kind = inner

Answer: A

NEW QUESTION 172
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, '
```

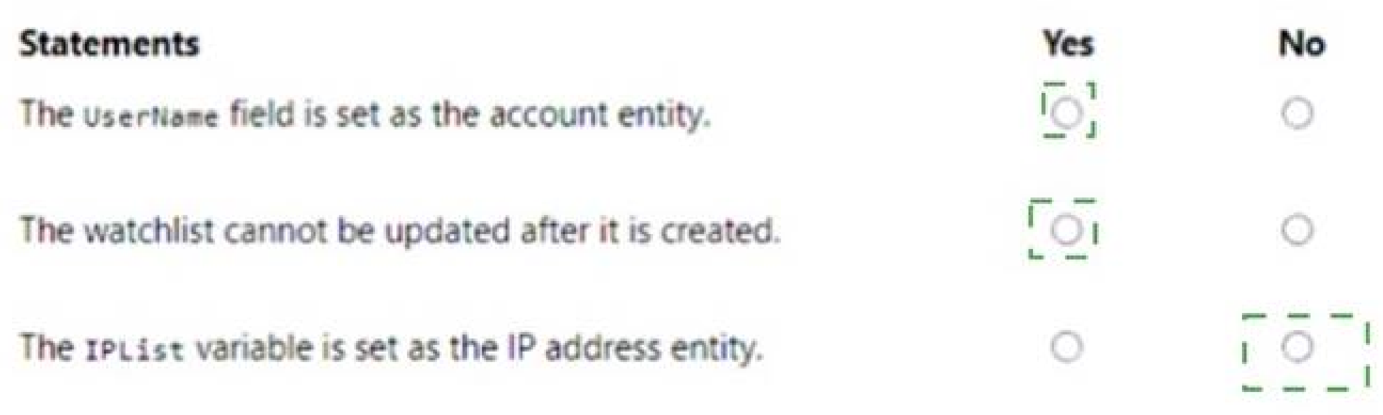


Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

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 177
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a playbook.
B. Associate a playbook to an incident.
C. Enable Entity behavior analytics.
D. Create a workbook.
E. Enable the Fusion rule.

Answer: AB

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

NEW QUESTION 181
- (Topic 4)
You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

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

Answer: B

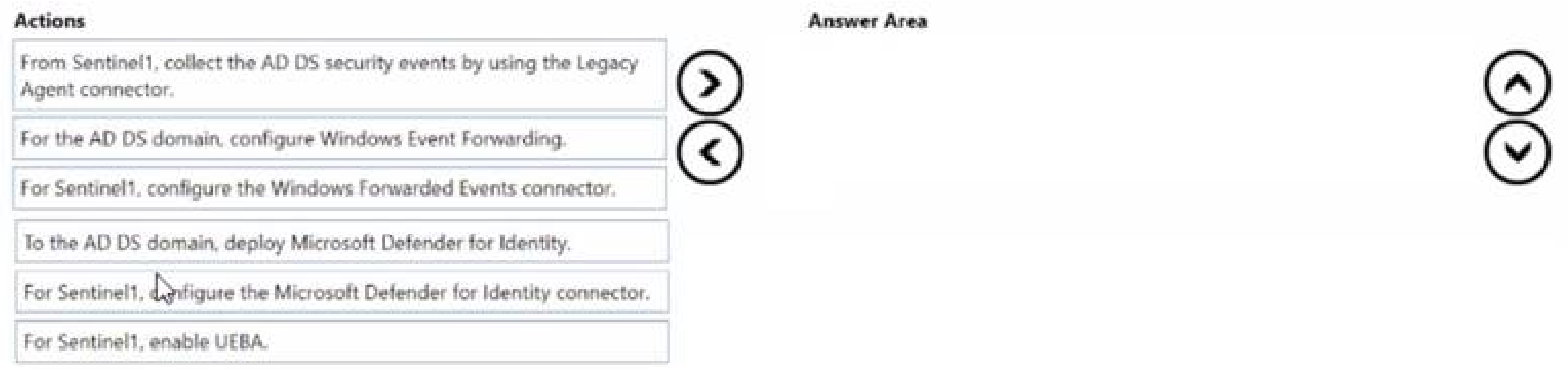
Explanation:
Defender for Cloud depends on the Log Analytics agent. Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage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

NEW QUESTION 185
- (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 186
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

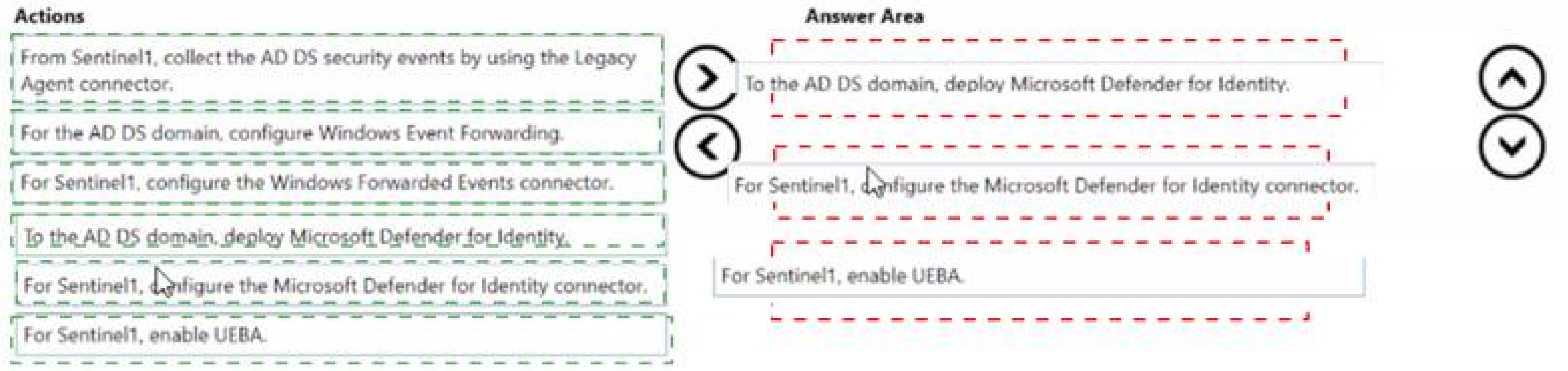
- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure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

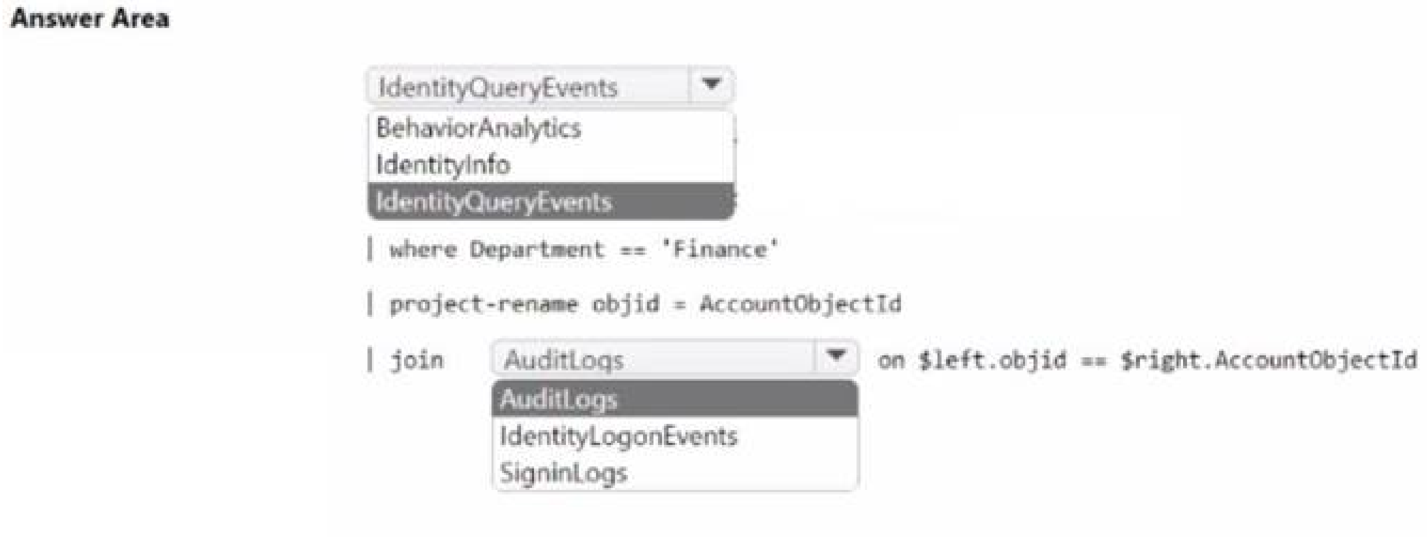
Answer Area

- 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 187

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.



