Exam Questions SC-200

Microsoft Security Operations Analyst

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

NEW QUESTION 1
- (Exam 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

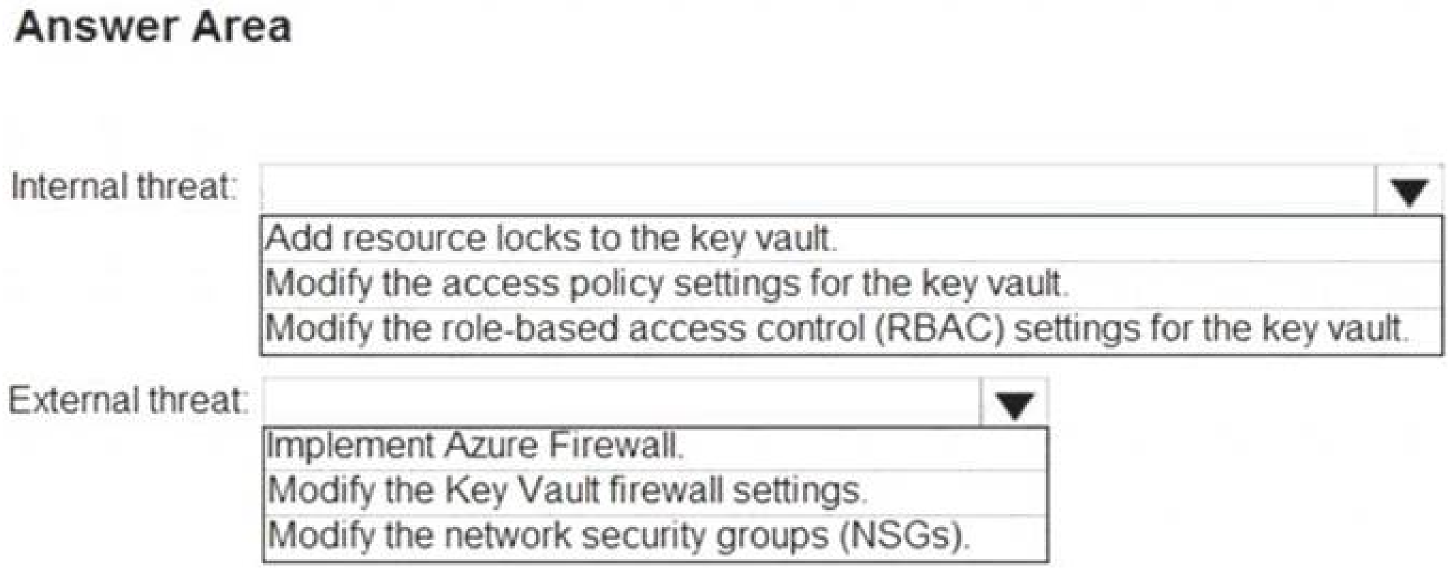
NEW QUESTION 2
- (Exam Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Office 365?

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



Answer Area

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

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 4
- (Exam Topic 1)
You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

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

Answer: B

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

NEW QUESTION 5
- (Exam 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

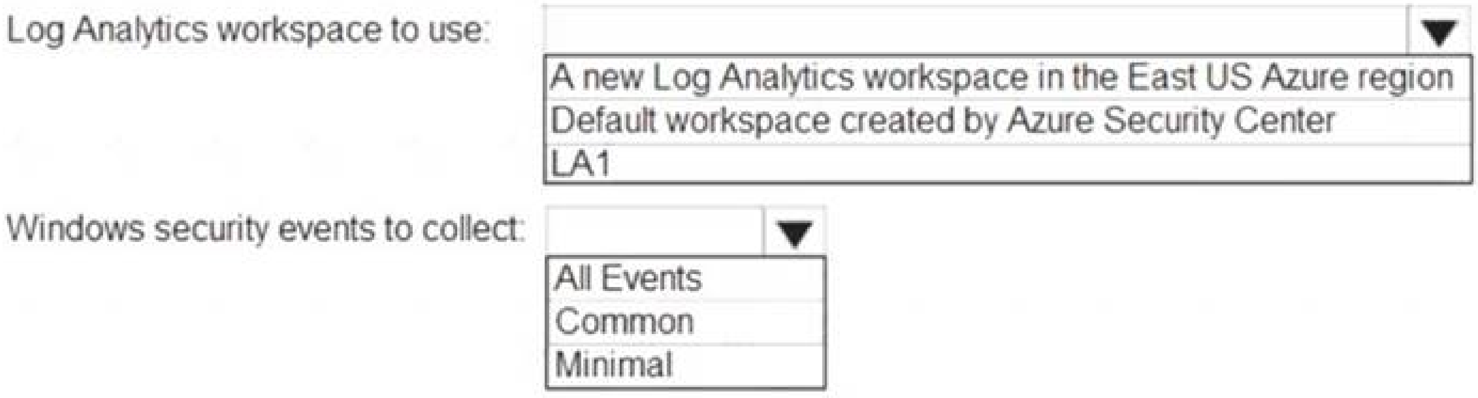
NEW QUESTION 6
- (Exam Topic 2)
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

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

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION 7
- (Exam 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:
Graphical user interface, application Description automatically generated

