Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

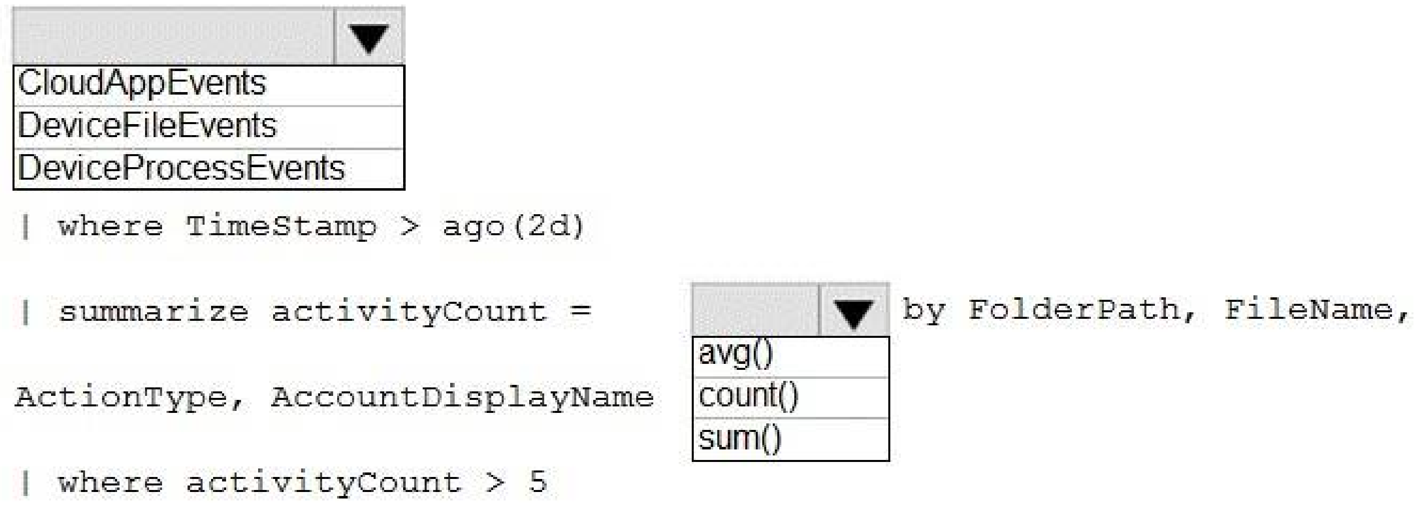
* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
HOTSPOT - (Topic 1)
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

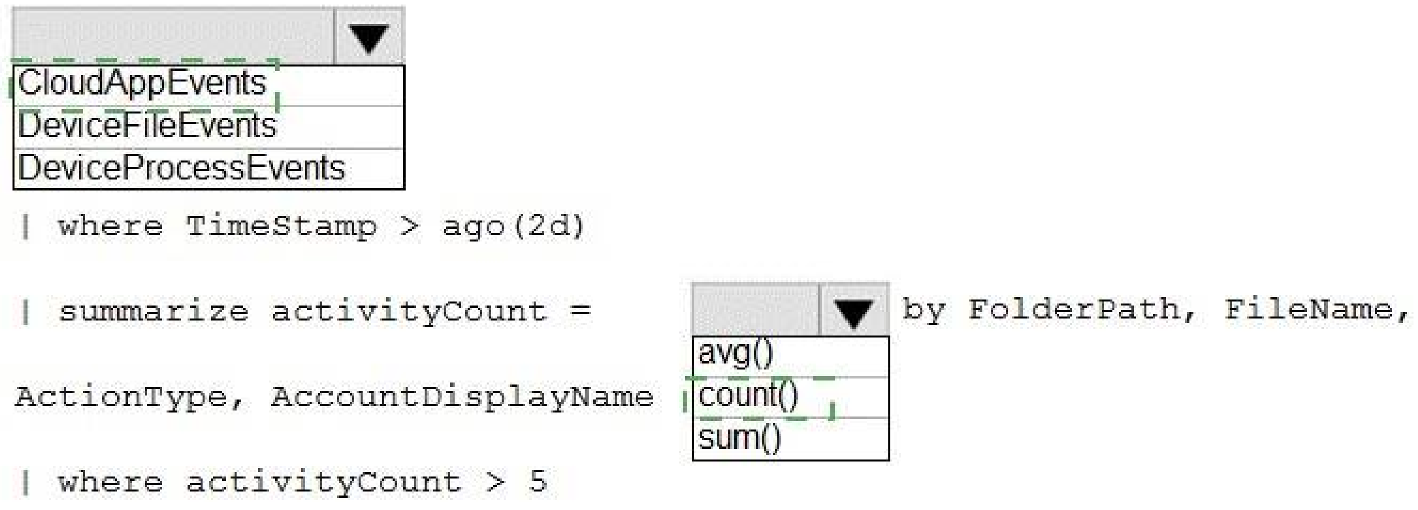
```
| where TimeStamp > ago(2d)
| summarize activityCount =            by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

avg()
count()
sum()

A. Mastered
B. Not Mastered

Answer: A

Explanation:



CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount =            by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

avg()
count()
sum()

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 complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

Answer: D

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

A. executive
B. sales

C. marketing

Answer: B

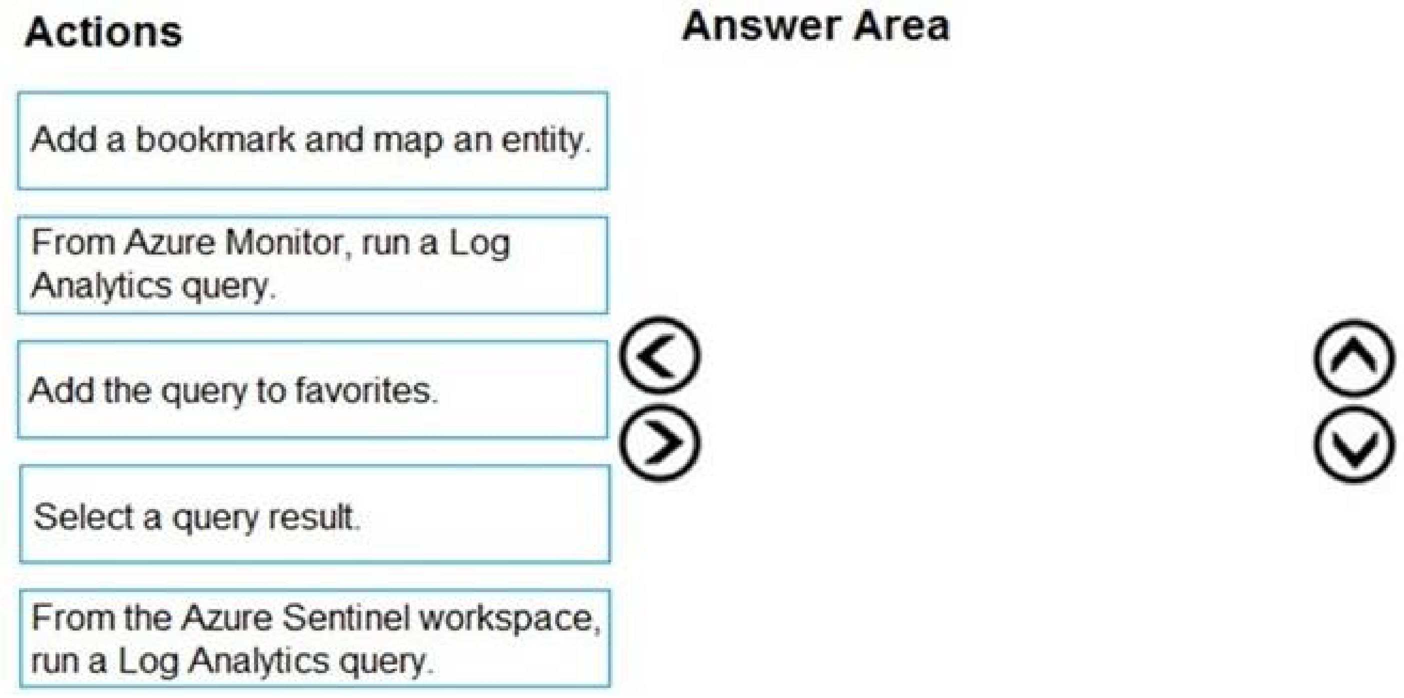
Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender- atp/microsoft- defender-atp-ios

NEW QUESTION 5
- (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 6
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

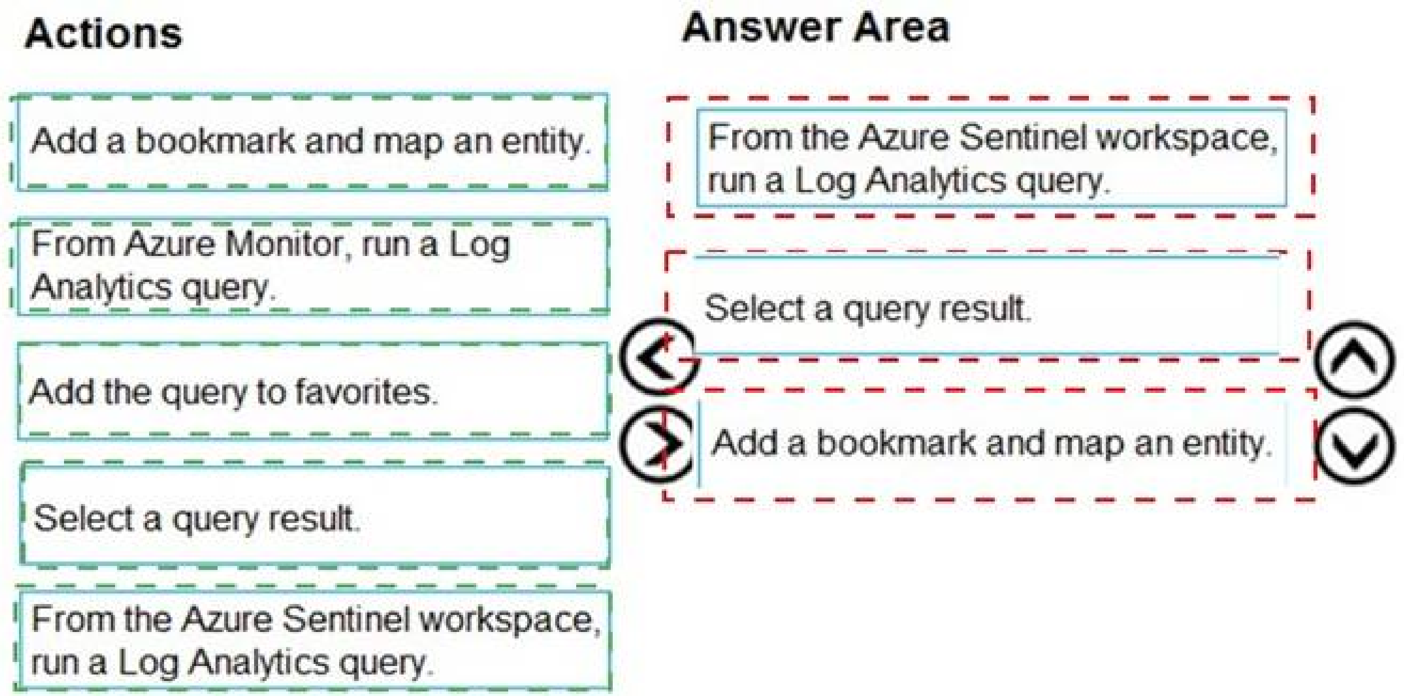
From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

Add a bookmark and map an entity.

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Select a query result.

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

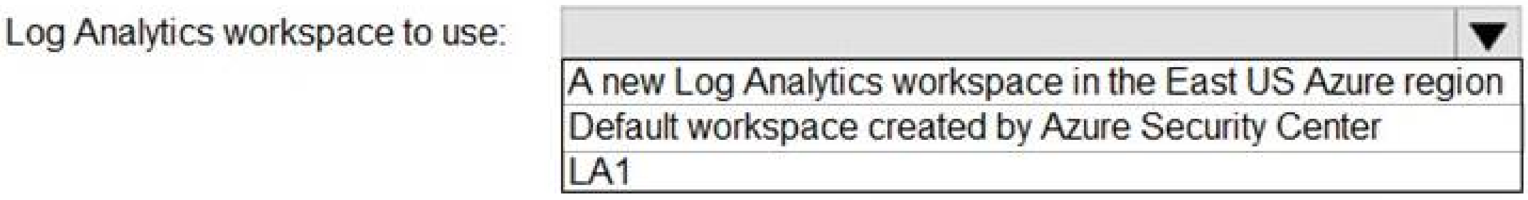
Answer Area

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

Select a query result.

Add a bookmark and map an entity.

NEW QUESTION 7
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

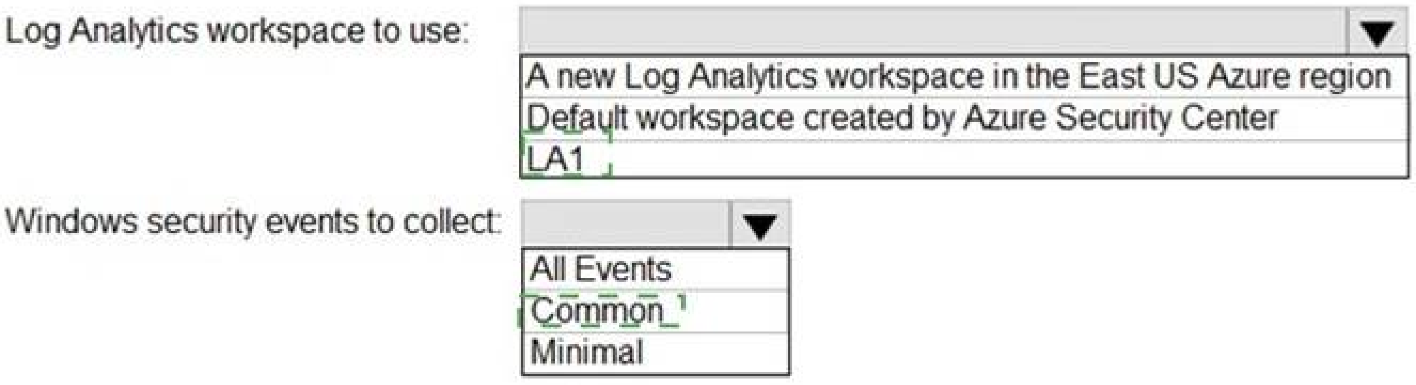
Windows security events to collect:

- All Events
- Common
- Minimal

A. Mastered
B. Not Mastered

Answer: A

Explanation:



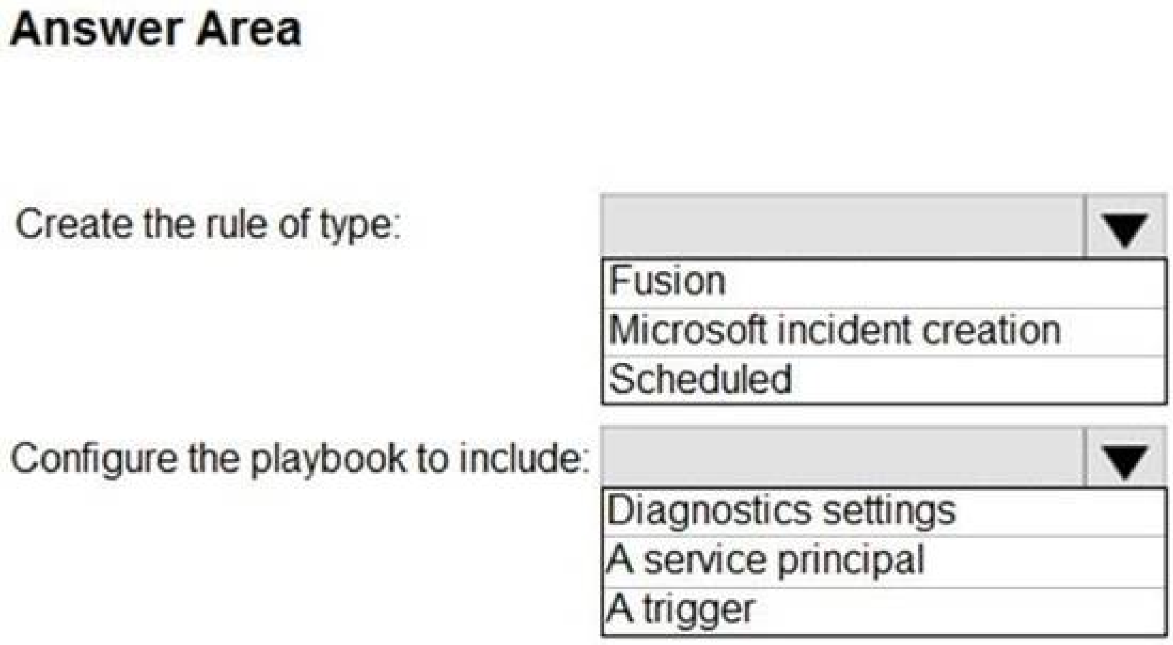
Log Analytics workspace to use:

- 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 8
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

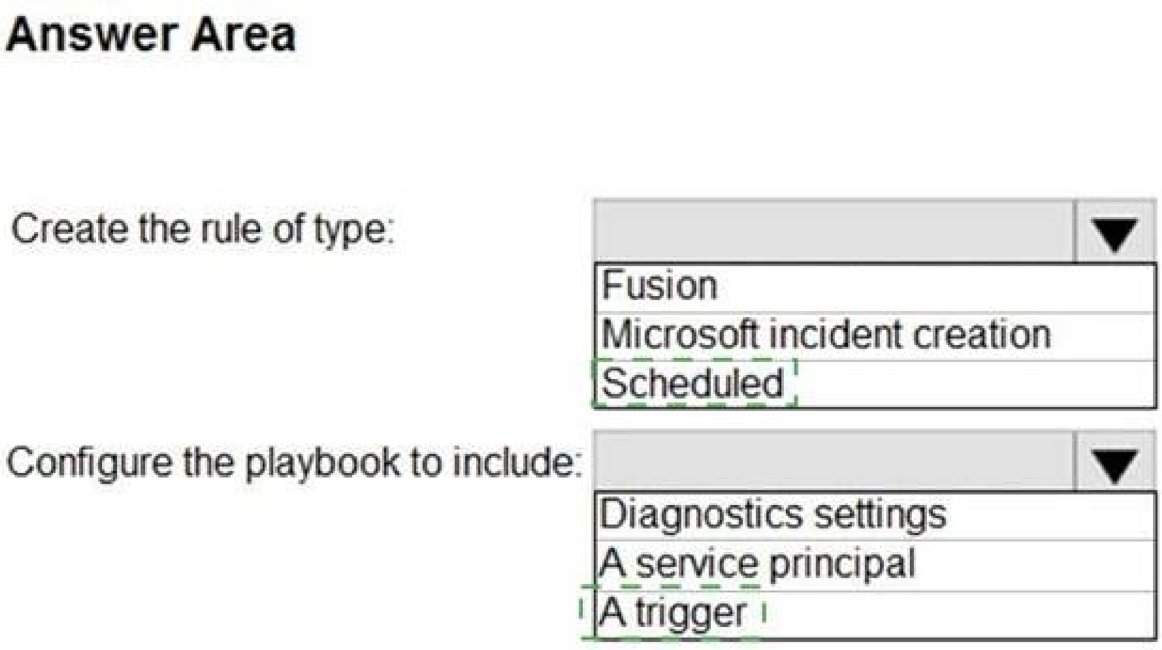
Configure the playbook to include:

- 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]

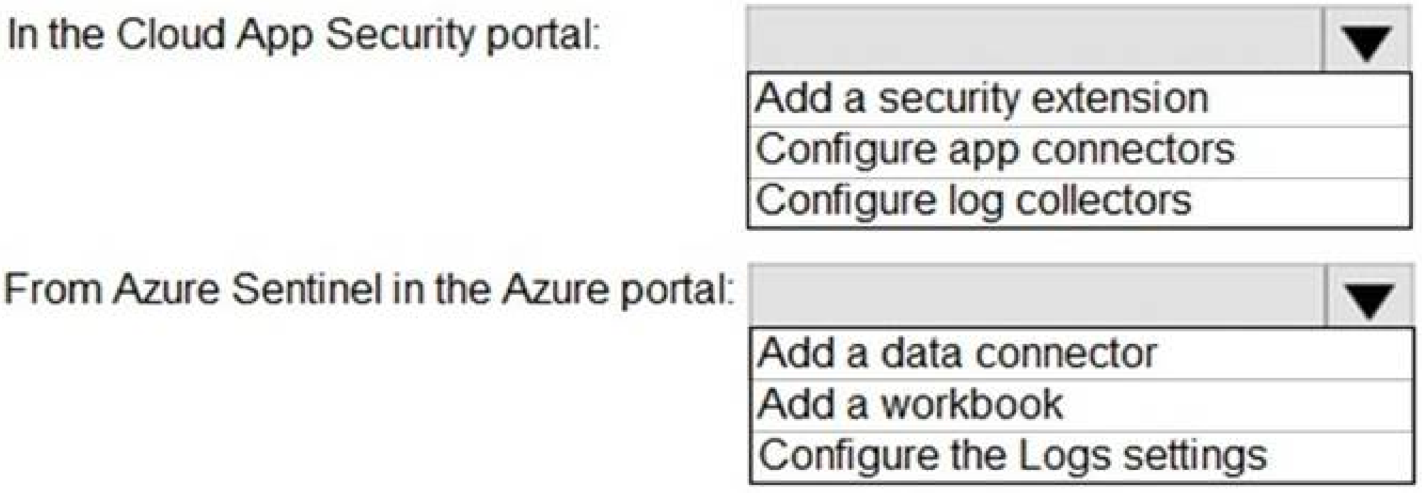
Configure the playbook to include: ▼
- Diagnostics settings
- A service principal
- [✓ A trigger]

NEW QUESTION 9
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.
Which policy should you modify?

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

Answer: D

NEW QUESTION 10
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.



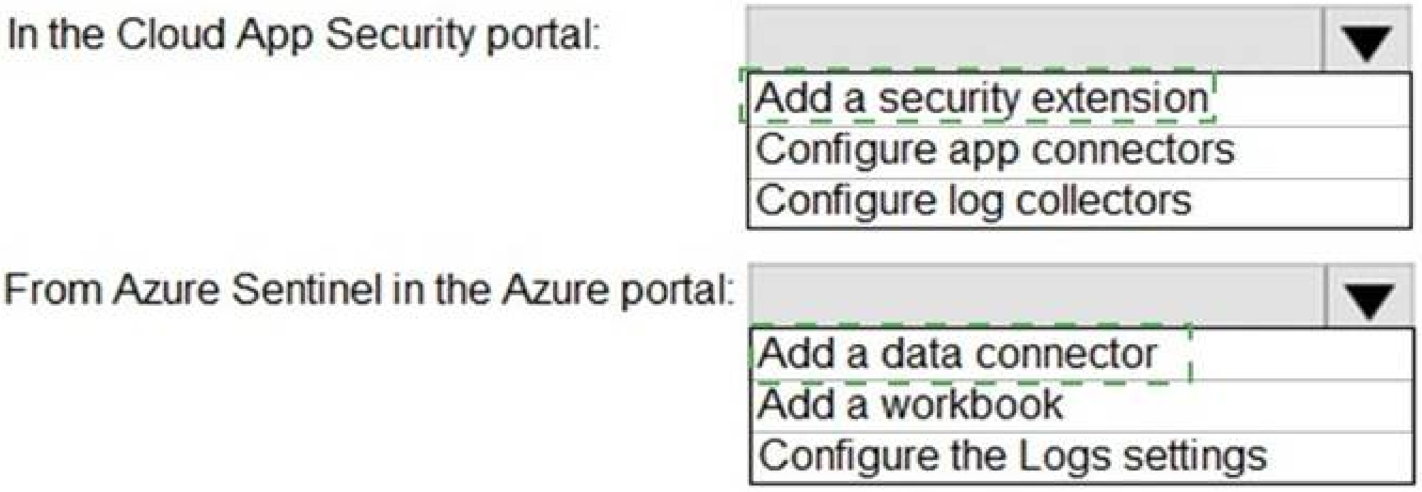
In the Cloud App Security portal: ▼
- Add a security extension
- Configure app connectors
- Configure log collectors

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

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

Answer: C

NEW QUESTION 15
- (Topic 2)
You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

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

Answer: C

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

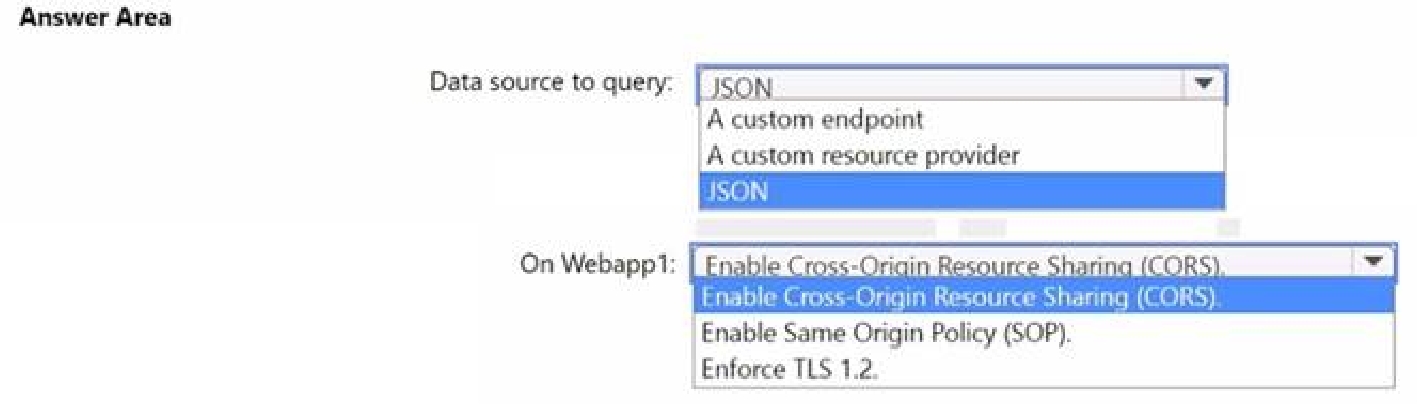
NEW QUESTION 17
- (Topic 2)
You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

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

Answer: C

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

NEW QUESTION 19
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

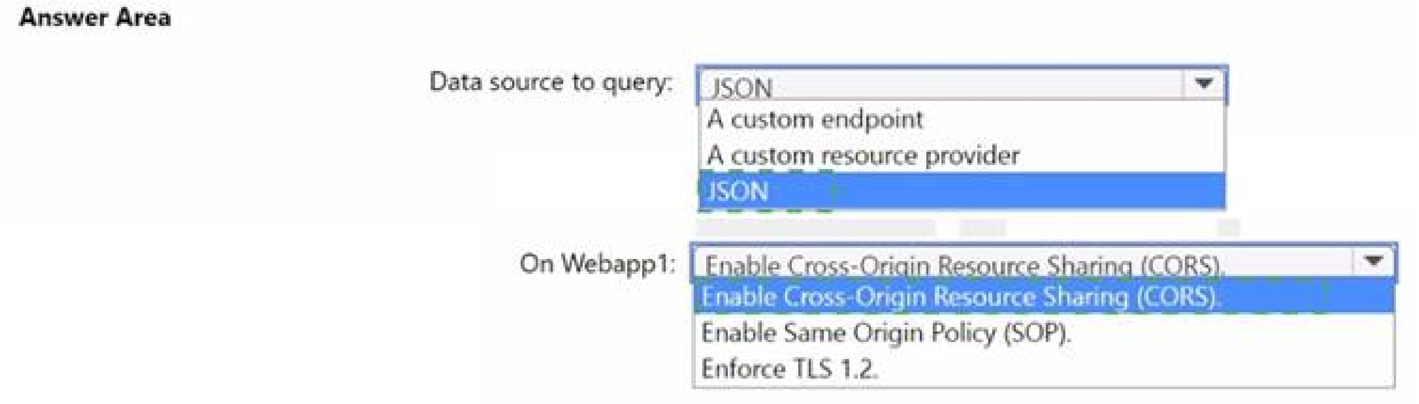
Data source to query: JSON
A custom endpoint
A custom resource provider
JSON

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

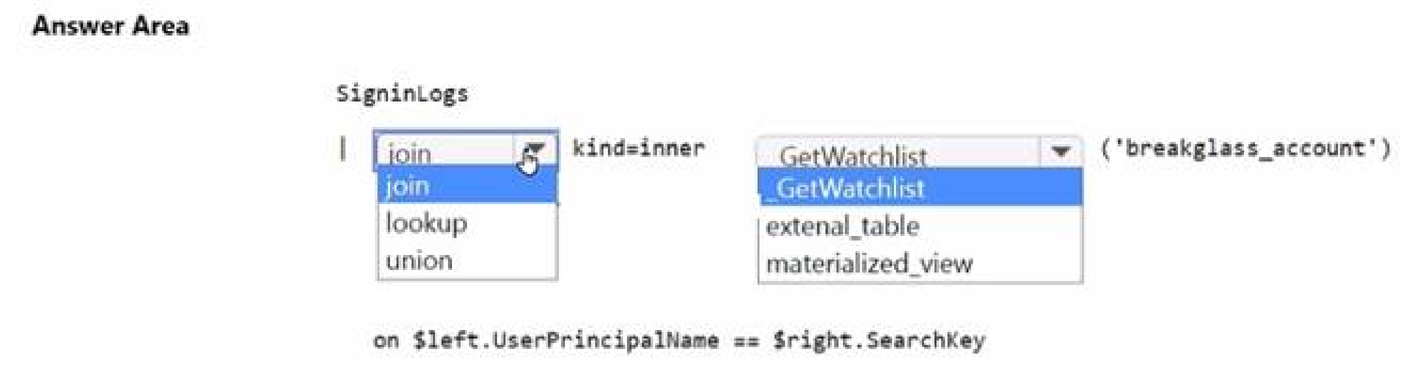
On Webapp1: Enable Cross-Origin Resource Sharing (CORS).
Enable Cross-Origin Resource Sharing (CORS).
Enable Same Origin Policy (SOP).
Enforce TLS 1.2.

NEW QUESTION 24
- (Topic 3)
You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements. What should you create first?

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

Answer: C

NEW QUESTION 29
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.



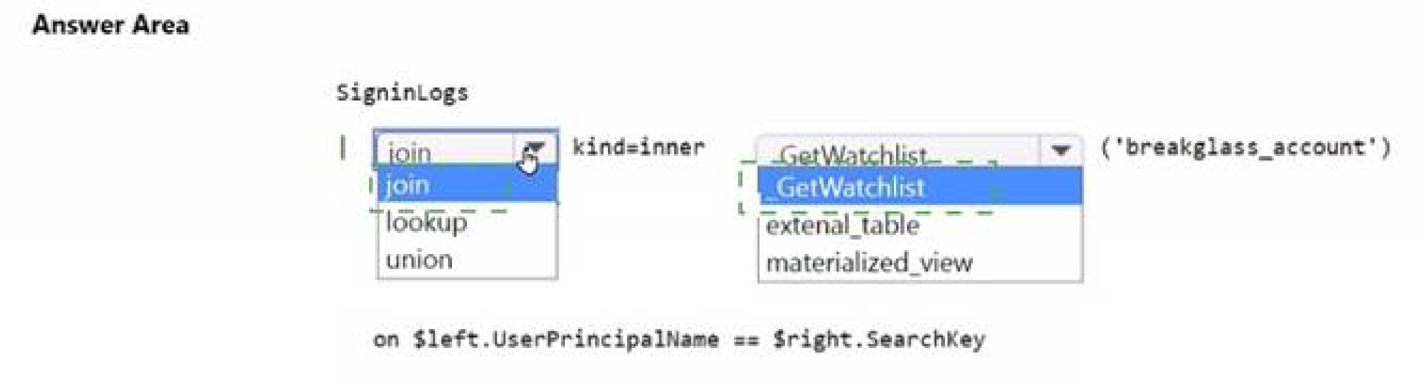
Answer Area

