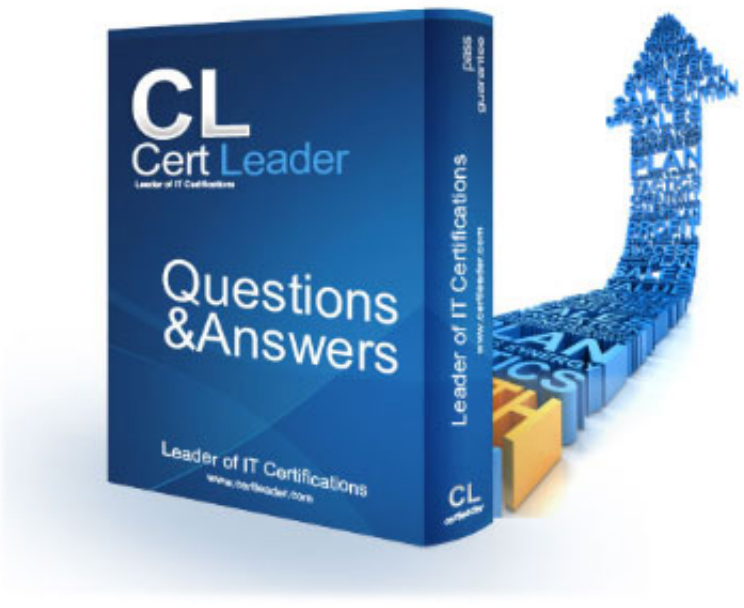
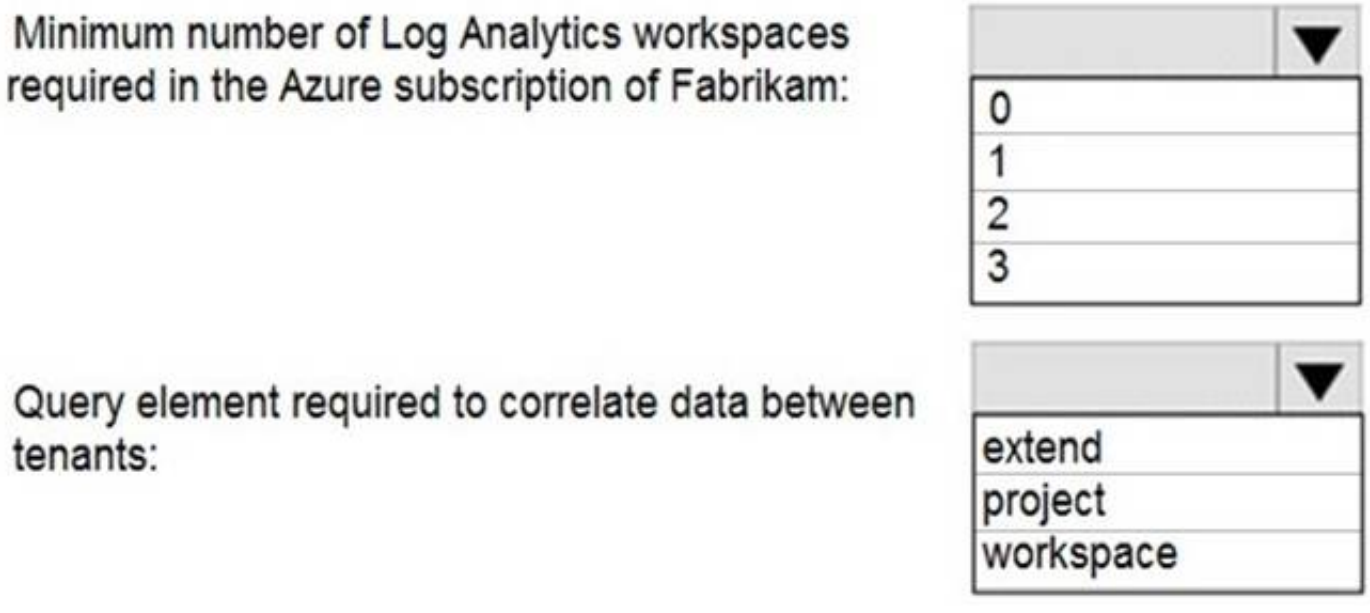
SC-200 Dumps

Microsoft Security Operations Analyst

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



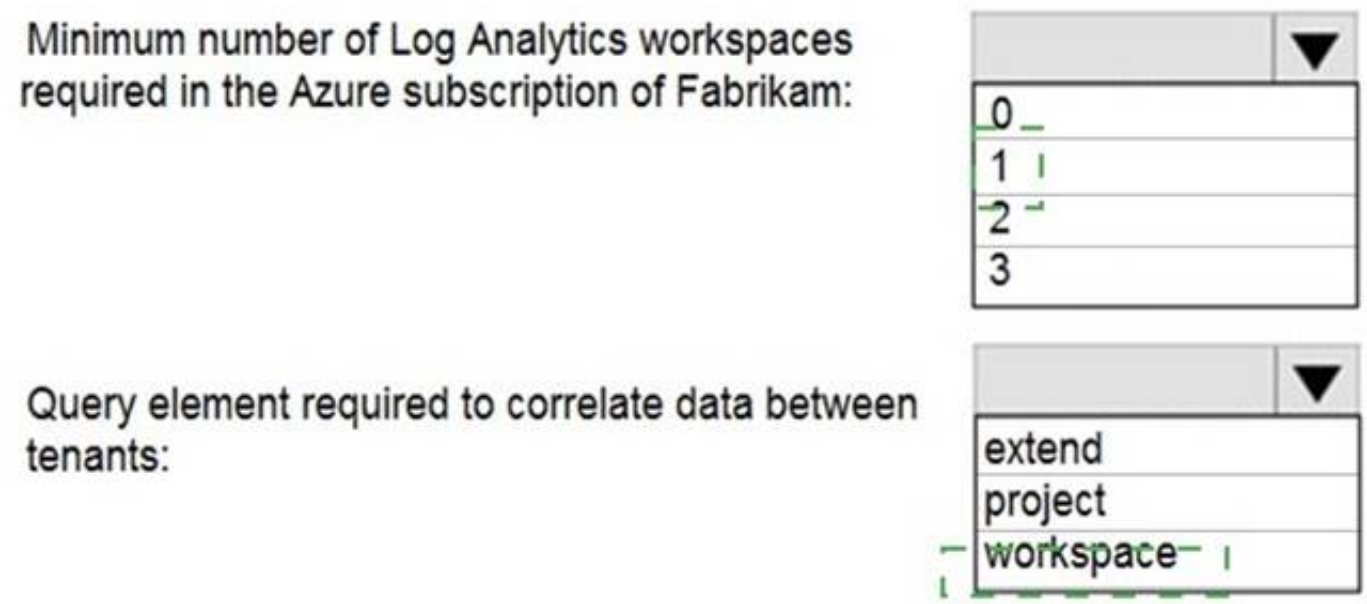
NEW QUESTION 1
HOTSPOT - (Topic 1)
You need to implement Azure Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 2
- (Topic 1)
You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

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

Answer: B

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

NEW QUESTION 3
- (Topic 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)

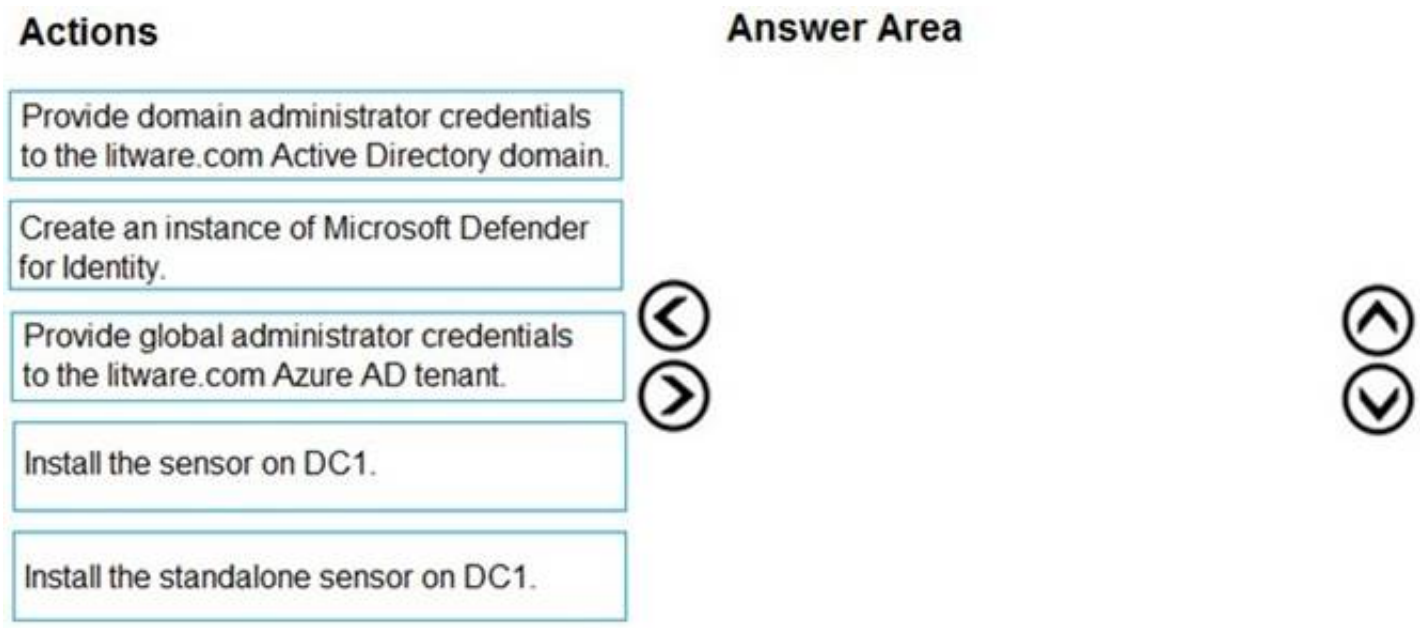
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

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
DRAG DROP - (Topic 2)
You need to configure DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

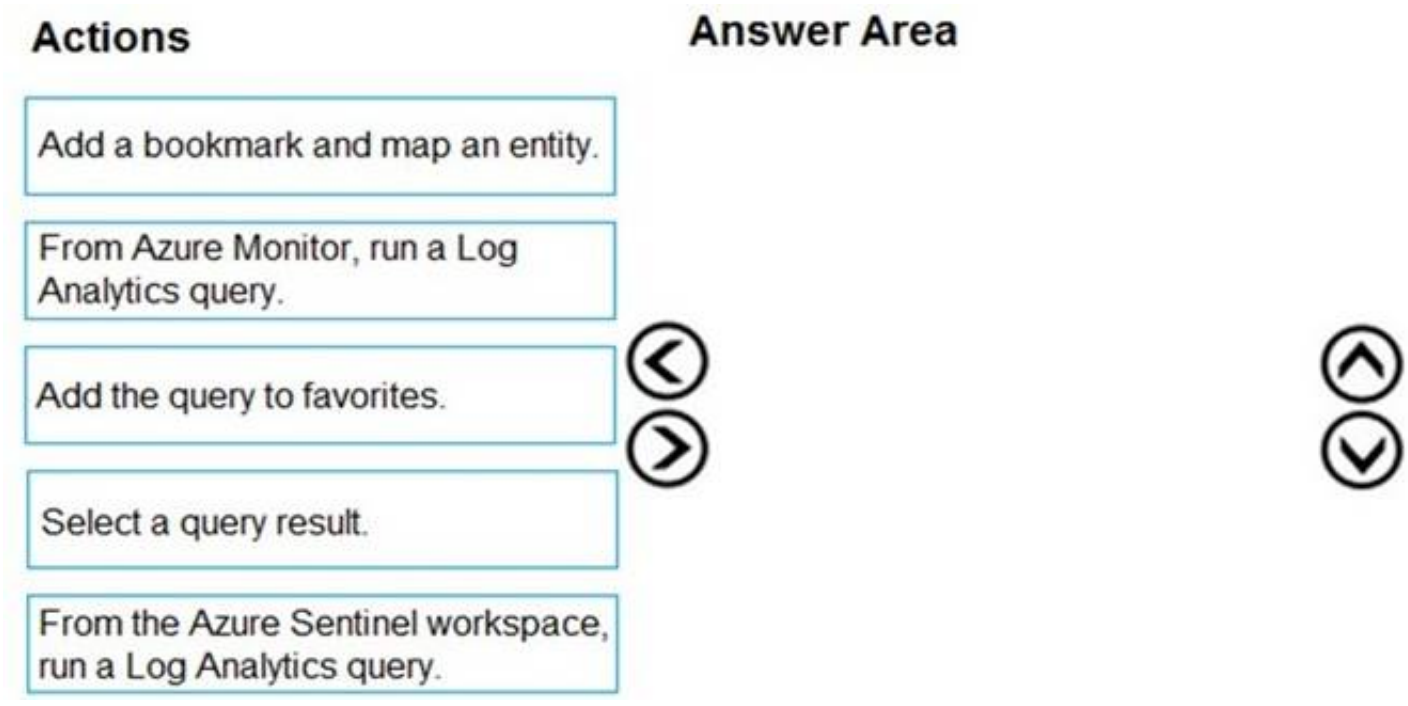
Explanation:
Text Description automatically generated with medium confidence
Step 1: log in to https://portal.atp.azure.com as a global admin
Step 2: Create the instance
Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor.