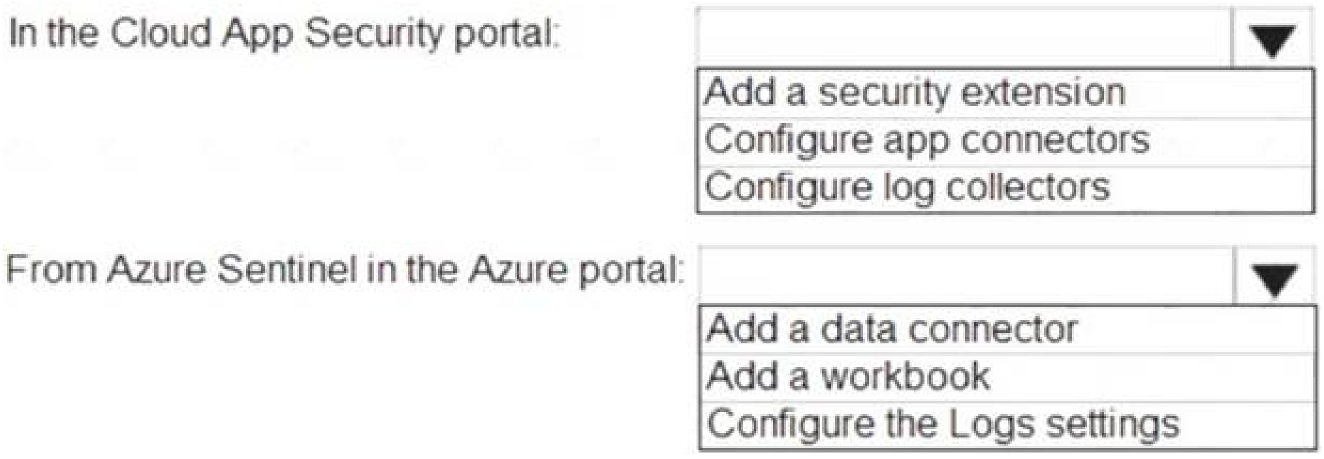
NEW QUESTION 8
- (Exam Topic 2)
You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

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 9
- (Exam 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:

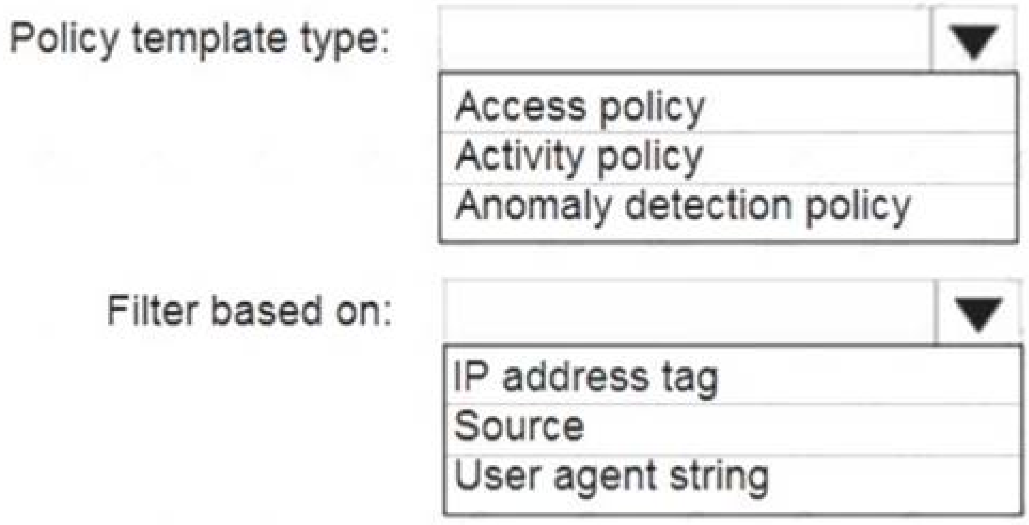
- Add a data connector
- Add a workbook
- Configure the Logs settings

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

NEW QUESTION 10
- (Exam Topic 3)
You purchase a Microsoft 365 subscription.
You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Policy template type:

- Access policy
- Activity policy
- Anomaly detection policy

Filter based on:

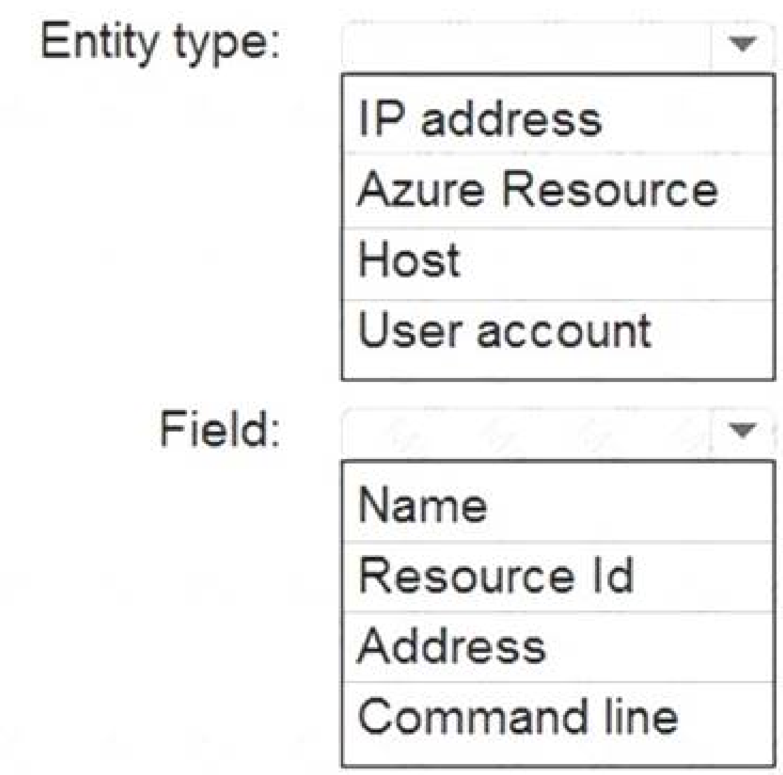
- IP address tag
- Source
- User agent string