```
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 30
- (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 34
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

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

Answer: D

NEW QUESTION 35
- (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 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 41
- (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 46
- (Topic 4)
You use Microsoft Sentinel.
You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point

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

Answer: DE

NEW QUESTION 50
- (Topic 4)
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

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

Answer: B

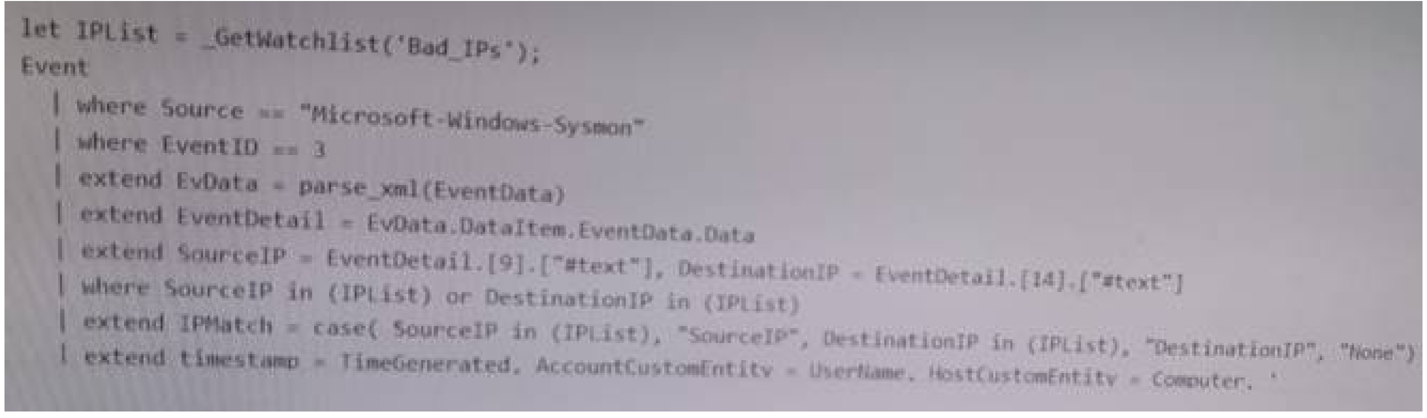
NEW QUESTION 55
- (Topic 4)
You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

A. Modify the properties of the connector.

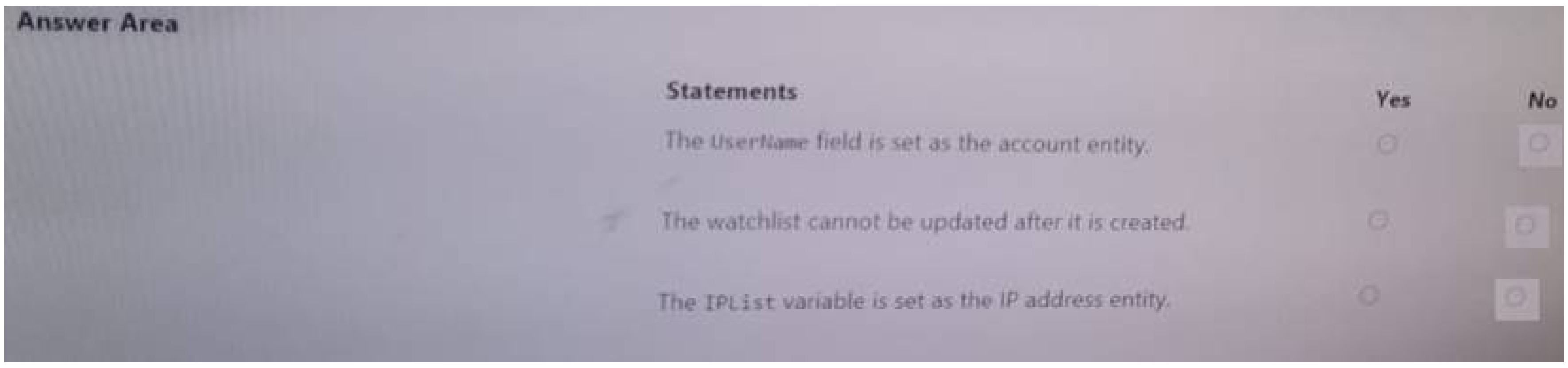
B. Create a Data Collection Rule (DCR).
C. Create a scheduled query rule.
D. Enable User and Entity Behavior Analytics (UEBA)

Answer: D

NEW QUESTION 59
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, '
```



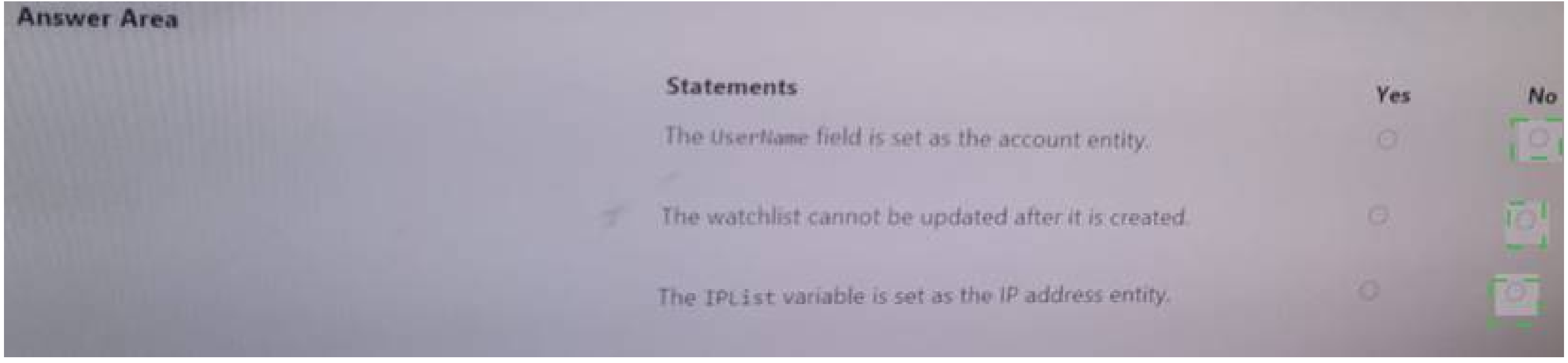
Answer Area

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

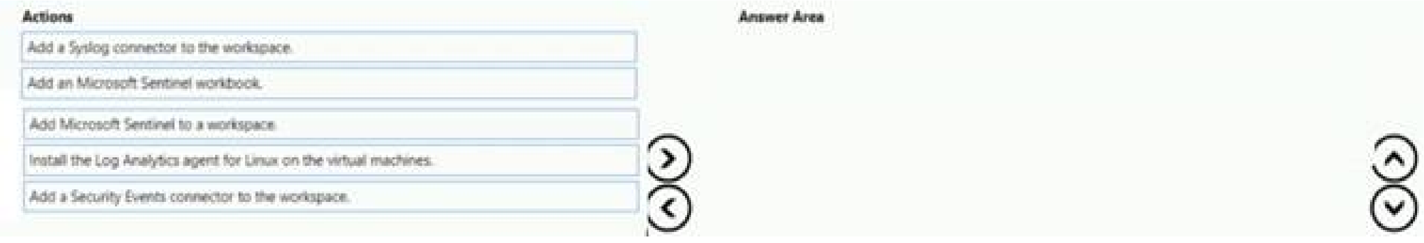
Explanation:



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 63
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

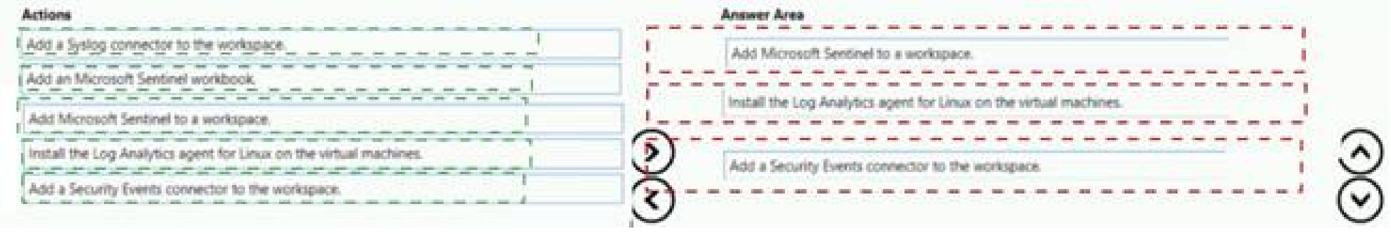
- Add a Syslog connector to the workspace.
- Add an Microsoft Sentinel workbook.
- Add Microsoft Sentinel to a workspace.
- Install the Log Analytics agent for Linux on the virtual machines.
- Add a Security Events connector to the workspace.

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 67
- (Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
? Microsoft Excel macros that download scripts from untrusted websites
? Users that open executable attachments in Microsoft Outlook
? Outlook rules and forms exploits
What should you use?

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

Answer: B

Explanation:

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

NEW QUESTION 70
- (Topic 4)
You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

A. Modify the access control settings for the key vault.
B. Enable the Key Vault firewall.
C. Create an application security group.
D. Modify the access policy for the key vault.

Answer: B

Explanation:

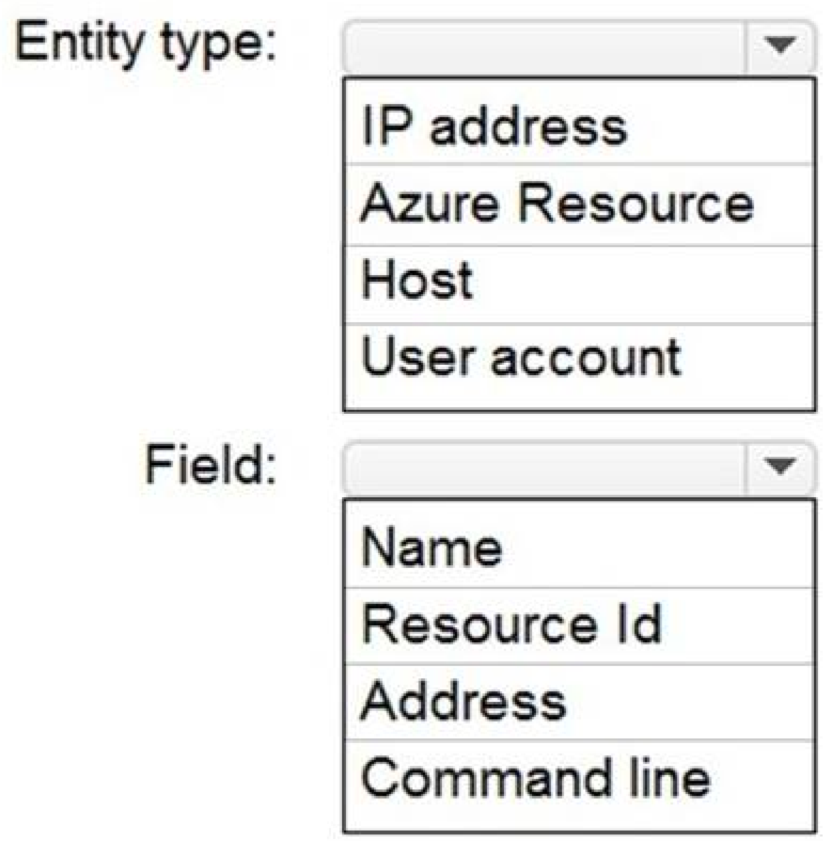
Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

NEW QUESTION 74
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.
You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

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

Answer: A

NEW QUESTION 79
HOTSPOT - (Topic 4)
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Entity type:

- IP address
- Azure Resource
- Host
- User account

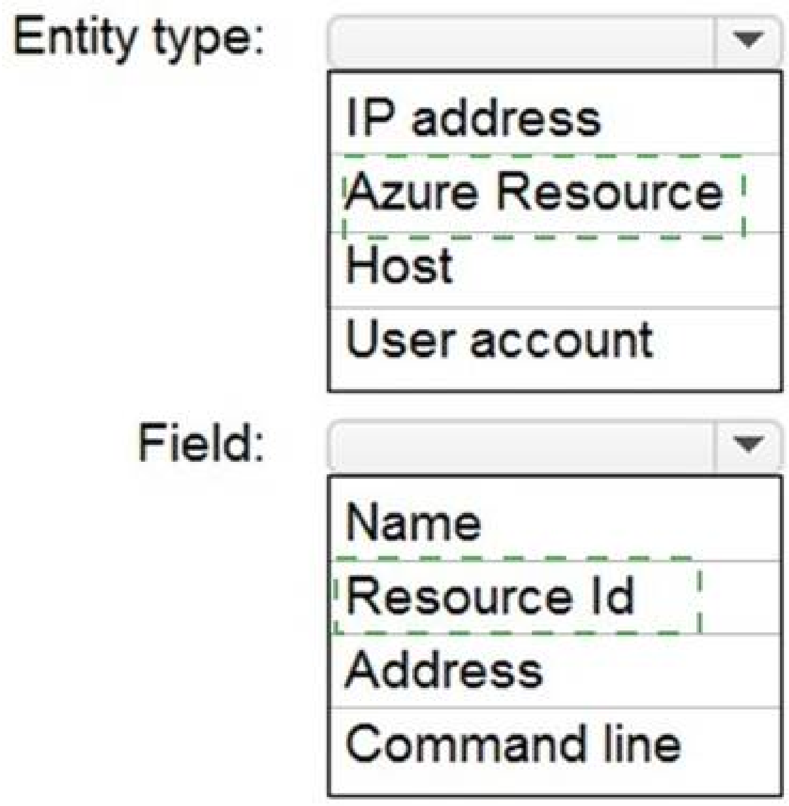
Field:

- Name
- Resource Id
- Address
- Command line

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Entity type:

- IP address
- Azure Resource
- Host
- User account

Field:

- Name
- Resource Id
- Address
- Command line

NEW QUESTION 83
- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
• App name: App1
• IP address: 192.168.1.2
• Computer name: Device1
• Used client app: Microsoft Edge
• Email address: user1@company.com
• Sign-in URL: https://www.company.com
Which entities can be investigated by using UEBA?

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

Answer: D

NEW QUESTION 88
- (Topic 4)
You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.
You need to identify all the changes made to Domain Admins group during the past 30 days.
What should you use?

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

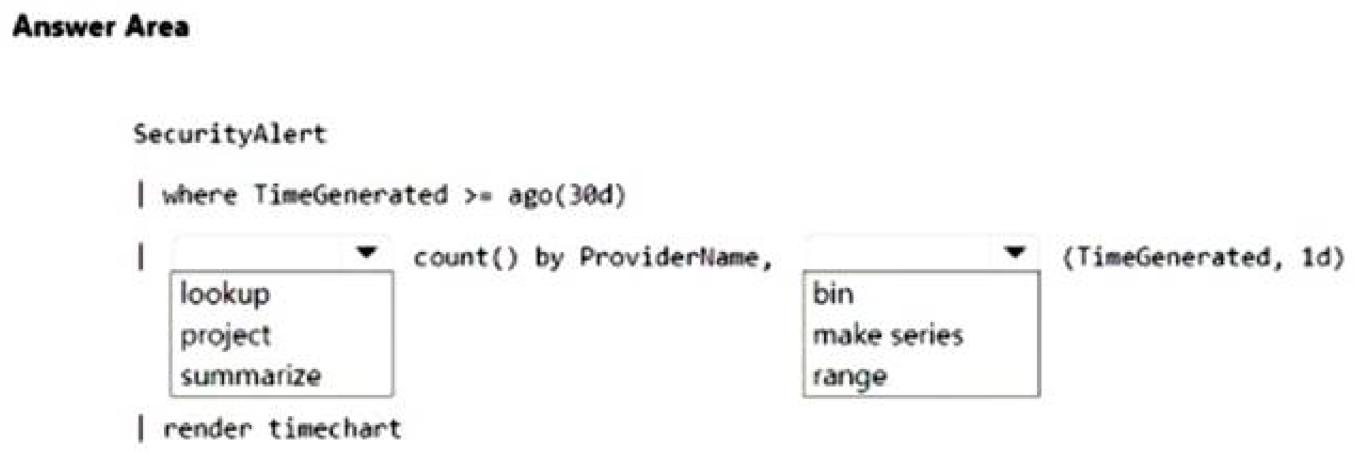
Answer: C

NEW QUESTION 90
- (Topic 4)
You have a Microsoft Sentinel workspace that has user and Entity Behavior Analytics (UEBA) enabled for Signin Logs.
You need to ensure that failed interactive sign-ins are detected. The solution must minimize administrative effort.
What should you use?

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

Answer: B

NEW QUESTION 92
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
```

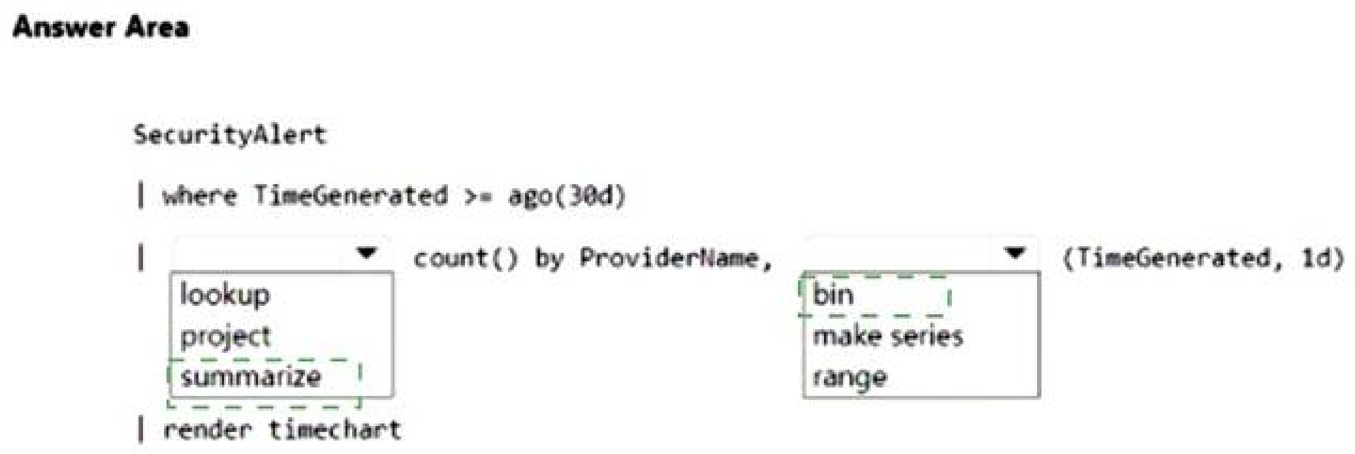
lookup
project
summarize

bin
make series
range

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

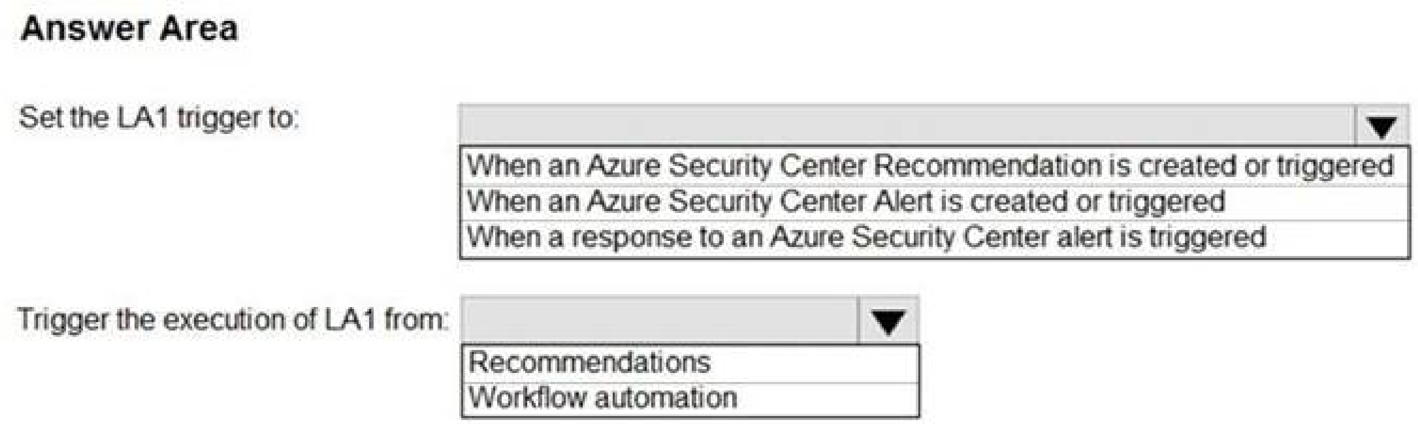
```
SecurityAlert
| where TimeGenerated >= ago(30d)
| [▼] count() by ProviderName, [▼] (TimeGenerated, 1d)
| render timechart
```

lookup
project
summarize

bin
make series
range

NEW QUESTION 95
HOTSPOT - (Topic 4)
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
View the window
You need to test LA1 in Security Center.