NEW QUESTION 6
- (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

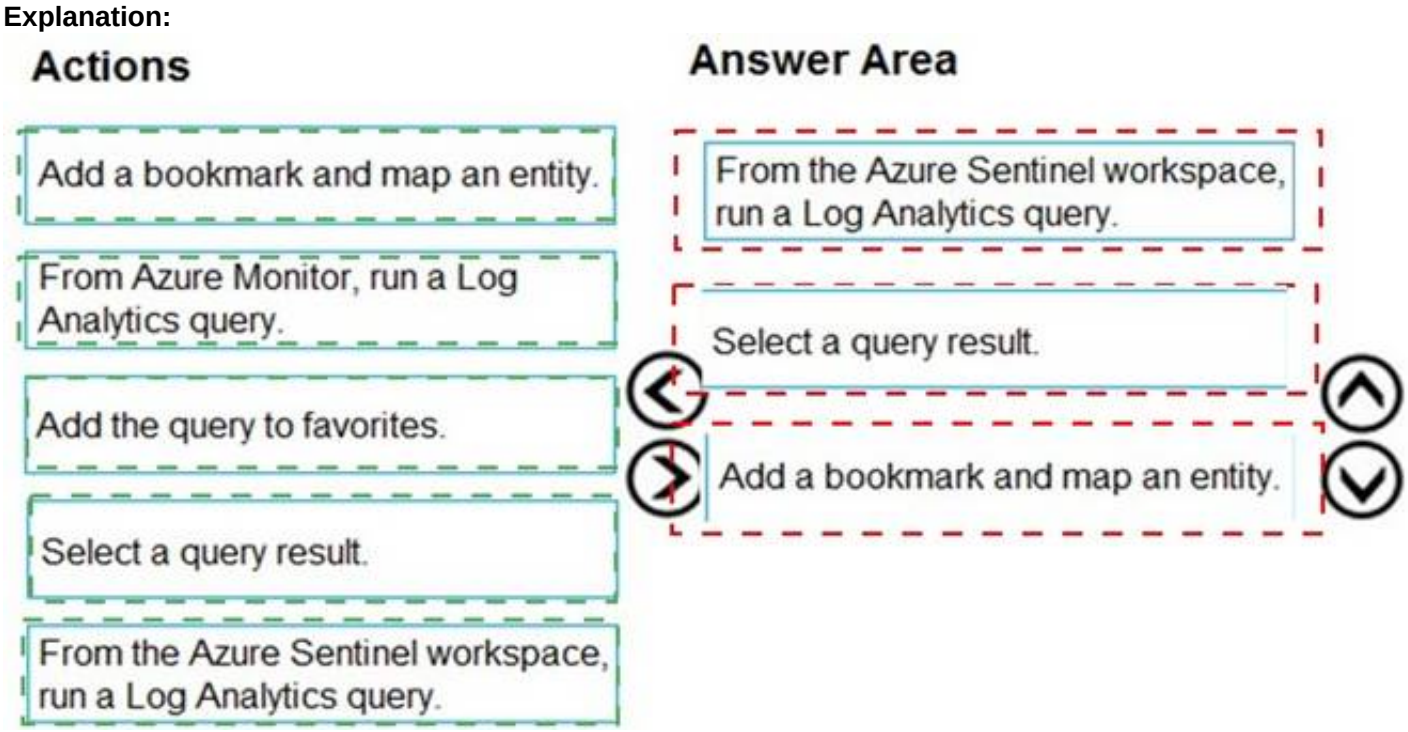
NEW QUESTION 7
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



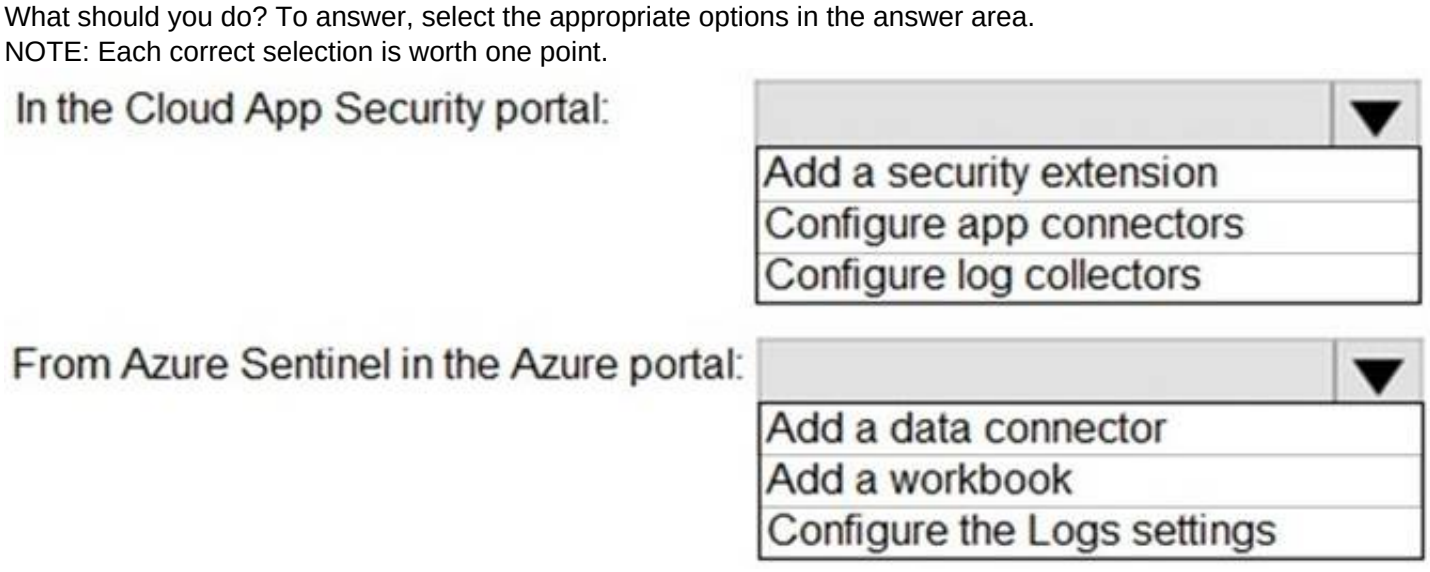
A. Mastered
B. Not Mastered

Answer: A

Explanation:



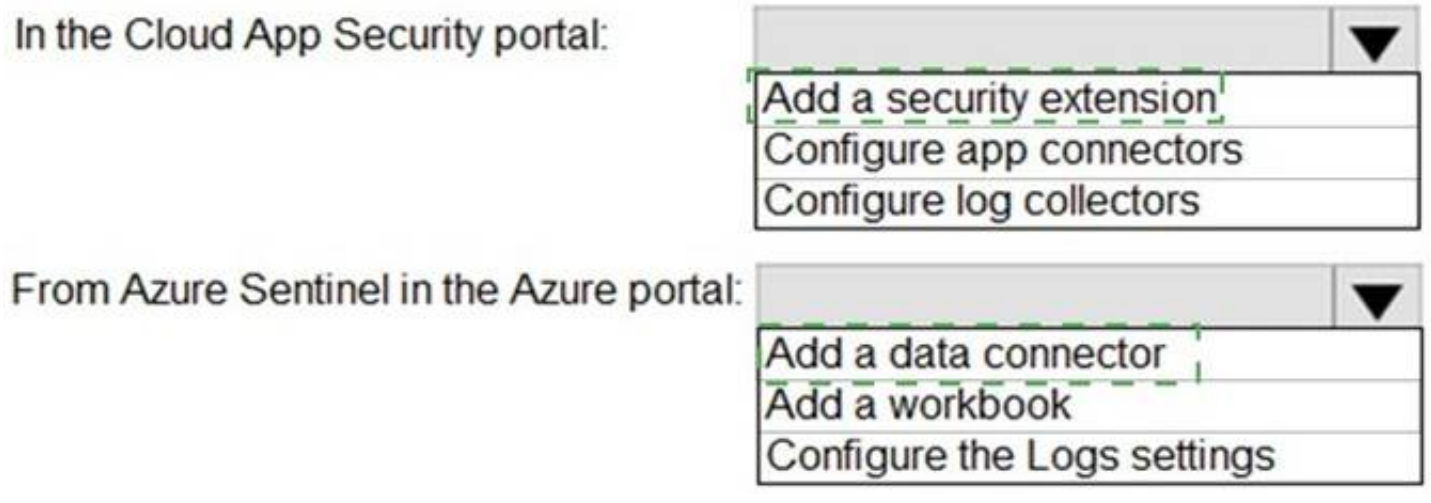
NEW QUESTION 8
HOTSPOT - (Topic 2)
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 9
- (Topic 2)
You need to implement the Azure Information Protection requirements. What should you configure first?

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

Answer: D

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

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

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

Answer: C

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

NEW QUESTION 10
- (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

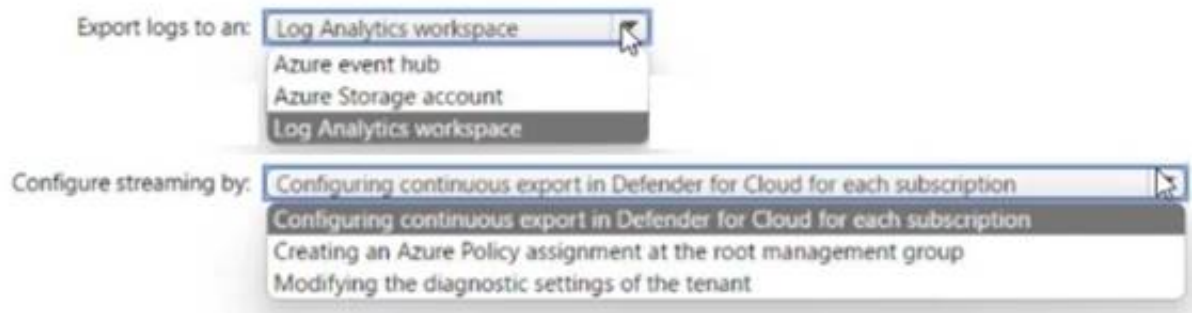
NEW QUESTION 11
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

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

Answer: D

NEW QUESTION 15
HOTSPOT - (Topic 4)
You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point

Answer Area

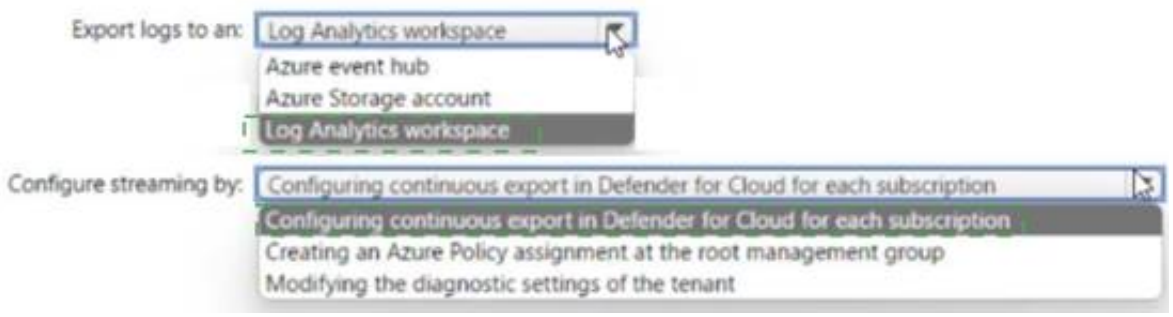


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



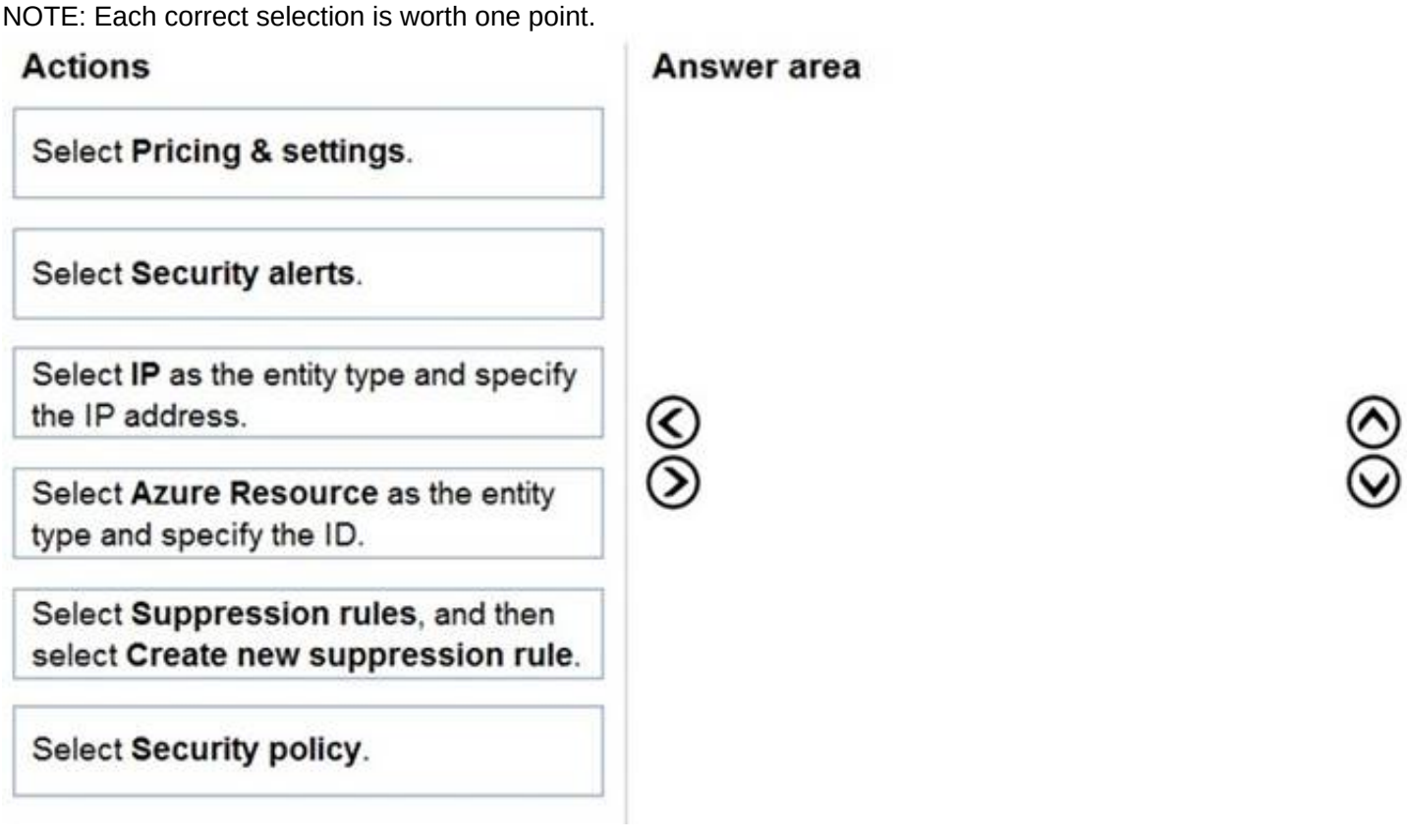
NEW QUESTION 20
- (Topic 4)
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