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

NEW QUESTION 10
- (Exam Topic 3)
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:

Field:

A. Mastered
B. Not Mastered

Answer: A

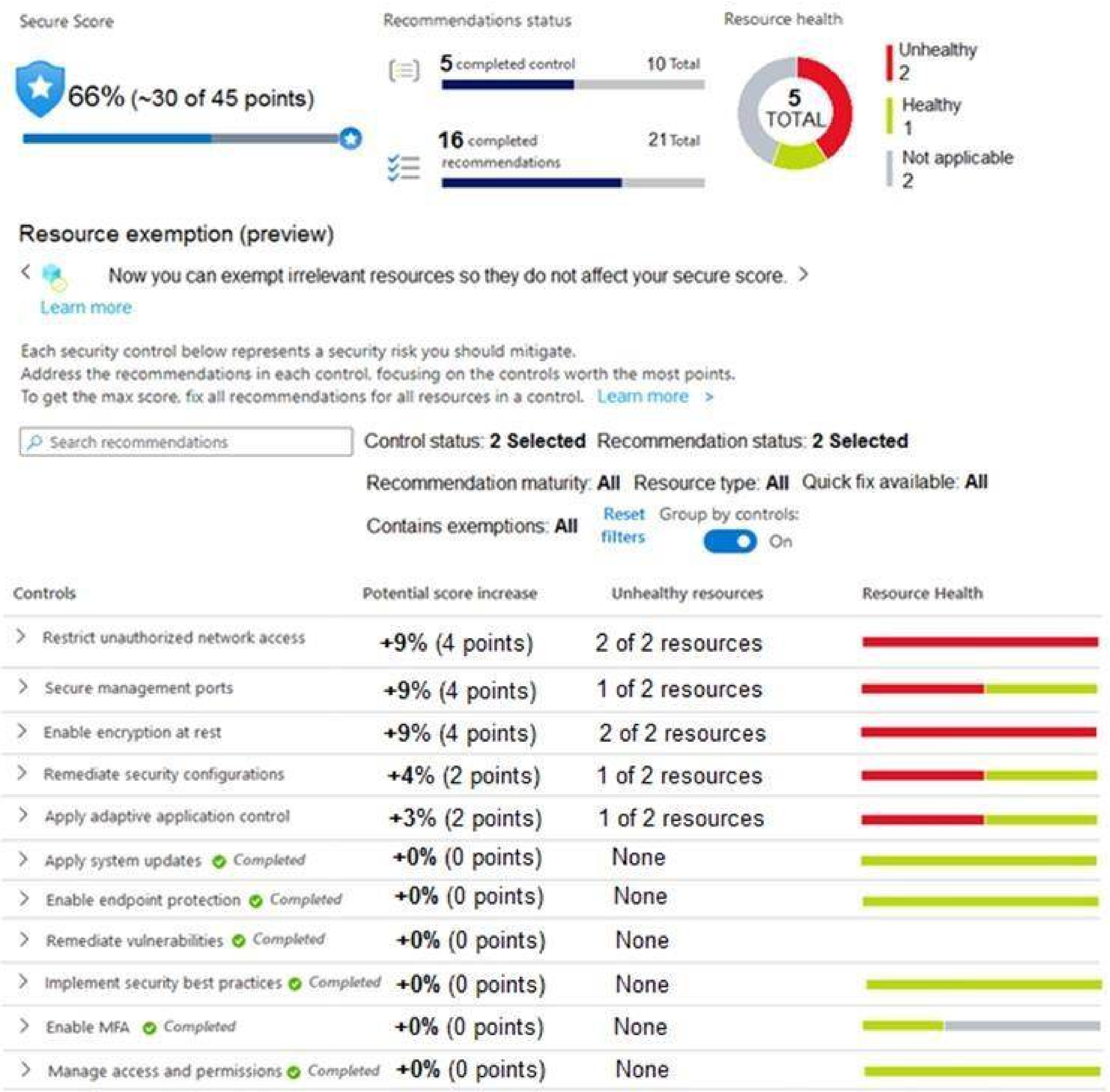
Explanation:
Graphical user interface, application Description automatically generated
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts

NEW QUESTION 11
- (Exam Topic 3)
You have a Microsoft Sentinel workspace named Workspace1.
You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.
What should you create in Workspace1?

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

Answer: A

NEW QUESTION 12
- (Exam Topic 3)
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Secure Score

66% (~30 of 45 points)

Recommendations status

5 completed control 10 Total

16 completed recommendations 21 Total

Resource health

5 TOTAL

Unhealthy 2

Healthy 1

Not applicable 2

Resource exemption (preview)

Now you can exempt irrelevant resources so they do not affect your secure score.