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



Answer Area

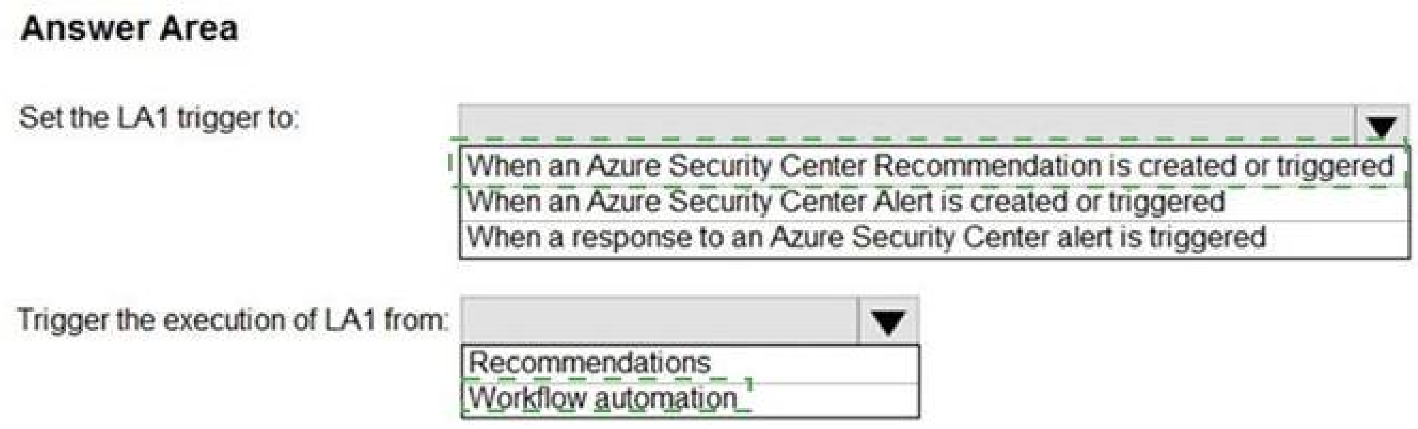
Set the LA1 trigger to:
- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

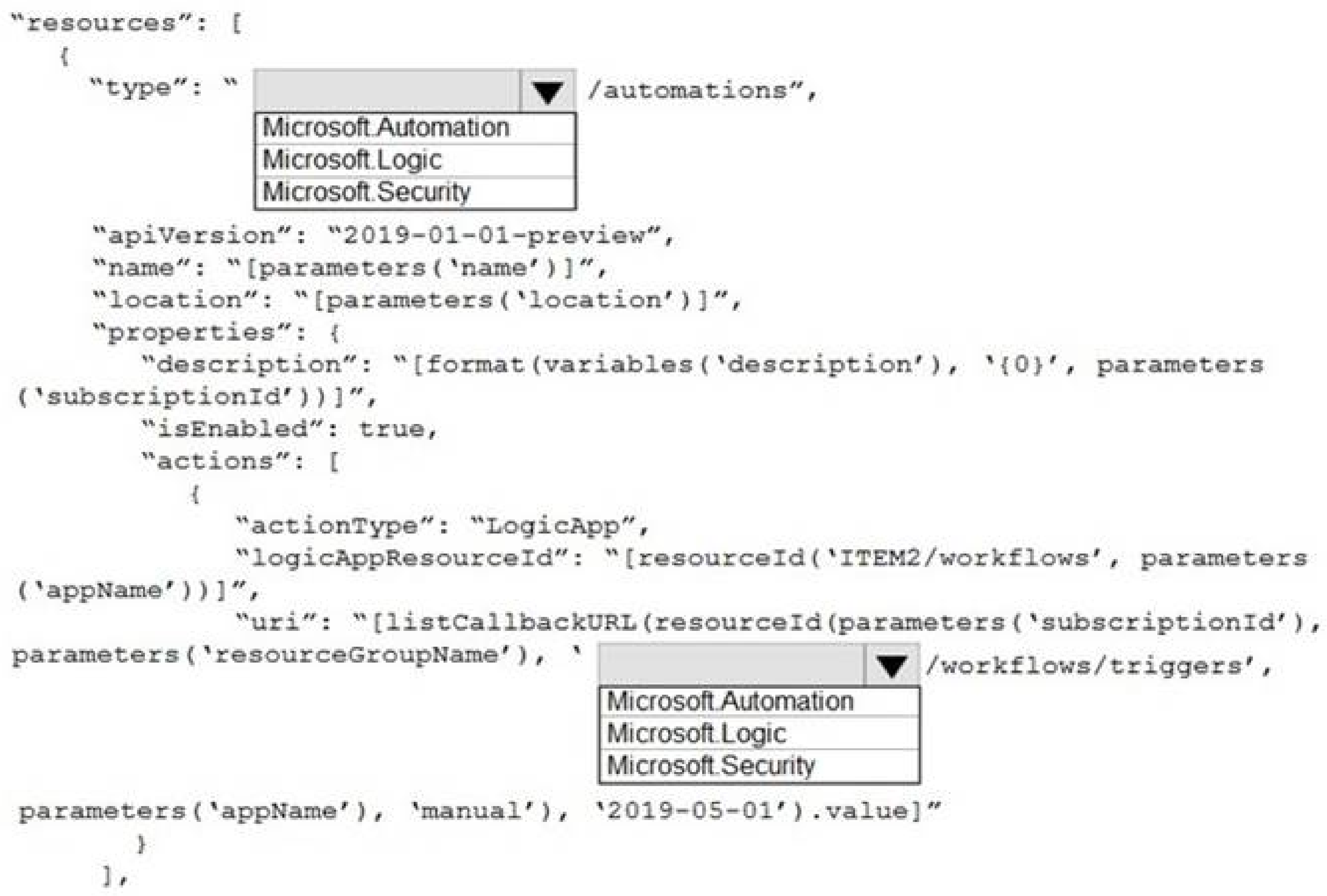


Answer Area

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

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

NEW QUESTION 96
HOTSPOT - (Topic 4)
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

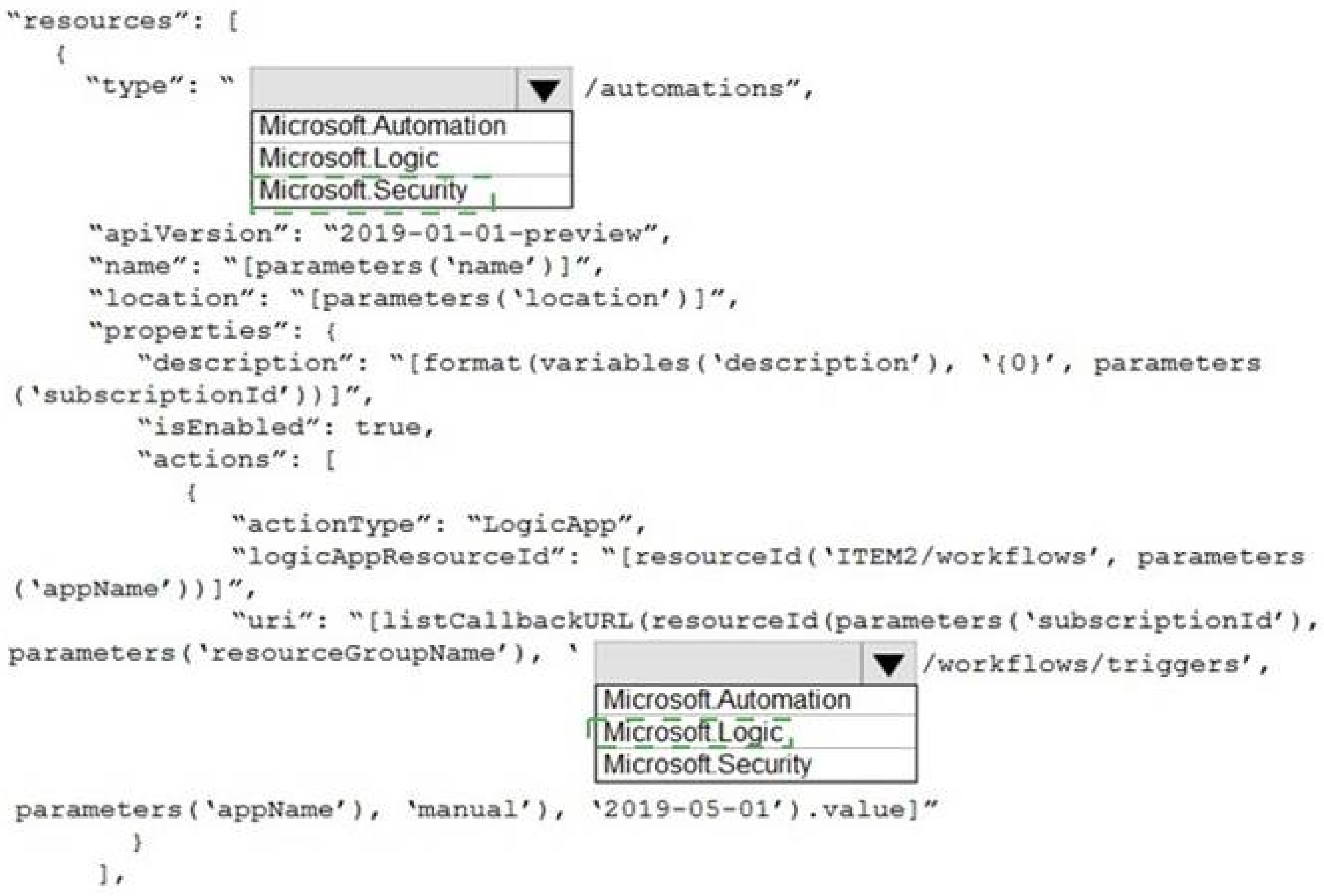


```
“resources”: [
  {
    “type”: “ [Microsoft.Automation | Microsoft.Logic | Microsoft.Security] /automations”,
    “apiVersion”: “2019-01-01-preview”,
    “name”: “[parameters(‘name’)]”,
    “location”: “[parameters(‘location’)]”,
    “properties”: {
      “description”: “[format(variables(‘description’),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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



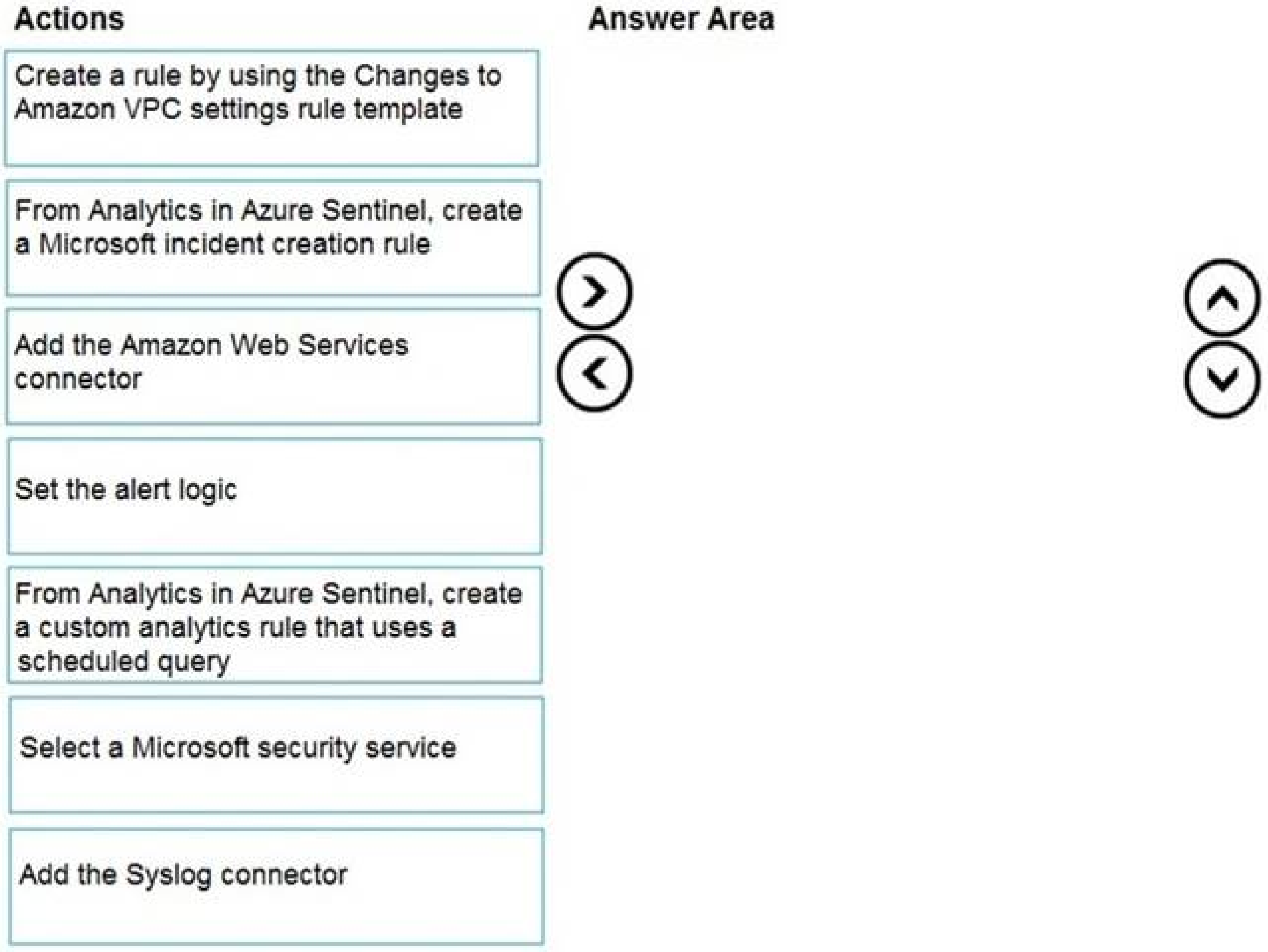
```
"resources": [
   {
     "type": "  [Microsoft.Automation | Microsoft.Logic | Microsoft.Security]  /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'),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

NEW QUESTION 99
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You have a GitHub account named Account1 that contains 10 repositories.
You need to ensure that Defender for Cloud can assess the repositories in Account1. What should you do first in the Microsoft Defender for Cloud portal?

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

Answer: A

NEW QUESTION 101
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

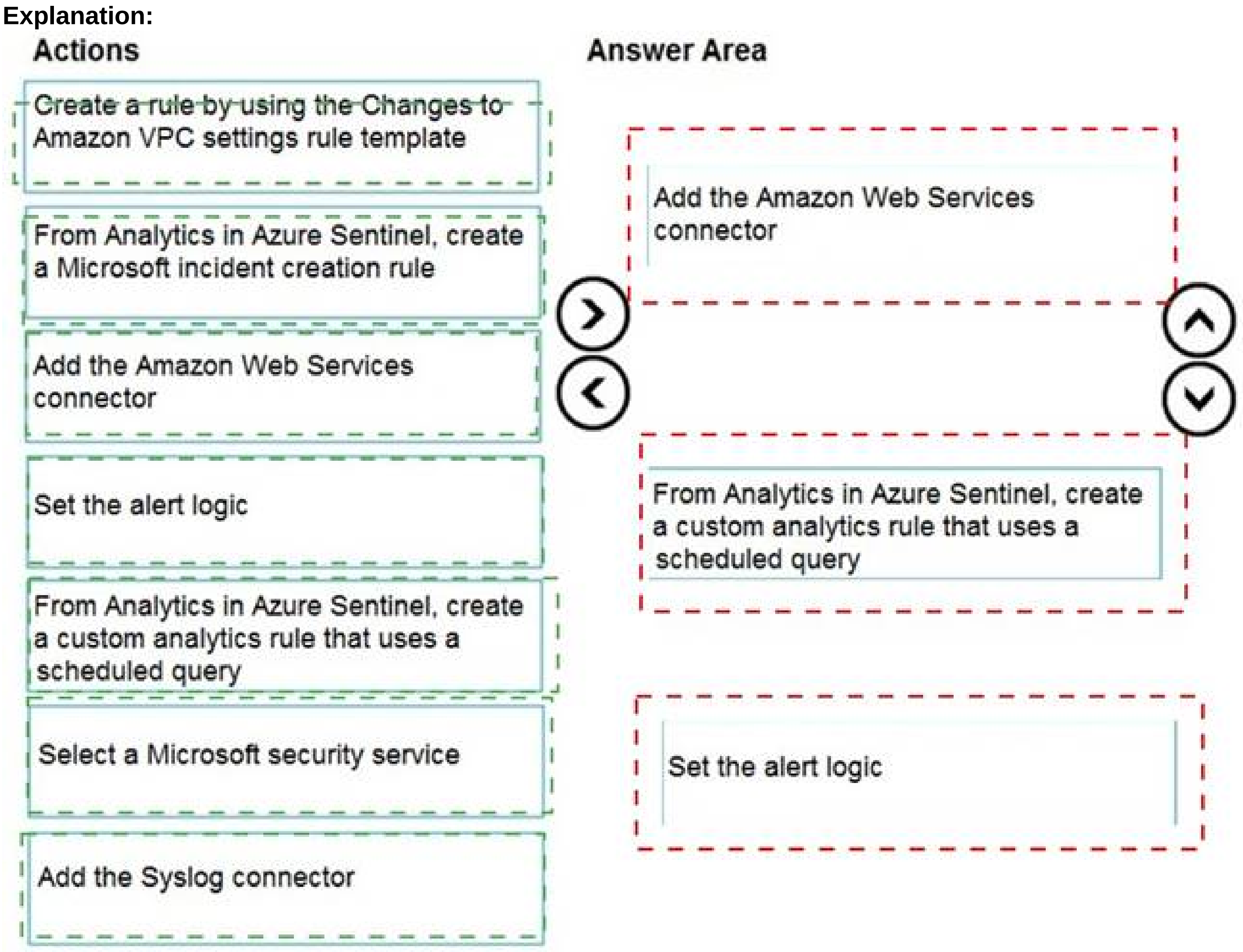
Answer Area

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 103
- (Topic 4)
You have a Microsoft Sentinel workspace.
You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.
What are two ways to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 105
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You plan to create a hunting query from Microsoft Defender.
You need to create a custom tracked query that will be used to assess the threat status of the subscription.
From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Policies & rules
B. Explorer
C. Threat analytics
D. Advanced Hunting

Answer: D

NEW QUESTION 106
- (Topic 4)
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

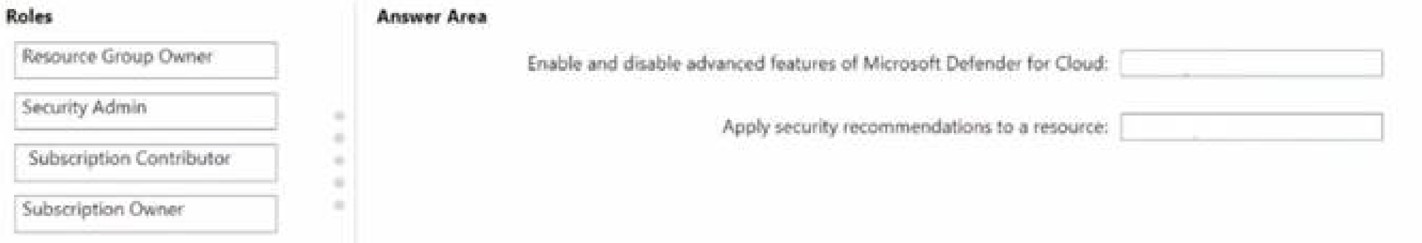
A. Impossible travel
B. Activity from anonymous IP addresses
C. Activity from infrequent country
D. Malware detection

Answer: C

Explanation:
Activity from a country/region that could indicate malicious activity. This policy profiles your environment and triggers alerts when activity is detected from a location that was not recently or was never visited by any user in the organization. Activity from the same user in different locations within a time period that is shorter than

the expected travel time between the two locations. This can indicate a credential breach, however, it's also possible that the user's actual location is masked, for example, by using a VPN.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION 110
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
• Enable and disable advanced features of Microsoft Defender for Cloud.
• Apply security recommendations to a resource. The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



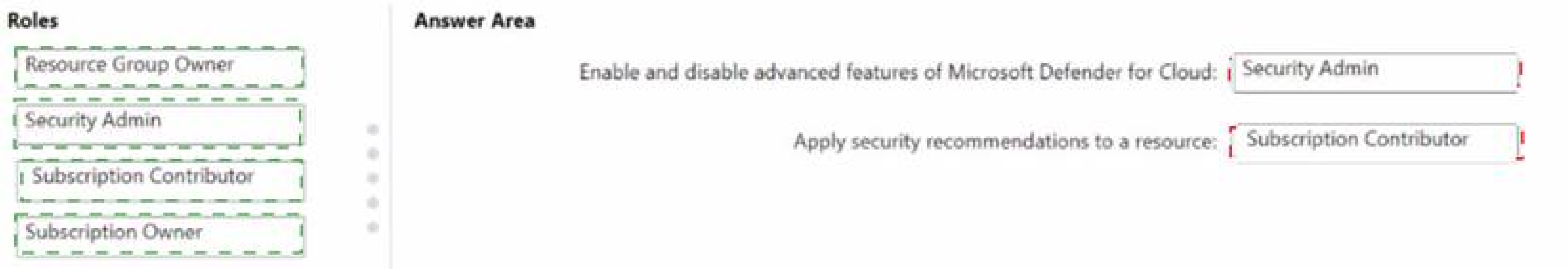
Roles
Resource Group Owner
Security Admin
Subscription Contributor
Subscription Owner

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Roles
Resource Group Owner
Security Admin
Subscription Contributor
Subscription Owner

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

NEW QUESTION 112
- (Topic 4)
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?