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

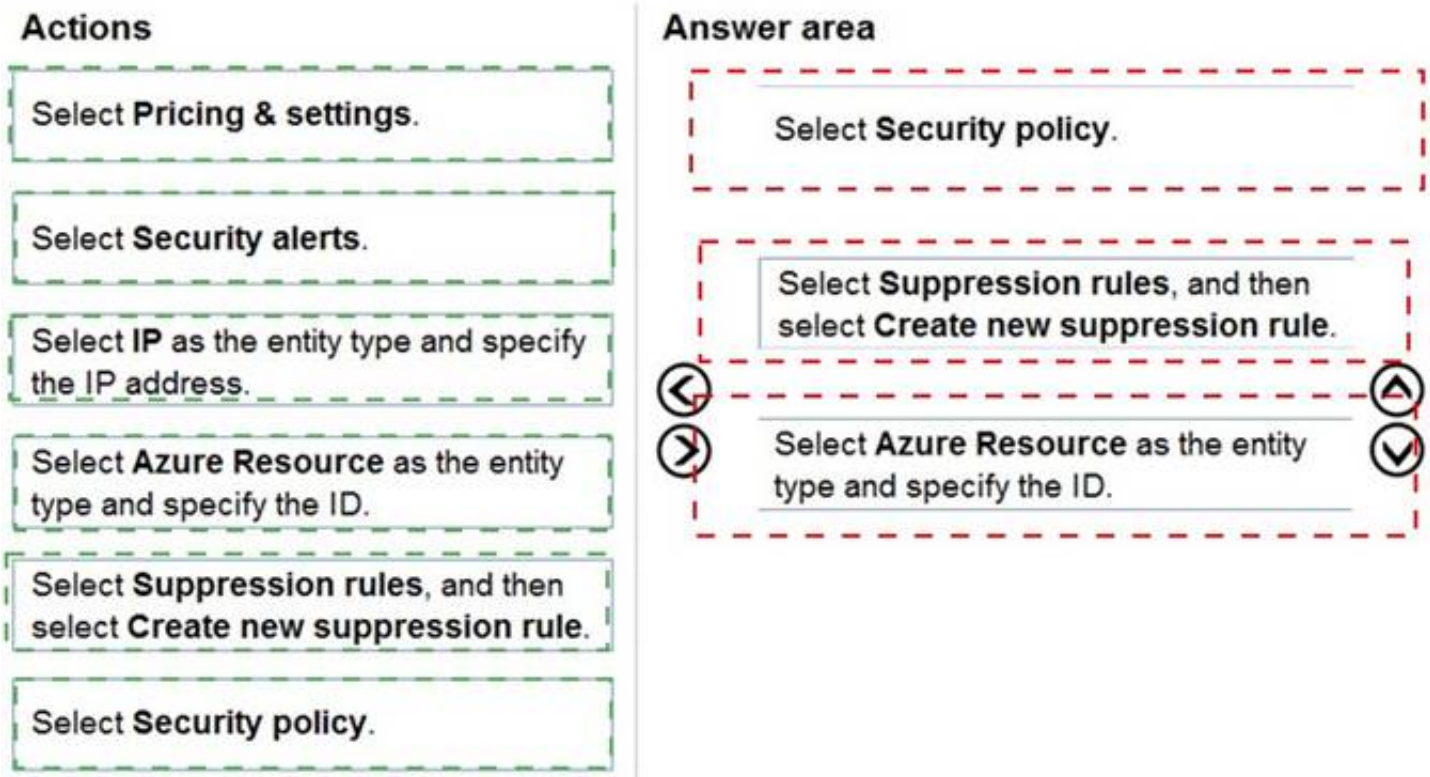
NEW QUESTION 24
DRAG DROP - (Topic 4)
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 25
- (Topic 4)
You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert. What should you create first?

A. a repository connection
B. awatchlist
C. an analytics rule
D. an automation rule

Answer: D

NEW QUESTION 30
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark. Does this meet the goal?

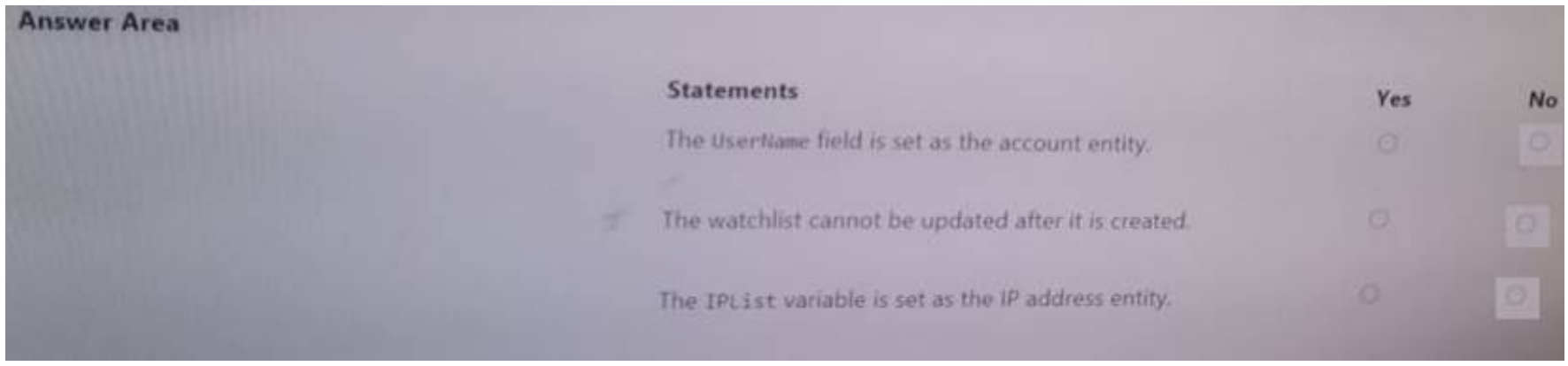
A. Yes
B. No

Answer: B

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

NEW QUESTION 35
HOTSPOT - (Topic 4)
You have the following SQL query.

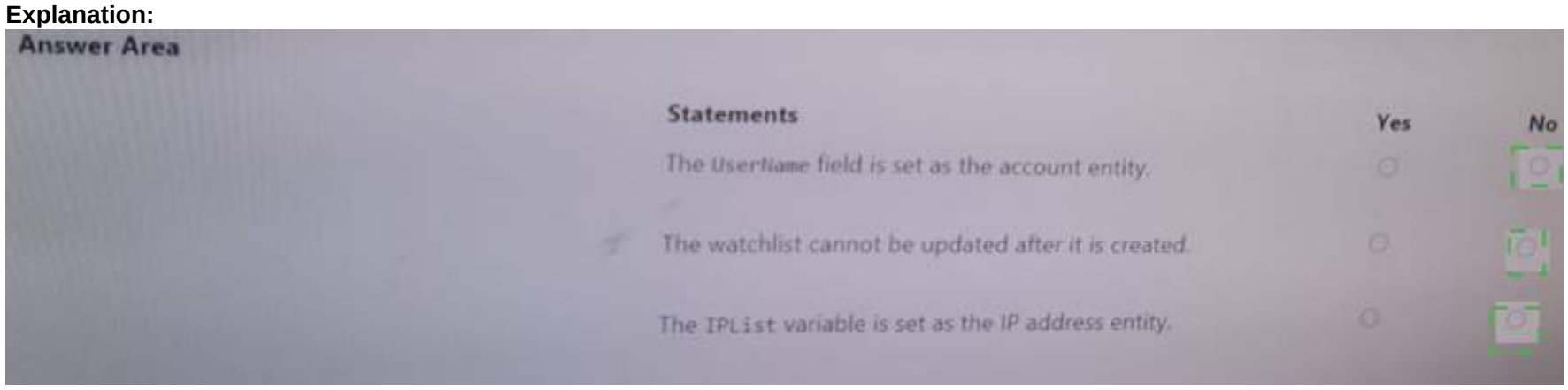
```
let IPList = _GetWatchlist('Bad_IPs');
Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID == 3
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
   | 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, '
```



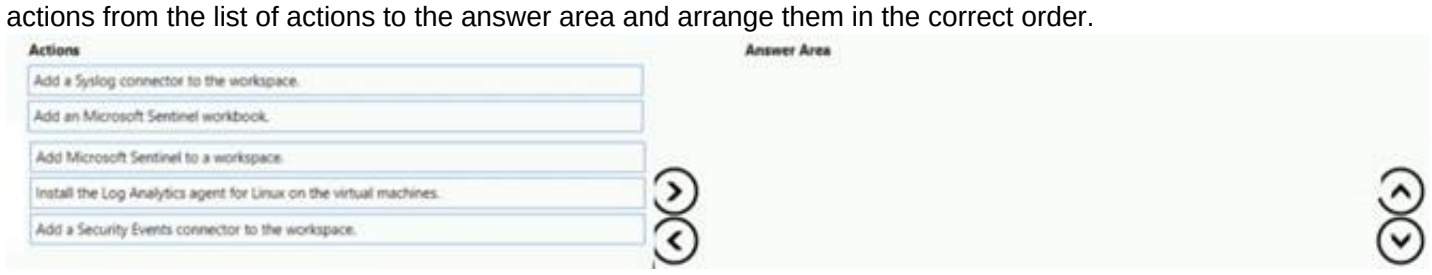
A. Mastered
B. Not Mastered

Answer: A

Explanation:



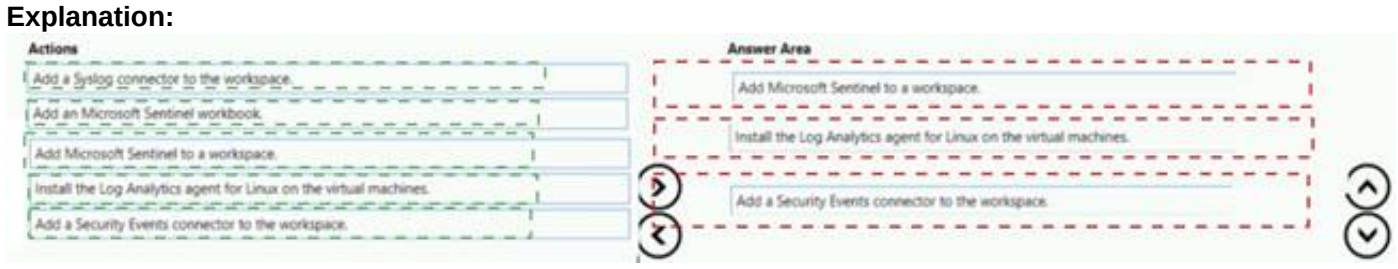
NEW QUESTION 38
DRAG DROP - (Topic 4)
You have an Azure subscription that contains 100 Linux virtual machines.
You need to configure Microsoft Sentinel to collect event logs from the virtual machines. Which three actions should you perform in sequence? To answer, move the appropriate
actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 40
DRAG DROP - (Topic 4)
You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

You need to delegate the following tasks:
• Enable Microsoft Defender for Servers on virtual machines.
• Review security recommendations and enable server vulnerability scans. The solution must use the principle of least privilege.
Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user 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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 43
- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
• App name: App1
• IP address: 192.168.1.2
• Computer name: Device1
• Used client app: Microsoft Edge
• Email address: user1@company.com
• Sign-in URL: https://www.company.com
Which entities can be investigated by using UEBA?