Learn more

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

Search recommendations

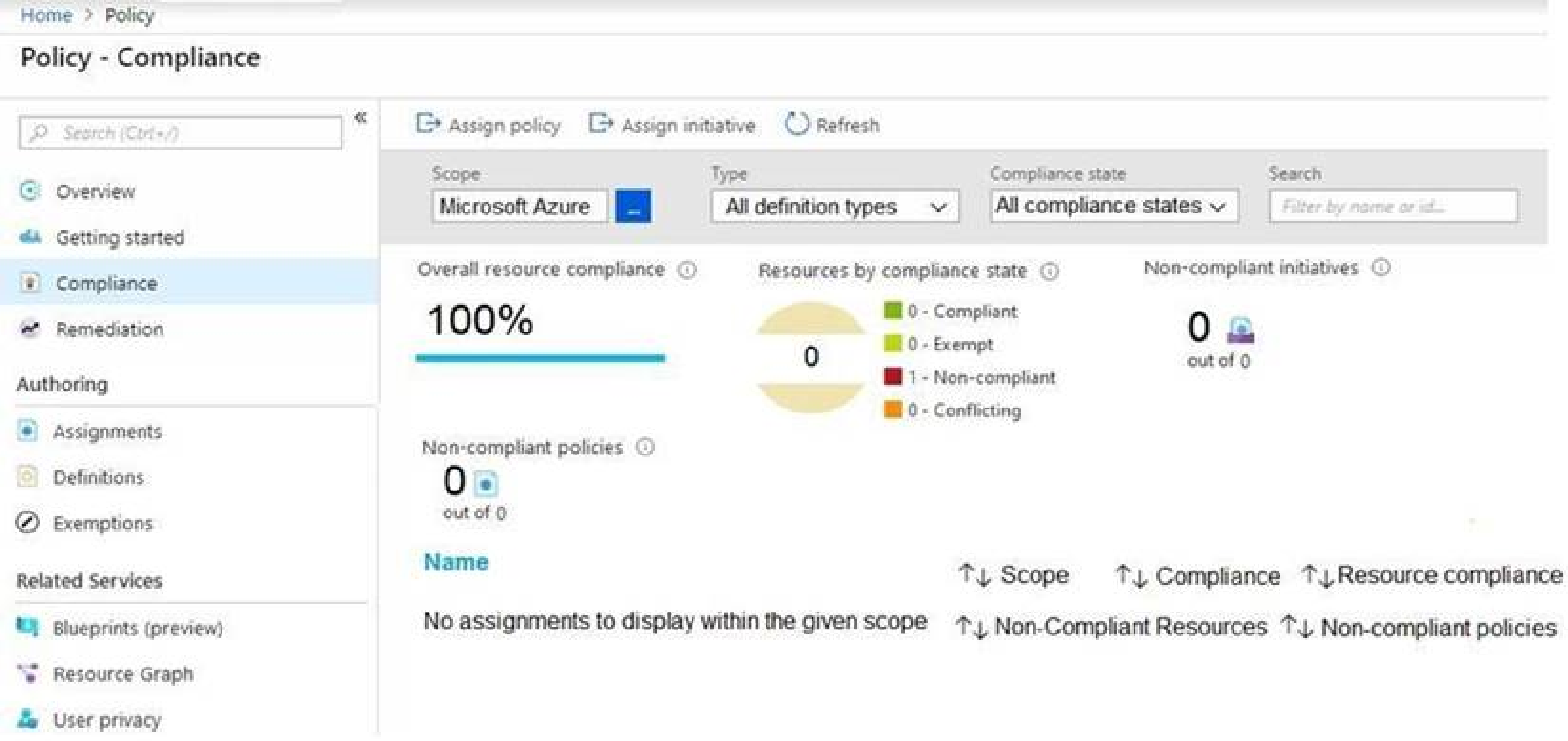
Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** Reset filters Group by controls: On

Controls	Potential score increase	Unhealthy resources	Resource Health
Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	
Secure management ports	+9% (4 points)	1 of 2 resources	
Enable encryption at rest	+9% (4 points)	2 of 2 resources	
Remediate security configurations	+4% (2 points)	1 of 2 resources	
Apply adaptive application control	+3% (2 points)	1 of 2 resources	
Apply system updates ✓ Completed	+0% (0 points)	None	
Enable endpoint protection ✓ Completed	+0% (0 points)	None	
Remediate vulnerabilities ✓ Completed	+0% (0 points)	None	
Implement security best practices ✓ Completed	+0% (0 points)	None	
Enable MFA ✓ Completed	+0% (0 points)	None	
Manage access and permissions ✓ Completed	+0% (0 points)	None	

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



Home > Policy

Policy - Compliance

Scope: Microsoft Azure

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or id...