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

Answer: B

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

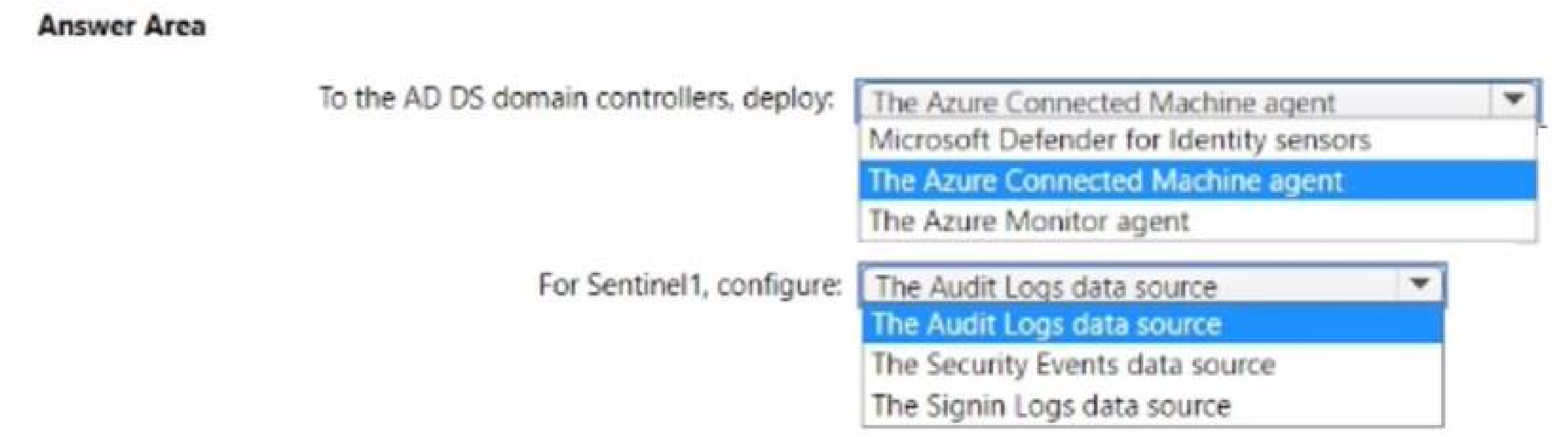
NEW QUESTION 113
- (Topic 4)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation. You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the 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 114
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

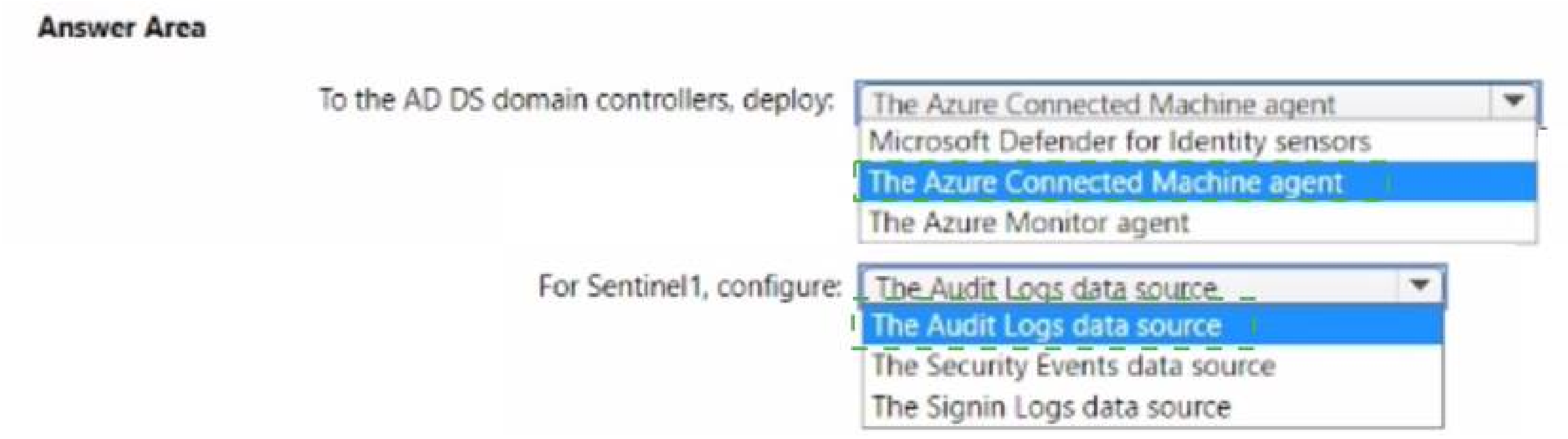
To the AD DS domain controllers, deploy: The Azure Connected Machine agent ▼
- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent
- The Azure Monitor agent

For Sentinel1, configure: The Audit Logs data source ▼
- The Audit Logs data source
- The Security Events data source
- The Signin Logs data source

A. Mastered
B. Not Mastered

Answer: A

Explanation:

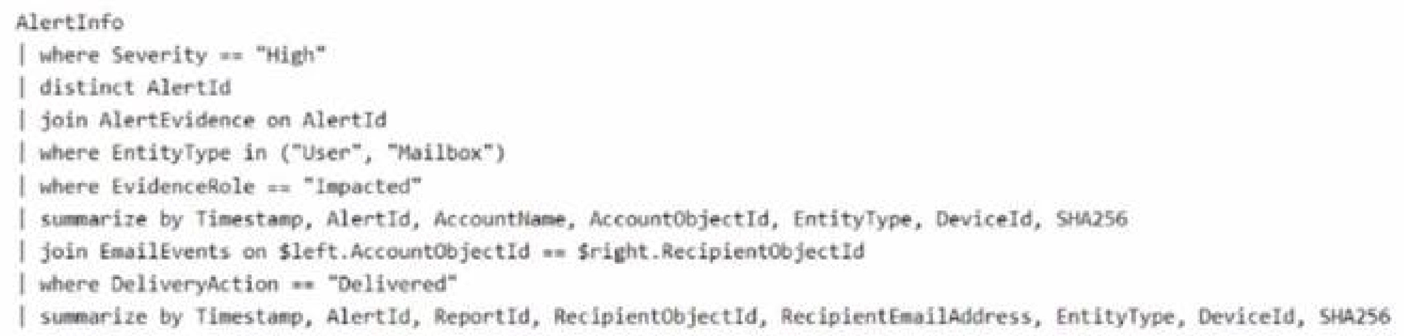


Answer Area

To the AD DS domain controllers, deploy: The Azure Connected Machine agent ▼
- Microsoft Defender for Identity sensors
- [✓ The Azure Connected Machine agent]
- The Azure Monitor agent

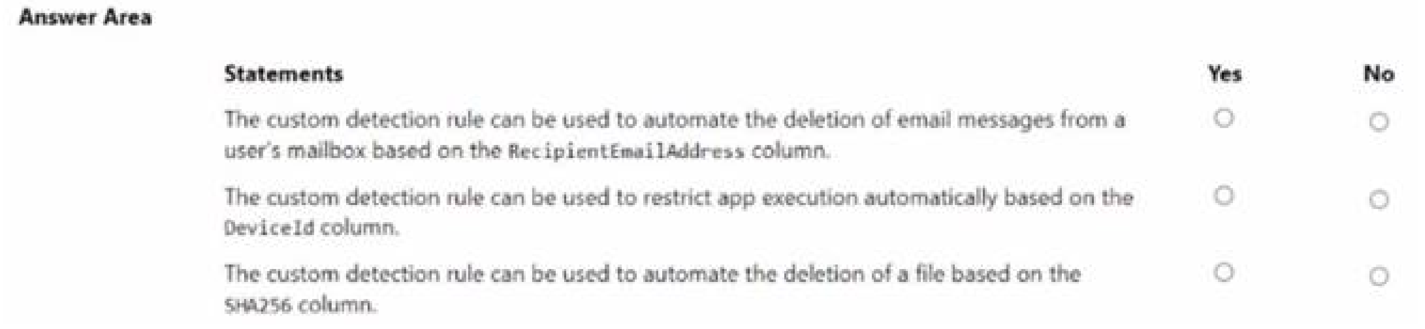
For Sentinel1, configure: The Audit Logs data source ▼
- [✓ The Audit Logs data source]
- The Security Events data source
- The Signin Logs data source

NEW QUESTION 115
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.



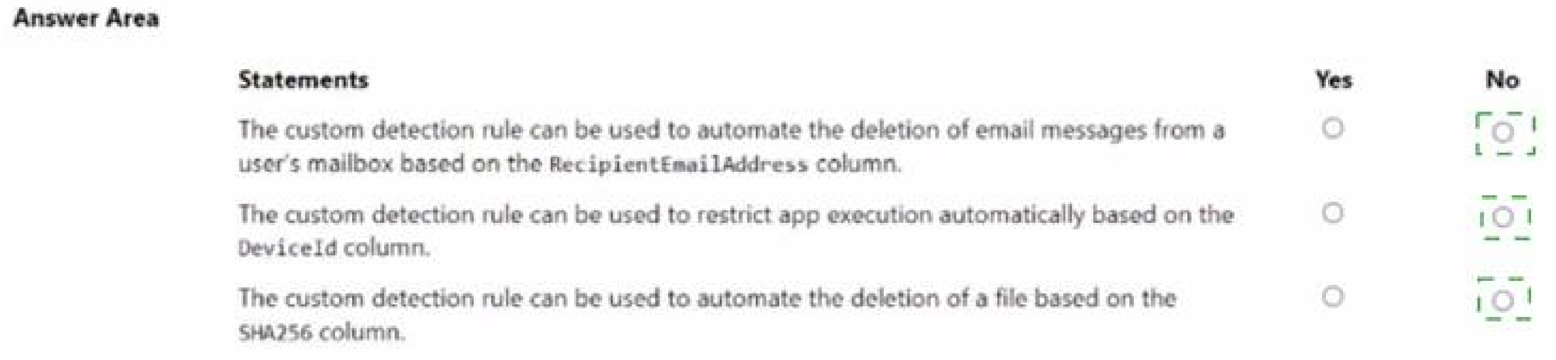
Answer Area

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.	○	[✓ ○]

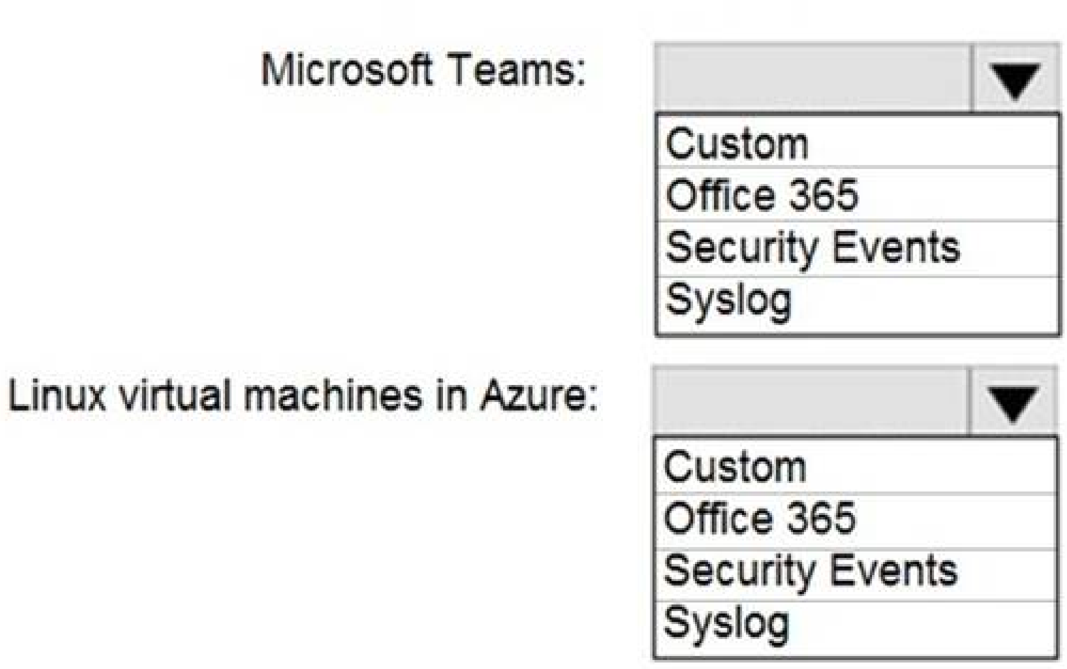
NEW QUESTION 120
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 124
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.



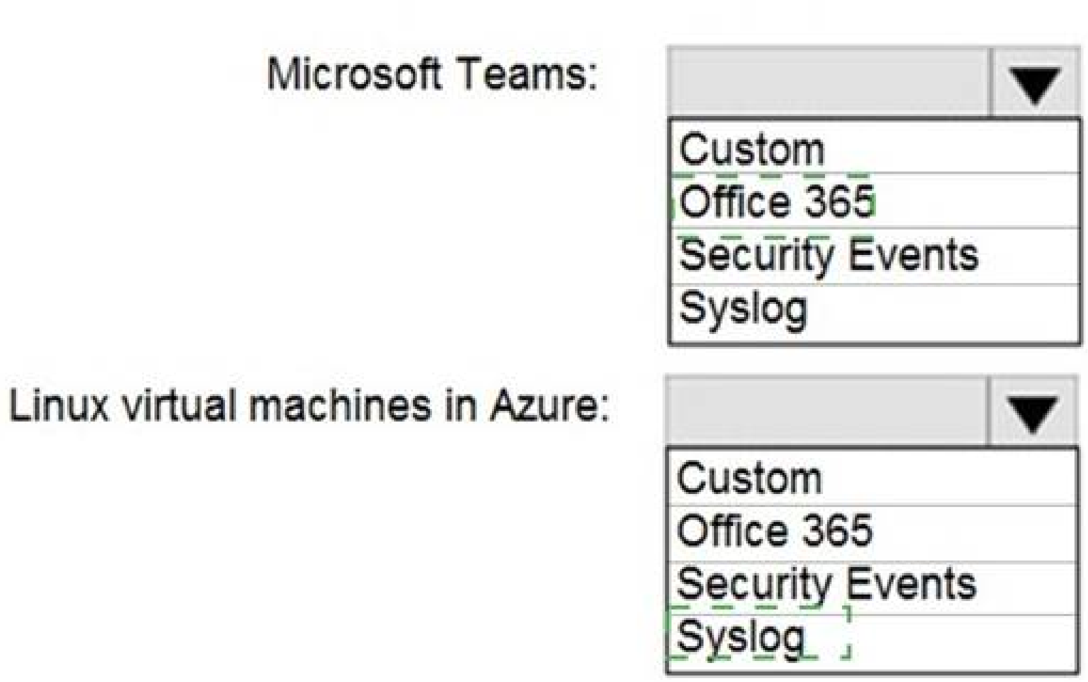
Microsoft Teams:
- Custom
- Office 365
- Security Events
- Syslog

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 129
- (Topic 4)
You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: A

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

NEW QUESTION 130
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.
You need to identify which blobs were deleted. What should you review?

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

Answer: B

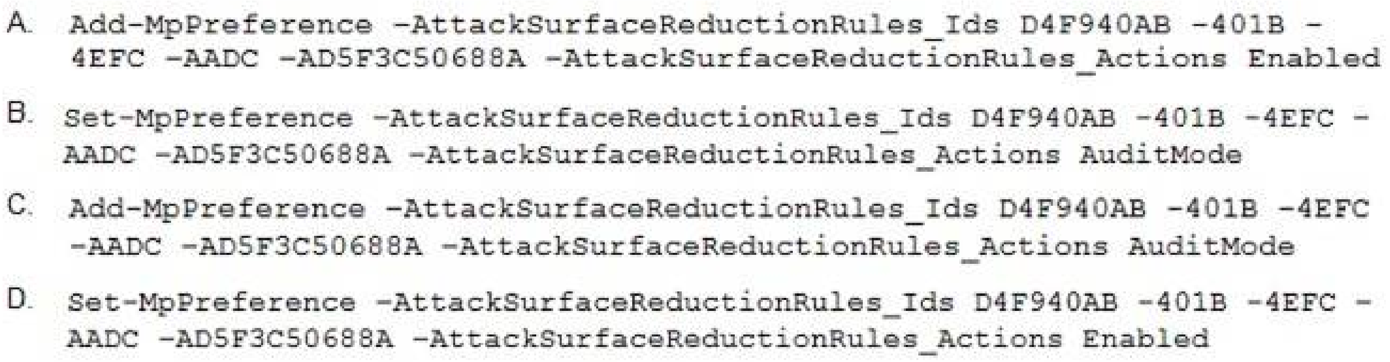
NEW QUESTION 134
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You need to add threat indicators for all the IP addresses in a range of 171.23.3432- 171.2334.63. The solution must minimize administrative effort.
What should you do in the Microsoft 365 Defender portal?

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

Answer: D

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

NEW QUESTION 137
- (Topic 4)
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.



```
A. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
   4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
   AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC
   -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
   AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

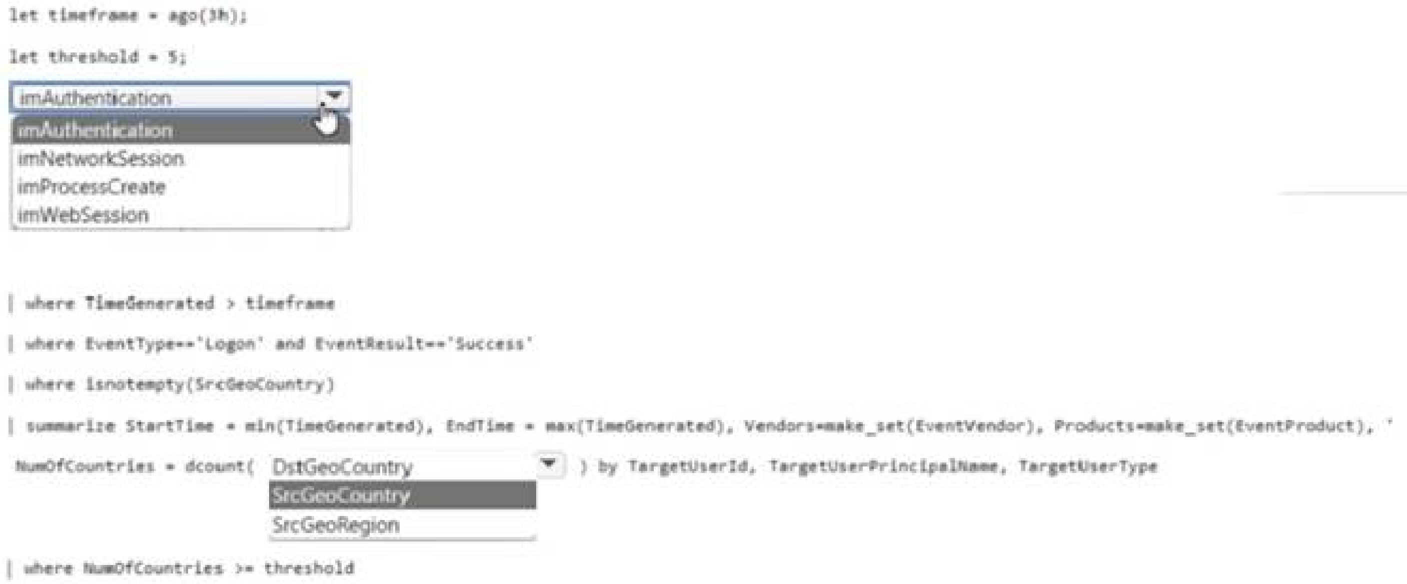
A. Option A
B. Option B
C. Option C
D. Option D

Answer: BC

Explanation:

Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface- reduction

NEW QUESTION 138
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.
How should you complete the query? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point

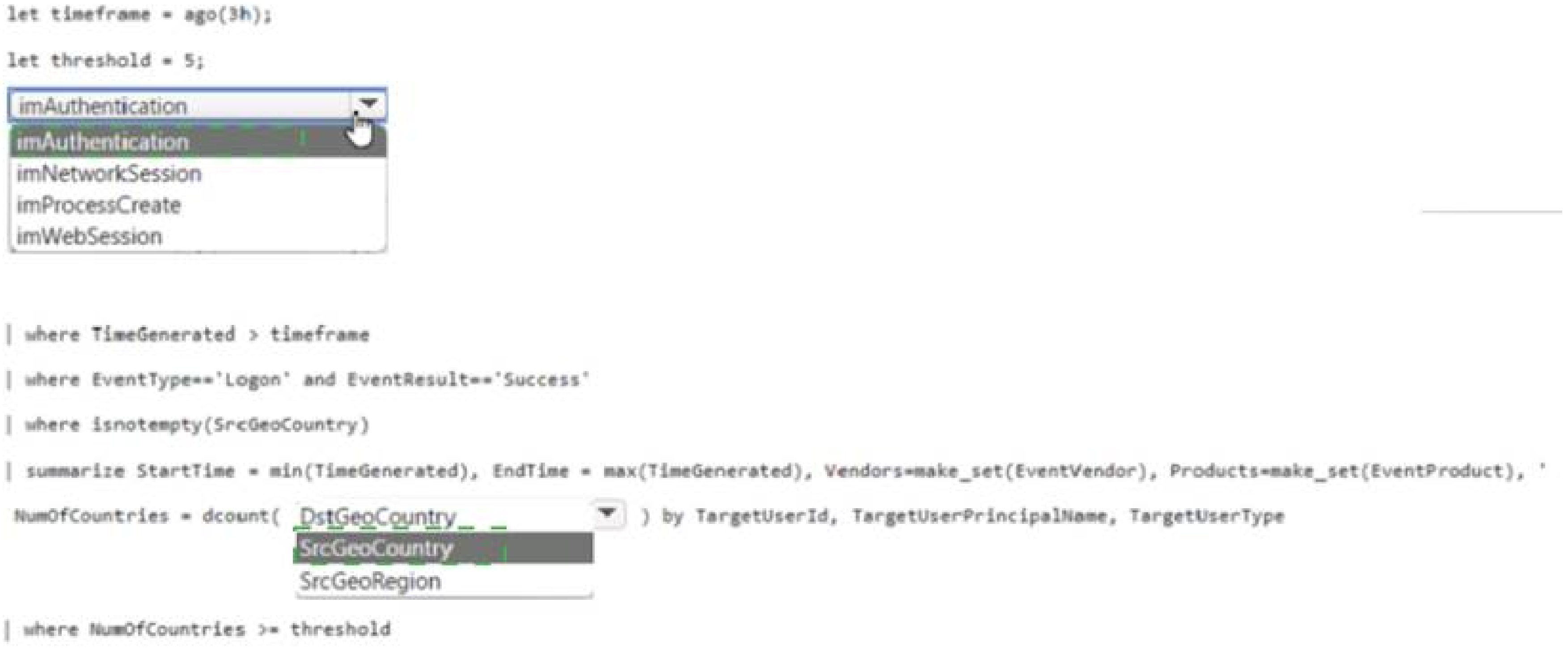


```
let timeframe = ago(3h);
let threshold = 5;
imAuthentication
| where TimeGenerated > timeframe
| where EventType=='Logon' and EventResult=='Success'
| where isnotempty(SrcGeoCountry)
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct),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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

NEW QUESTION 139
- (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

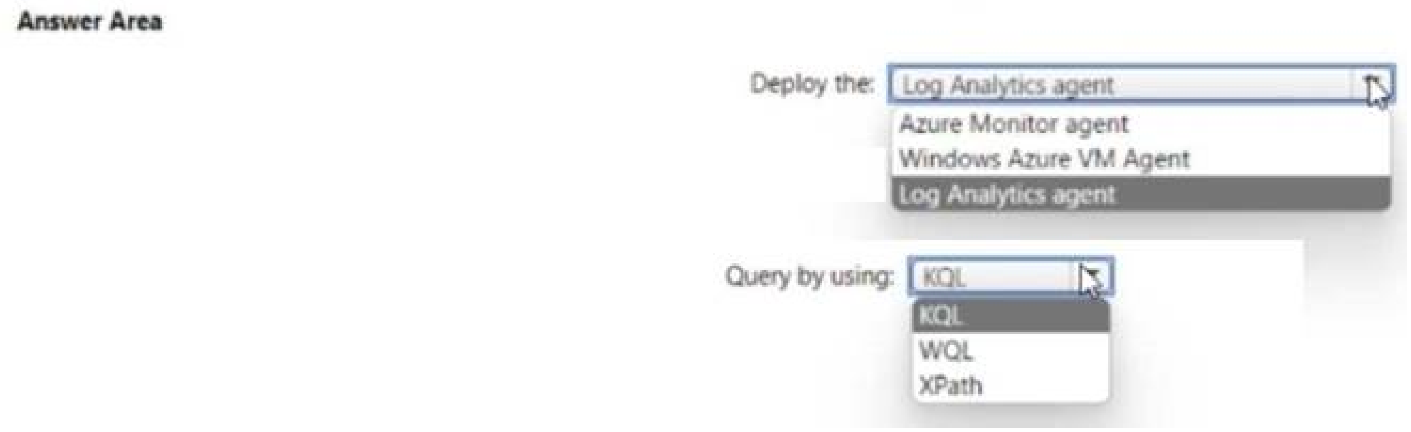
NEW QUESTION 140

- (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 142
HOTSPOT - (Topic 4)
You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.


Answer Area

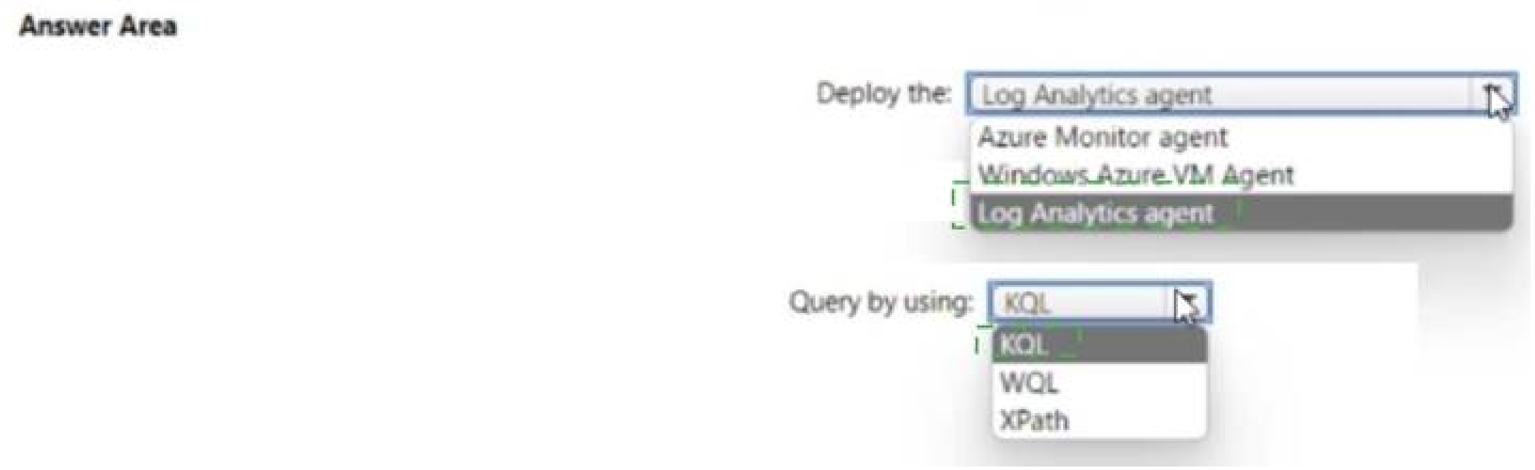
Deploy the: Log Analytics agent

Query by using: KQL

A. Mastered
B. Not Mastered

Answer: A

Explanation:


Answer Area

Deploy the: Log Analytics agent

Query by using: KQL

NEW QUESTION 147
- (Topic 4)
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

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

Answer: D

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

NEW QUESTION 148
- (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 152
- (Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned an Azure Active Directory Premium Plan 2 license
You need to identify whether the identity of User1 was compromised during the last 90 days.
What should you use?

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

Answer: B

NEW QUESTION 153
- (Topic 4)
You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.
You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.
Which role should you assign to User1?

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

Answer: B

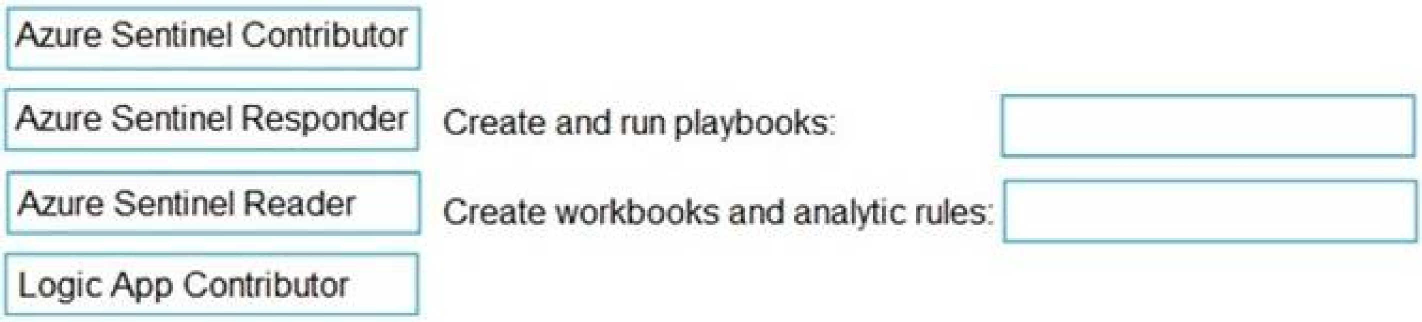
NEW QUESTION 154
- (Topic 4)
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

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 157
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.