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

Answer: D

NEW QUESTION 47
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

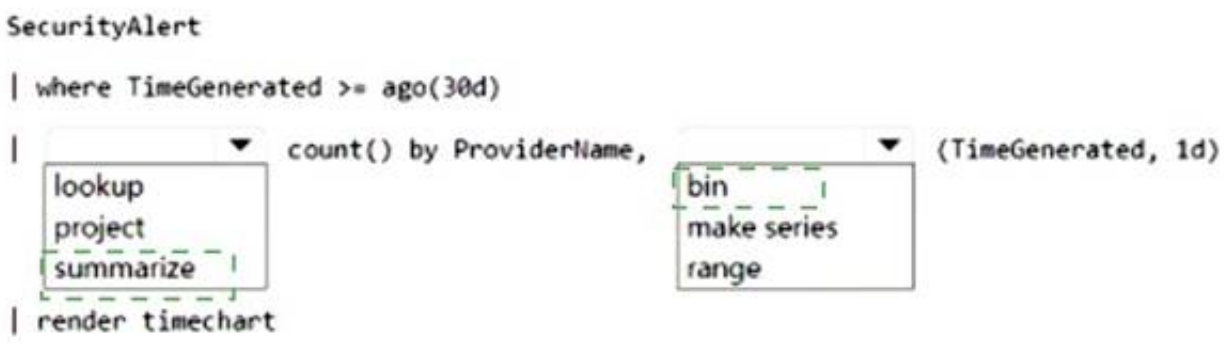
```
SecurityAlert
| where TimeGenerated >= ago(30d)
| [lookup / project / summarize] count() by ProviderName, [bin / make series / range] (TimeGenerated, 1d)
| render timechart
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 52
- (Topic 4)
You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts. What should you do?

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

Answer: B

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

NEW QUESTION 54
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

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

Answer: BC

NEW QUESTION 59
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.
You need to simulate an attack on the virtual machine that will generate an alert. What should you do first?

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

Answer: B

NEW QUESTION 61
HOTSPOT - (Topic 4)
You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.
How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

A. Mastered
B. Not Mastered

Answer: A

Explanation:

"resources": [
   {
     "type": "   /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'), '   /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
        ],

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

NEW QUESTION 62
- (Topic 4)
You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

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

Answer: D

Explanation:
You can use alerts suppression rules to suppress false positives or other unwanted

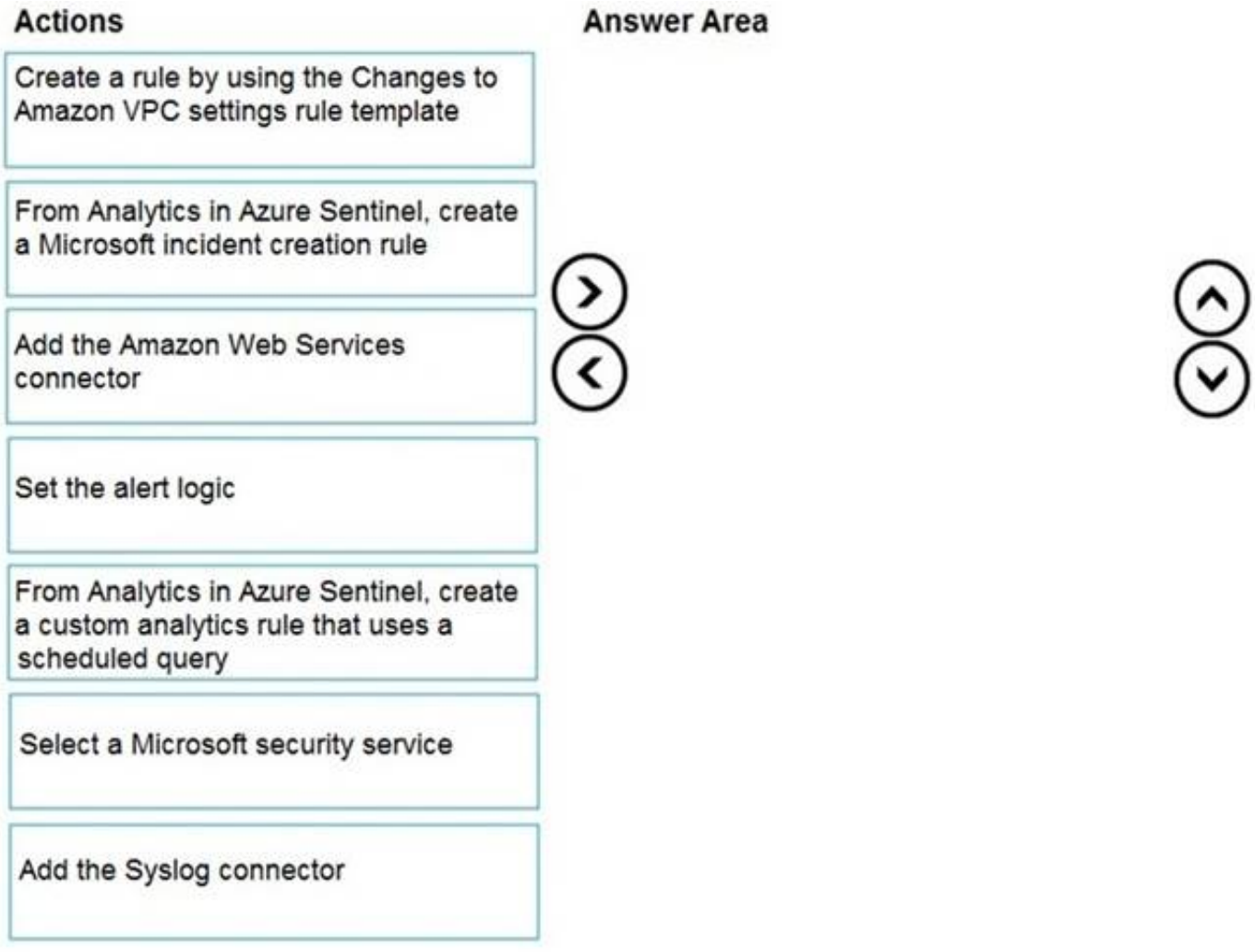
security alerts from Defender for Cloud.
Note: To create a rule directly in the Azure portal:
* 1. From Defender for Cloud's security alerts page:
Select the specific alert you don't want to see anymore, and from the details pane, select Take action.
Or, select the suppression rules link at the top of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

NEW QUESTION 66
- (Topic 4)
You have a custom Microsoft Sentinel workbook named Workbooks.
You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.
What should you do?

A. In the query editor interface, configure Settings.
B. In the query editor interface, select Advanced Editor
C. In the grid query, include the project operator.
D. In the grid query, include the take operator.

Answer: B

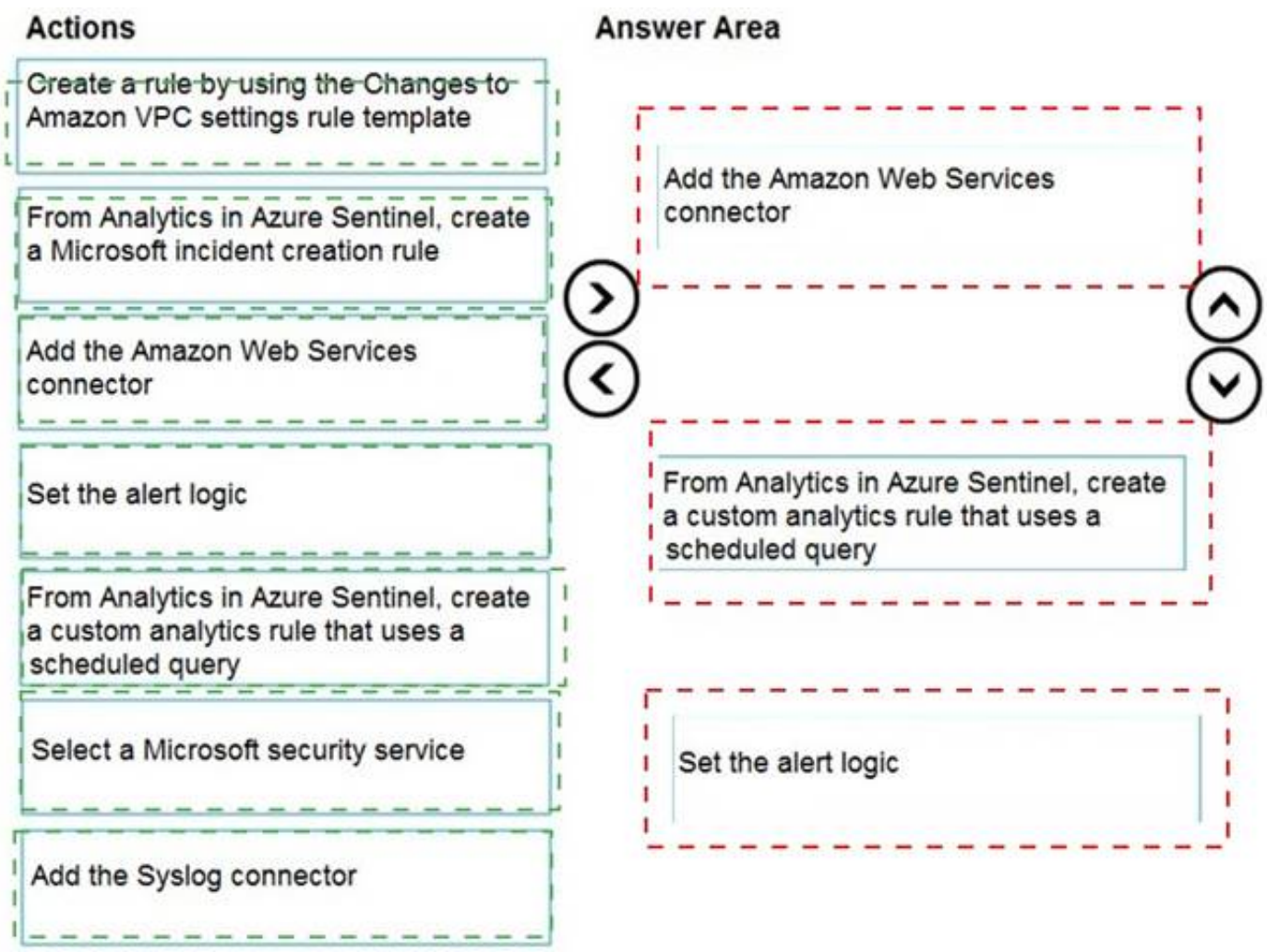
NEW QUESTION 70
DRAG DROP - (Topic 4)
You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
a Microsoft 365 E5



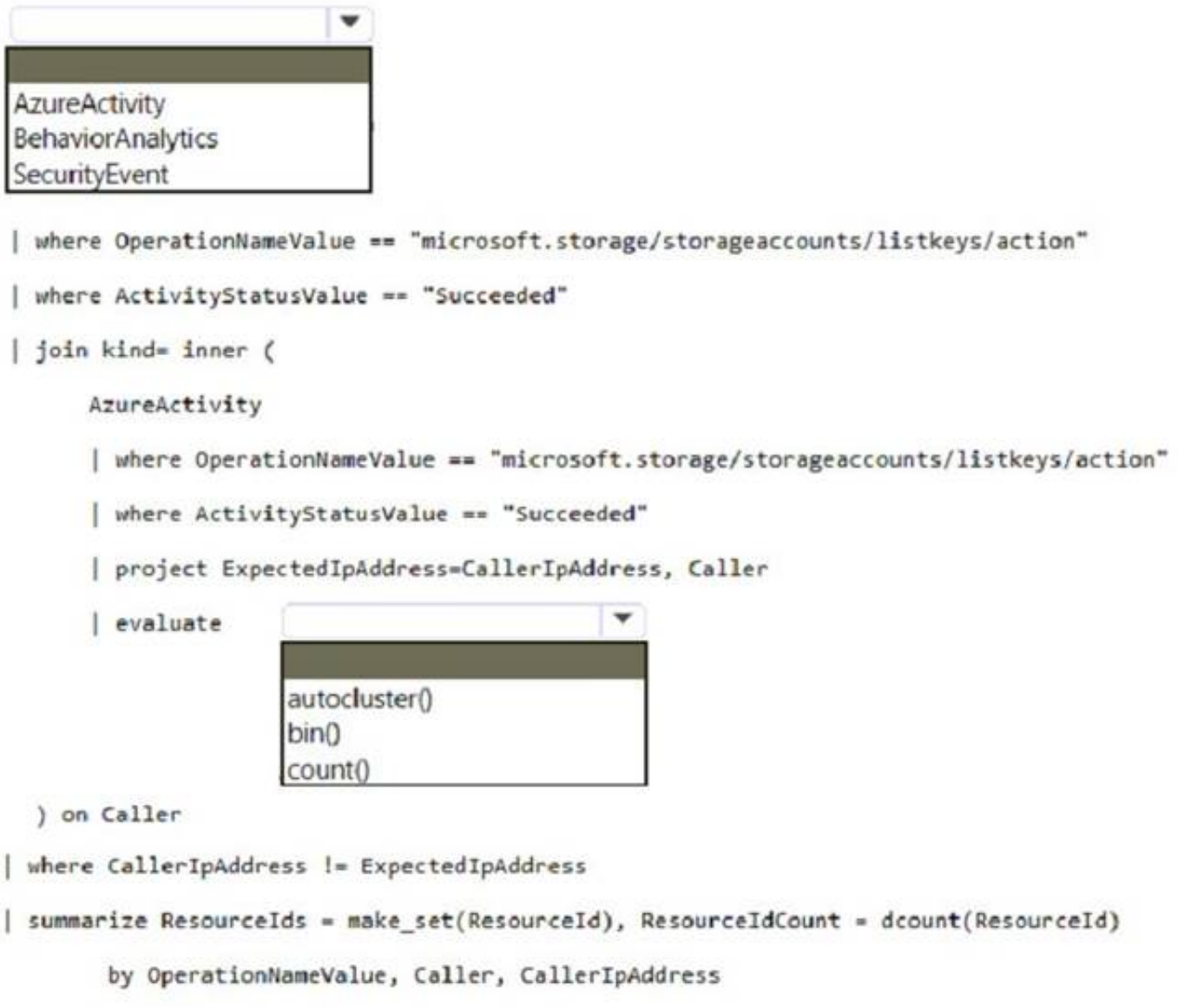
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 73
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:
Box 2: autocluster()
Example: description: |
'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this
type, it would be interesting to see if the account performing this activity or the source IP address from
which it is being done is anomalous.
The query below generates known clusters of ip address per caller, notice that users which only had single
operations do not appear in this list as we cannot learn from it their normal activity (only based on a single
event). The activities for listing storage account keys is correlated with this learned
clusters of expected activities and activity which is not expected is returned.'