Overall resource compliance: 100%

Resources by compliance state: 0

🟩 0 - Compliant
🟩 0 - Exempt
🟥 1 - Non-compliant
🟧 0 - Conflicting

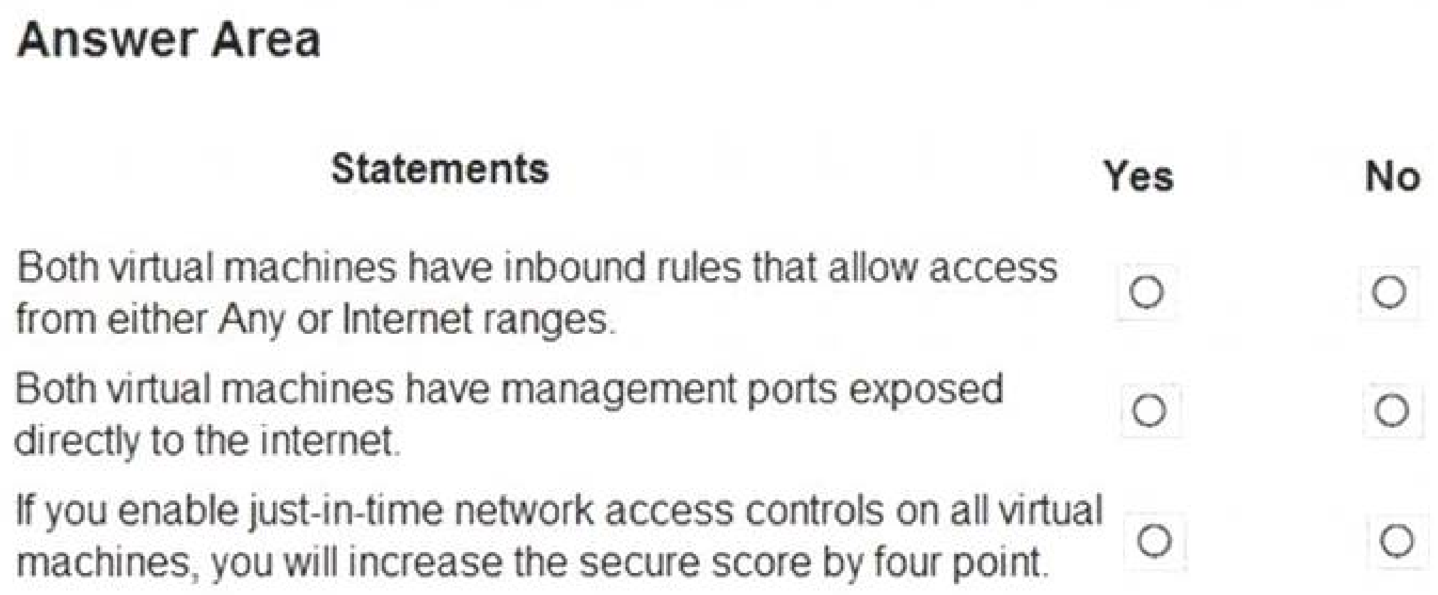
Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name ↑↓ Scope ↑↓ Compliance ↑↓ Resource compliance ↑↓ Non-Compliant Resources ↑↓ Non-compliant policies

No assignments to display within the given scope

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



Answer Area

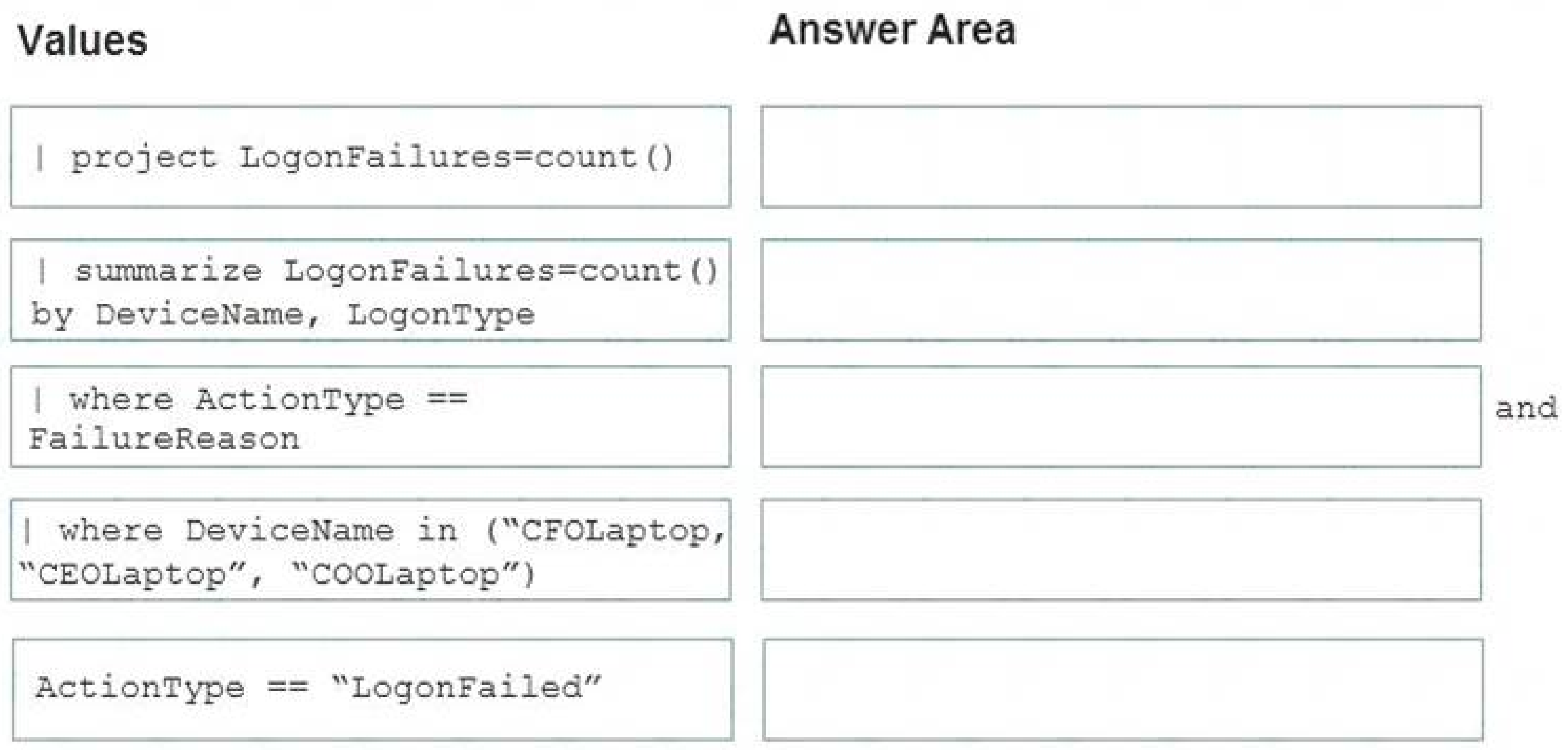
Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1

NEW QUESTION 15
- (Exam Topic 3)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect 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.