Answer Area

IdentityQueryEvents ▼
BehaviorAnalytics
IdentityInfo
IdentityQueryEvents

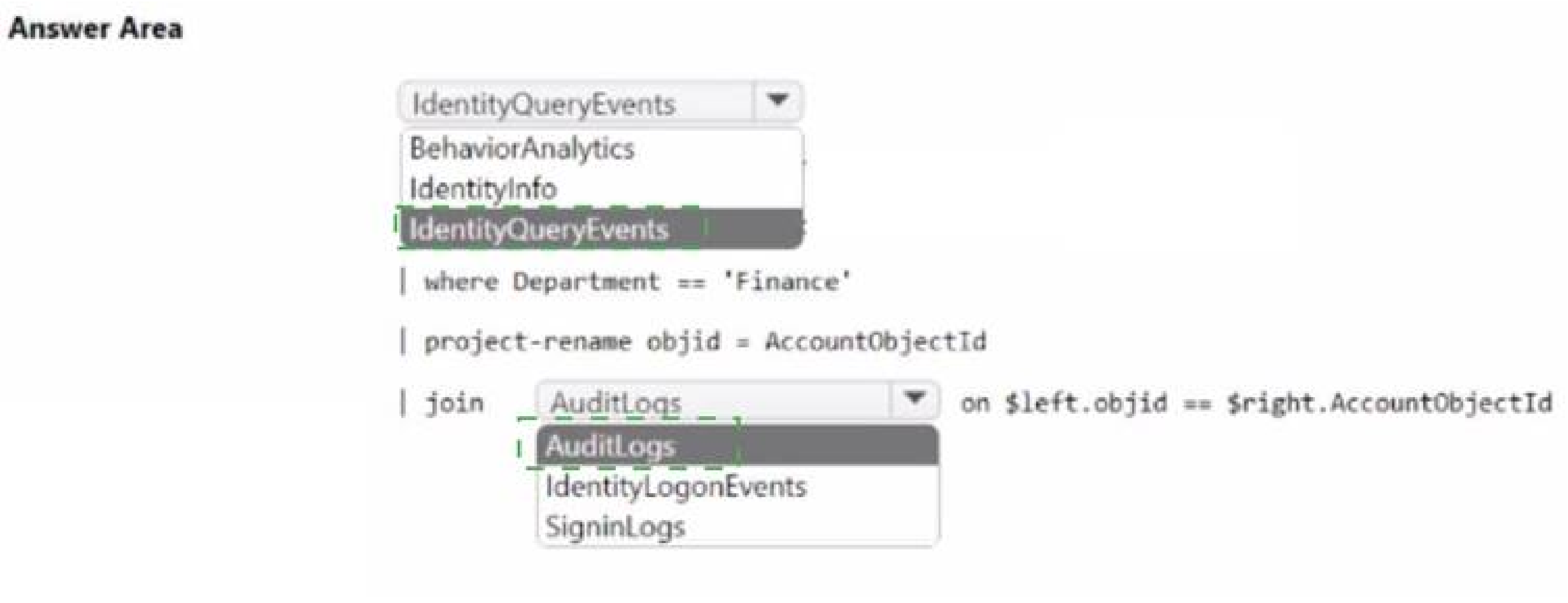
```
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join  [AuditLogs ▼]  on $left.objid == $right.AccountObjectId
```

AuditLogs
IdentityLogonEvents
SigninLogs

A. Mastered
B. Not Mastered

Answer: A

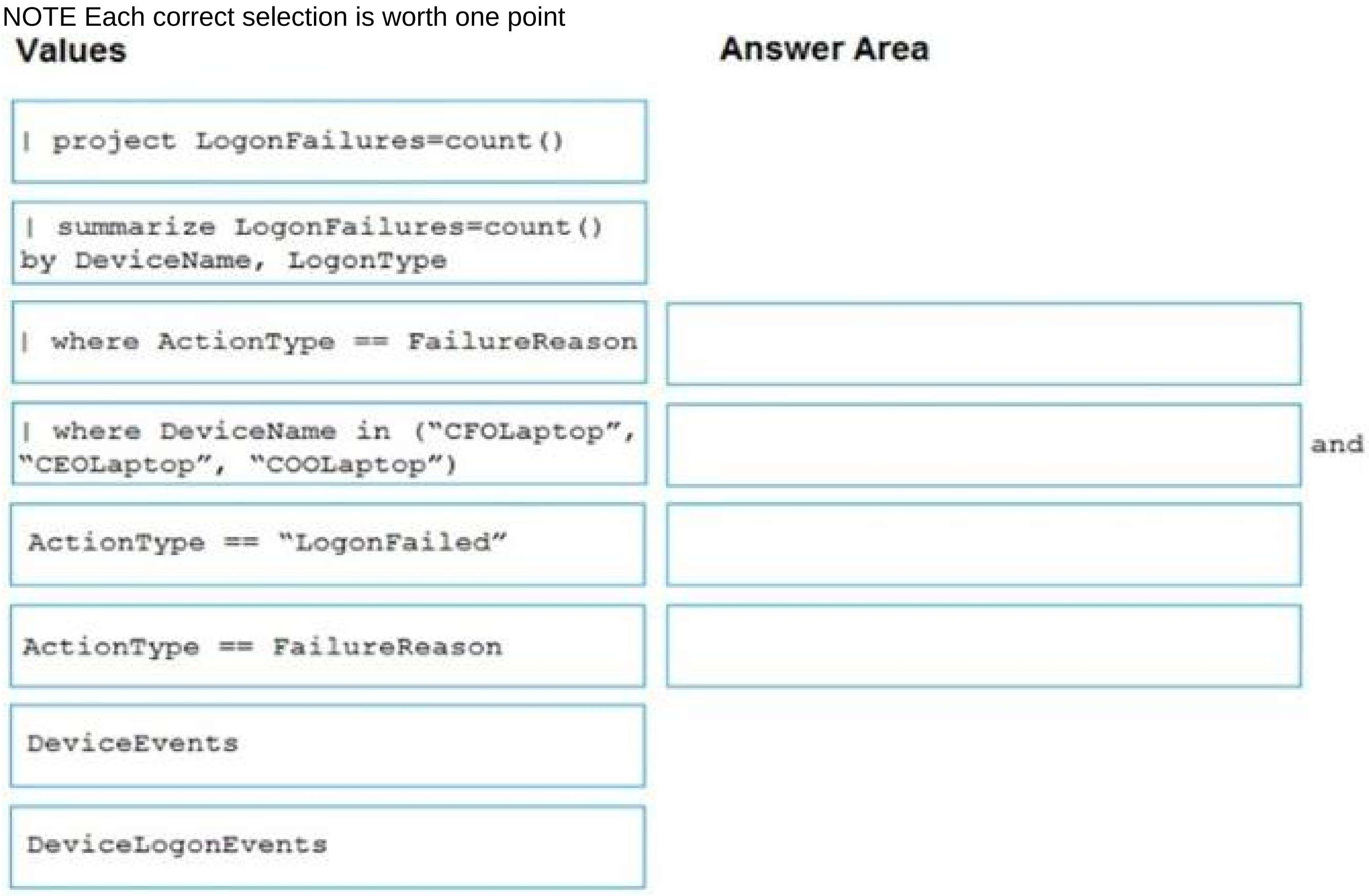
Explanation:



Answer Area

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

NEW QUESTION 190
DRAG DROP - (Topic 4)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point



Values

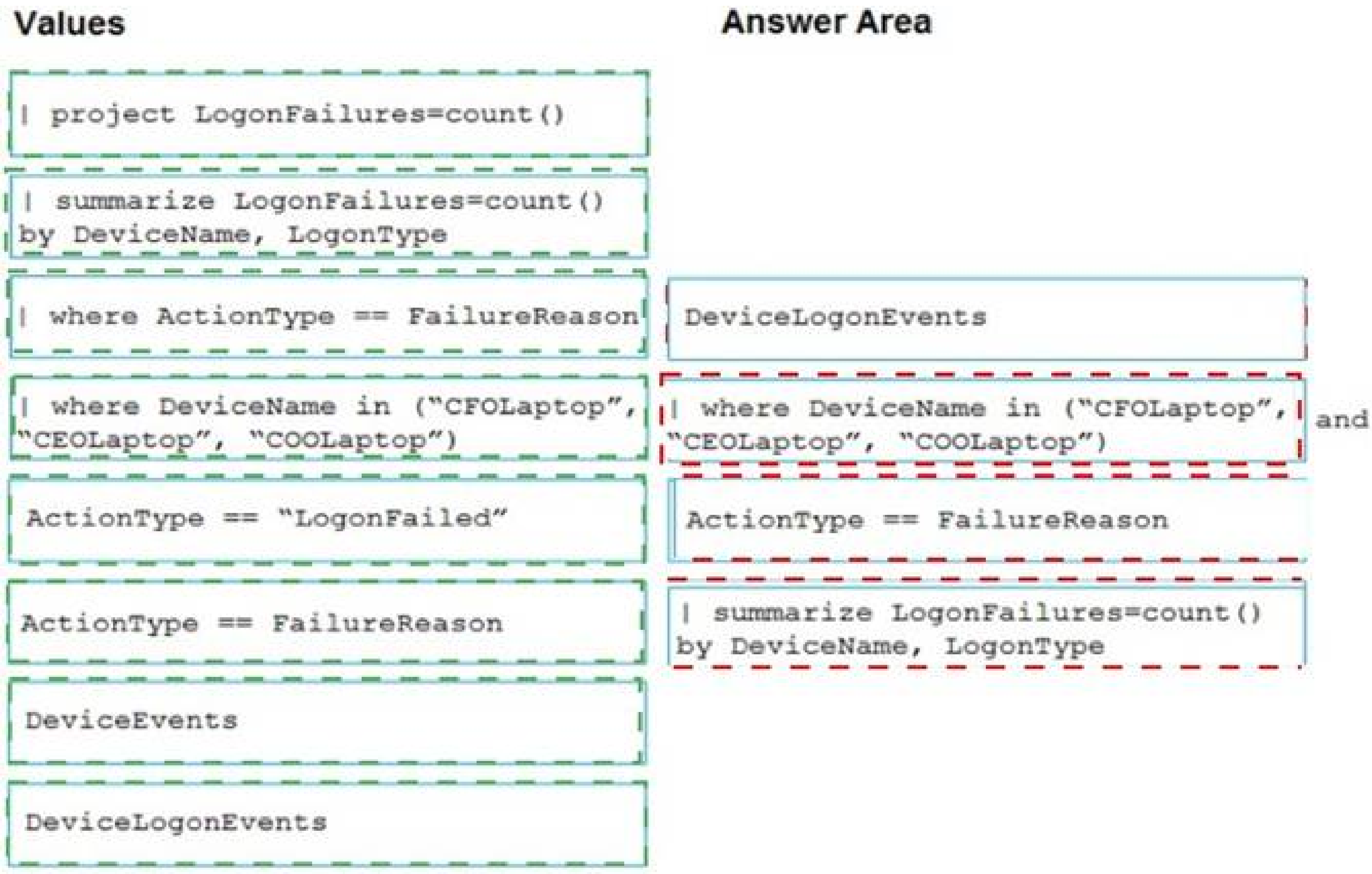
```
| project LogonFailures=count()
| summarize LogonFailures=count()
by DeviceName, LogonType
| where ActionType == FailureReason
| where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")
ActionType == "LogonFailed"
ActionType == FailureReason
DeviceEvents
DeviceLogonEvents
```

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Values

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

Answer Area

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

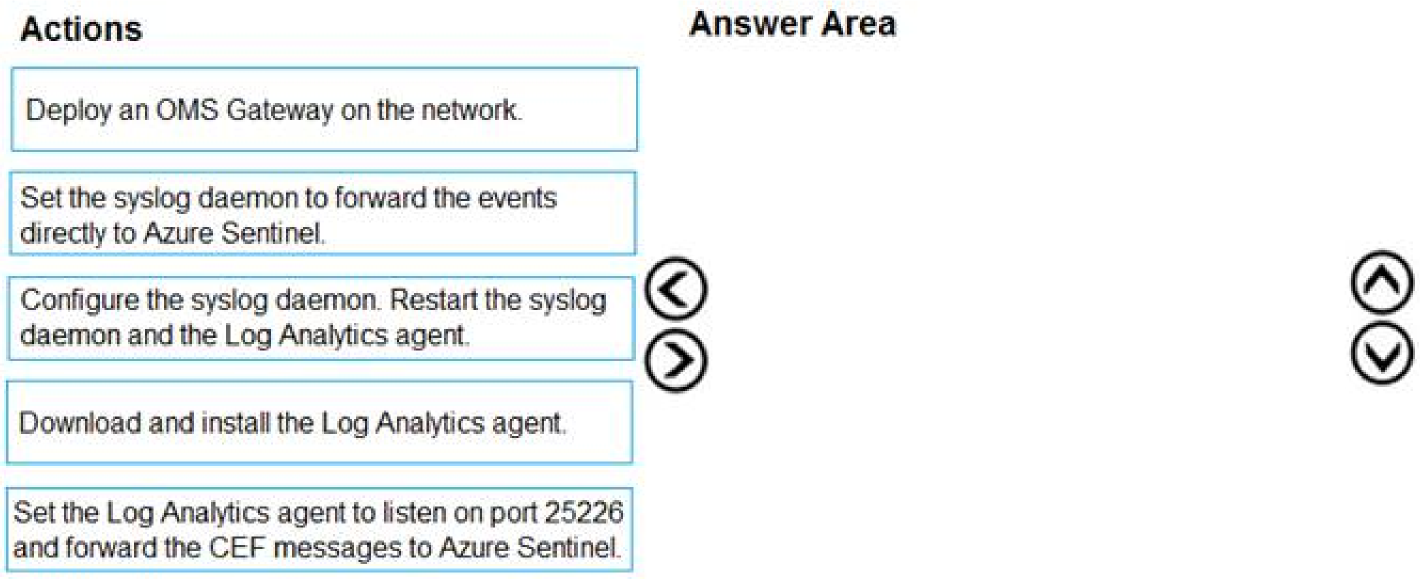
NEW QUESTION 195
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

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 197
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.