```
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner ( AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
```

NEW QUESTION 74
- (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 77
- (Topic 4)
You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

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

Answer: B

NEW QUESTION 80
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 85
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 88
HOTSPOT - (Topic 4)
You have an Azure subscription that contains a quest user named Userl and a Microsoft Sentinel workspace named workspacel.
You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The
solution must use the principle of least privilege.
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 91
- (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 94
- (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 97
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender fof Ctoud.
You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.
You need to onboard EC2-1 to Defender for Cloud. What should you install on EC2-1?

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

Answer: A

NEW QUESTION 101
- (Topic 4)
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure
Sentinel deployment to generate alerts based on queries to LogsWest. What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.
B. Modify the workspace settings of the existing Azure Sentinel deployment
C. Add Microsoft Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

Answer: C

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

NEW QUESTION 106
HOTSPOT - (Topic 4)

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

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

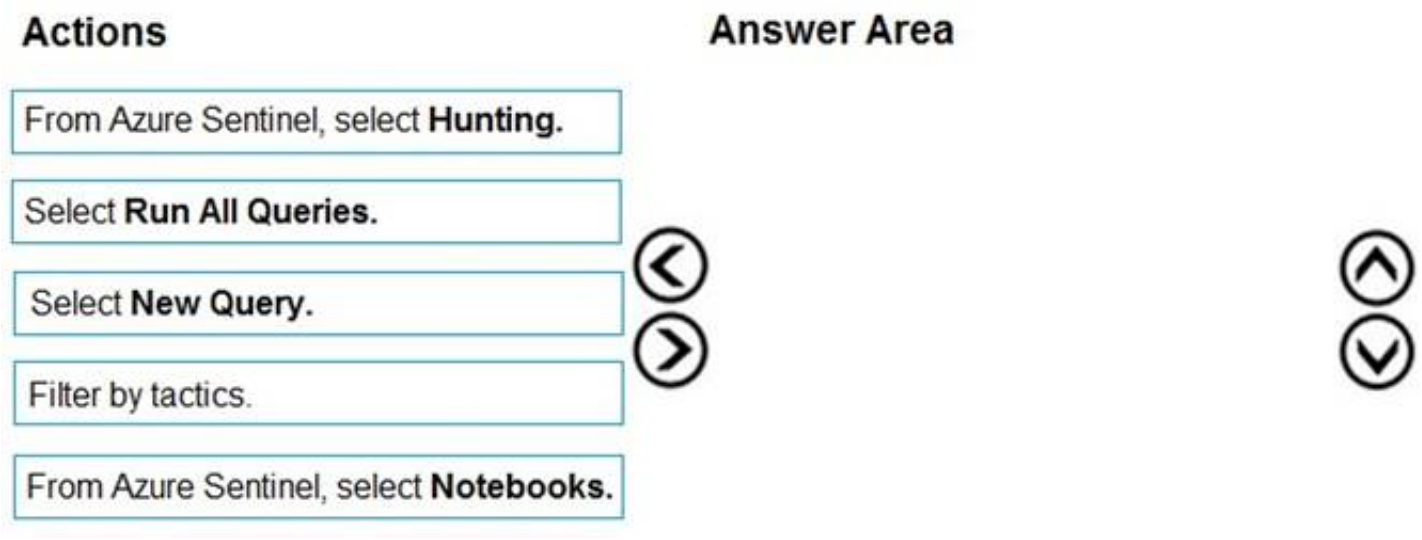
NEW QUESTION 108
- (Topic 4)
You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.
What should you do?

A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

Answer: A

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

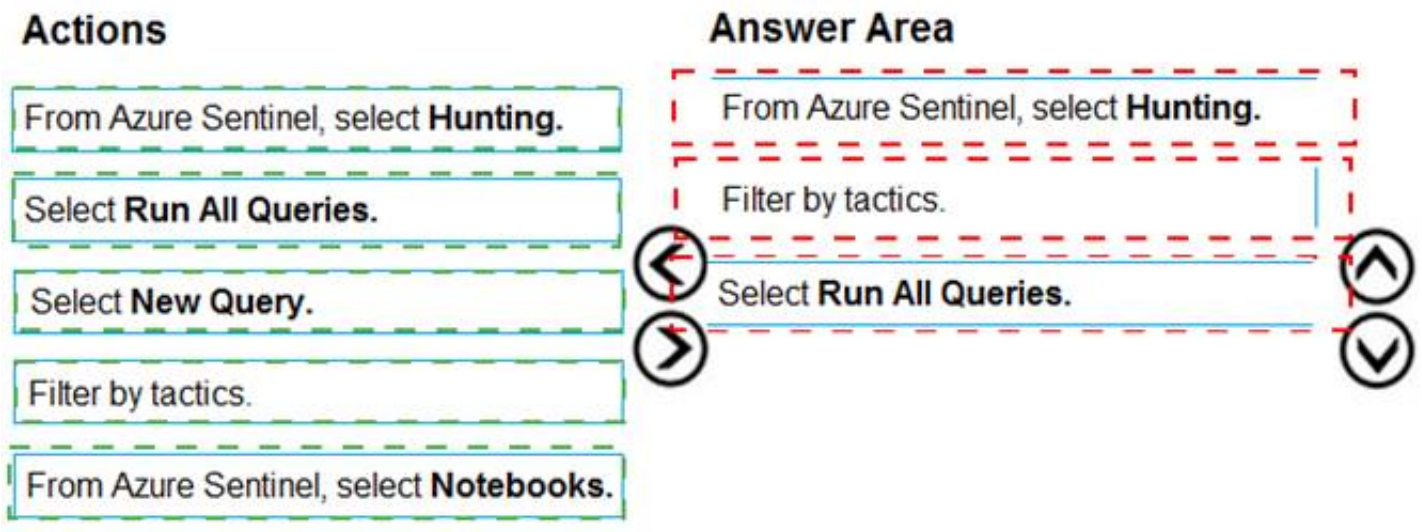
NEW QUESTION 109
DRAG DROP - (Topic 4)
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



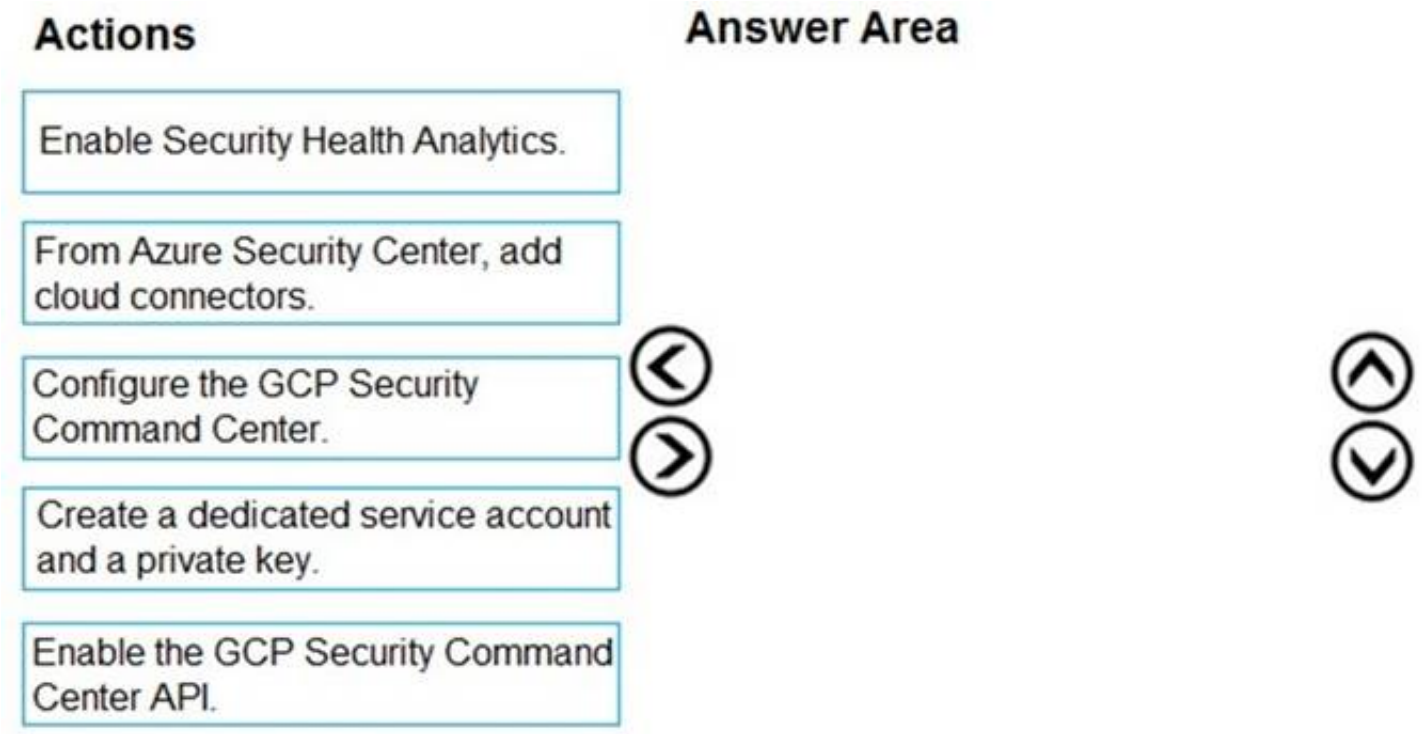
A. Mastered
B. Not Mastered

Answer: A

Explanation:



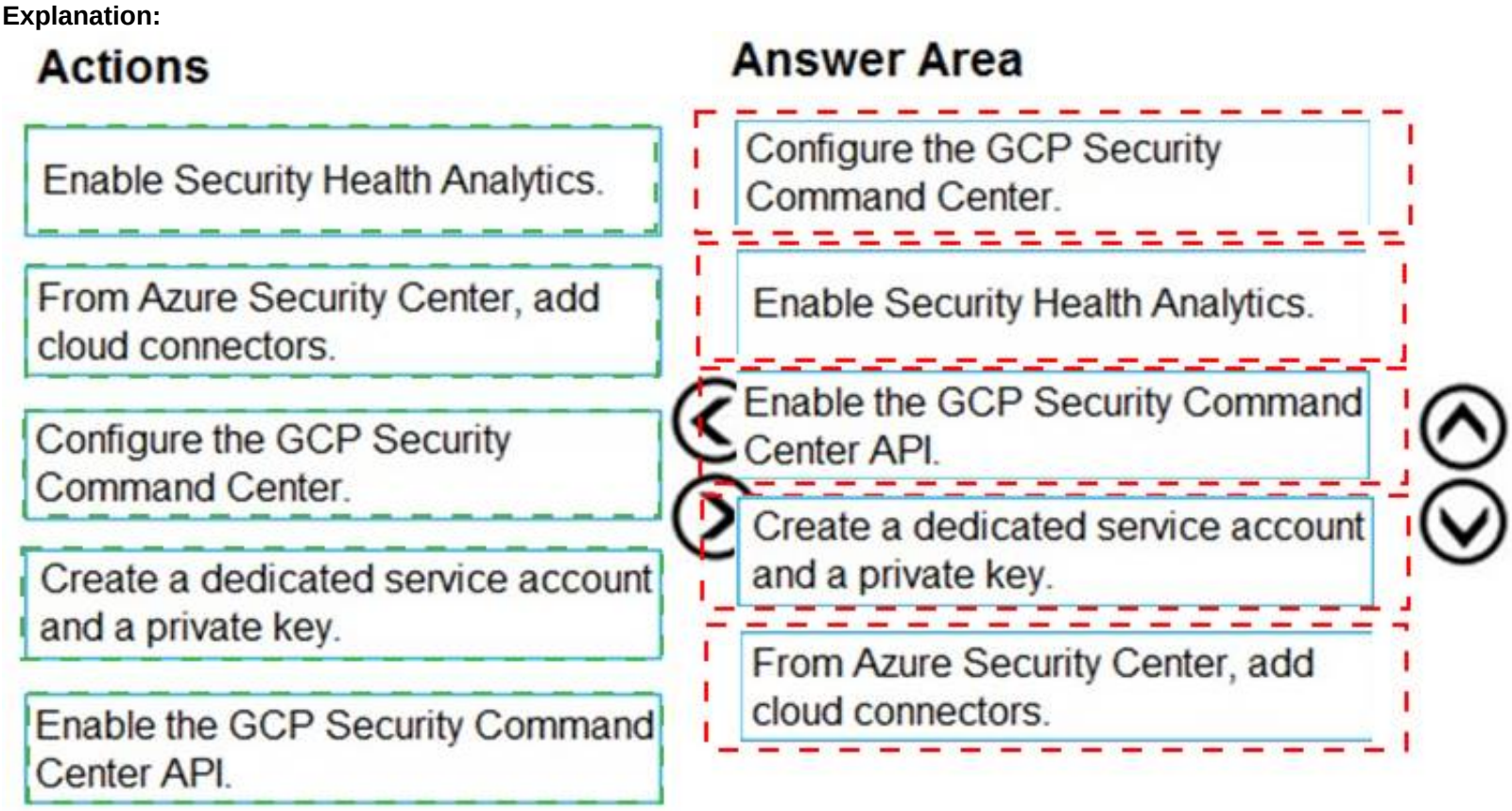
NEW QUESTION 112
DRAG DROP - (Topic 4)
You have resources in Azure and Google cloud.
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 116
- (Topic 4)
You have a Microsoft Sentinel workspace.
You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.
You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.
• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort What should do?

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

Answer: A

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

NEW QUESTION 121
- (Topic 4)
You have 50 Microsoft Sentinel workspaces.