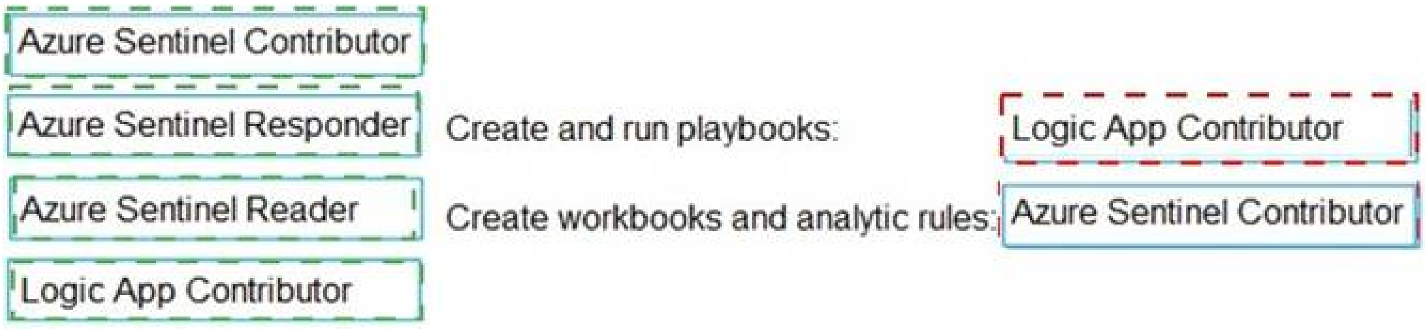

Azure Sentinel Contributor
Azure Sentinel Responder
Azure Sentinel Reader
Logic App Contributor

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

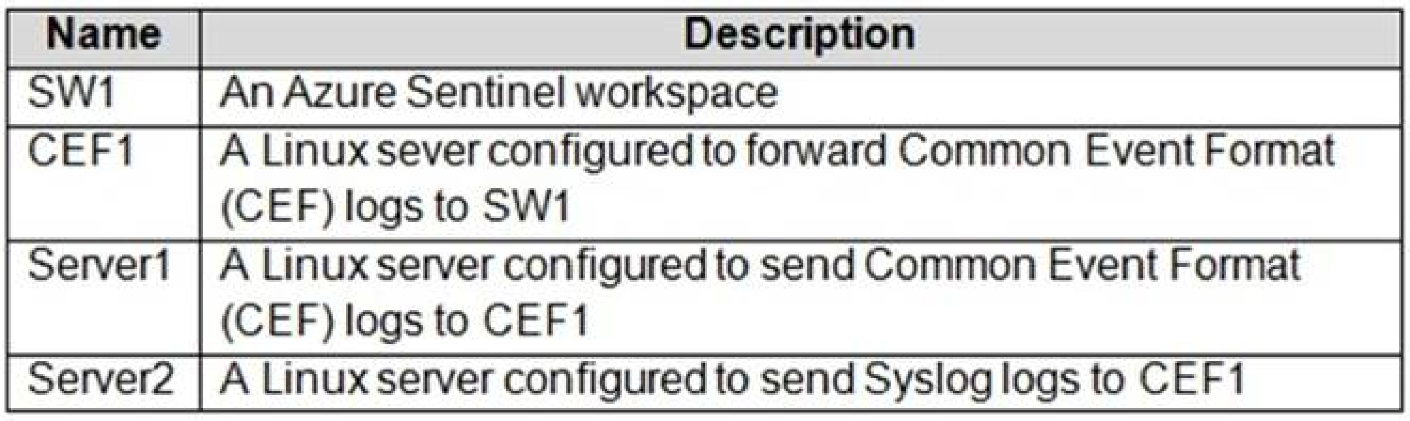
Create workbooks and analytic rules: Azure Sentinel Contributor

NEW QUESTION 161
- (Topic 4)
You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

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

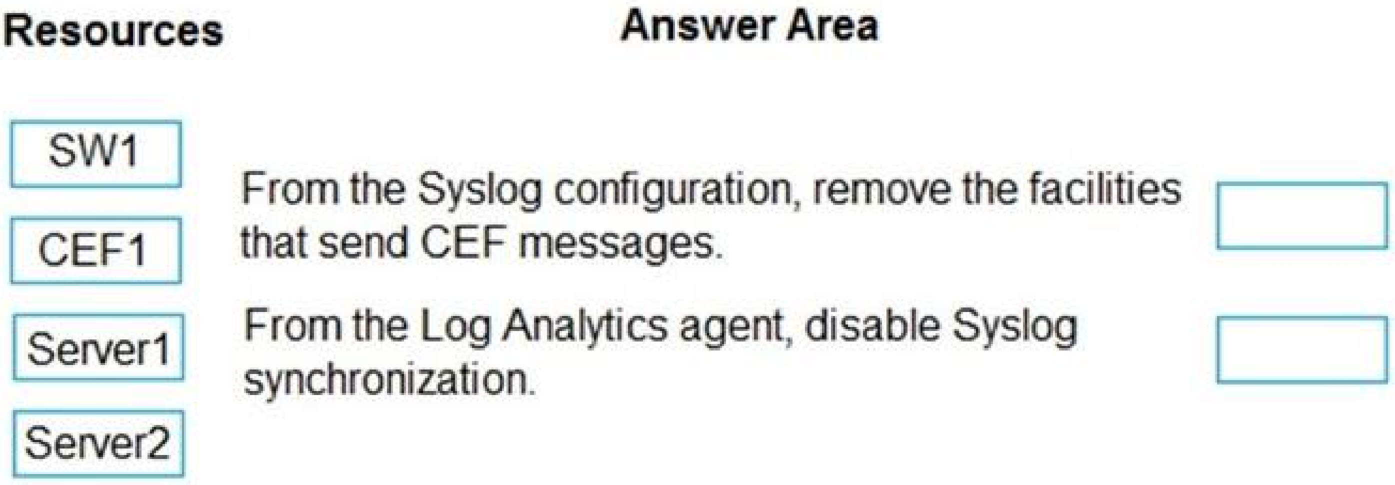
Answer: D

NEW QUESTION 166
DRAG DROP - (Topic 4)
You have the resources shown in the following table.



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

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



Resources

SW1

CEF1

Server1

Server2

Answer Area

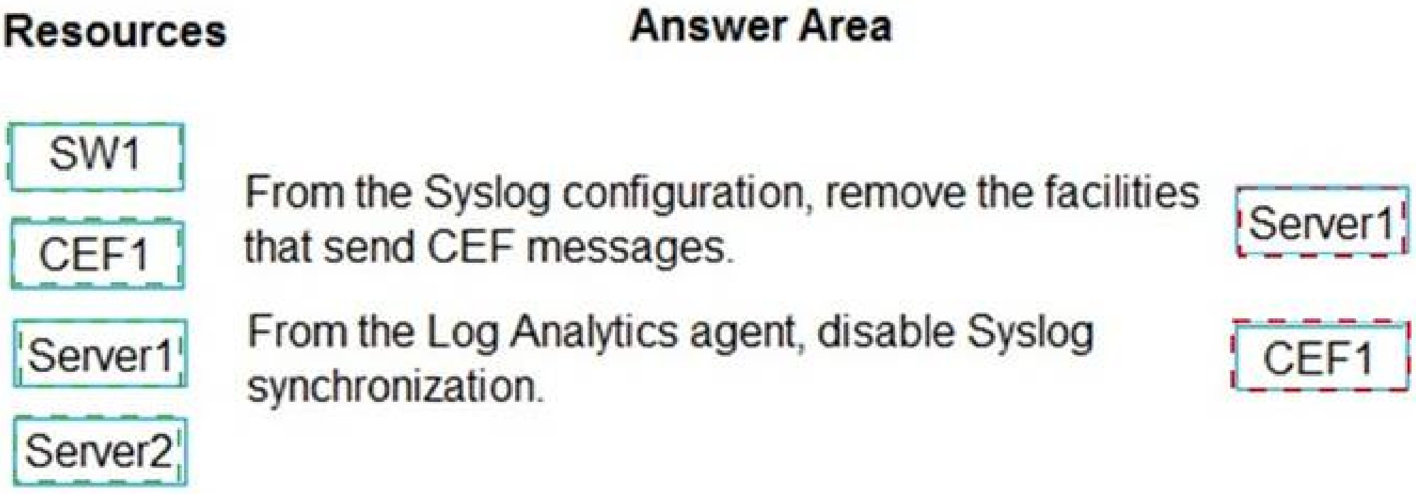
From the Syslog configuration, remove the facilities that send CEF messages.

From the Log Analytics agent, disable Syslog synchronization.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Resources

SW1

CEF1

Server1

Server2

Answer Area

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

From the Log Analytics agent, disable Syslog synchronization. CEF1

NEW QUESTION 171
- (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 Mitigate the threat section.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 174
- (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

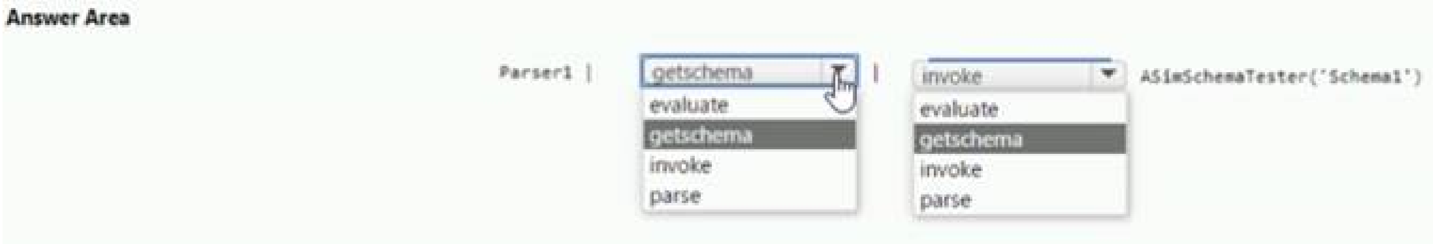
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

NEW QUESTION 178
- (Topic 4)
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

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

Answer: A

NEW QUESTION 179
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.
You need to validate Schema1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

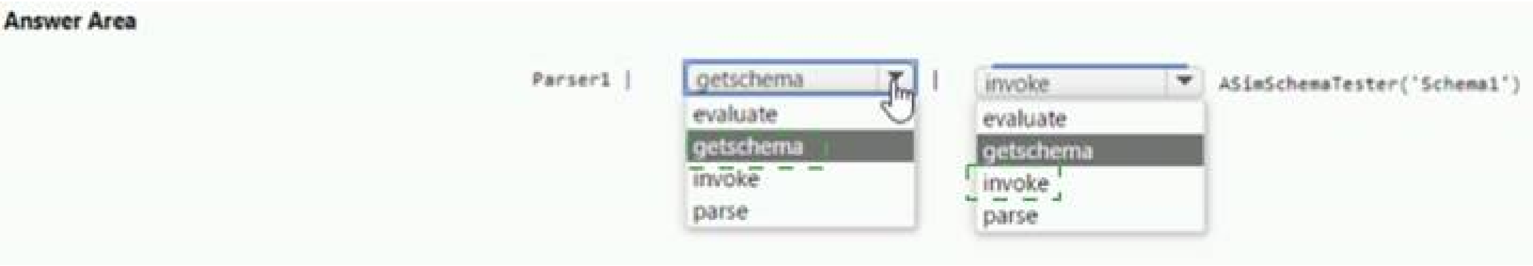

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 182
- (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

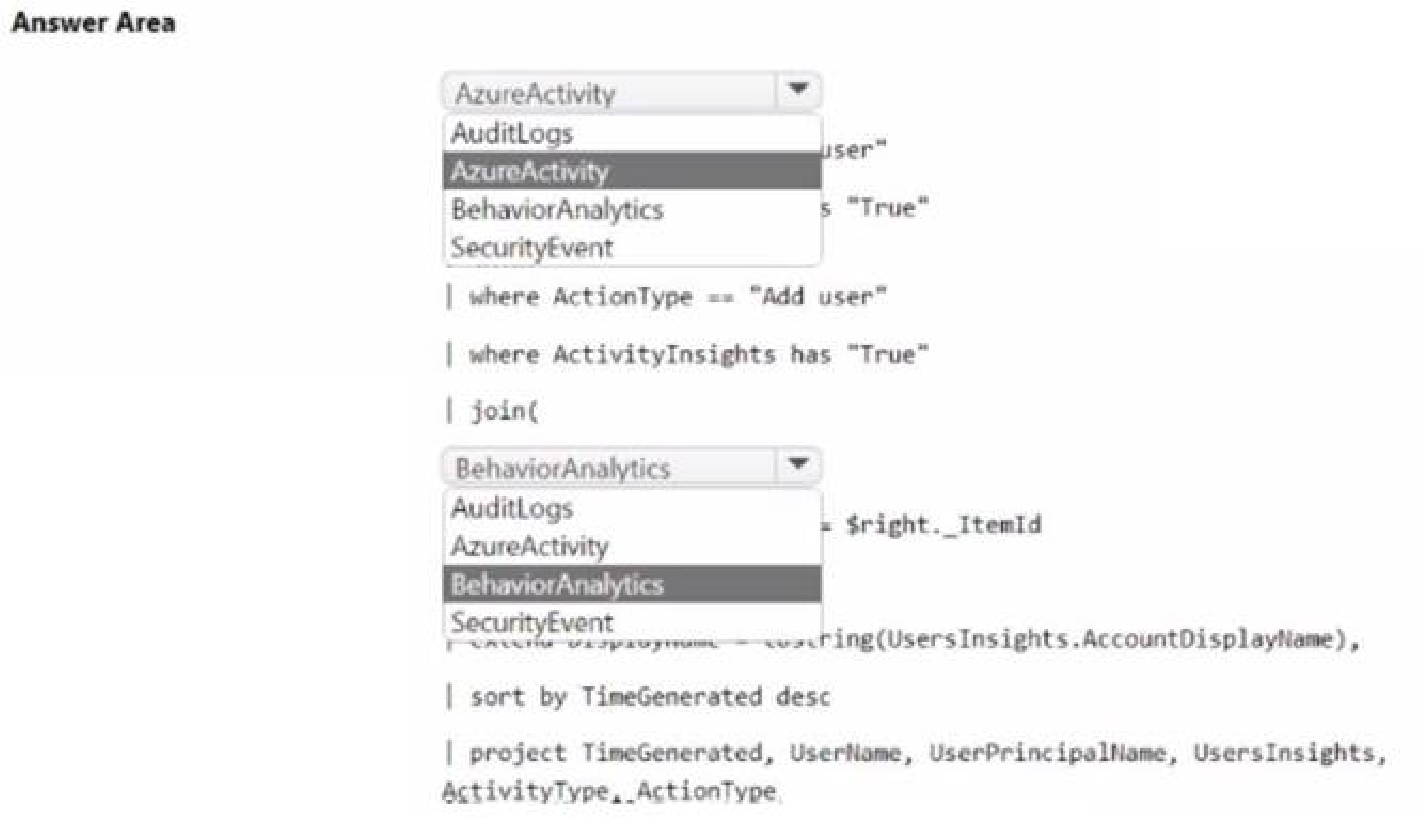
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

NEW QUESTION 183
- (Topic 4)
You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

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

Answer: B

NEW QUESTION 187
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You need to create a query that will detect when a user creates an unusually large numbers of Azure AD user accounts.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



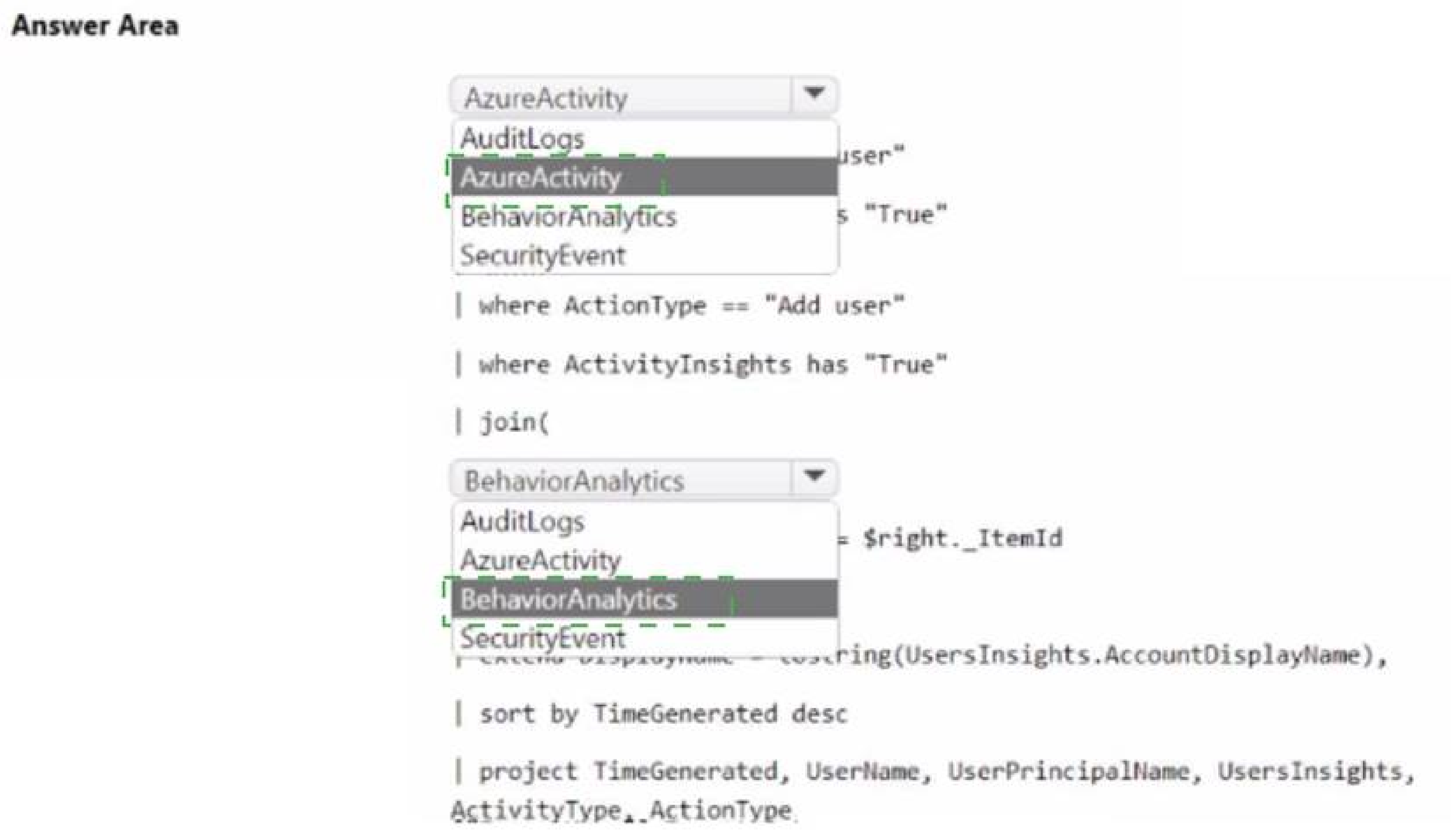
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

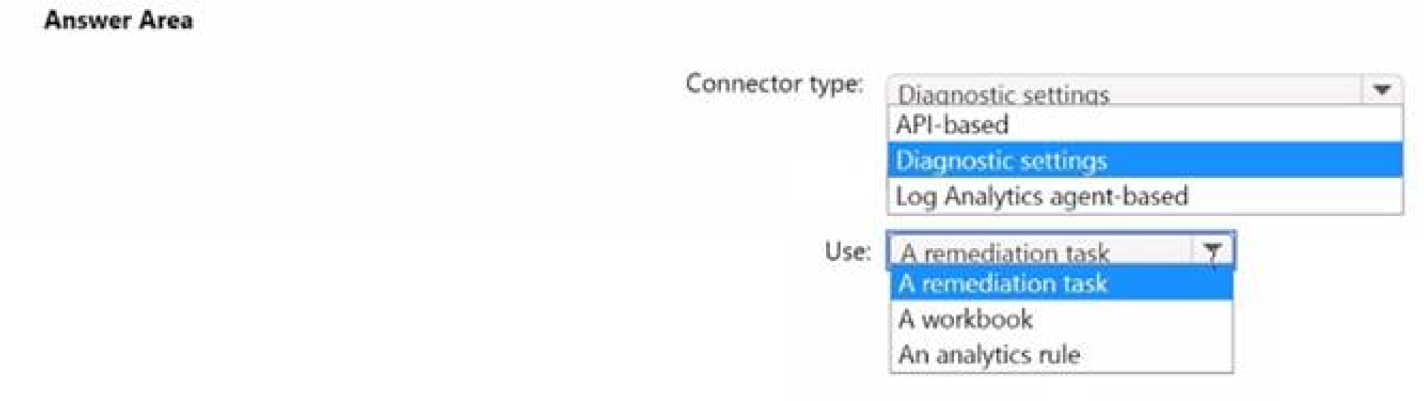
AzureActivity
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

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

BehaviorAnalytics
AuditLogs
AzureActivity
BehaviorAnalytics
SecurityEvent

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

NEW QUESTION 190
HOTSPOT - (Topic 4)
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

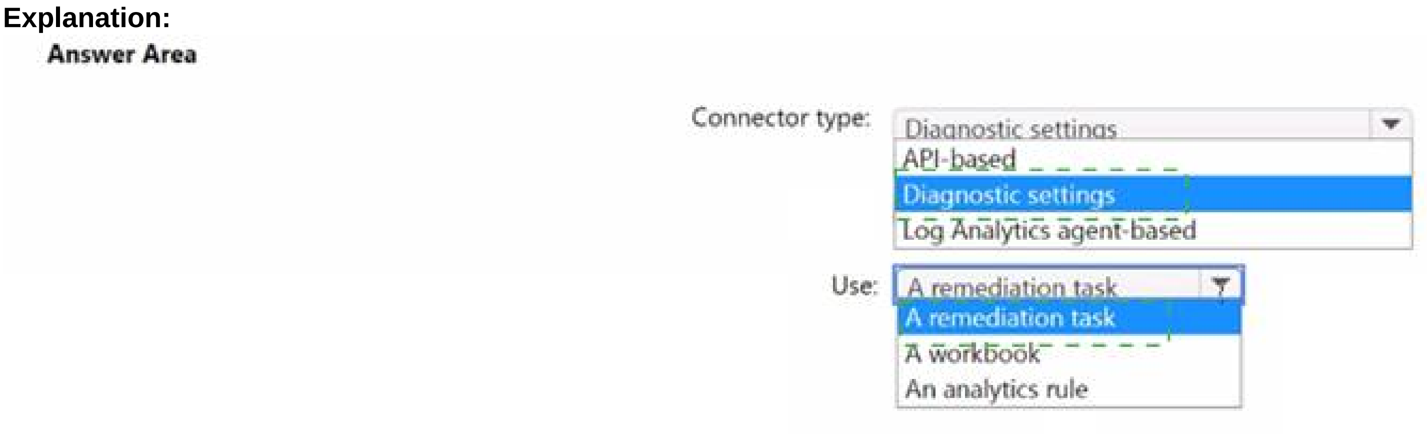
Connector type: Diagnostic settings
API-based
Diagnostic settings
Log Analytics agent-based

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

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

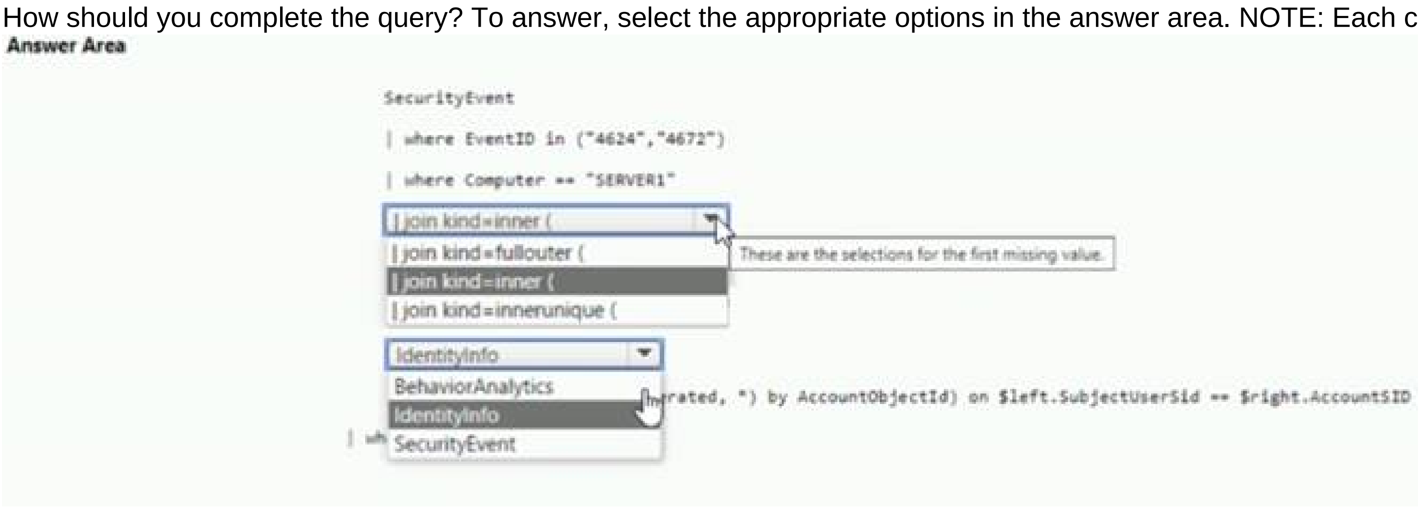
NEW QUESTION 194
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.
You enable agentless scanning.
You need to prevent Server1 from being scanned. The solution must minimize administrative effort.
What should you do?