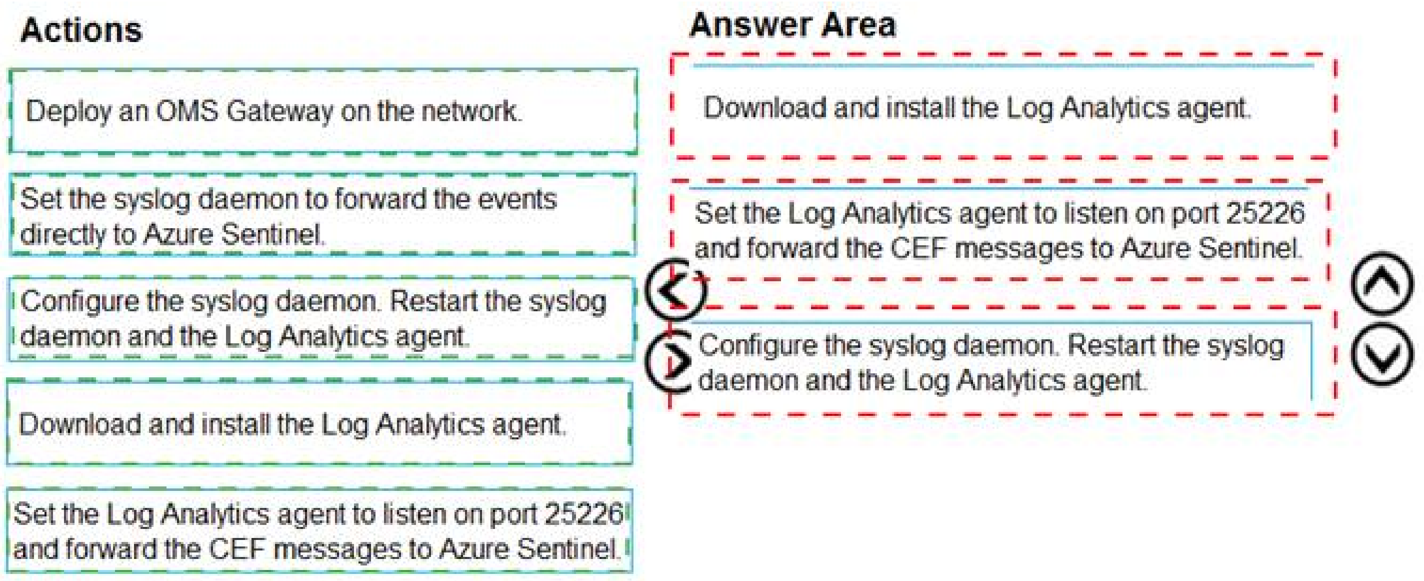
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

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.

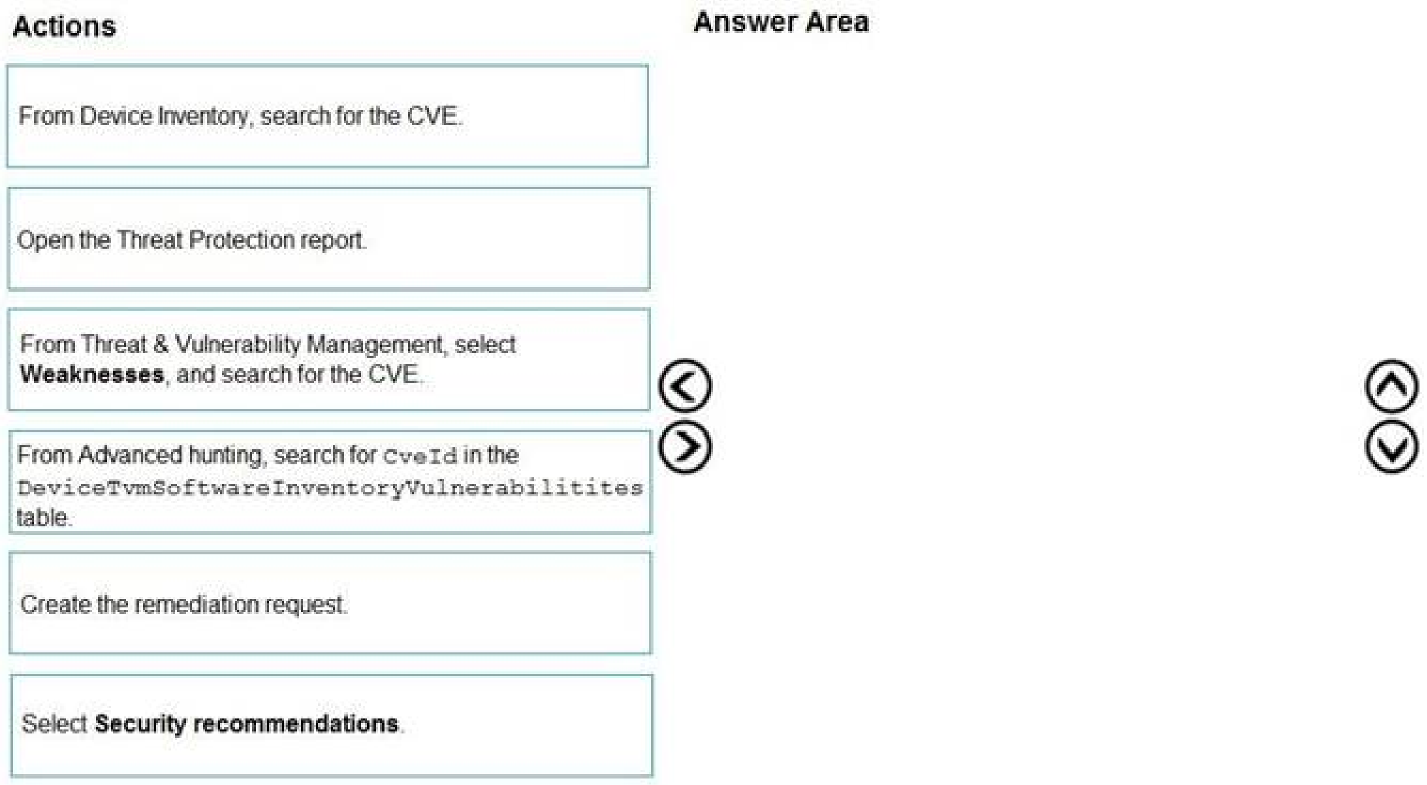
NEW QUESTION 201

DRAG DROP - (Topic 4)

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

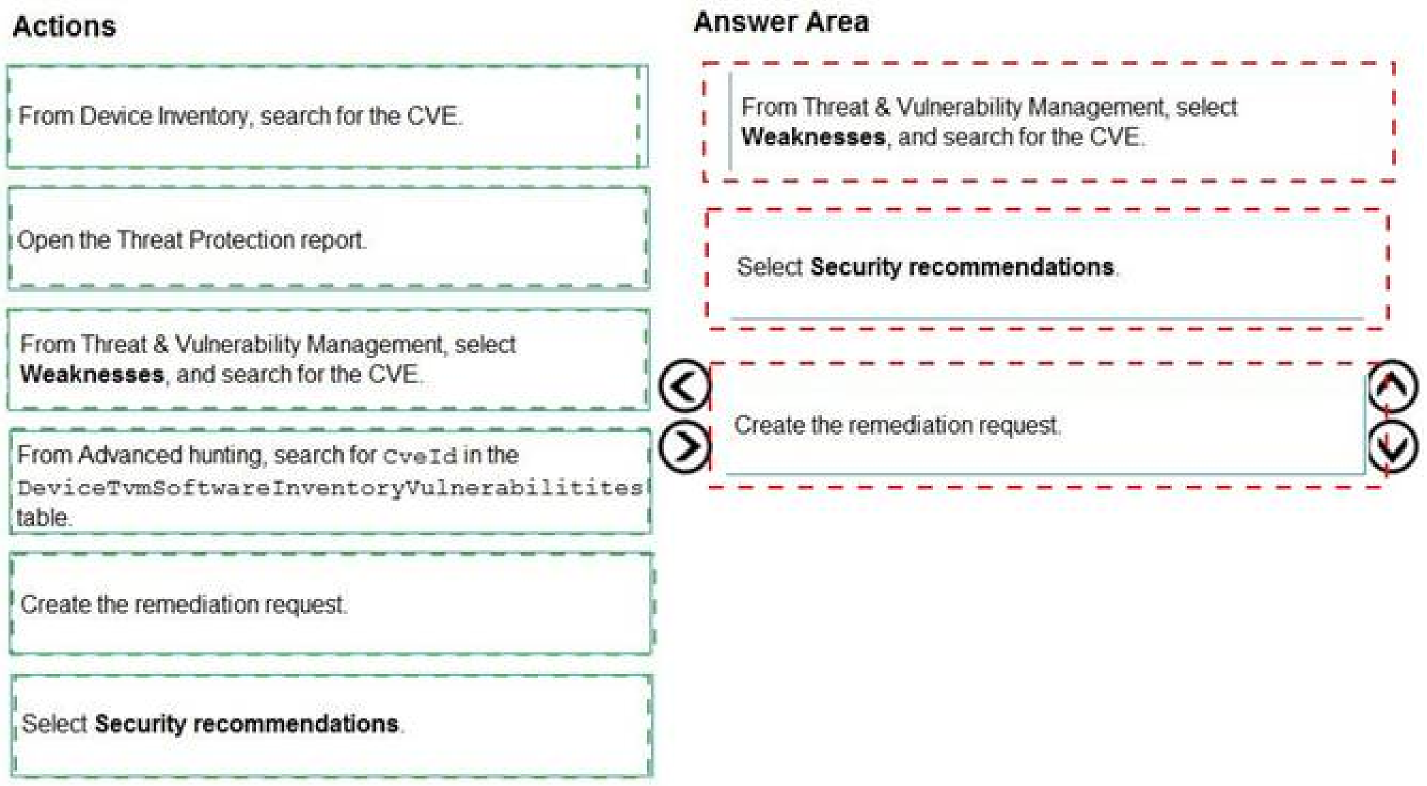
Answer Area

A. Mastered

B. Not Mastered

Answer: A

Explanation:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

NEW QUESTION 204
- (Topic 4)
You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.
You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.
What should you do first?