You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.
Which page should you use in the Azure portal?

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

Answer: D

NEW QUESTION 122
- (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 127
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.
You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: DE

NEW QUESTION 132
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.
How should you complete The KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 134
- (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 135
- (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?

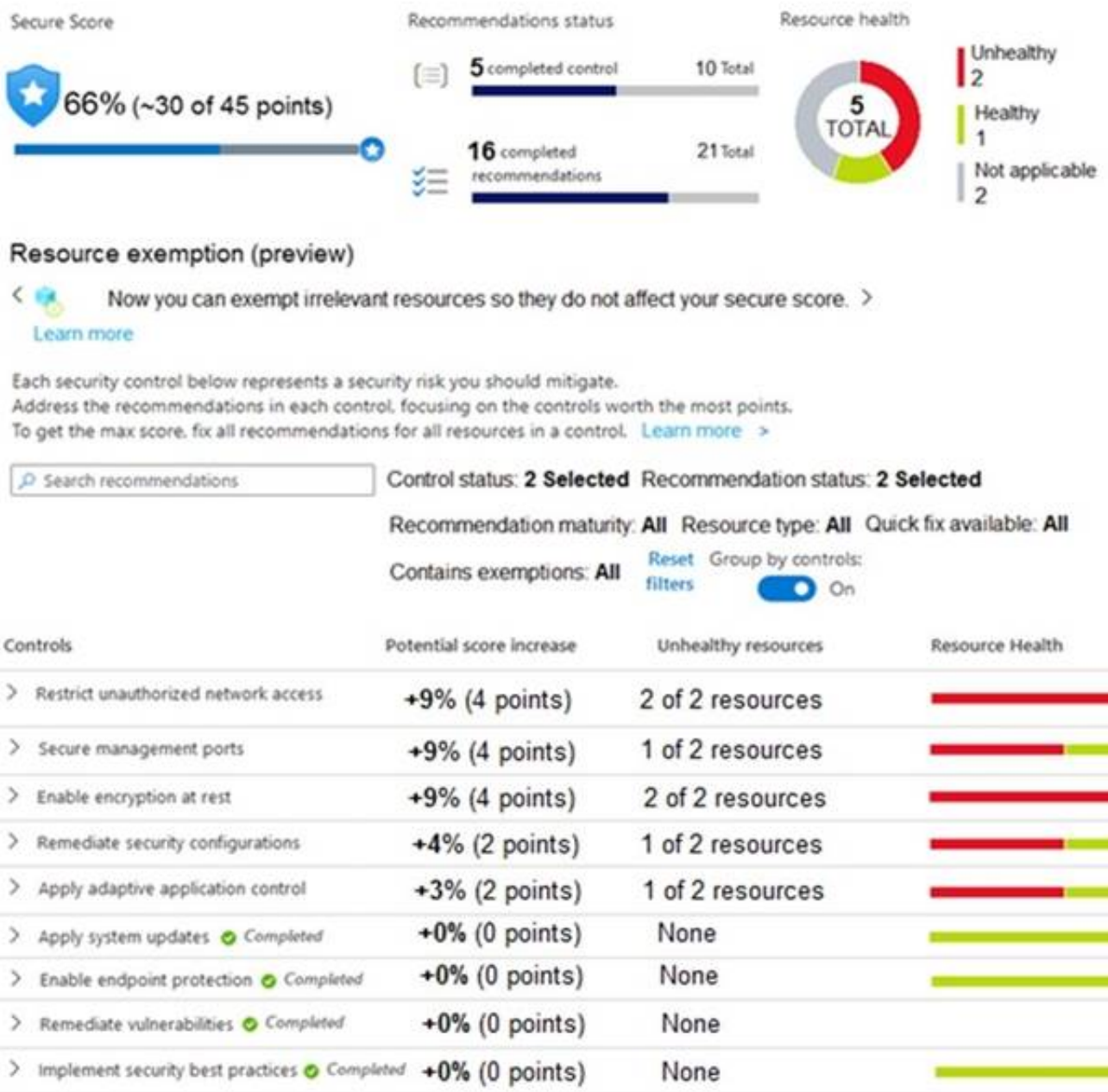
A. the Incidents blade of the Microsoft 365 Defender portal

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

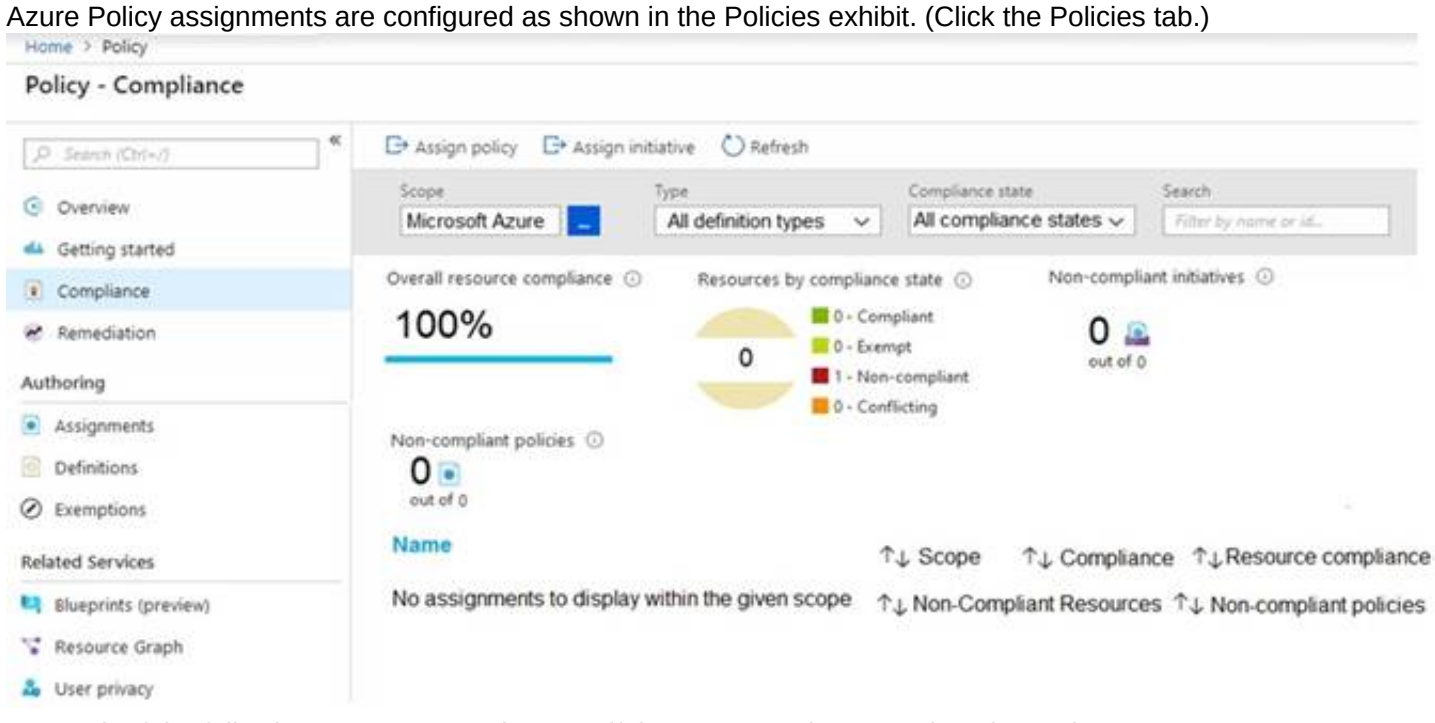
Answer: C

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 140
HOTSPOT - (Topic 4)
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 141
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a scheduled query rule for a data connector. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 143
- (Topic 4)
You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

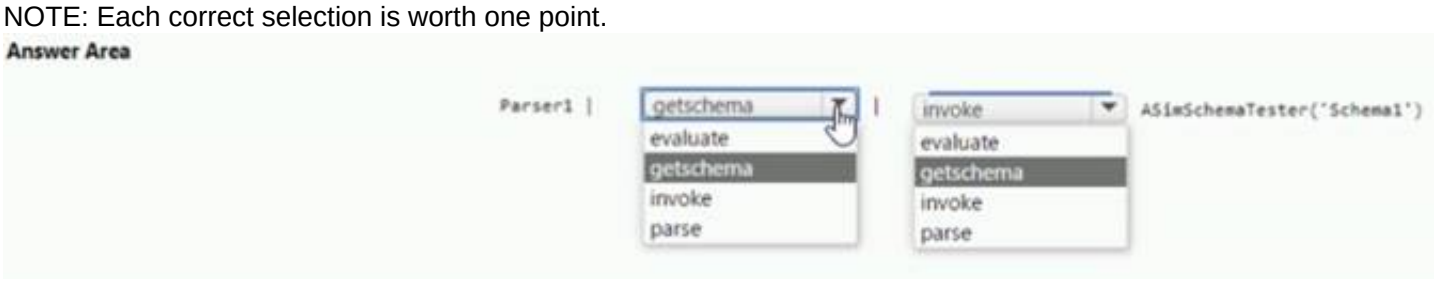
A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
B. Select Investigate files, and then filter App to Office 365.
C. Select Investigate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

Answer: DE

Explanation:

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

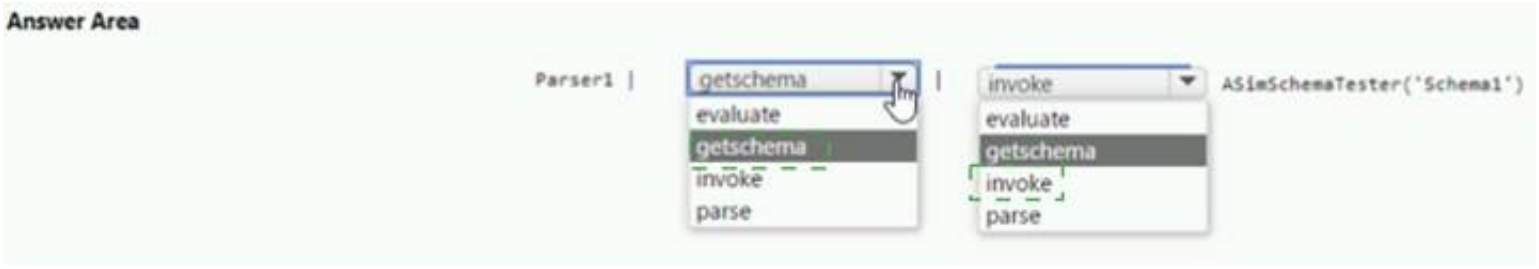
NEW QUESTION 146
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.
You need to validate Schema1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 148
- (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?

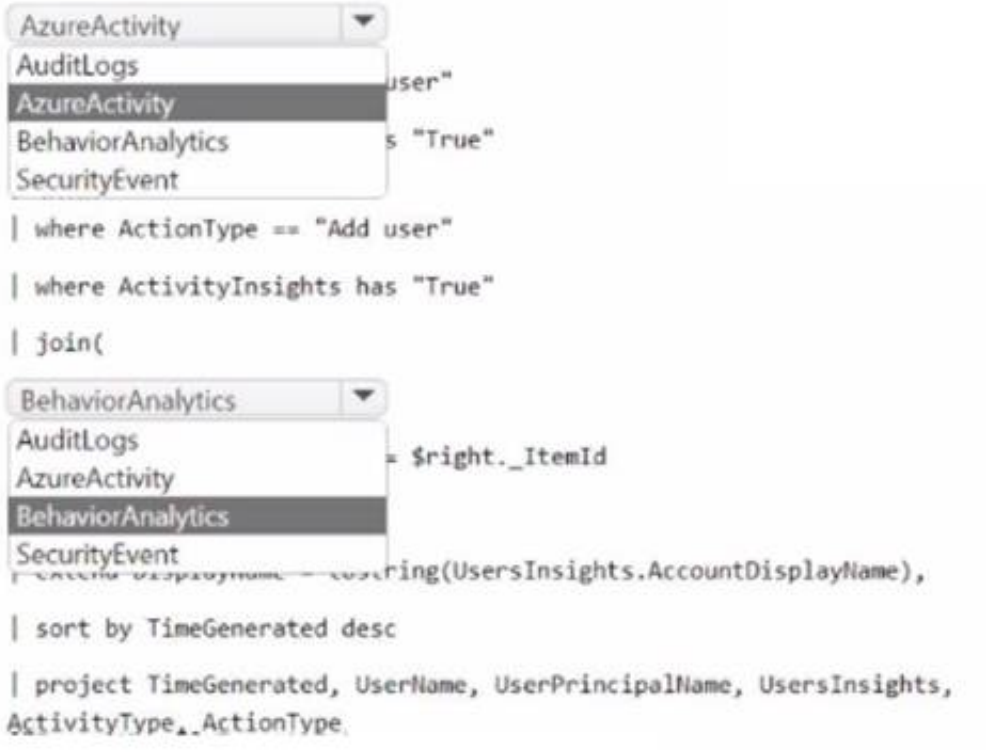
A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

Answer: C

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

NEW QUESTION 150
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

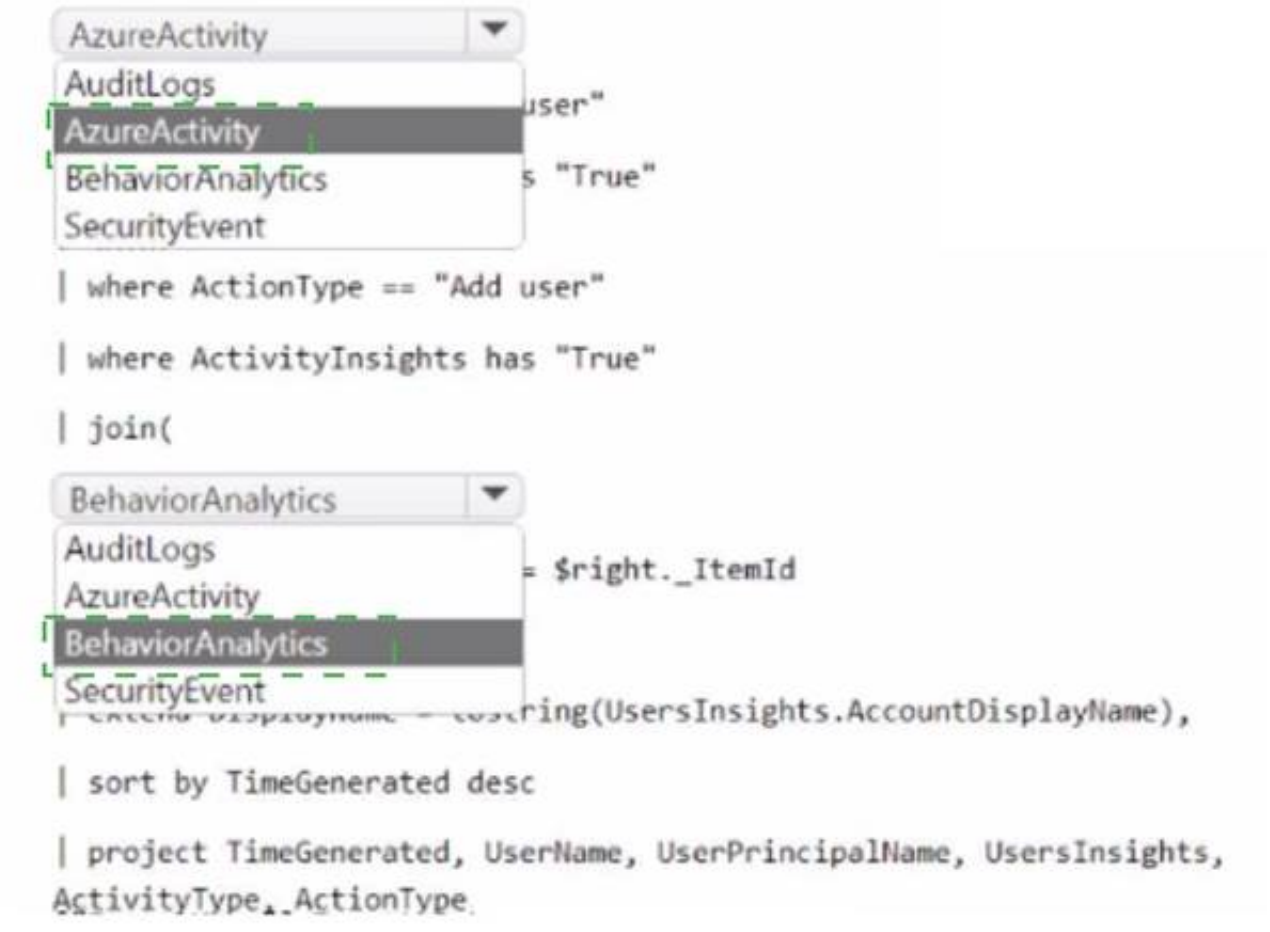


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 154
- (Topic 4)
You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender. Which two Bash commands should you run on the virtual machine?
Each correct answer
presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

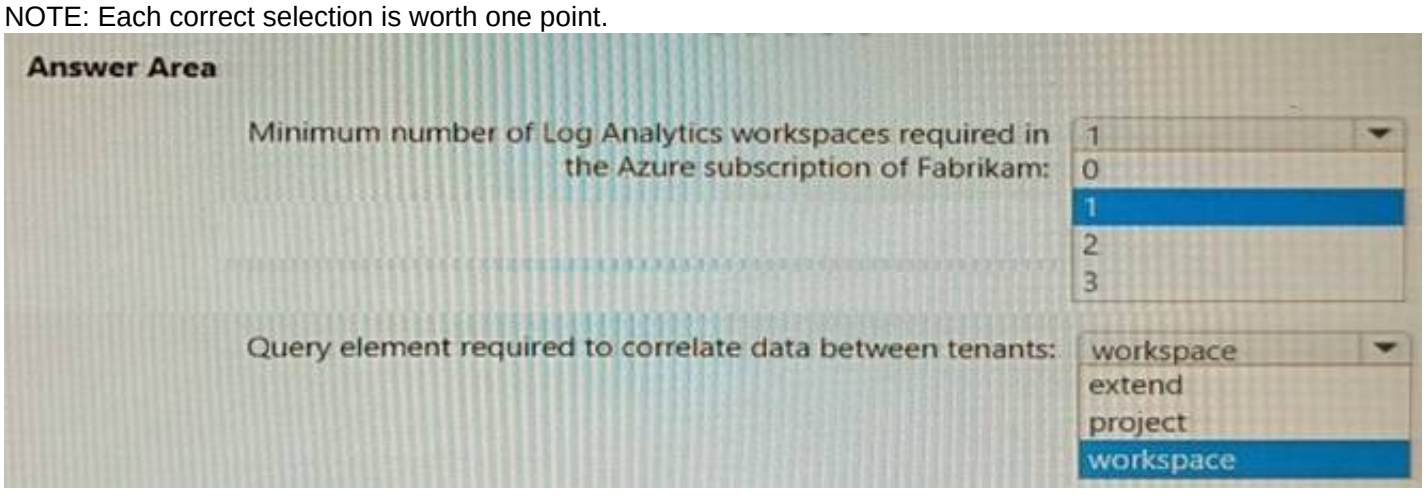
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your- azure-vms-linux-

NEW QUESTION 159
- (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

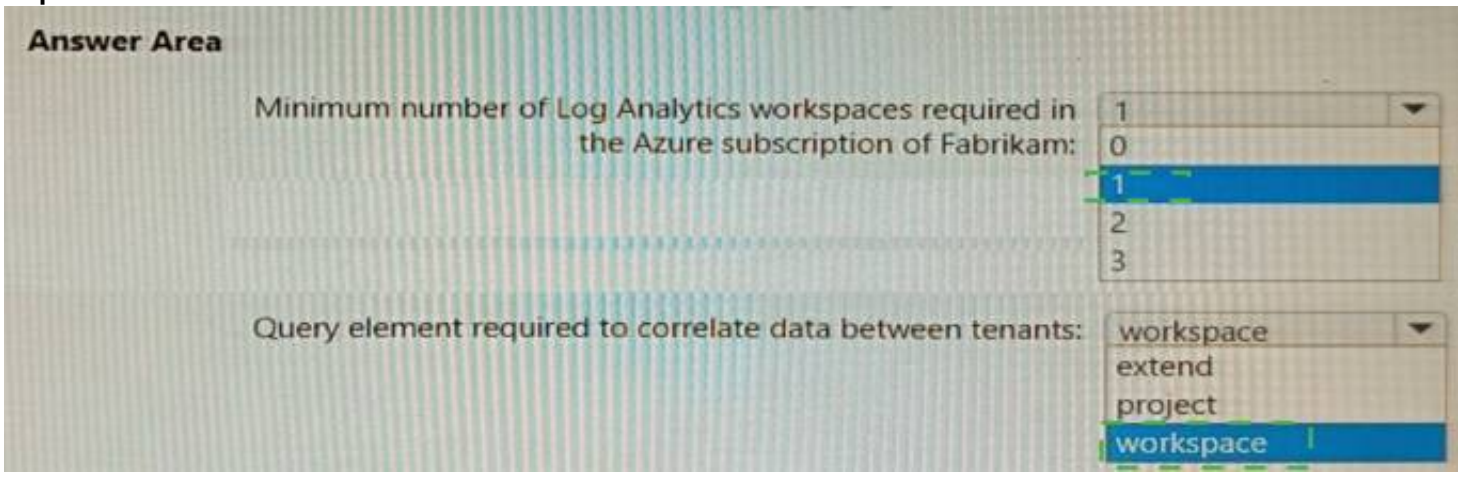
NEW QUESTION 163
HOTSPOT - (Topic 4)
You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 164
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

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

NEW QUESTION 167
- (Topic 4)