A. Create an exclusion tag.

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

Answer: D

NEW QUESTION 197
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.
You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:
• Only include security-sensitive actions by users that are NOT members of the IT department.
• Minimize the number of false positives.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



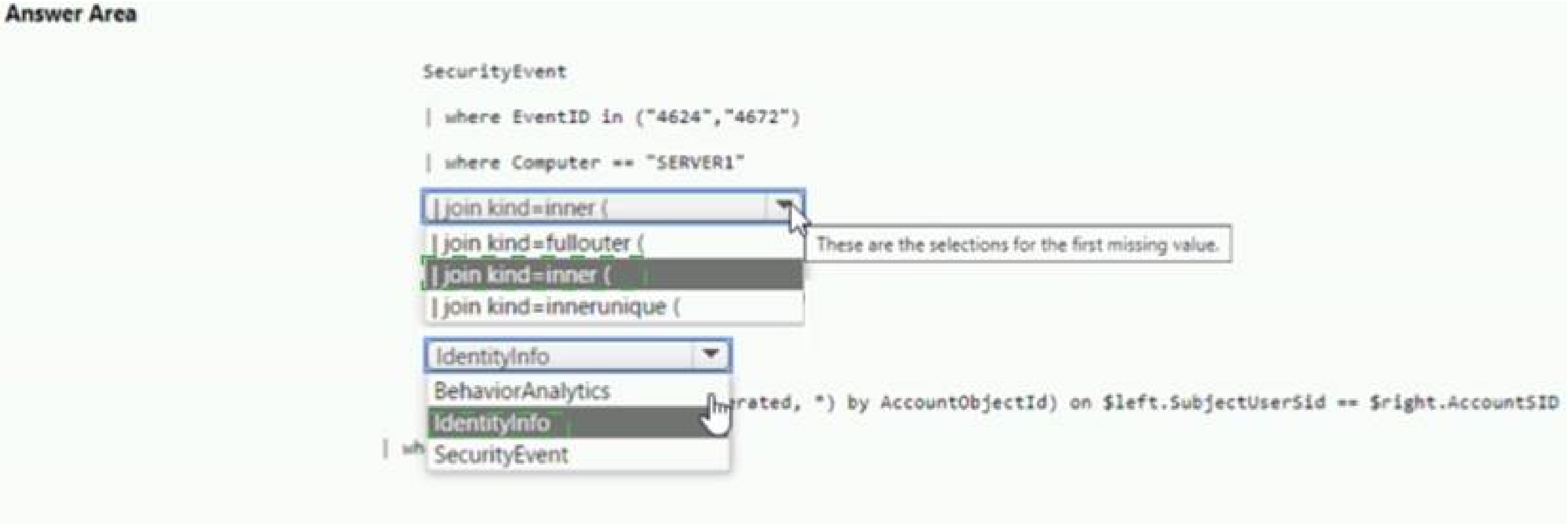
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

NEW QUESTION 200
- (Topic 4)
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

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

Answer: A

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

NEW QUESTION 202
- (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 AlertInfo, 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 207
- (Topic 4)
You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

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

Answer: D

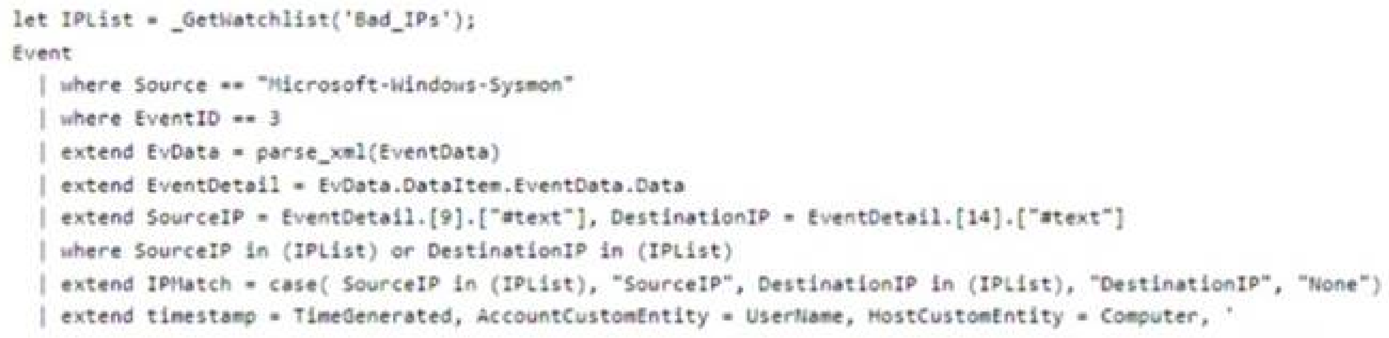
NEW QUESTION 209
- (Topic 4)
A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