A. From Azure Security Center, add a workflow automation.
B. On VM1, run the Get-MPThreatCatalog cmdlet.
C. On VM1 trigger a PowerShell alert.
D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

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

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 213
- (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

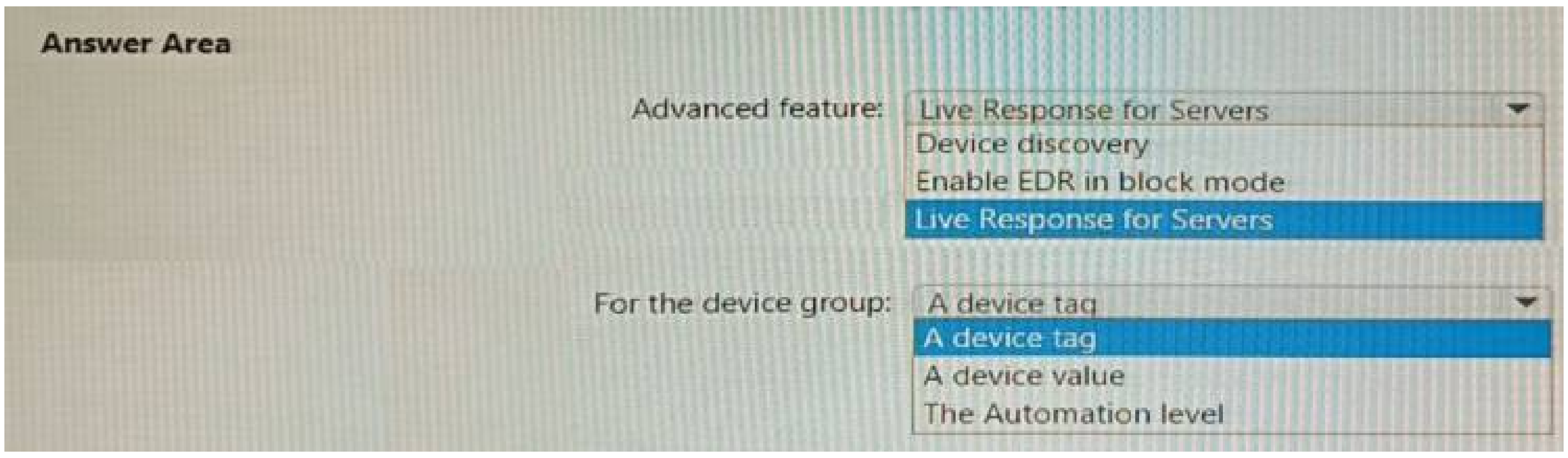
NEW QUESTION 215
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Enable Entity behavior analytics.
B. Associate a playbook to the analytics rule that triggered the incident.
C. Enable the Fusion rule.
D. Add a playbook.
E. Create a workbook.

Answer: AB

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

NEW QUESTION 216
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.
You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

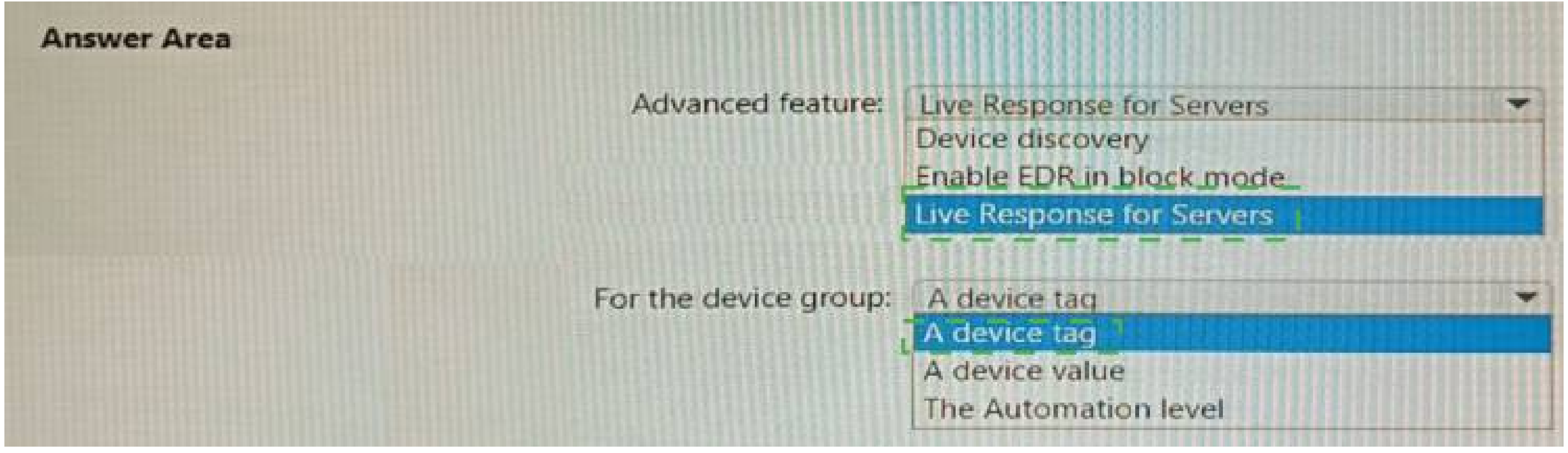
Advanced feature: Live Response for Servers
- Device discovery
- Enable EDR in block mode
- Live Response for Servers

For the device group: A device tag
- A device tag
- A device value
- The Automation level

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Advanced feature: Live Response for Servers
- Device discovery
- Enable EDR in block mode
- Live Response for Servers

For the device group: A device tag
- A device tag
- A device value
- The Automation level

NEW QUESTION 221
- (Topic 4)
You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

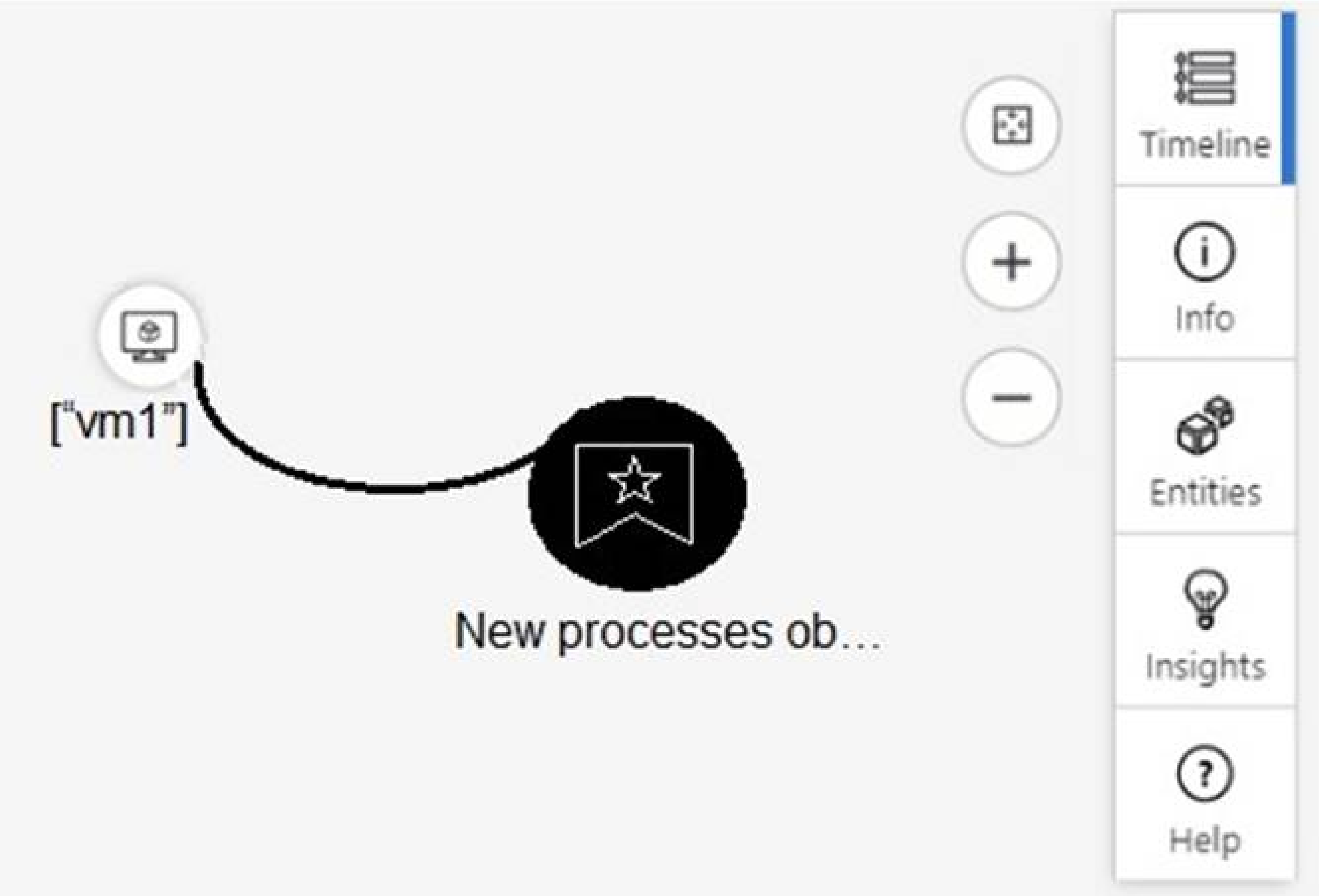
You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create a detection rule.