You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. You need to use Defender for Cloud to protect the Linux servers.

What should you install on the servers first?

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

Answer: B

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

NEW QUESTION 168
- (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

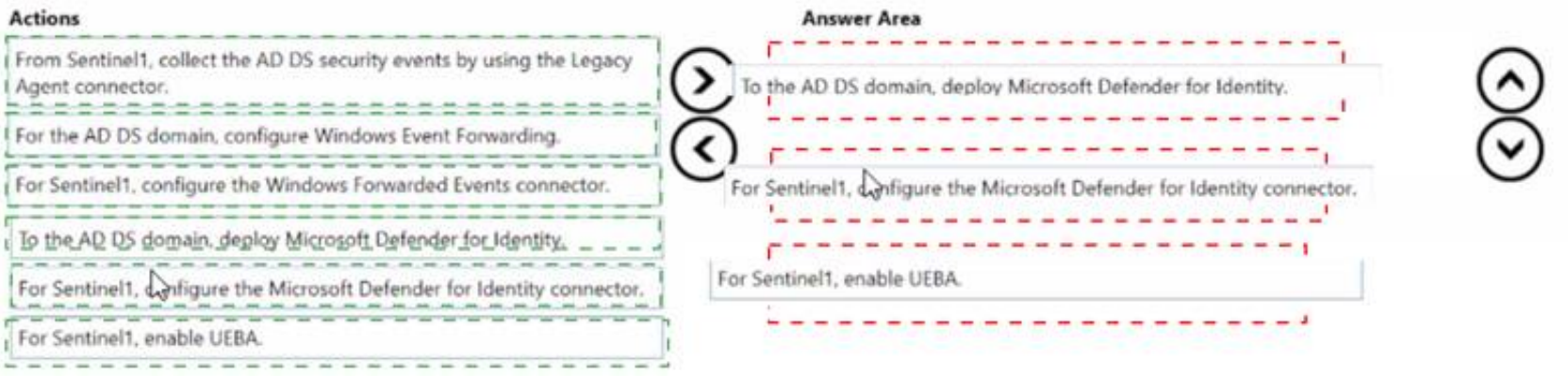
Answer: C

NEW QUESTION 169
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.

A. Mastered
B. Not Mastered

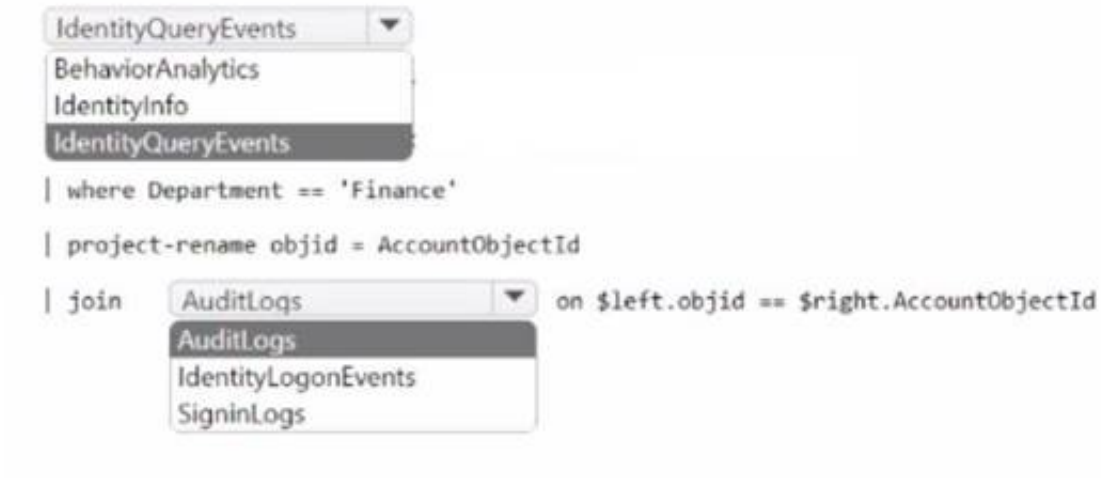
Answer: A

Explanation:



NEW QUESTION 172
HOTSPOT - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to identify all the interactive authentication attempts by the users in the finance department of your company.
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

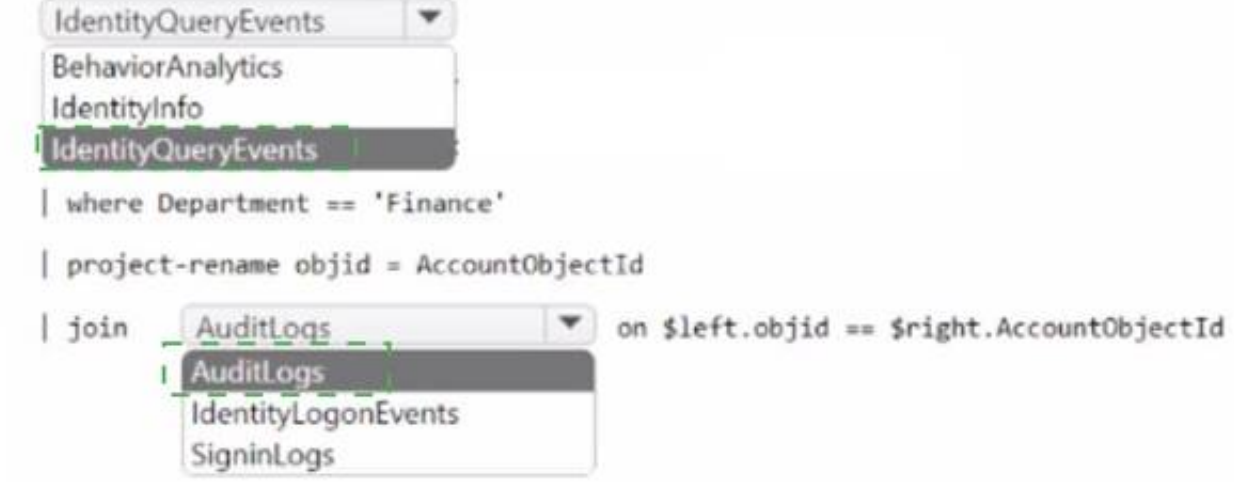


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 177
DRAG DROP - (Topic 4)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point

Values

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

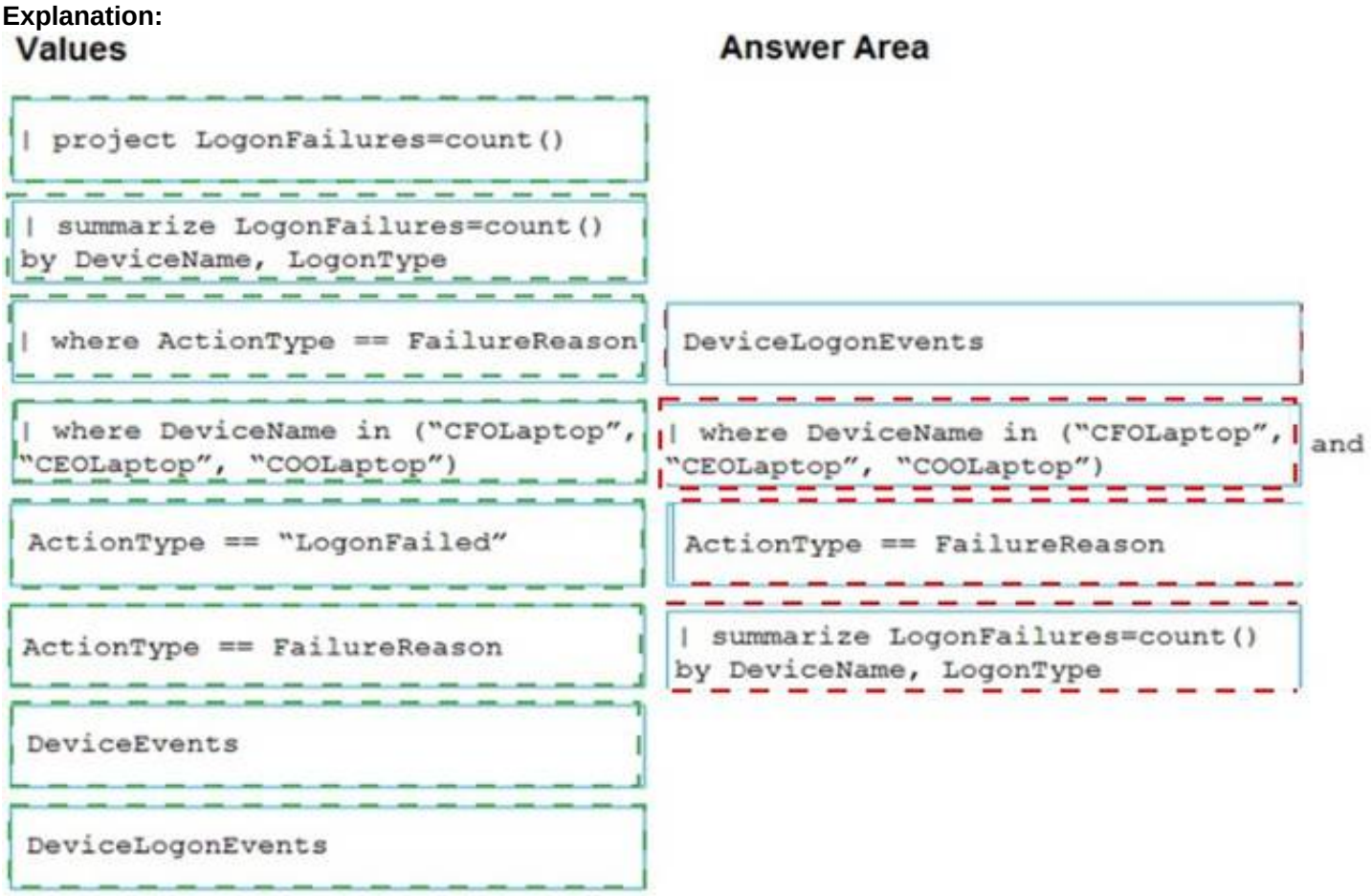
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 180
- (Topic 4)
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.
B. Change the state of the suppression rule to Disabled.
C. Modify the filter for the Security alerts page.
D. View the Windows event logs on the virtual machines.

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

NEW QUESTION 183
- (Topic 4)
Your company uses Microsoft Sentinel
A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

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

Answer: A

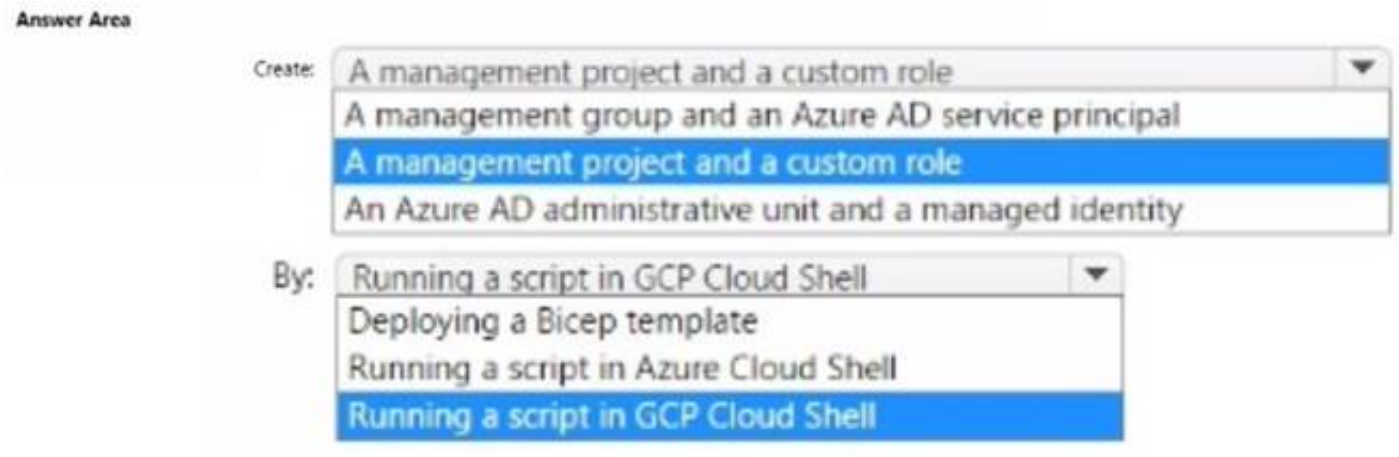
Explanation:
The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to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

NEW QUESTION 186
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Purview. Your company has a project named Project1.
You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.
What should you do?

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

Answer: D

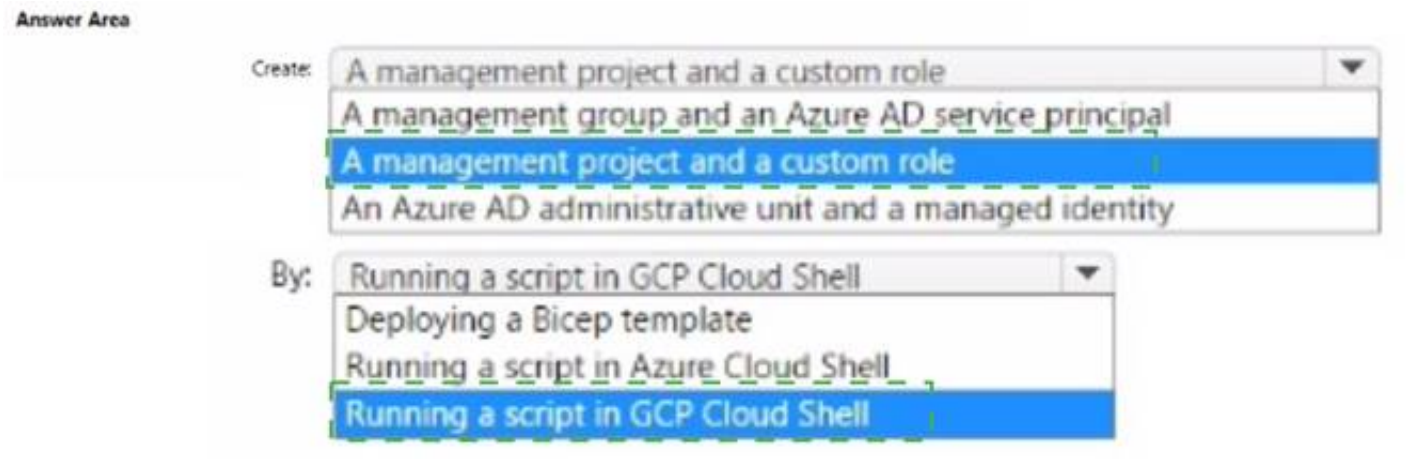
NEW QUESTION 189
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You create a Google Cloud Platform (GCP) organization named GCP1.
You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded 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.



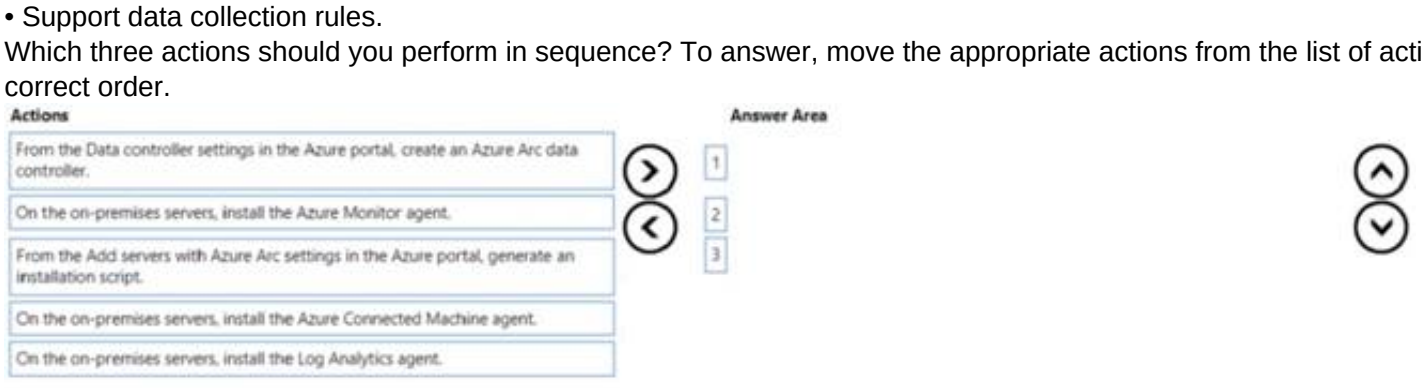
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 190
DRAG DROP - (Topic 4)
You have 50 on-premises servers.
You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:
• Provide threat and vulnerability management.
• Support data collection rules.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

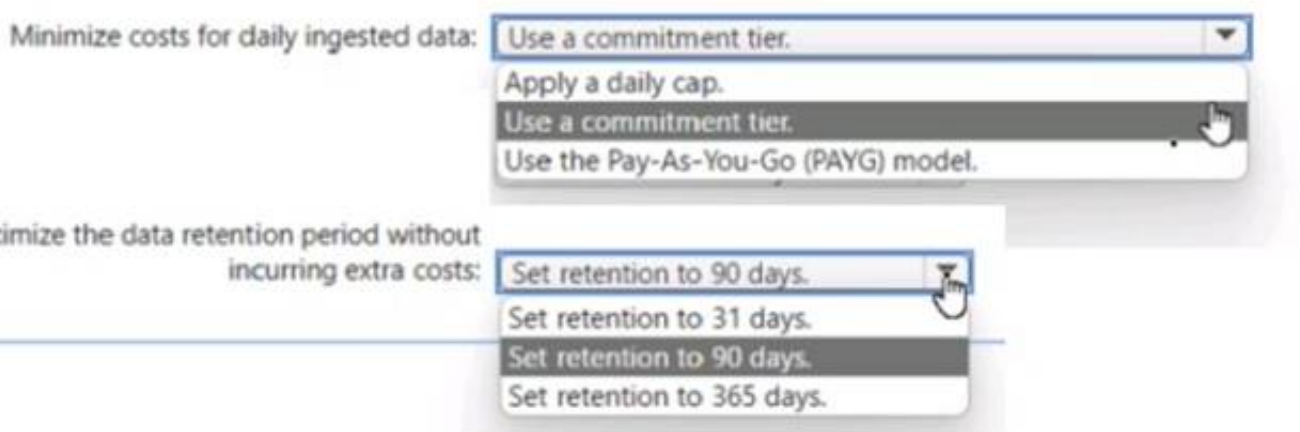
Explanation:
To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:
? On the on-premises servers, install the Azure Connected Machine agent.