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

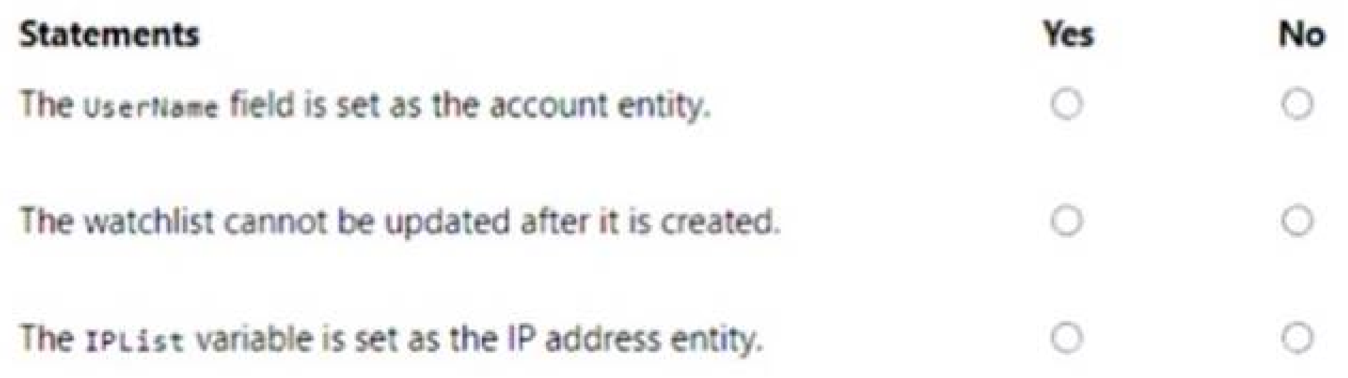
Answer: A

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

NEW QUESTION 211
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, '
```

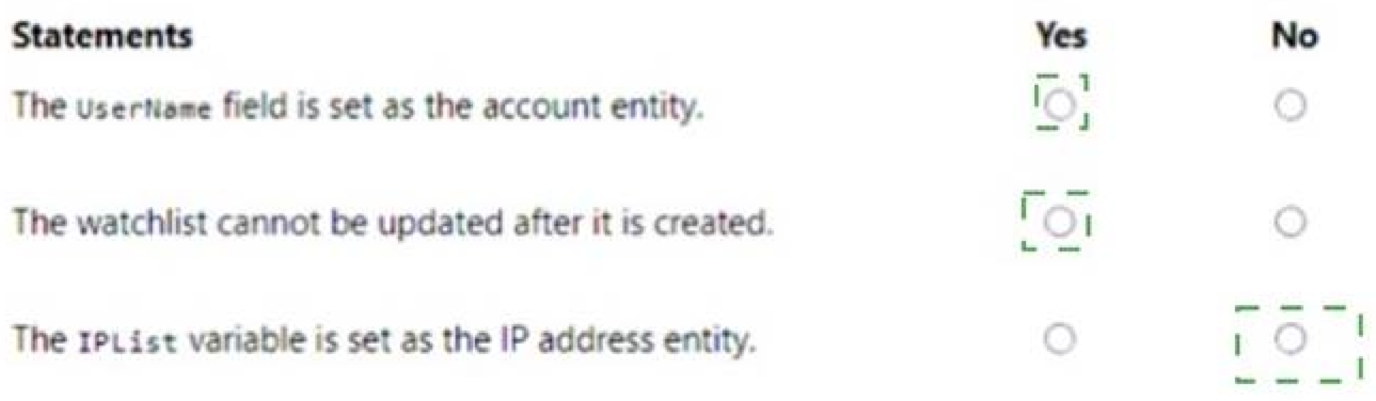


Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

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.	○	[✓ ○]

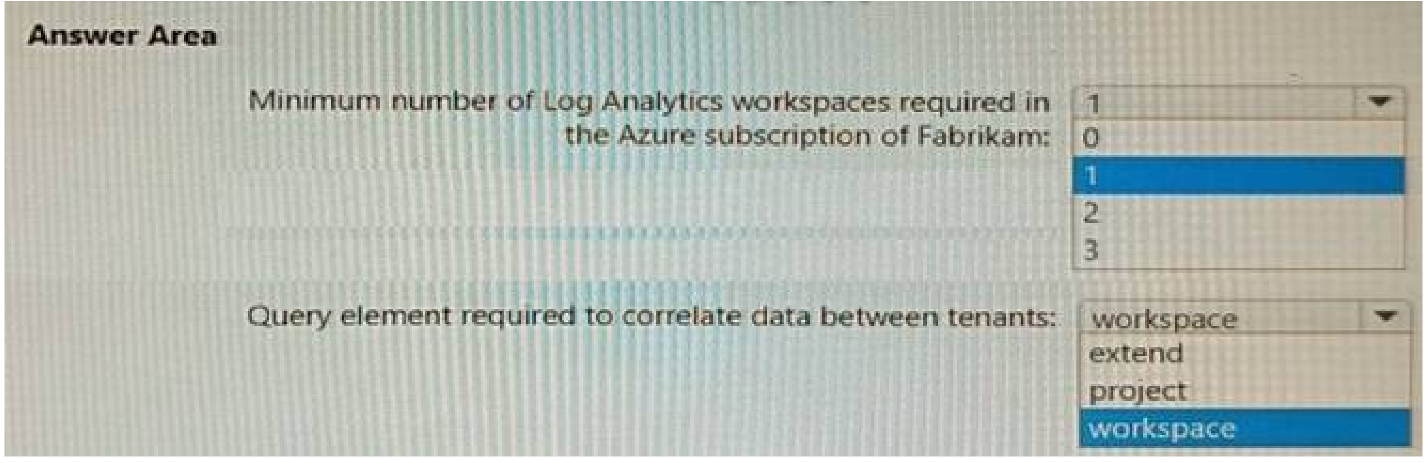
NEW QUESTION 215

HOTSPOT - (Topic 4)

You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.

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

NOTE: Each correct selection is worth one point.



Answer Area

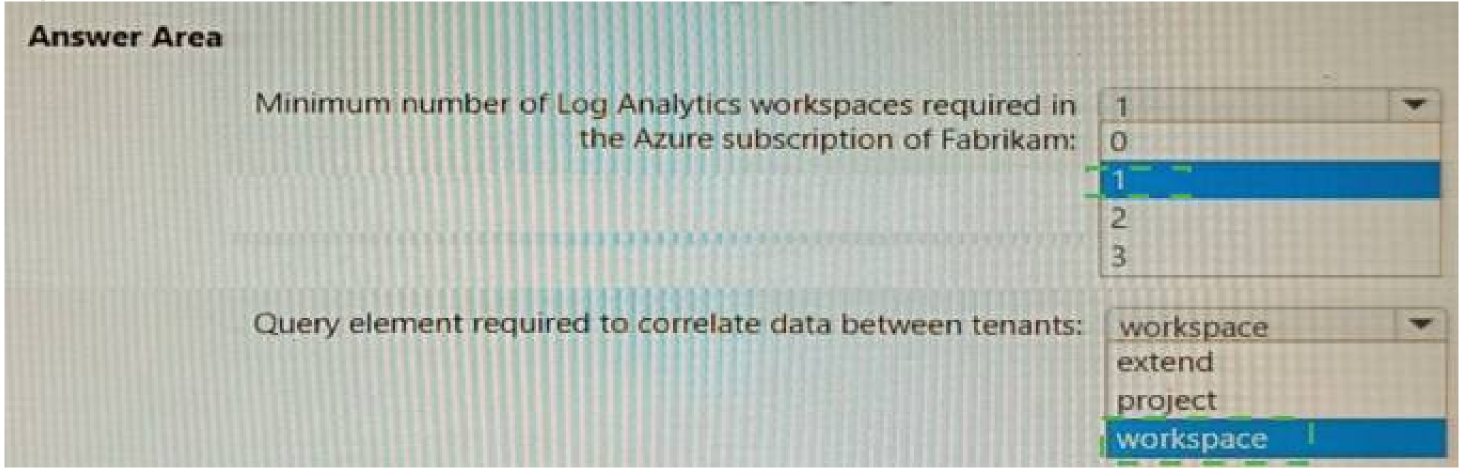
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Answer Area

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

Query element required to correlate data between tenants: workspace

NEW QUESTION 217

- (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 221

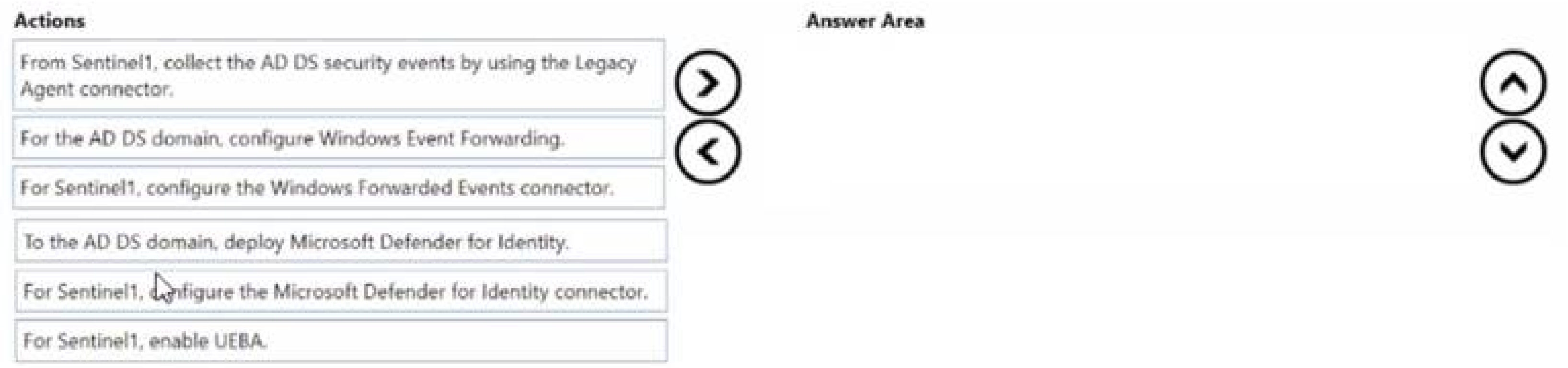
DRAG DROP - (Topic 4)

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

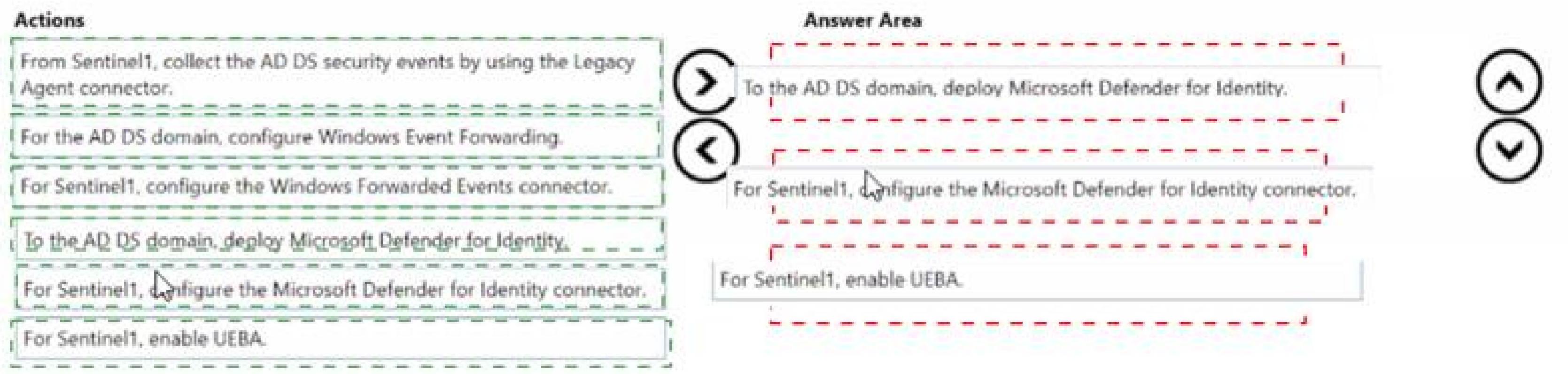
- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

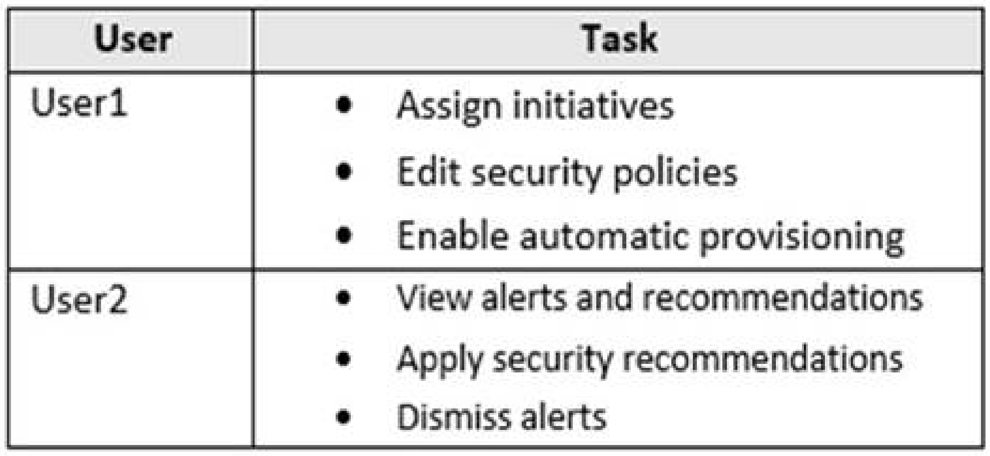
- From Sentinel1, collect the AD DS security events by using the Legacy Agent connector.
- For the AD DS domain, configure Windows Event Forwarding.
- For Sentinel1, configure the Windows Forwarded Events connector.
- To the AD DS domain, deploy Microsoft Defender for Identity.
- For Sentinel1, configure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

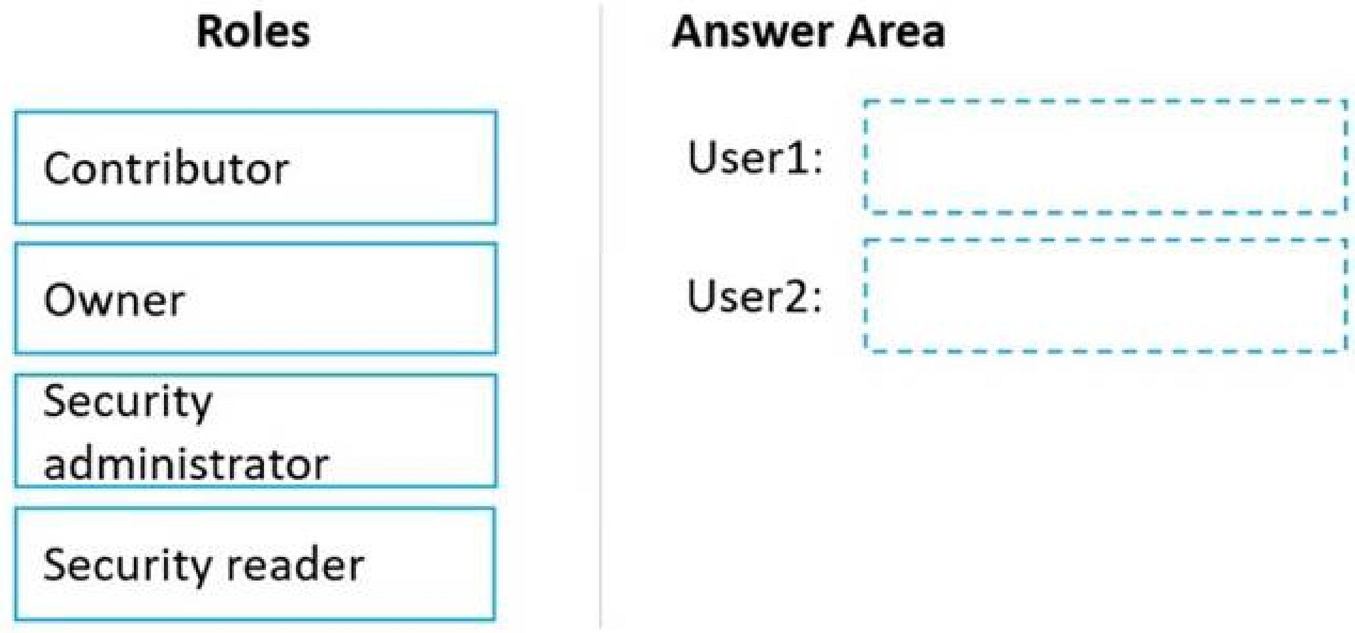
NEW QUESTION 226

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



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

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



Roles

- Contributor
- Owner
- Security administrator
- Security reader

Answer Area

User1:

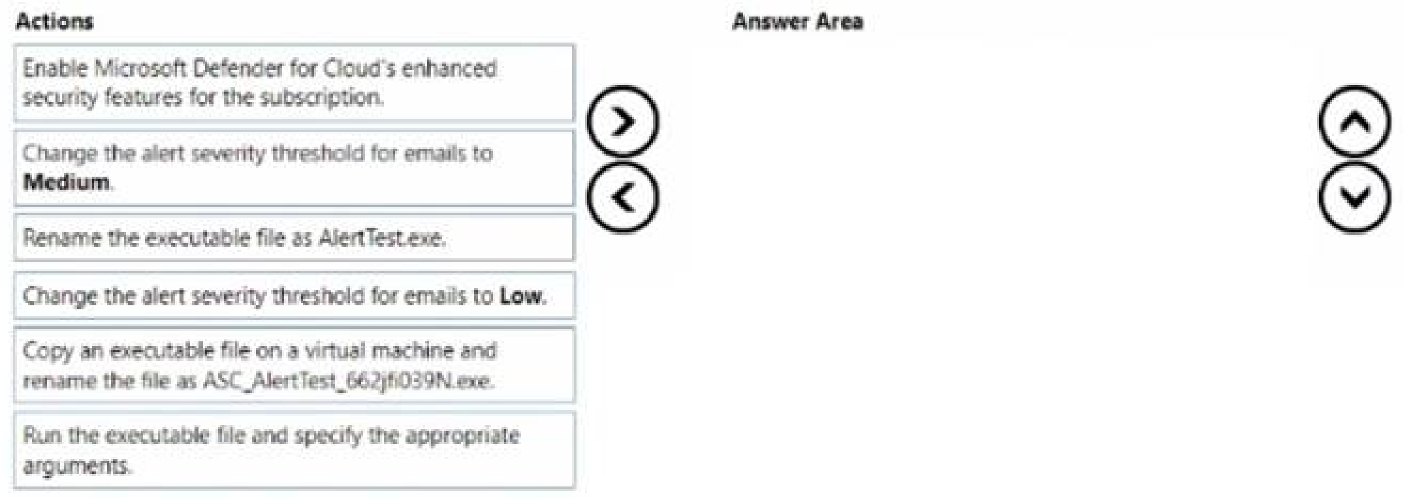
User2:

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 229
DRAG DROP - (Topic 4)
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



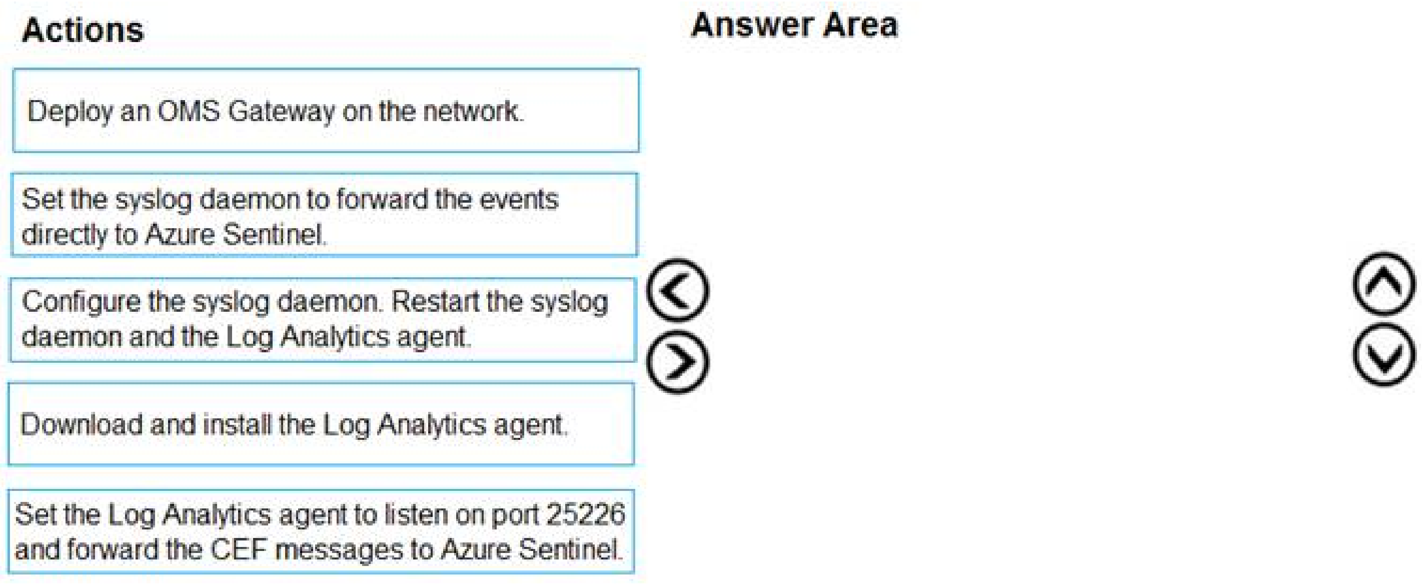
- Enable Microsoft Defender for Cloud's enhanced security features for the subscription.
- Change the alert severity threshold for emails to **Medium**.
- Rename the executable file as AlertTest.exe.
- Change the alert severity threshold for emails to **Low**.
- Copy an executable file on a virtual machine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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 233
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.

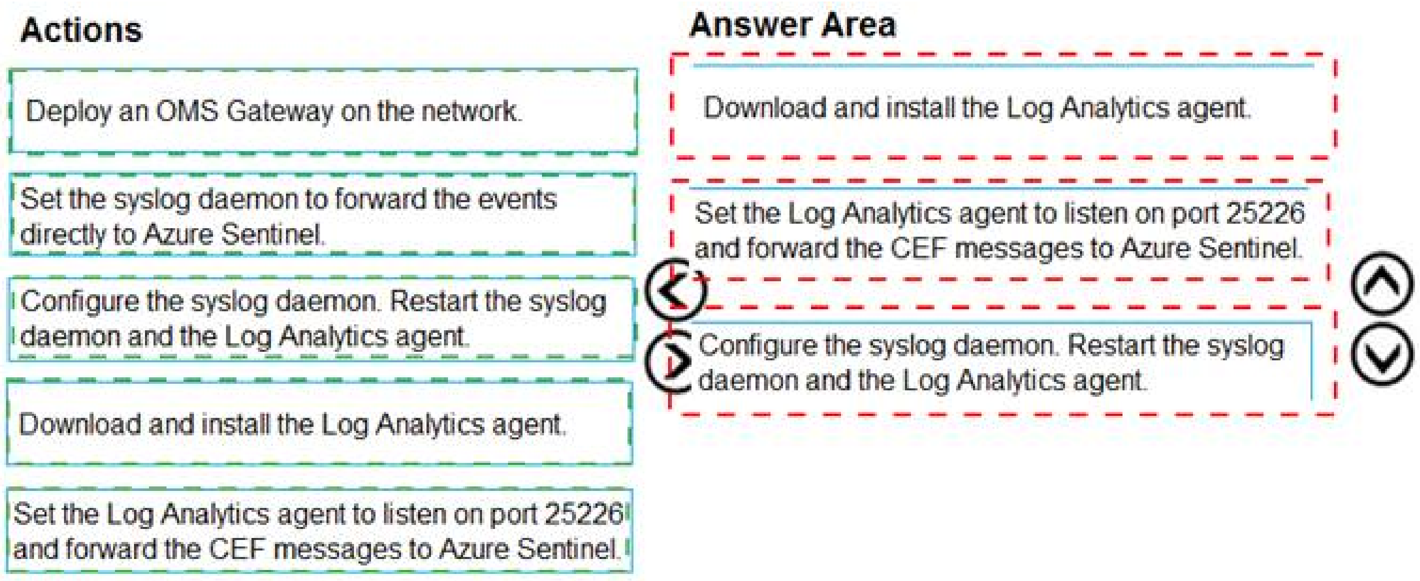


- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.
- Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
- Download and install the Log Analytics agent.
- Set the Log Analytics agent to listen on port 25226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

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.

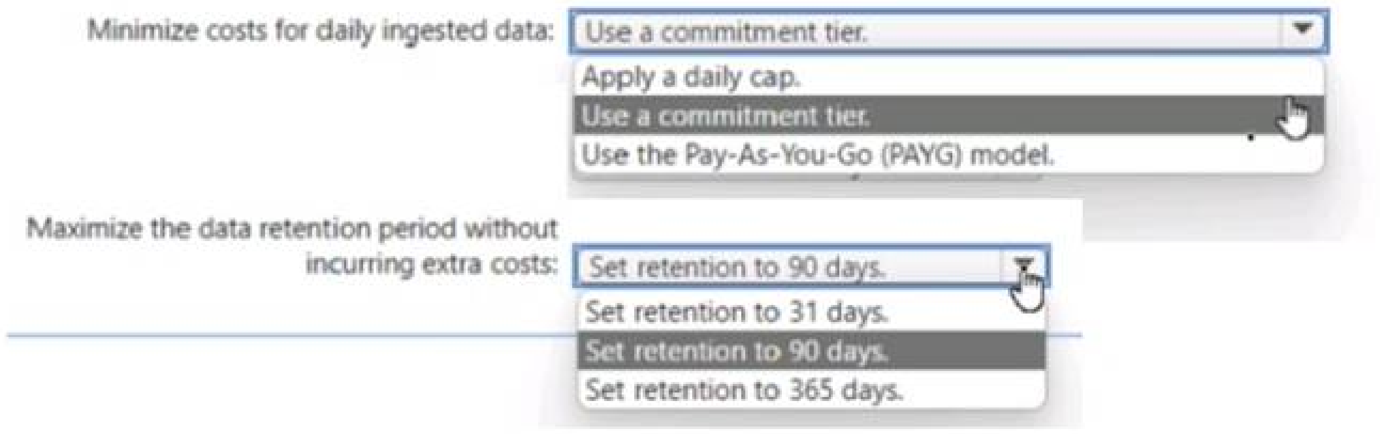
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

NEW QUESTION 238
- (Topic 4)
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.
What should you create first?

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

Answer: D

NEW QUESTION 243
HOTSPOT - (Topic 4)
You have an Azure subscription.
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.
You need to configure storage for the workspace. The solution must meet the following requirements:
• Minimize costs for daily ingested data.
• Maximize the data retention period without incurring extra costs.
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



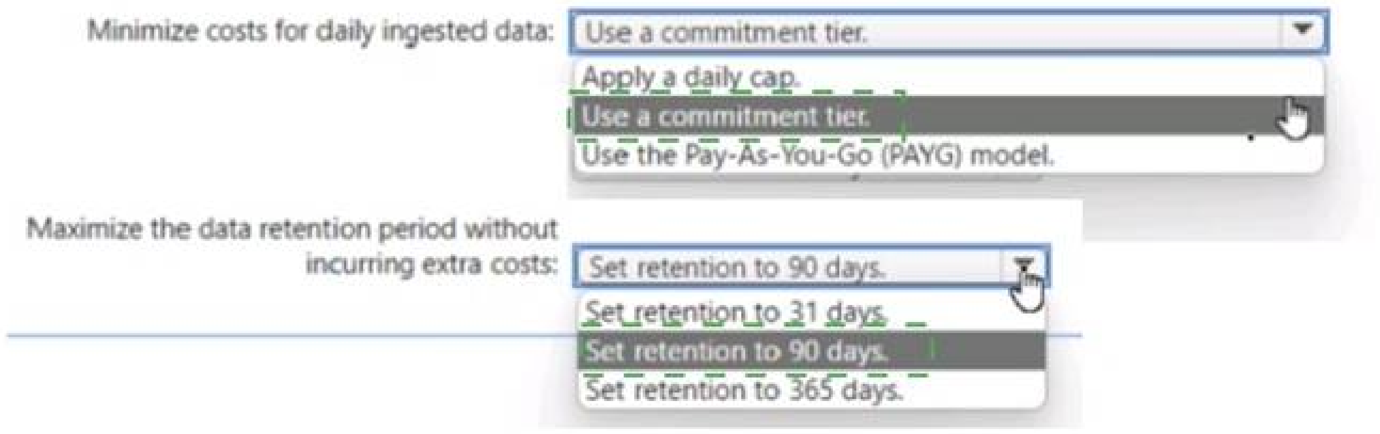
Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

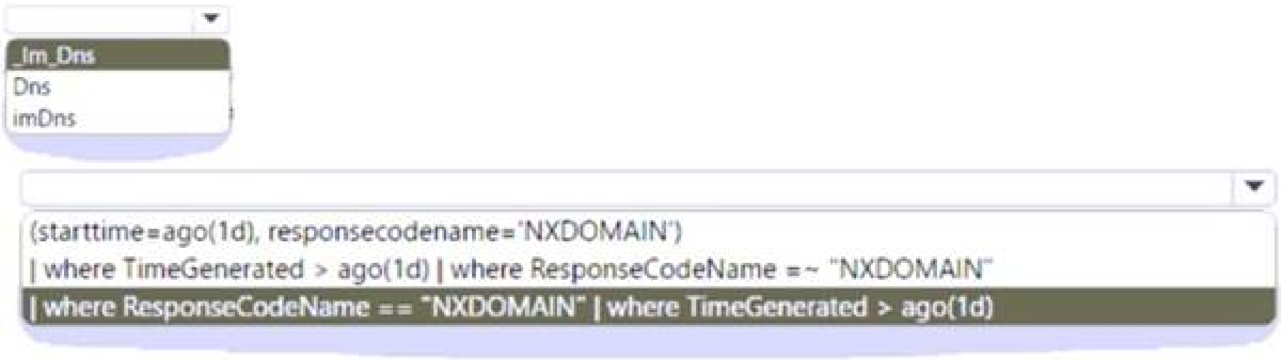


Minimize costs for daily ingested data: Use a commitment tier.
Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

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

NEW QUESTION 247
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c

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



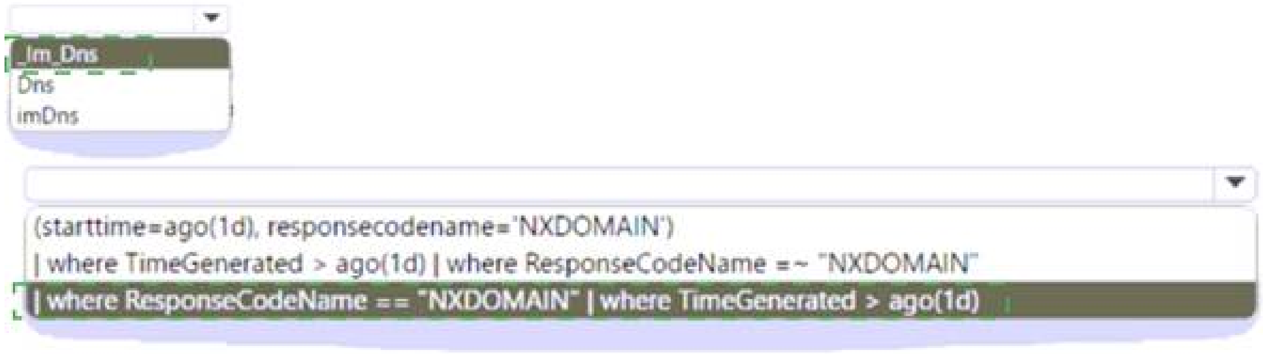
_Im_Dns
Dns
imDns

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



_Im_Dns
Dns
imDns

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

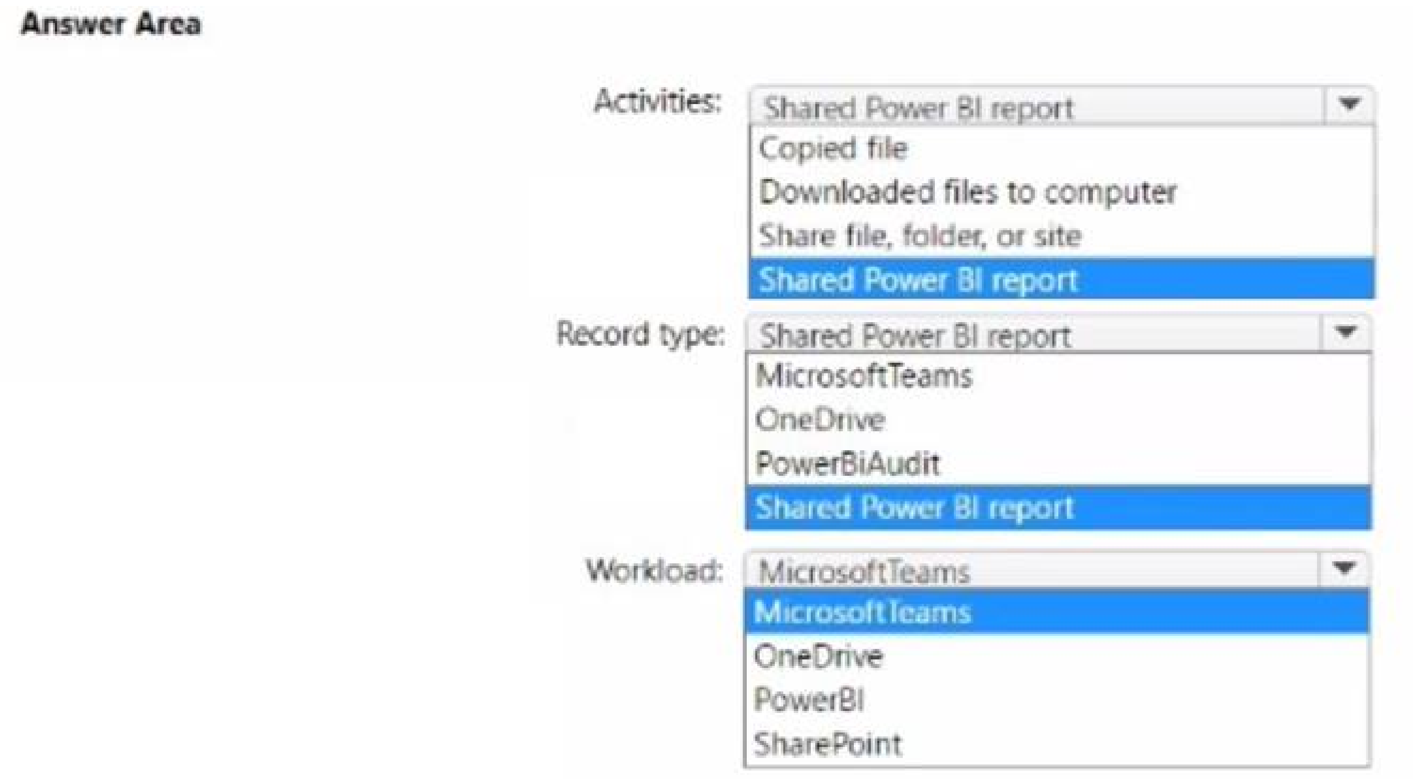
NEW QUESTION 251
- (Topic 4)
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

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

Answer: D

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

NEW QUESTION 255
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.
User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.
You need to identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

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

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

Workload: MicrosoftTeams
- MicrosoftTeams
- OneDrive
- PowerBI
- SharePoint

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 256
- (Topic 4)
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BCE

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

NEW QUESTION 258
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

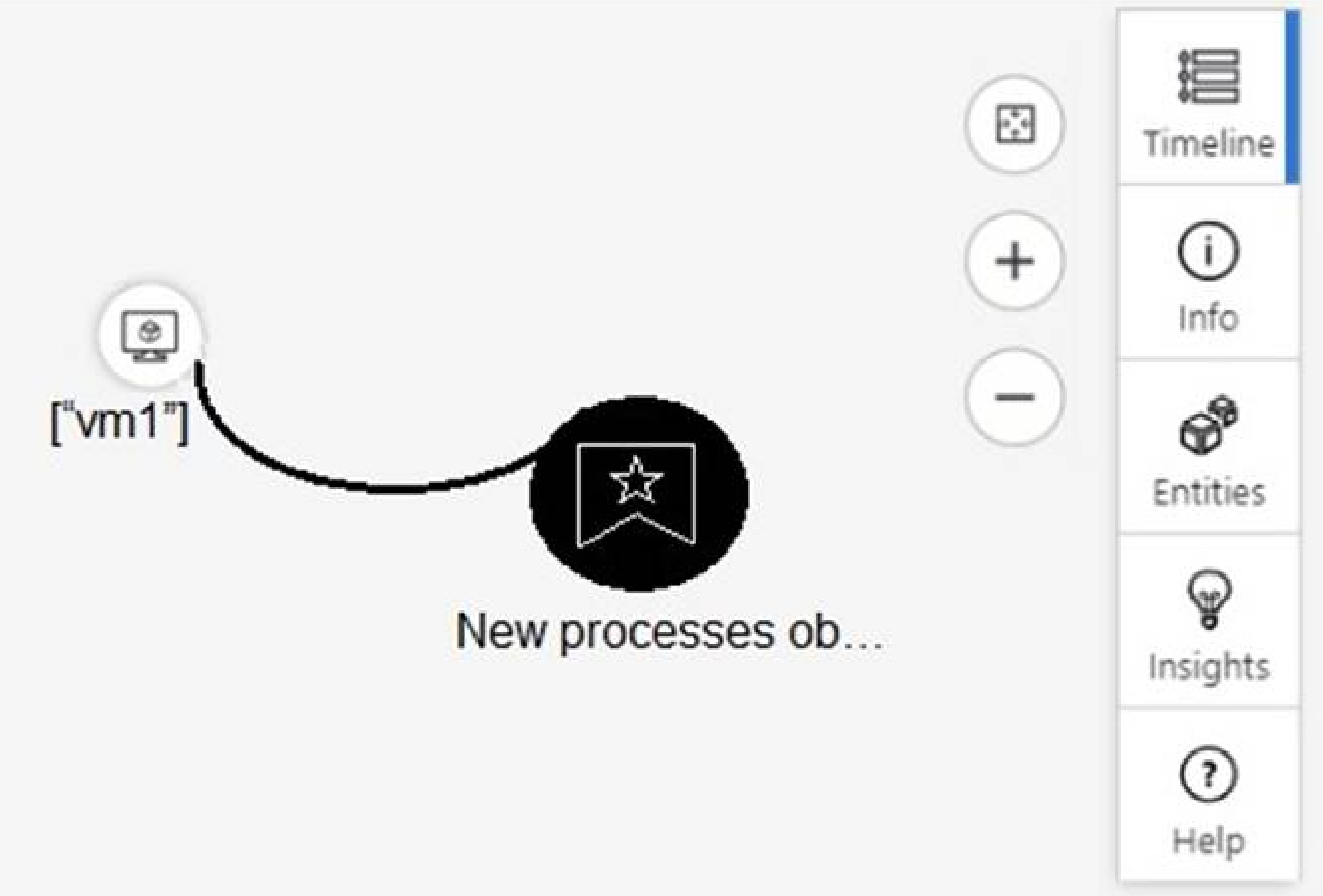
A. Yes
B. No

Answer: B

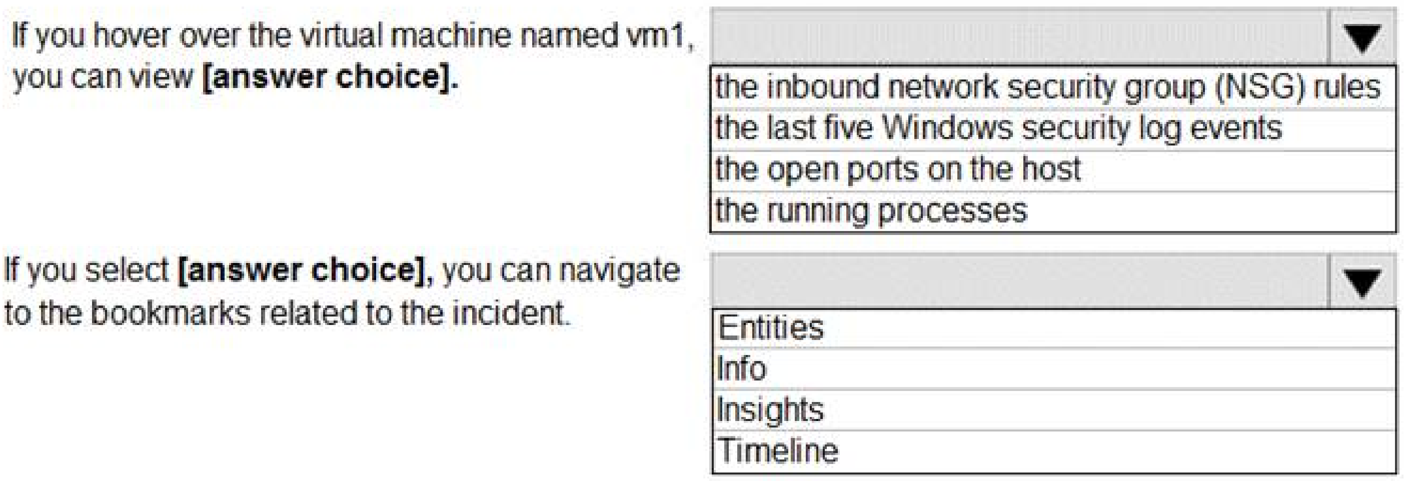
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken- accounts

NEW QUESTION 262