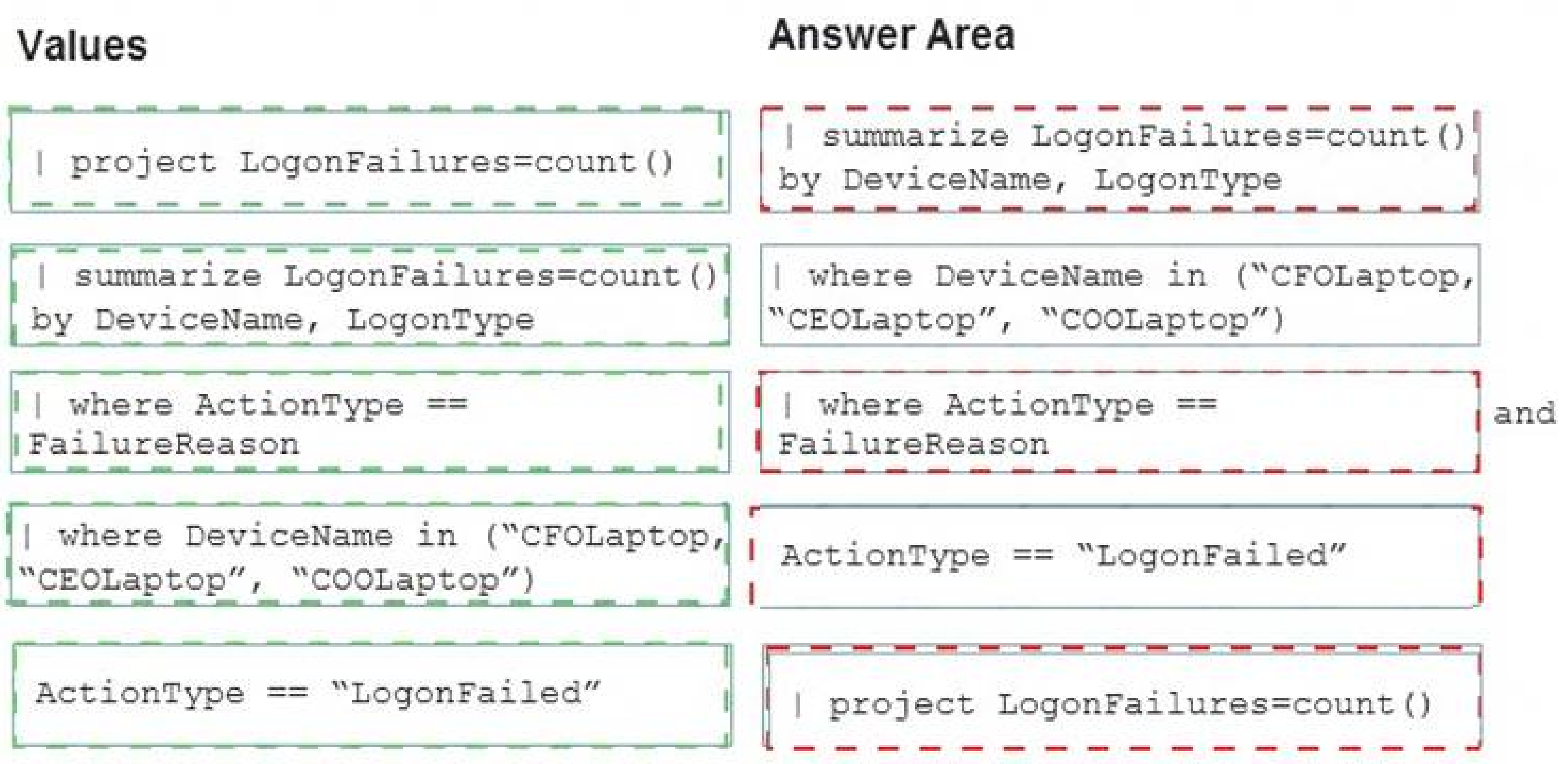


Values	Answer Area	
`| project LogonFailures=count()`		
`| summarize LogonFailures=count() by DeviceName, LogonType`		
`| where ActionType == FailureReason`		and
`| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")`		
`ActionType == "LogonFailed"`		

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Values

| project LogonFailures=count()

| summarize LogonFailures=count() by DeviceName, LogonType

| where ActionType == FailureReason

| where DeviceName in ("CFOLaptop, "CEOLaptop", "COOLaptop")

ActionType == "LogonFailed"

Answer Area

| summarize LogonFailures=count() by DeviceName, LogonType

| where DeviceName in ("CFOLaptop, "CEOLaptop", "COOLaptop")

| where ActionType == FailureReason and

ActionType == "LogonFailed"

| project LogonFailures=count()