B. Create a suppression rule.
C. Add | order by Timestamp to the query.
D. Block DeviceProcessEvents with DeviceNetworkEvents.
E. Add DeviceId and ReportId to the output of the query.

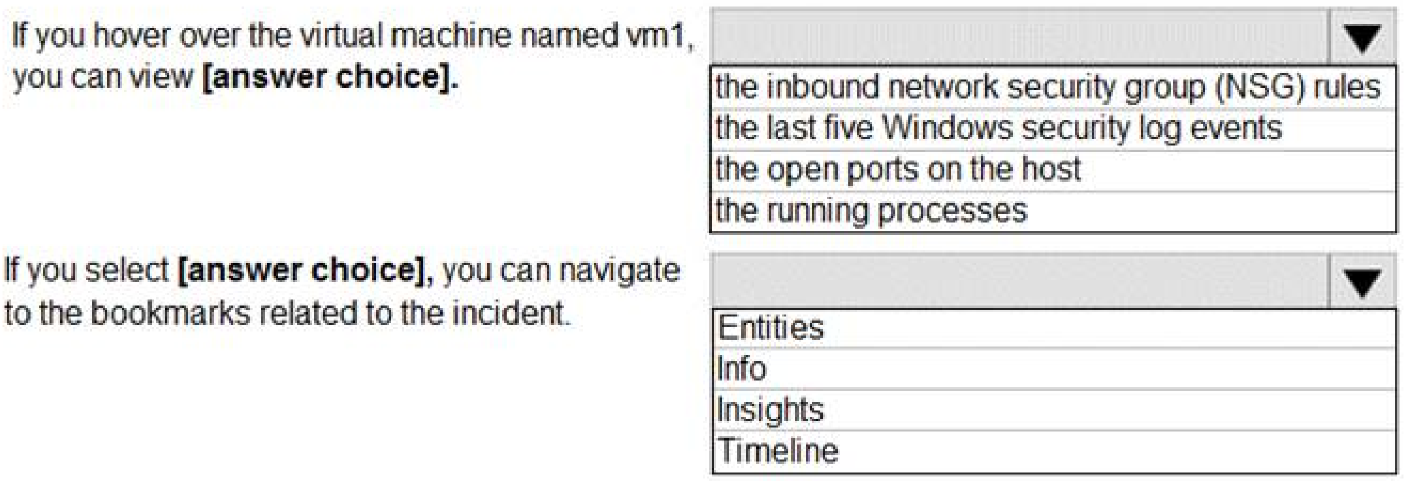
Answer: AE

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

NEW QUESTION 226
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

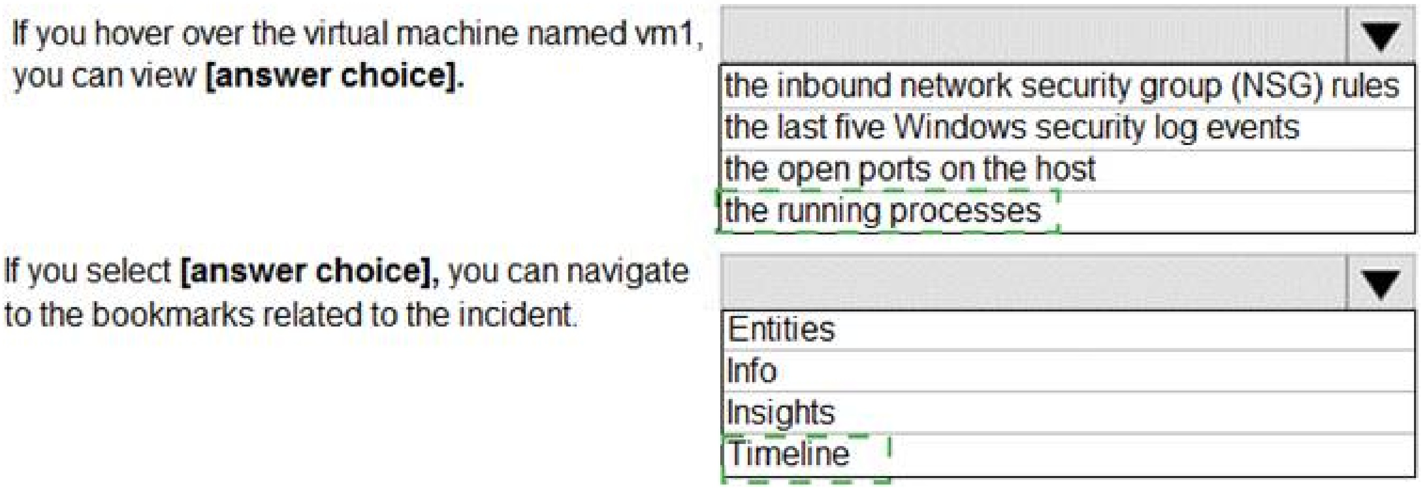
If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- 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 230
- (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 232
- (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 233
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

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

Answer: B

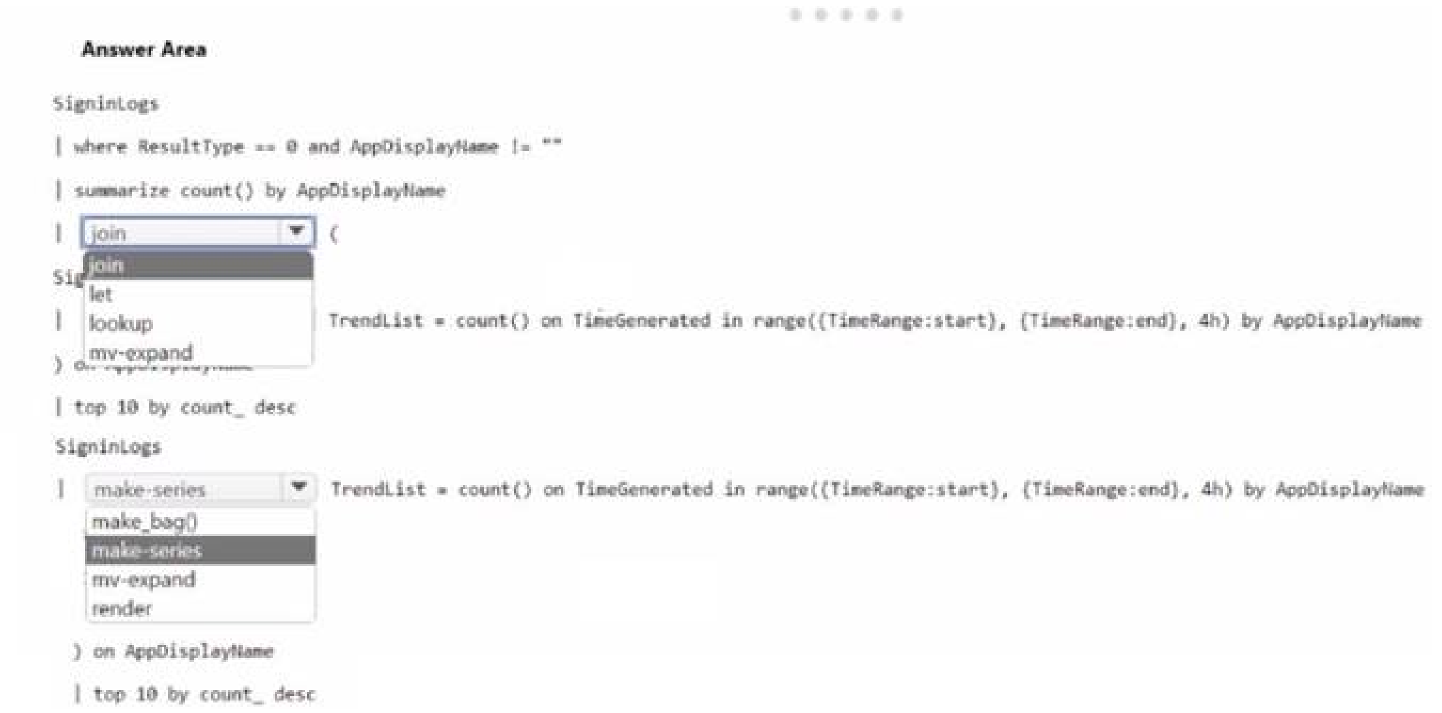
NEW QUESTION 237
- (Topic 4)
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part 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 242
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to configure a report visual for a custom workbook. The solution must meet the following requirements:
• The count and usage trend of AppDisplayName must be included
• The TrendList column must be useable in a sparkline visual,
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



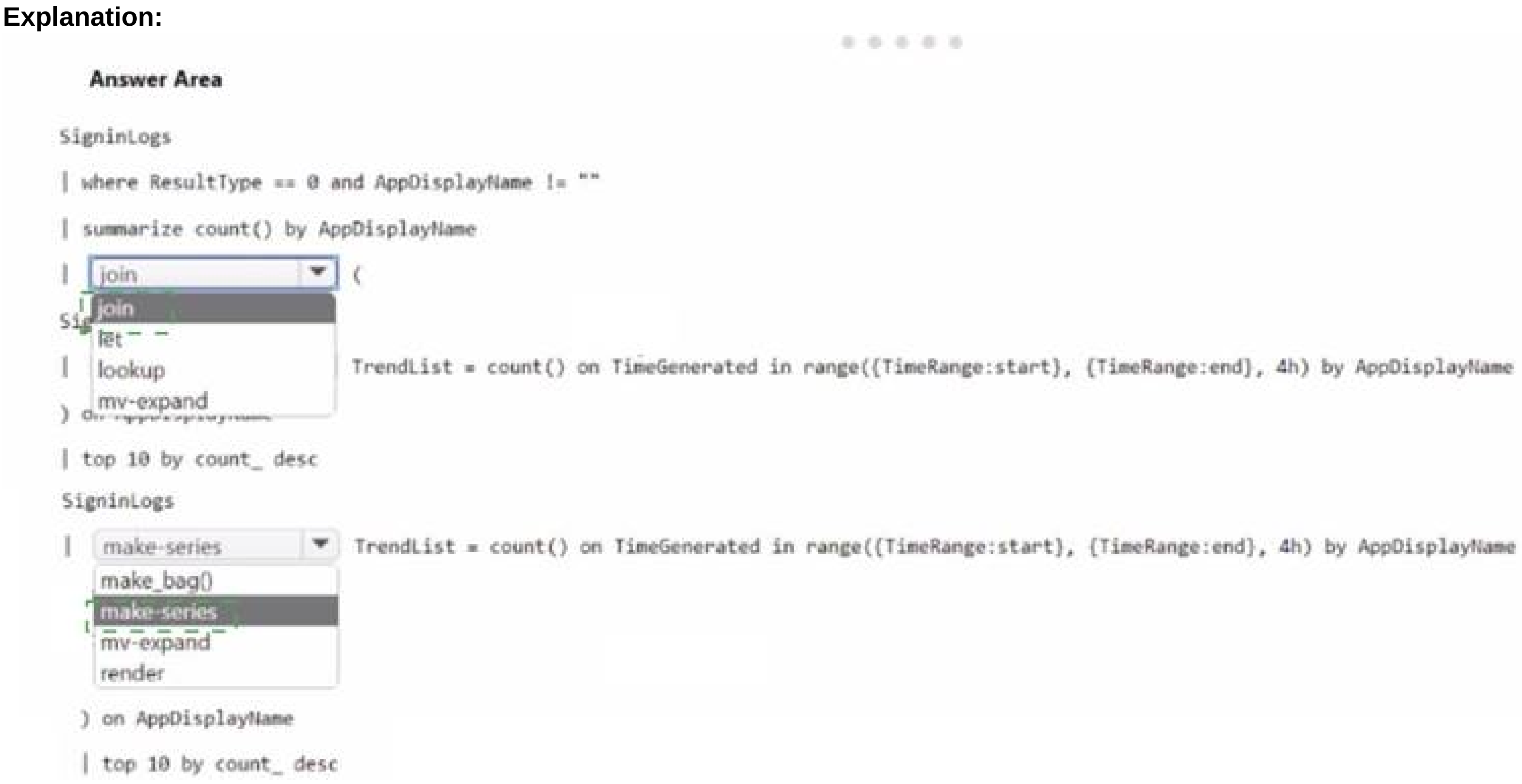
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 243
- (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 248
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

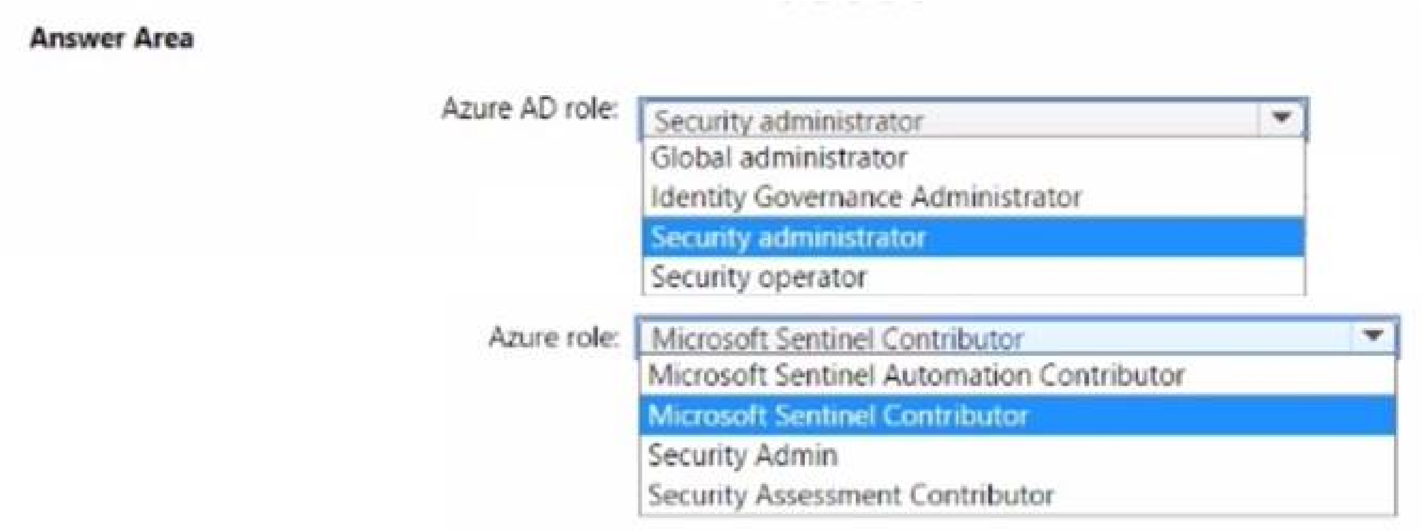
A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Answer: C

Explanation:
Reference:

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

NEW QUESTION 249
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.