? On the on-premises servers, install the Log Analytics agent.
? From the Data controller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

NEW QUESTION 192
- (Topic 4)
You create a custom analytics rule to detect threats in Azure Sentinel. You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

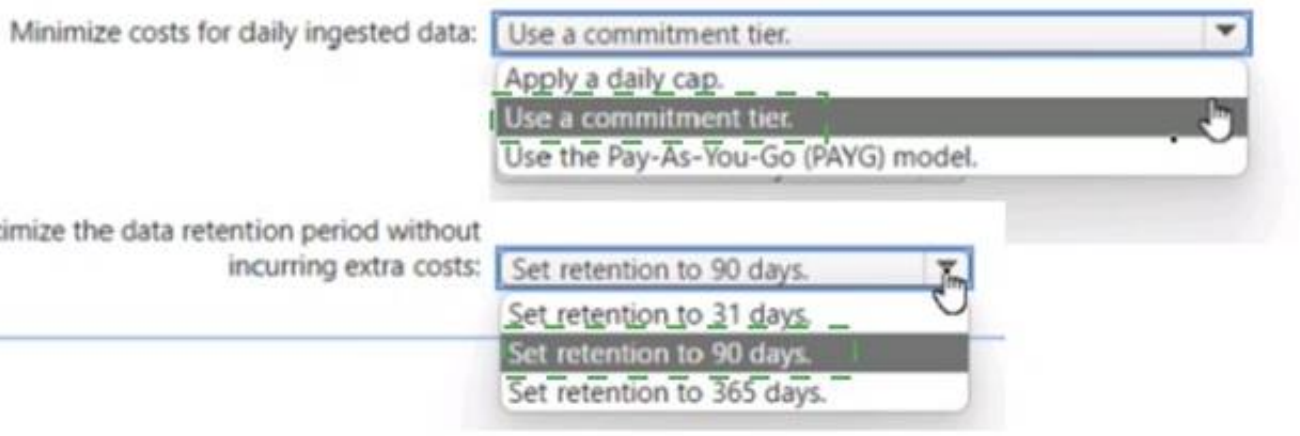
NEW QUESTION 194
HOTSPOT - (Topic 4)
You have an Azure subscription.
You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.
You need to configure storage for the workspace. The solution must meet the following requirements:
• Minimize 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.



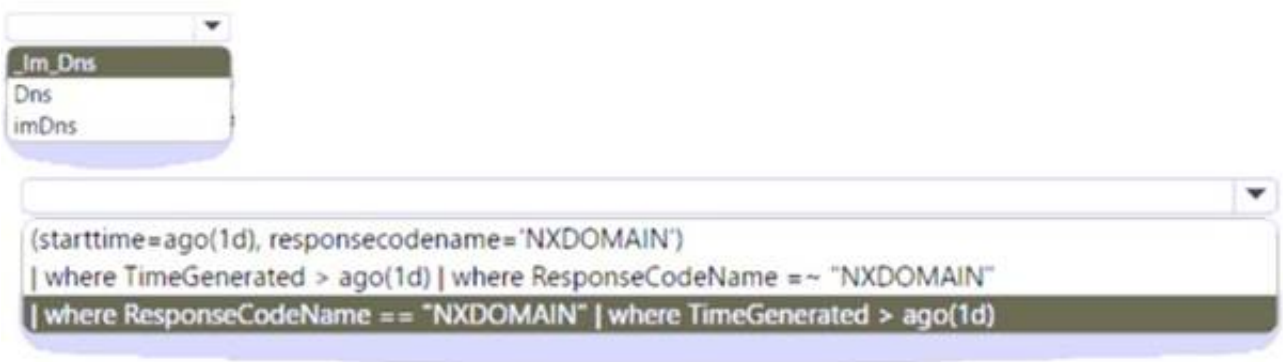
A. Mastered
B. Not Mastered

Answer: A

Explanation:



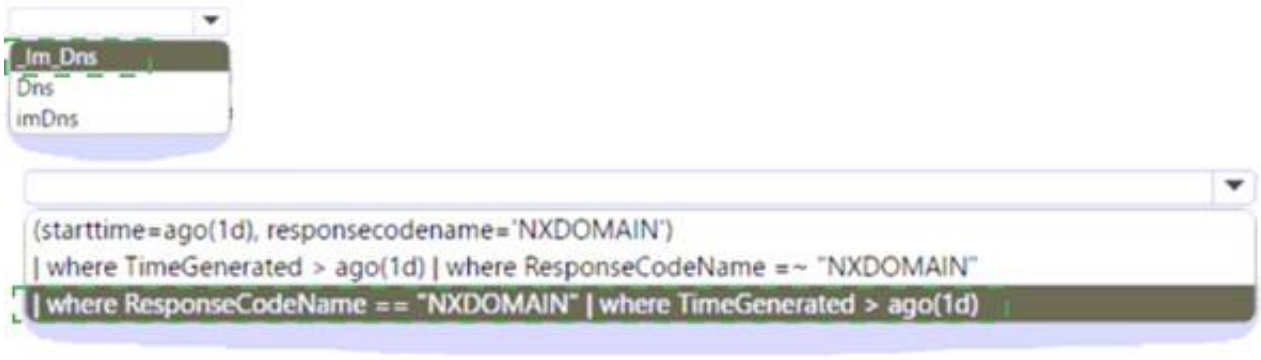
NEW QUESTION 196
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.
You need to query the ASIM DNS schema to list all the DNS events 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 197
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 202
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 206
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

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

Answer: B

NEW QUESTION 207
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to configure a report visual for a custom workbook. The solution must meet the following requirements:
• The count and usage trend of AppDisplayName must be included
• The TrendList column must be useable in a sparkline visual,
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 211
- (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 215
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 216
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.
You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

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

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

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

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

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

A. Mastered
B. Not Mastered

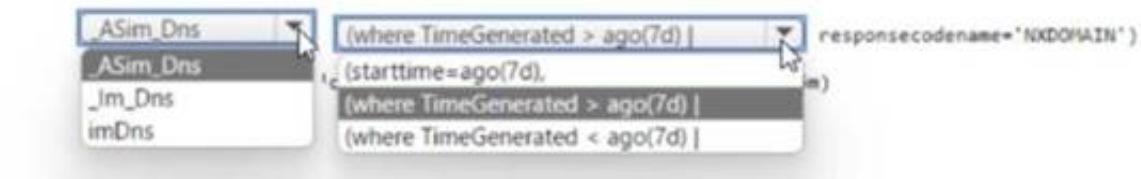
Answer: A

Explanation:

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

NEW QUESTION 217
HOTSPOT - (Topic 4)
You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query?
To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 221
- (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 222
- (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 227
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.
What should you use in the Microsoft 365 Defender portal?

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

Answer: A

NEW QUESTION 231
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-200 Exam with Our Prep Materials Via below:

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