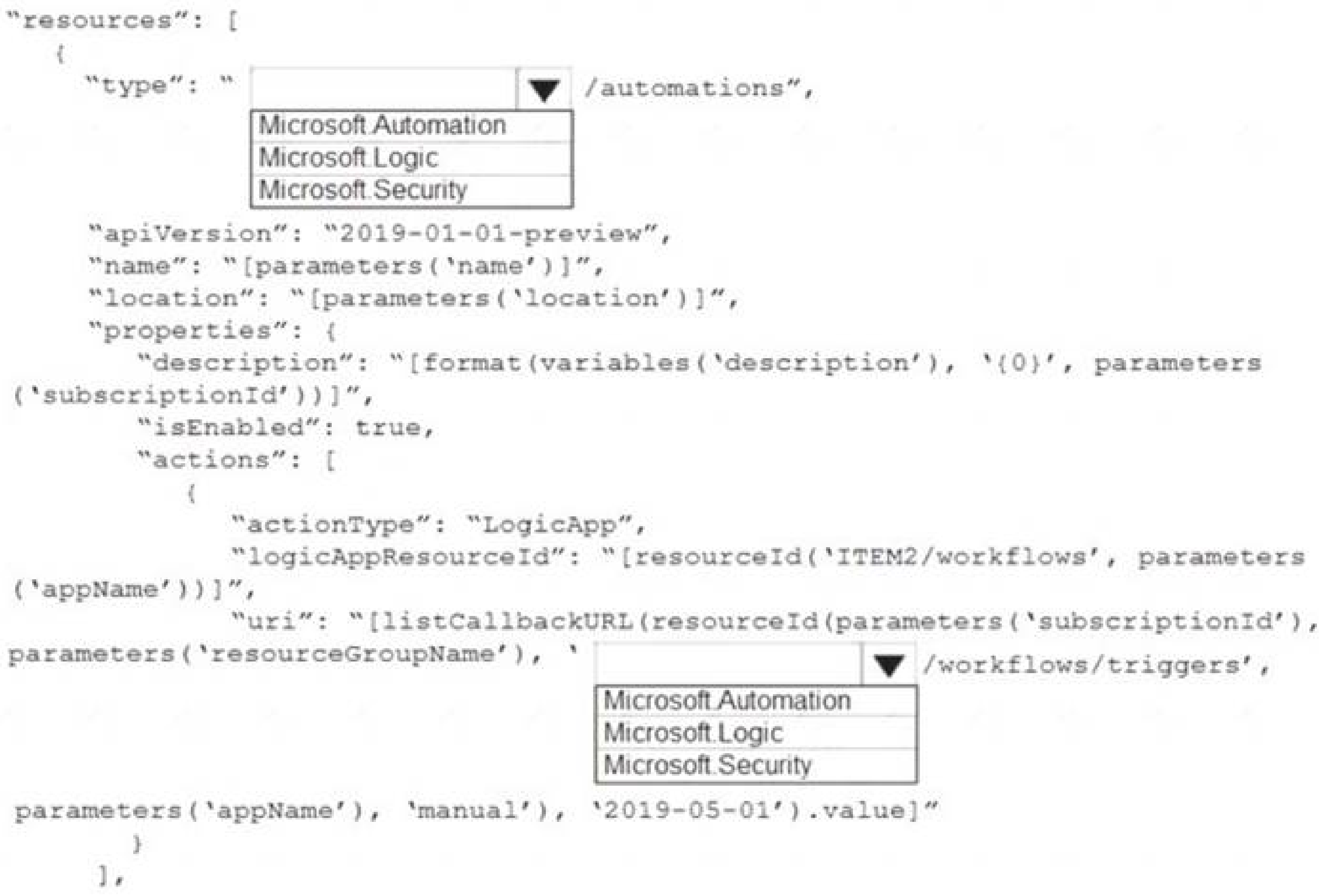
NEW QUESTION 20

- (Exam Topic 3)