Which roles should you assign to Used? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

Azure AD role: Security administrator

Global administrator
Identity Governance Administrator
Security administrator
Security operator

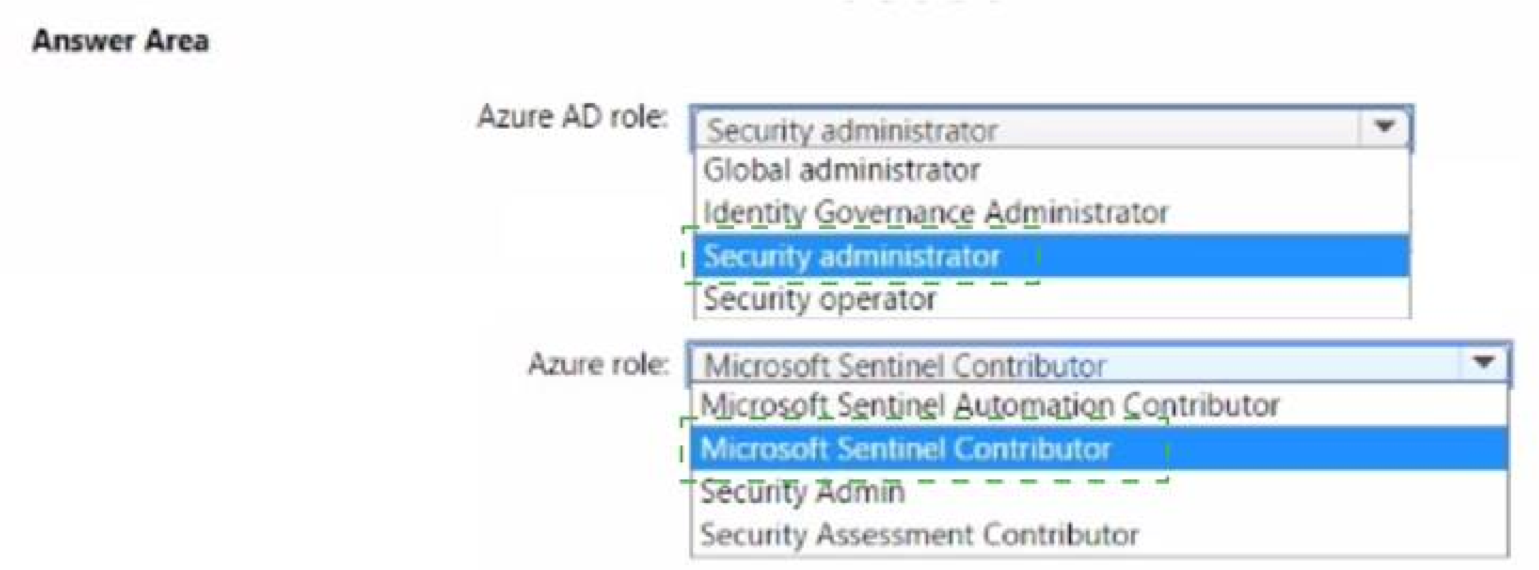
Azure role: Microsoft Sentinel Contributor

Microsoft Sentinel Automation Contributor
Microsoft Sentinel Contributor
Security Admin
Security Assessment Contributor

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

Azure AD role: Security administrator

Global administrator
Identity Governance Administrator
Security administrator
Security operator

Azure role: Microsoft Sentinel Contributor

Microsoft Sentinel Automation Contributor
Microsoft Sentinel Contributor
Security Admin
Security Assessment Contributor

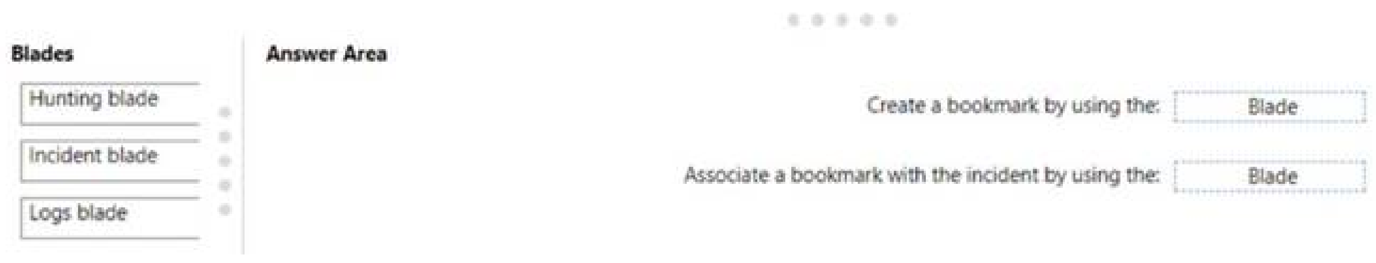
NEW QUESTION 252
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 257
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace that contains an Azure AD data connector. You need to associate a bookmark with an Azure AD-related incident.
What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade 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.



Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the: Blade

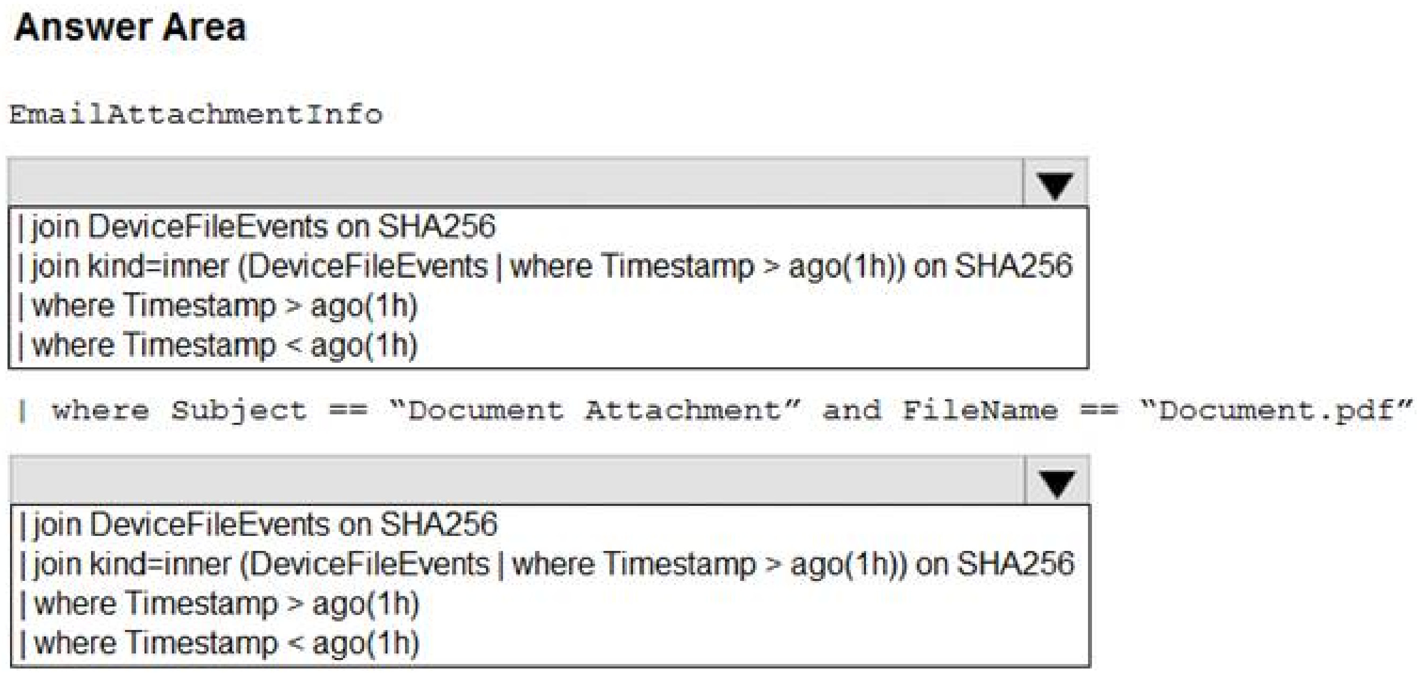
Associate a bookmark with the incident by using the: Blade

A. Mastered
B. Not Mastered

Answer: A

Explanation:
You can use the Logs blade or incident blade to create a bookmark of an Azure AD-related incident. Once the bookmark is created, you can associate it with the incident by using the incident blade. This allows you to quickly and easily access important information related to the incident in the future.

NEW QUESTION 258
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:
• Only show emails sent during the last hour.