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

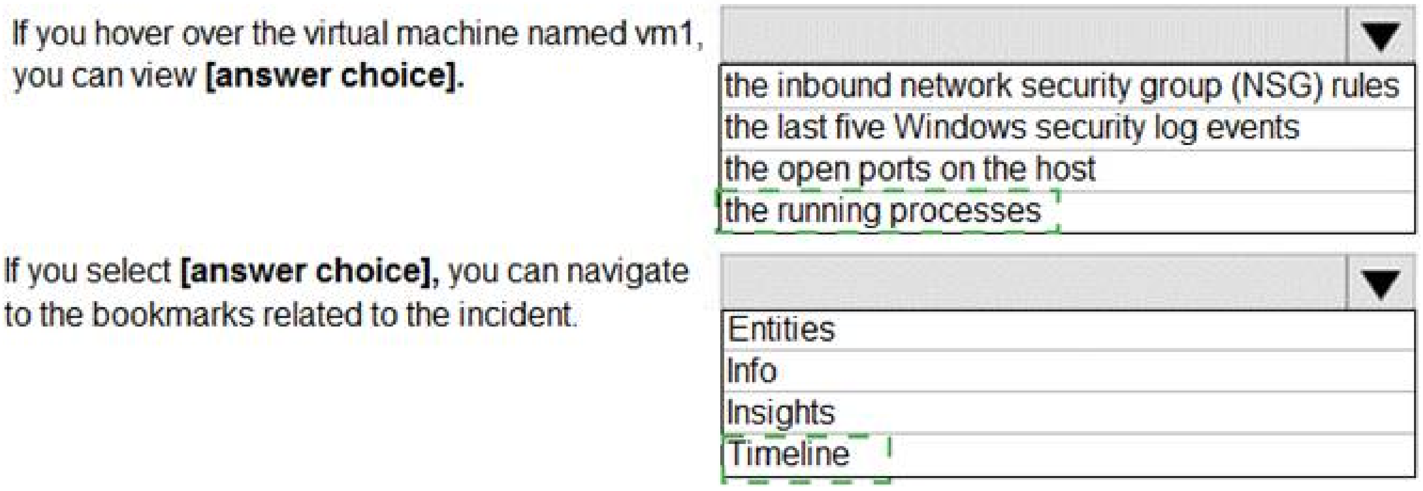
If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- 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 265
- (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 267
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 271
- (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 272
- (Topic 4)
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

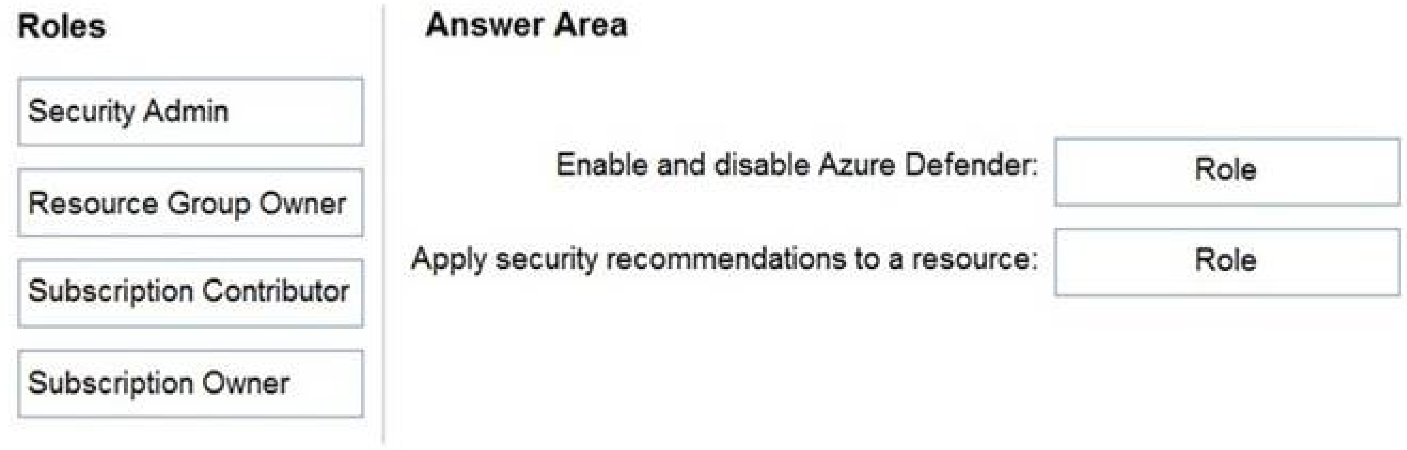
A. Playbooks
B. Analytics
C. Threat intelligence
D. Incidents

Answer: D

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

NEW QUESTION 276
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
? Enable and disable Azure Defender.
? Apply security recommendations to resource.
The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Roles

- Security Admin
- Resource Group Owner
- Subscription Contributor
- Subscription Owner

Answer Area

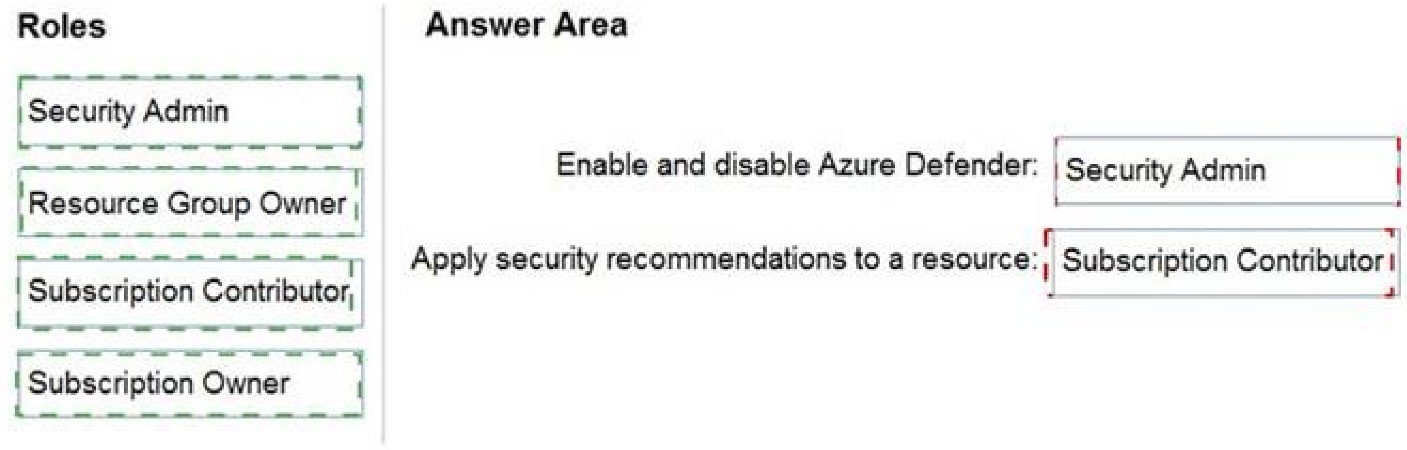
Enable and disable Azure Defender: Role

Apply security recommendations to a resource: Role

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Roles

- Security Admin
- Resource Group Owner
- Subscription Contributor
- Subscription Owner

Answer Area

Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Subscription Contributor

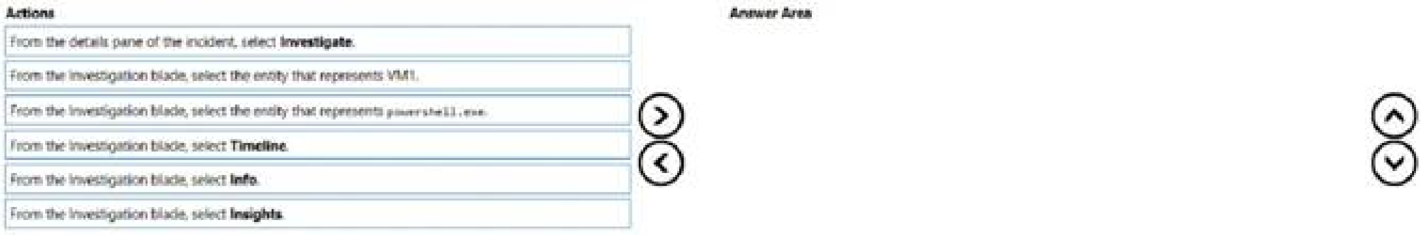
NEW QUESTION 278
- (Topic 4)
A company uses Azure Sentinel.
You need to create an automated threat response. What should you use?

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

Answer: B

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

NEW QUESTION 279
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
? The modification of local group memberships
? The purging of event logs
Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

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

Answer Area

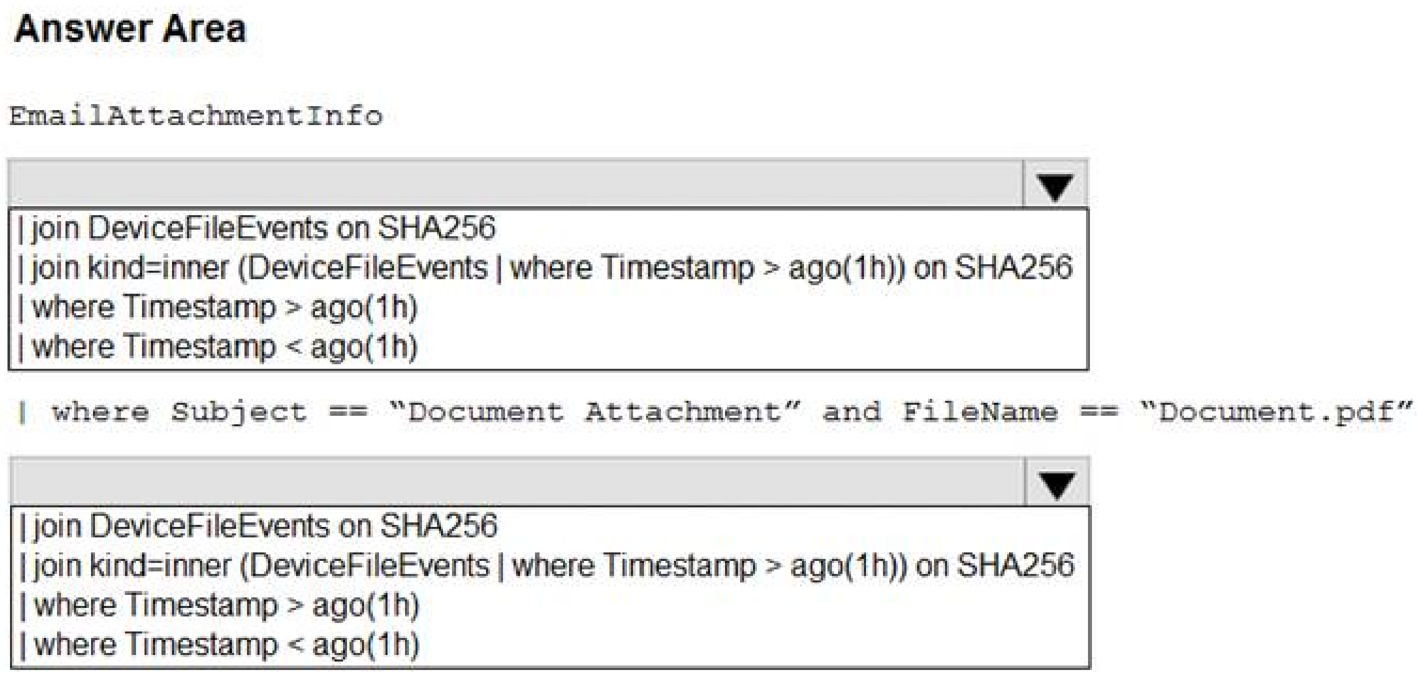
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: From the Investigation blade, select Insights

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

NEW QUESTION 282
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)

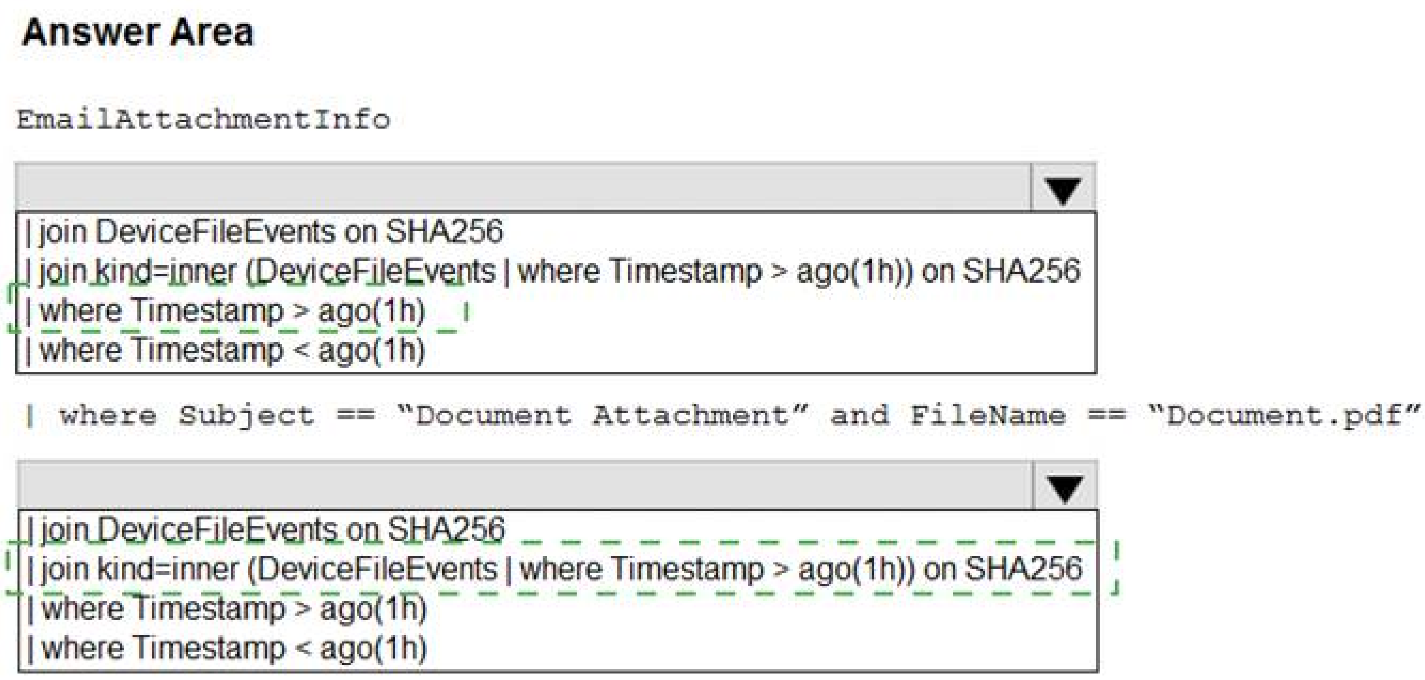
```
| where Subject == "Document Attachment" and FileName == "Document.pdf"
```

▼
| 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 287
- (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?

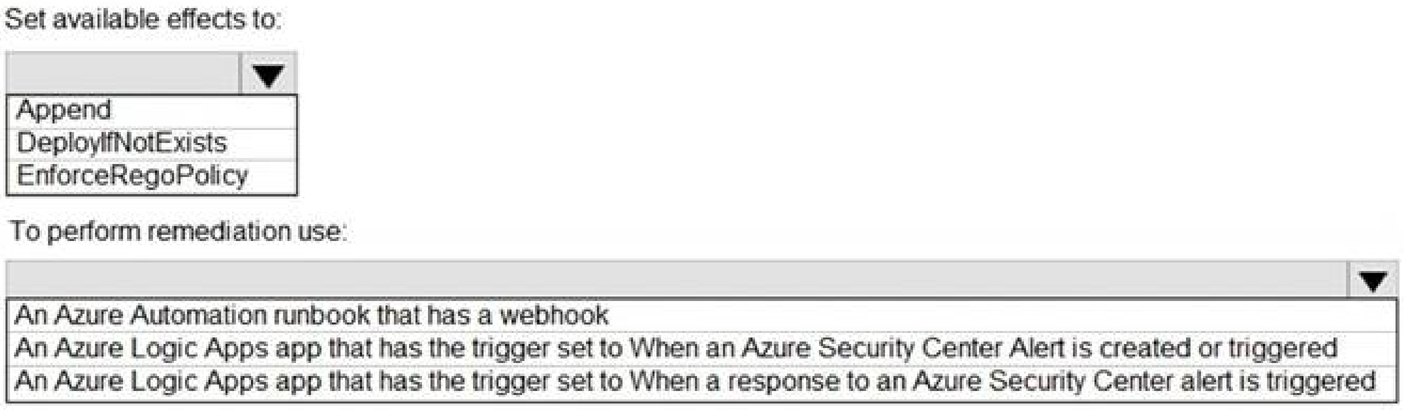
A. a workbook
B. a hunting query
C. a notebook

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 290
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically. What should you include in the solution? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point.



Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

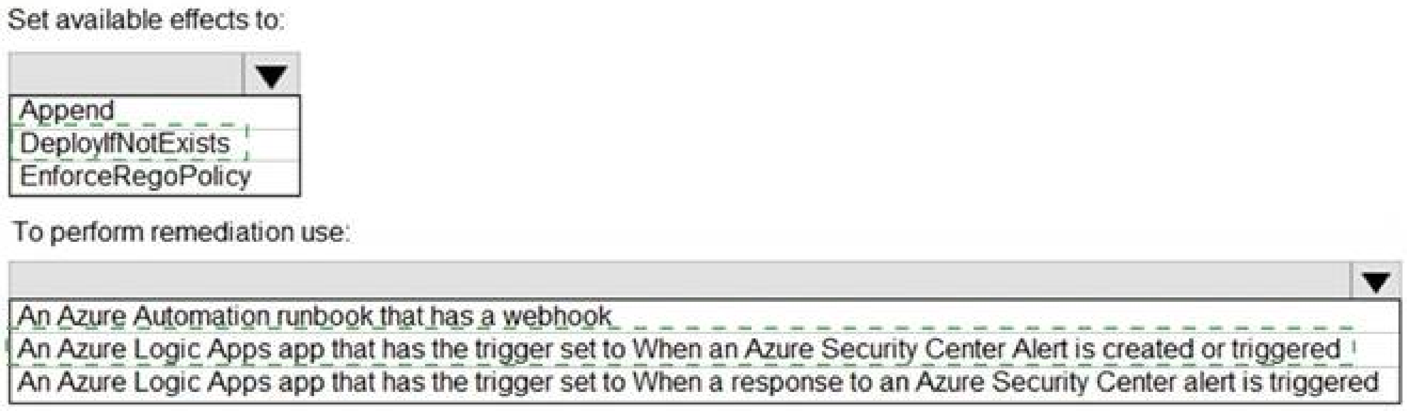
To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

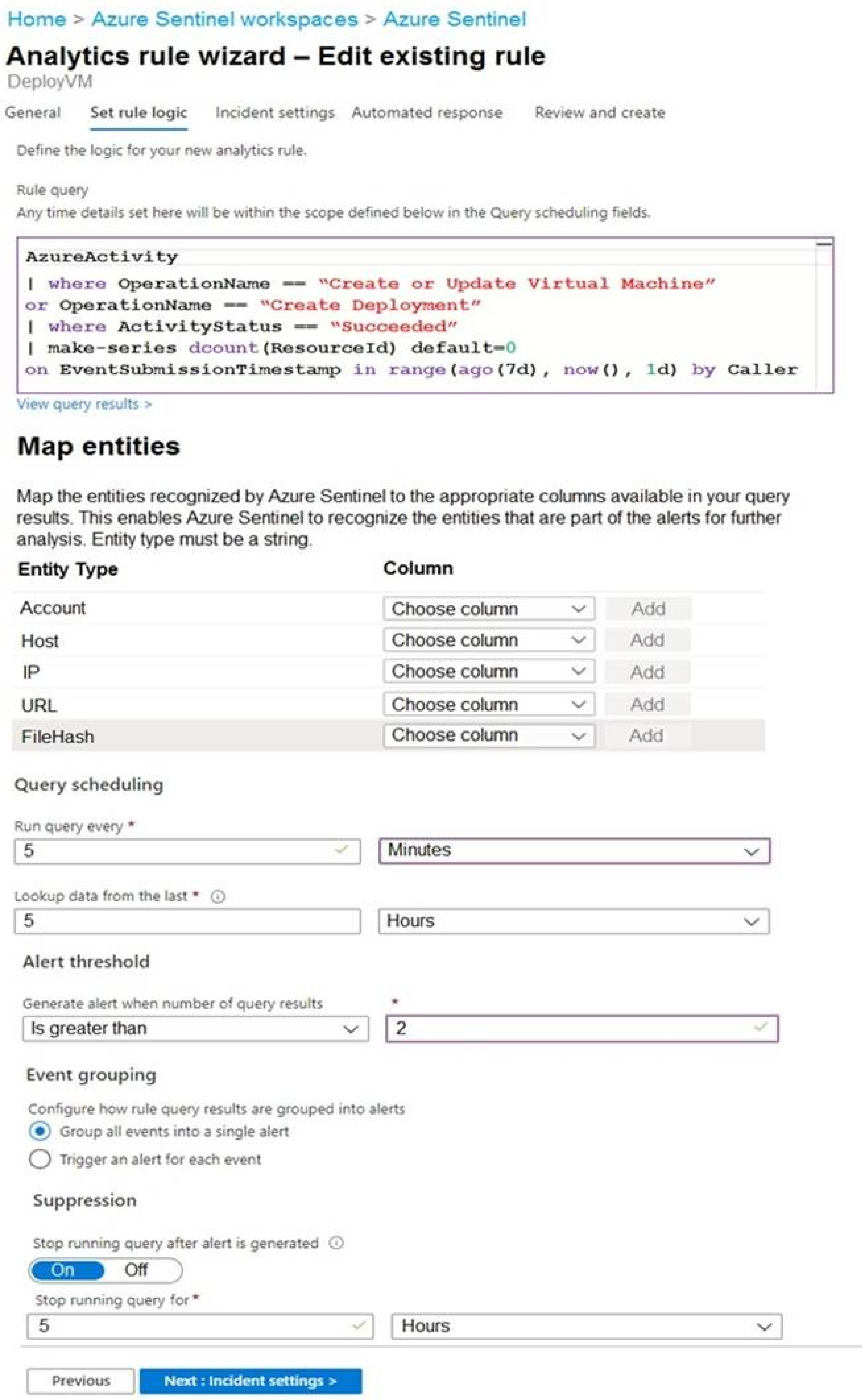
NEW QUESTION 293
- (Topic 4)
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center. What should you do?

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

Answer: B

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

NEW QUESTION 297
HOTSPOT - (Topic 4)
You use Azure Sentinel to monitor irregular Azure activity.
You create custom analytics rules to detect threats as shown in the following exhibit.



Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

Define the logic for your new analytics rule.

Rule query

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

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

View query results >

Map entities

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

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

Query scheduling

Run query every *: 5 Minutes

Lookup data from the last *: 5 Hours

Alert threshold

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

Event grouping

Configure how rule query results are grouped into alerts

● Group all events into a single alert

○ Trigger an alert for each event

Suppression

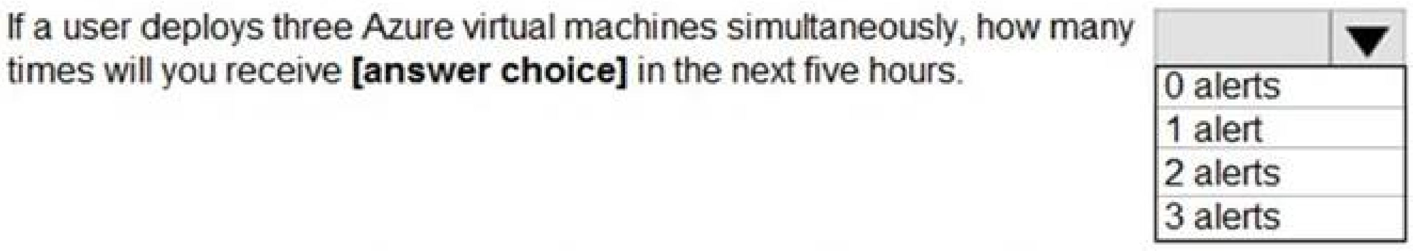
Stop running query after alert is generated: On

Stop running query for *: 5 Hours

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

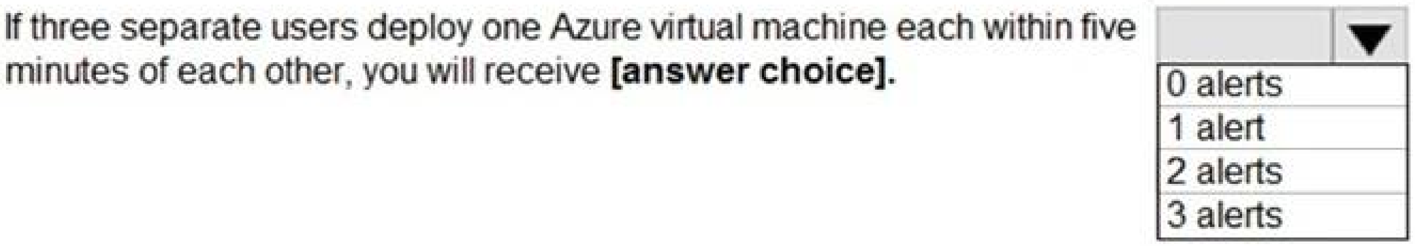
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



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

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts



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

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 301
- (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 303
- (Topic 4)
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.
You have three custom device groups.
You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: ACD

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

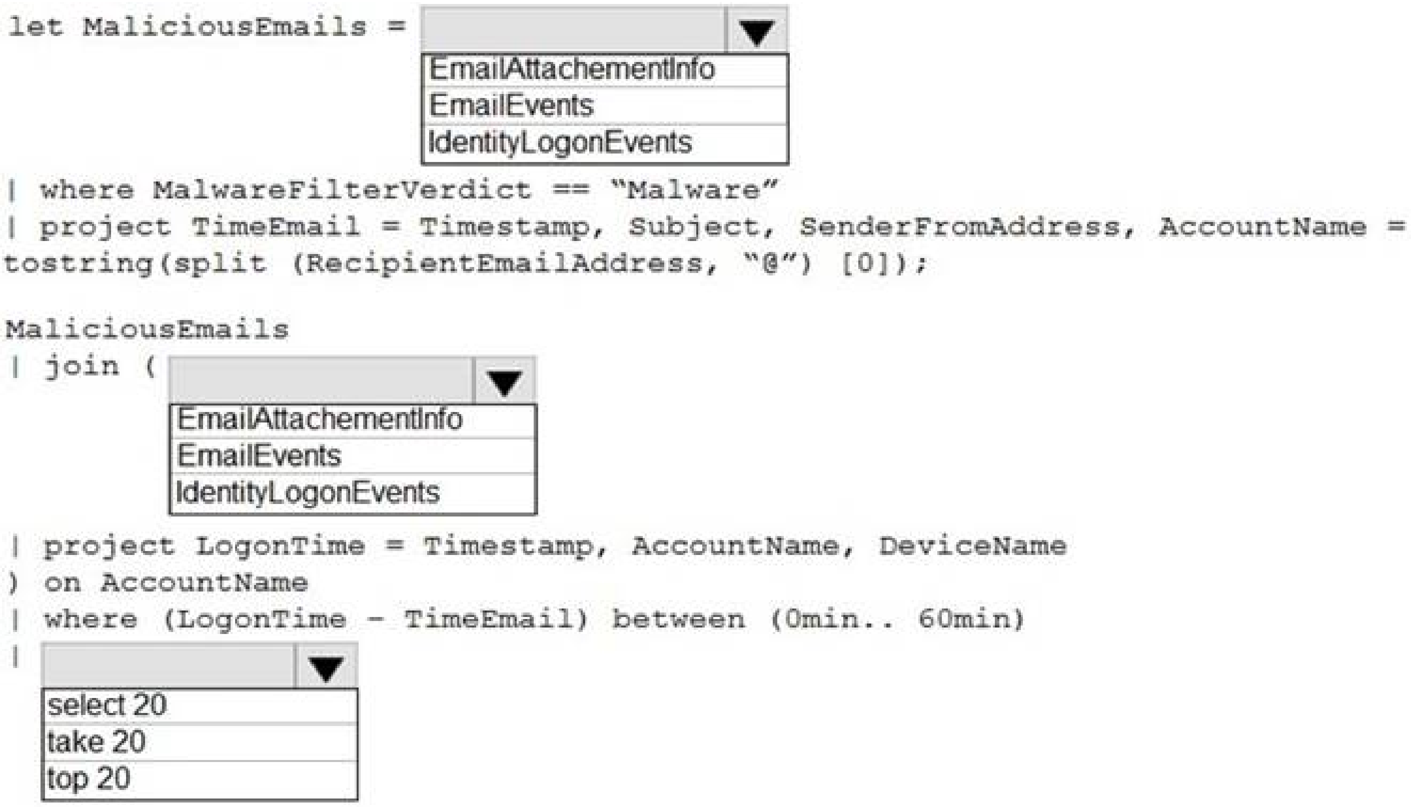
NEW QUESTION 308
- (Topic 4)
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

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 313
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

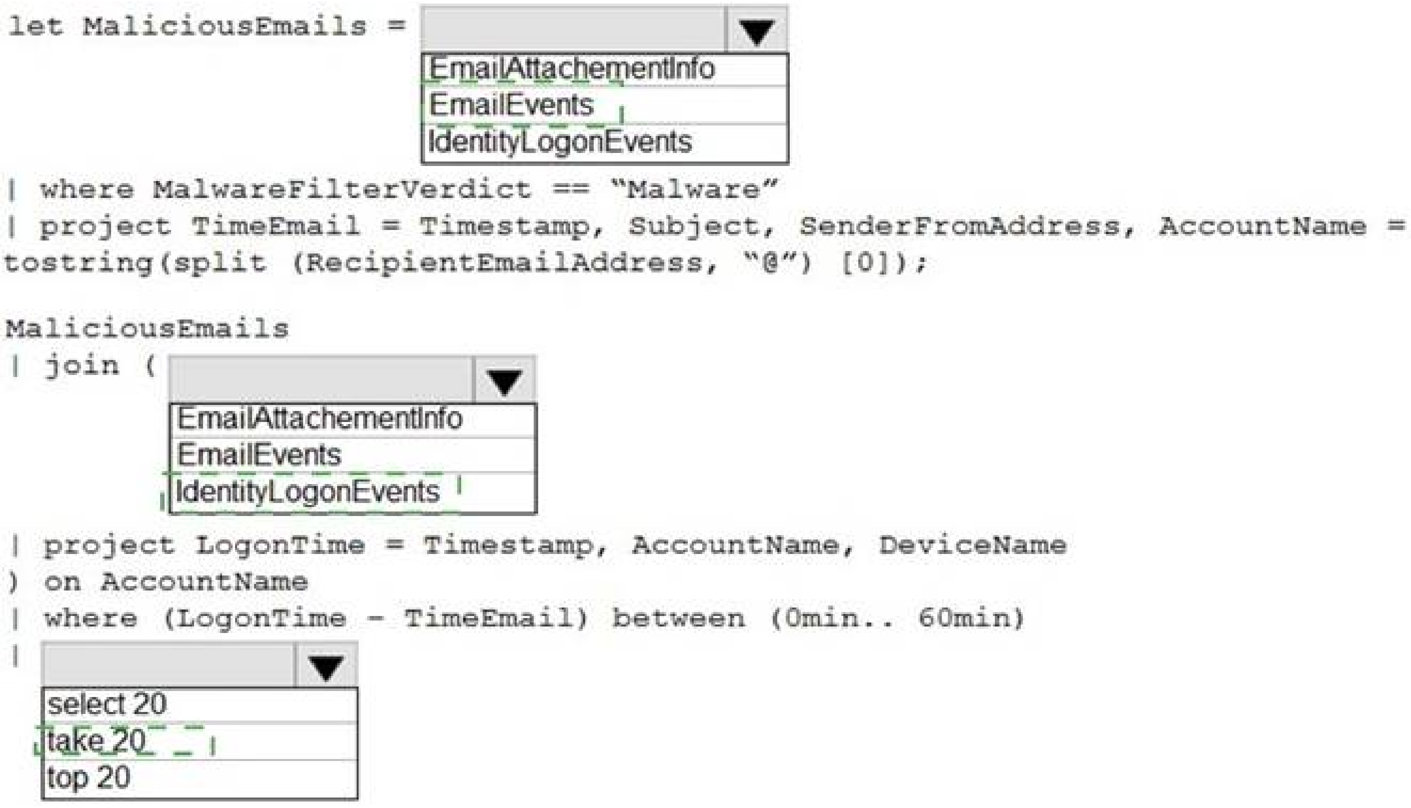
```
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
```

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 317

......

Relate Links

100% Pass Your SC-200 Exam with Exambible Prep Materials

https://www.exambible.com/SC-200-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/