• Optimize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

```
EmailAttachmentInfo
```

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

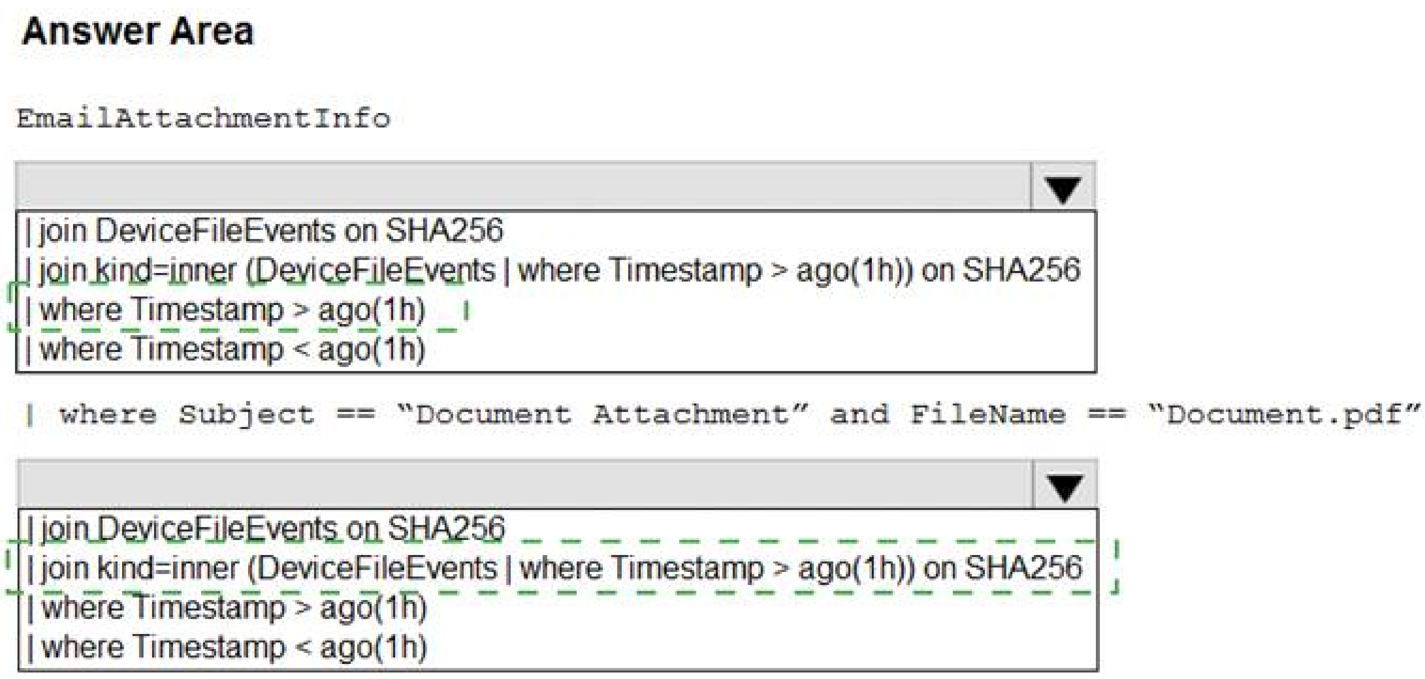
```
| where Subject == "Document Attachment" and FileName == "Document.pdf"
```

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

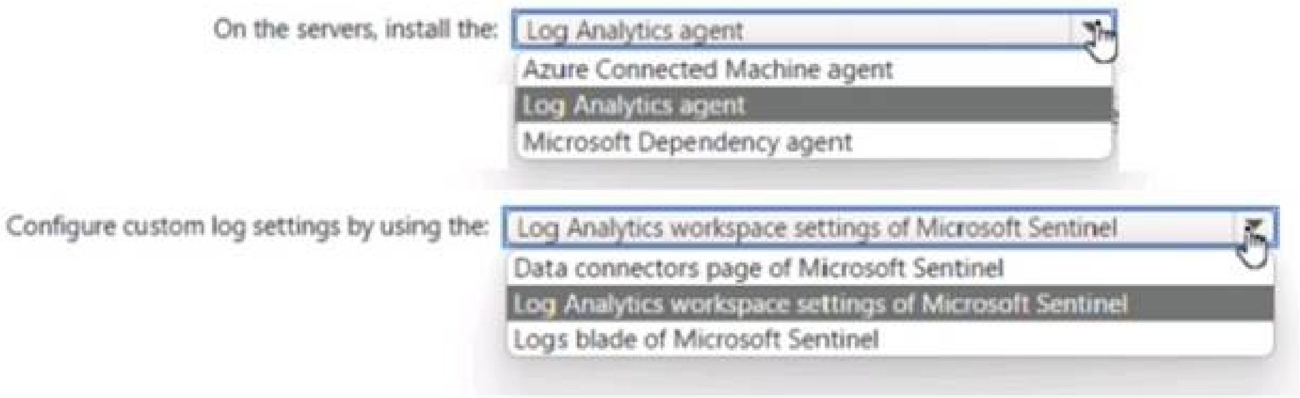
```
EmailAttachmentInfo
```

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

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

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

NEW QUESTION 263
HOTSPOT - (Topic 4)
Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.
You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options m the answer area.



On the servers, install the: Log Analytics agent

Azure Connected Machine agent
Log Analytics agent
Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

Data connectors page of Microsoft Sentinel
Log Analytics workspace settings of Microsoft Sentinel
Logs blade of Microsoft Sentinel

A. Mastered
B. Not Mastered

Answer: A

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

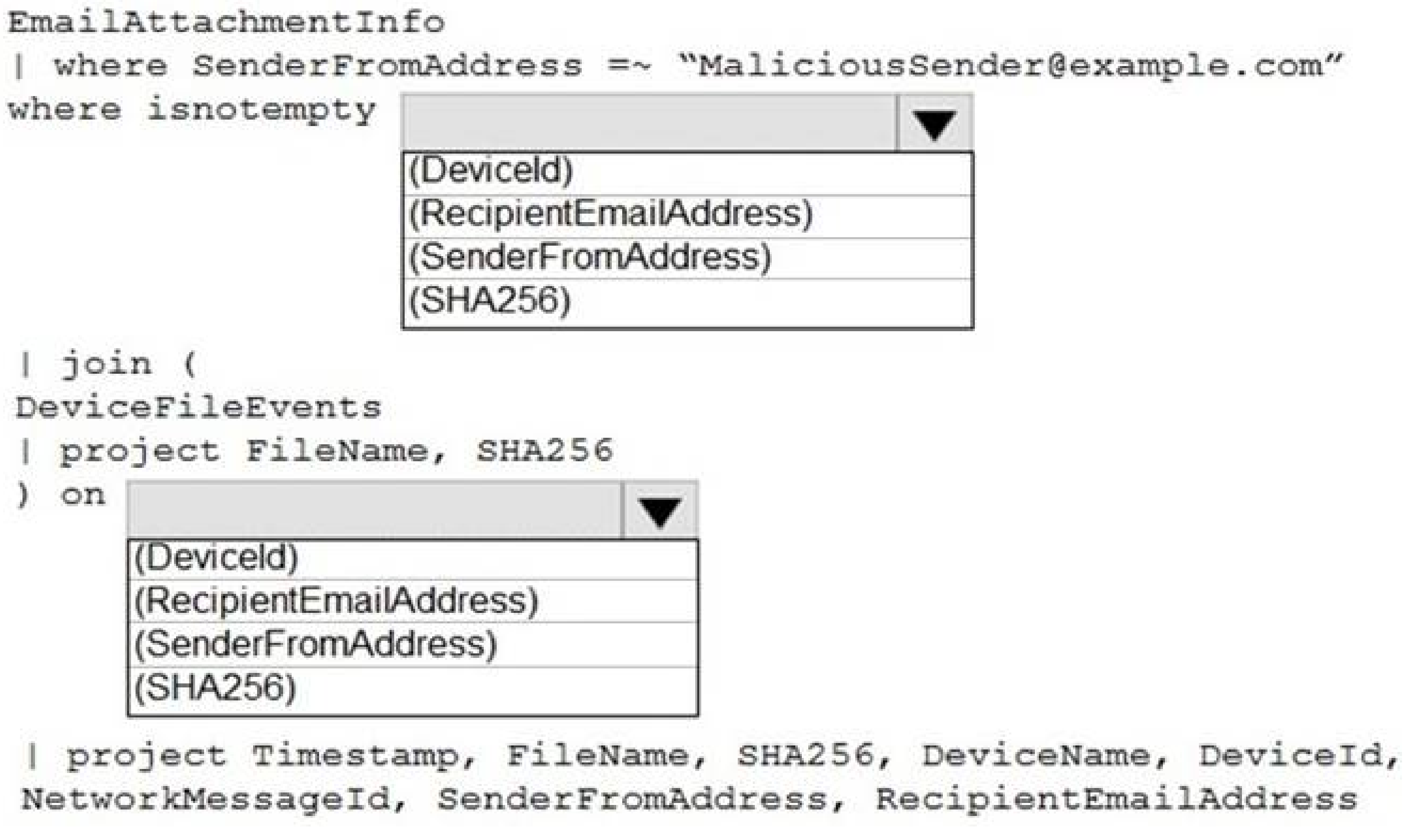
NEW QUESTION 265
- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a custom report that will visualise sign-in information over time.
What should you create first?

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

Answer: A

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

NEW QUESTION 266
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
```

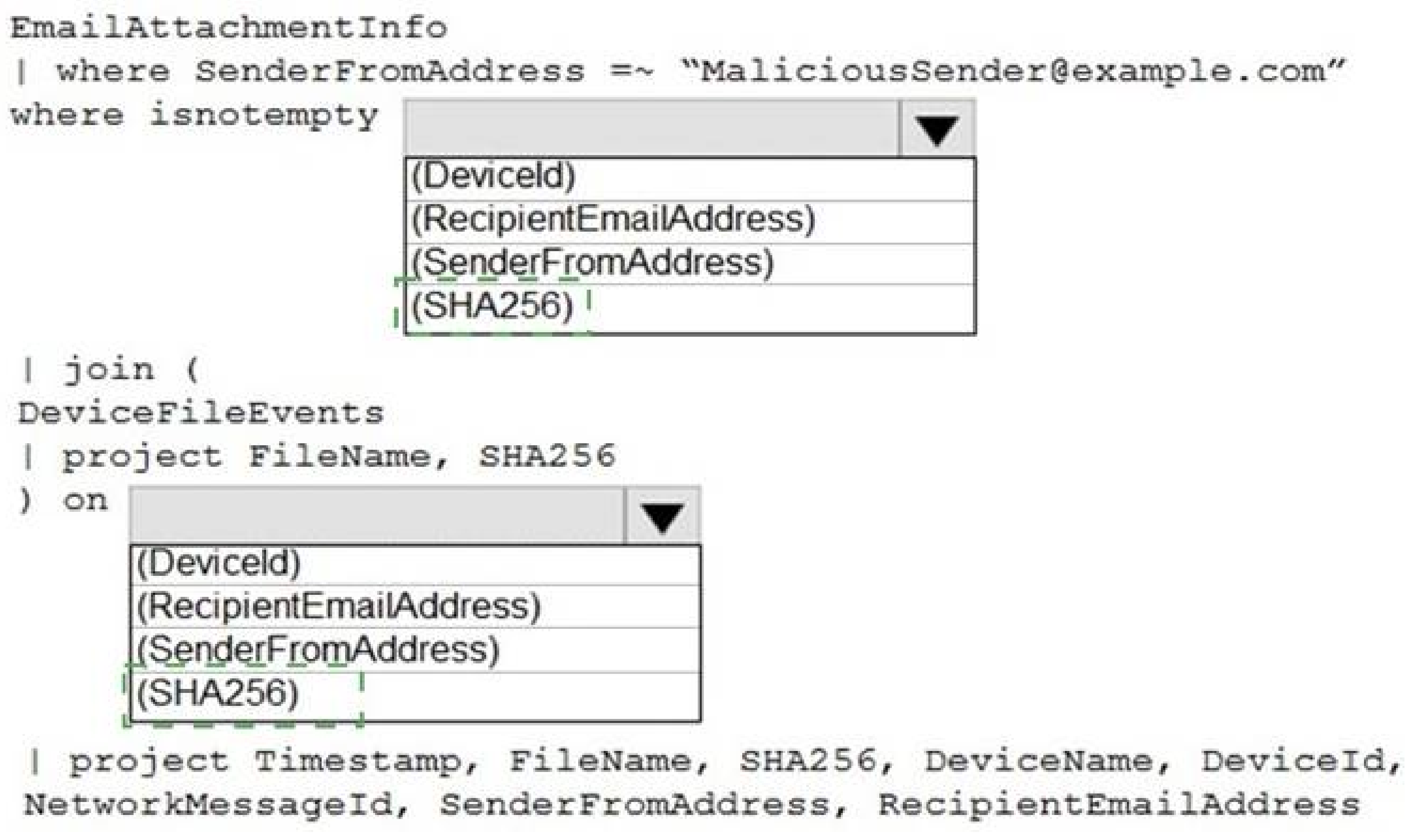
```
 | join (
 DeviceFileEvents
 | project FileName, SHA256
 ) on
```

```
 | 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
```

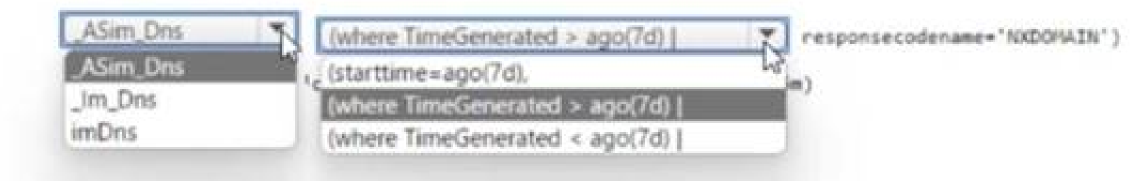
NEW QUESTION 269
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).
You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.
What should you install first on Server1?

A. the Microsoft Monitoring Agent
B. the Azure Arc agent
C. the Azure Monitor agent
D. the Azure Pipelines agent

Answer: C

NEW QUESTION 274
HOTSPOT - (Topic 4)
You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query?
To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area

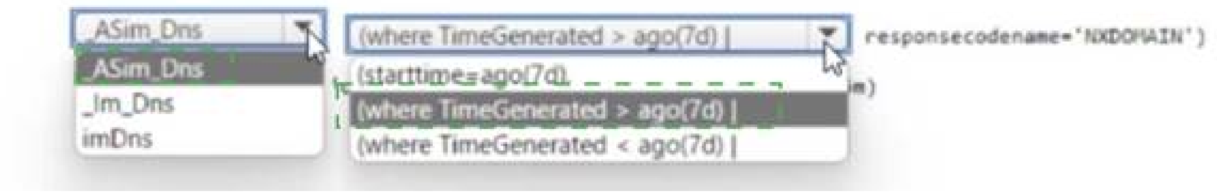


```
[_ASim_Dns ▼] [(where TimeGenerated > ago(7d) | ▼] responsecodename='NXDOMAIN')
 _ASim_Dns     (starttime=ago(7d),
 _Im_Dns       (where TimeGenerated > ago(7d) |
 imDns         (where TimeGenerated < ago(7d) |
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area



```
[_ASim_Dns ▼] [(where TimeGenerated > ago(7d) | ▼] responsecodename='NXDOMAIN')
 _ASim_Dns     (starttime=ago(7d),
 _Im_Dns       (where TimeGenerated > ago(7d) |
 imDns         (where TimeGenerated < ago(7d) |
```

NEW QUESTION 275
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.
You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort
Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting
B. Threat analytics
C. Incidents & alerts
D. Learning hub

Answer: B

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

NEW QUESTION 276
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.
What should you use in the Microsoft 365 Defender portal?

A. Incidents
B. Investigations
C. Advanced hunting
D. Remediation

Answer: A

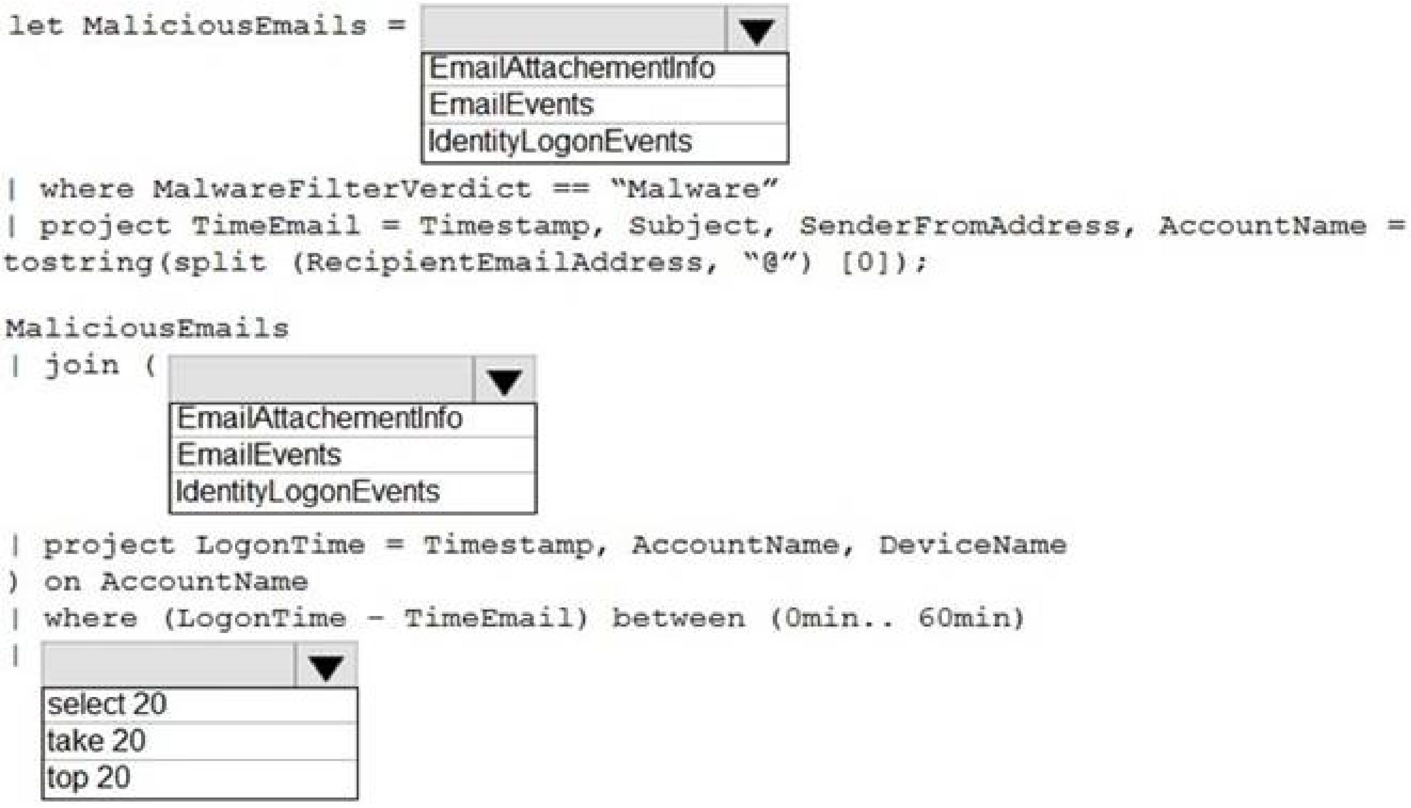
NEW QUESTION 278
- (Topic 4)
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

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

Answer: B

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

NEW QUESTION 279
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.

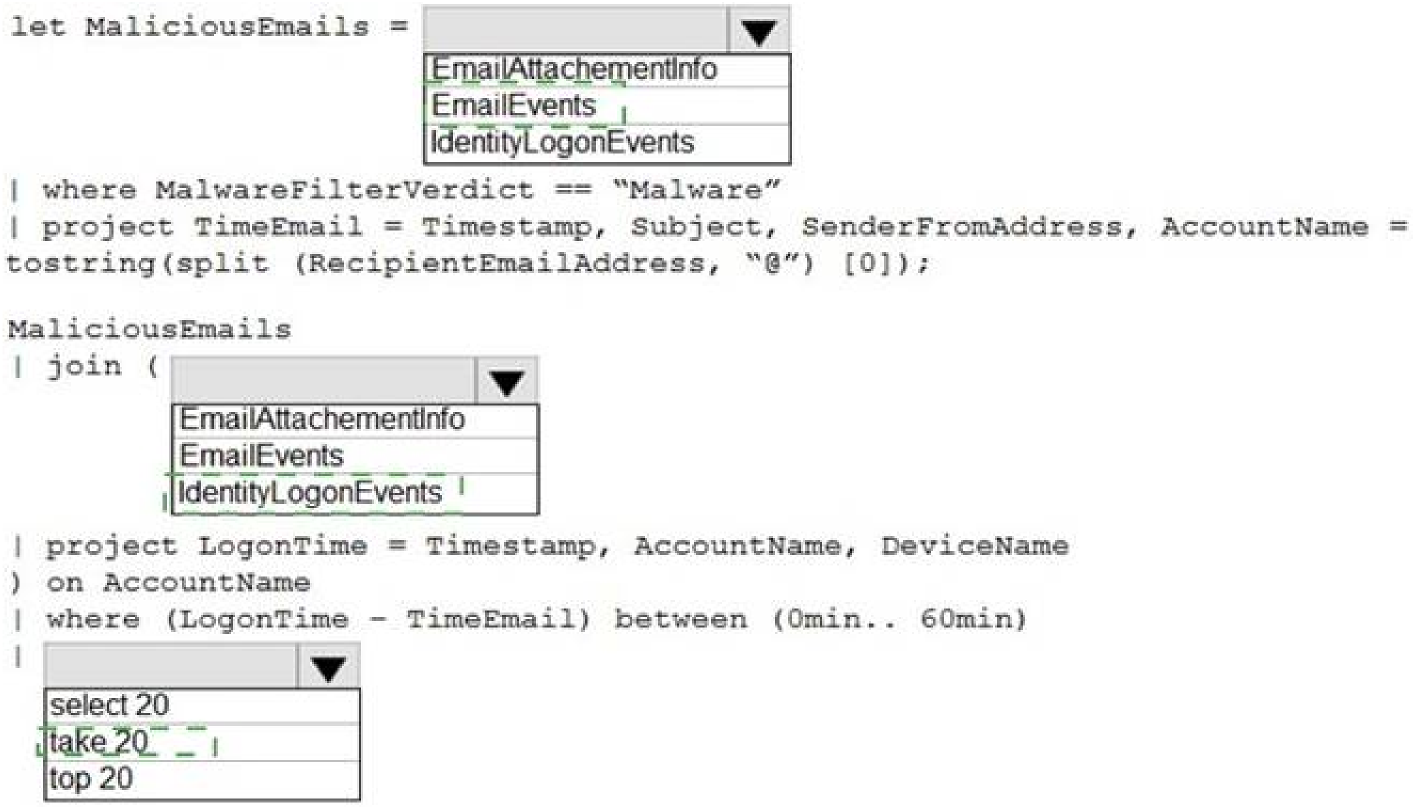


```
let MaliciousEmails =  [ ▼ ]
                        EmailAttachementInfo
                        EmailEvents
                        IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [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 284

......