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION 24

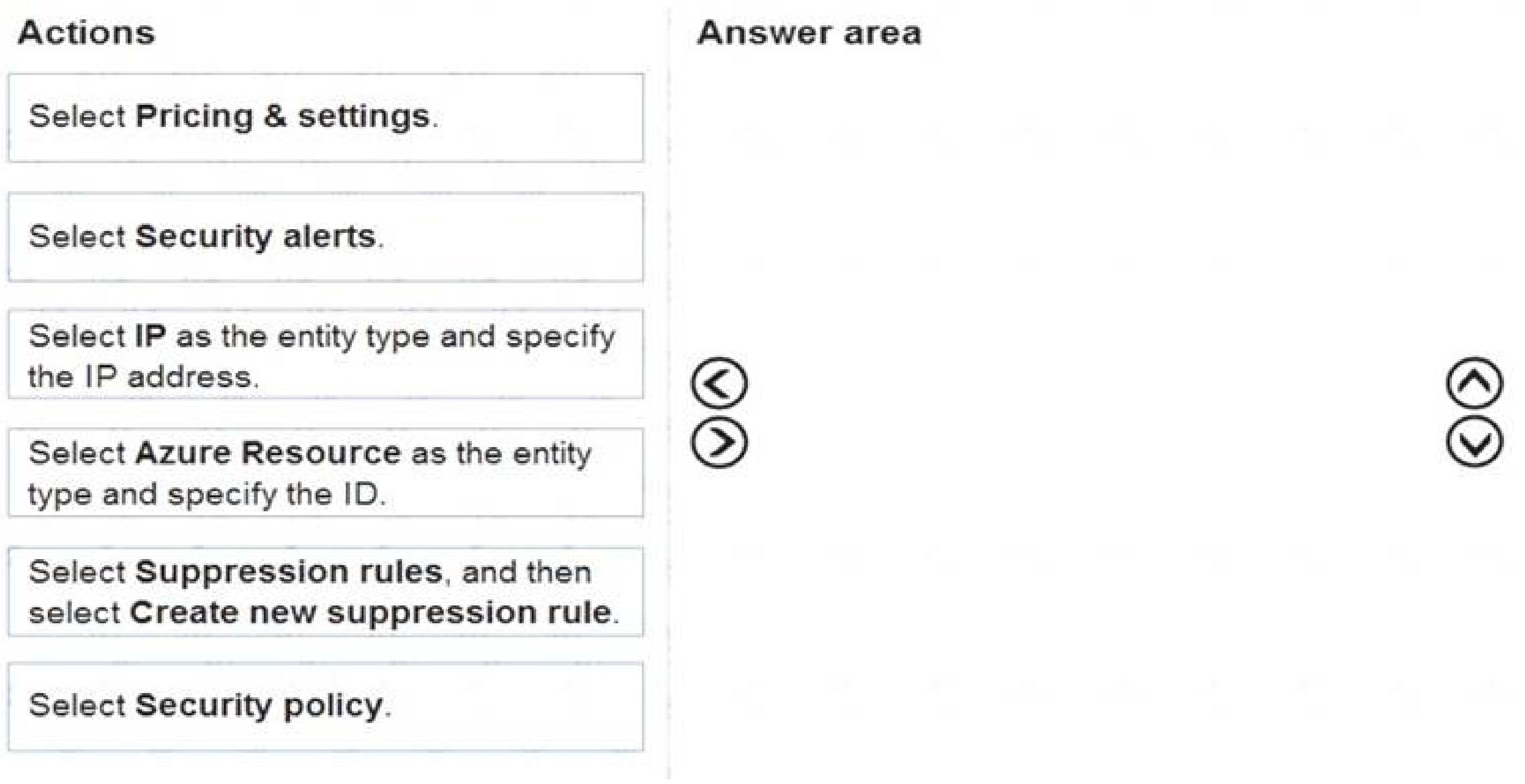
- (Exam Topic 3)

You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



Actions

Select Pricing & settings.

Select Security alerts.

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

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

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

Select Security policy.

Answer area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts

NEW QUESTION 25
- (Exam Topic 3)
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 28
- (Exam Topic 3)
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 30
- (Exam Topic 3)
You have an Azure subscription that uses Microsoft Defender for Endpoint.
You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.
What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. endpoint detection and response (EDR) in block mode
B. custom network indicators
C. web content filtering
D. Live response for servers

Answer: A

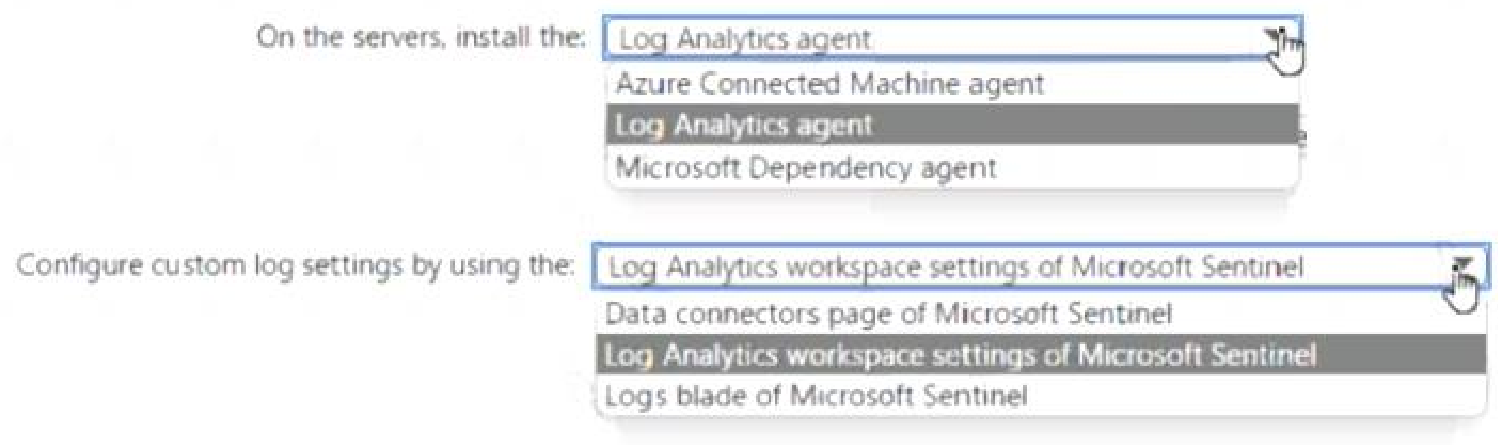
NEW QUESTION 32
- (Exam Topic 3)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

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

NEW QUESTION 33
- (Exam Topic 3)
Your on-premises network contains 100 servers that run Windows Server. You have an Azure subscription that uses Microsoft Sentinel.
You need to upload custom logs from the on-premises servers to Microsoft Sentinel. What should you do? To answer, select the appropriate options m the answer area.



On the servers, install the: Log Analytics agent

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

Azure Connected Machine agent
Log Analytics agent
Microsoft Dependency agent
Data connectors page of Microsoft Sentinel
Log Analytics workspace settings of Microsoft Sentinel
Logs blade of Microsoft Sentinel

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 34
- (Exam Topic 3)
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: C

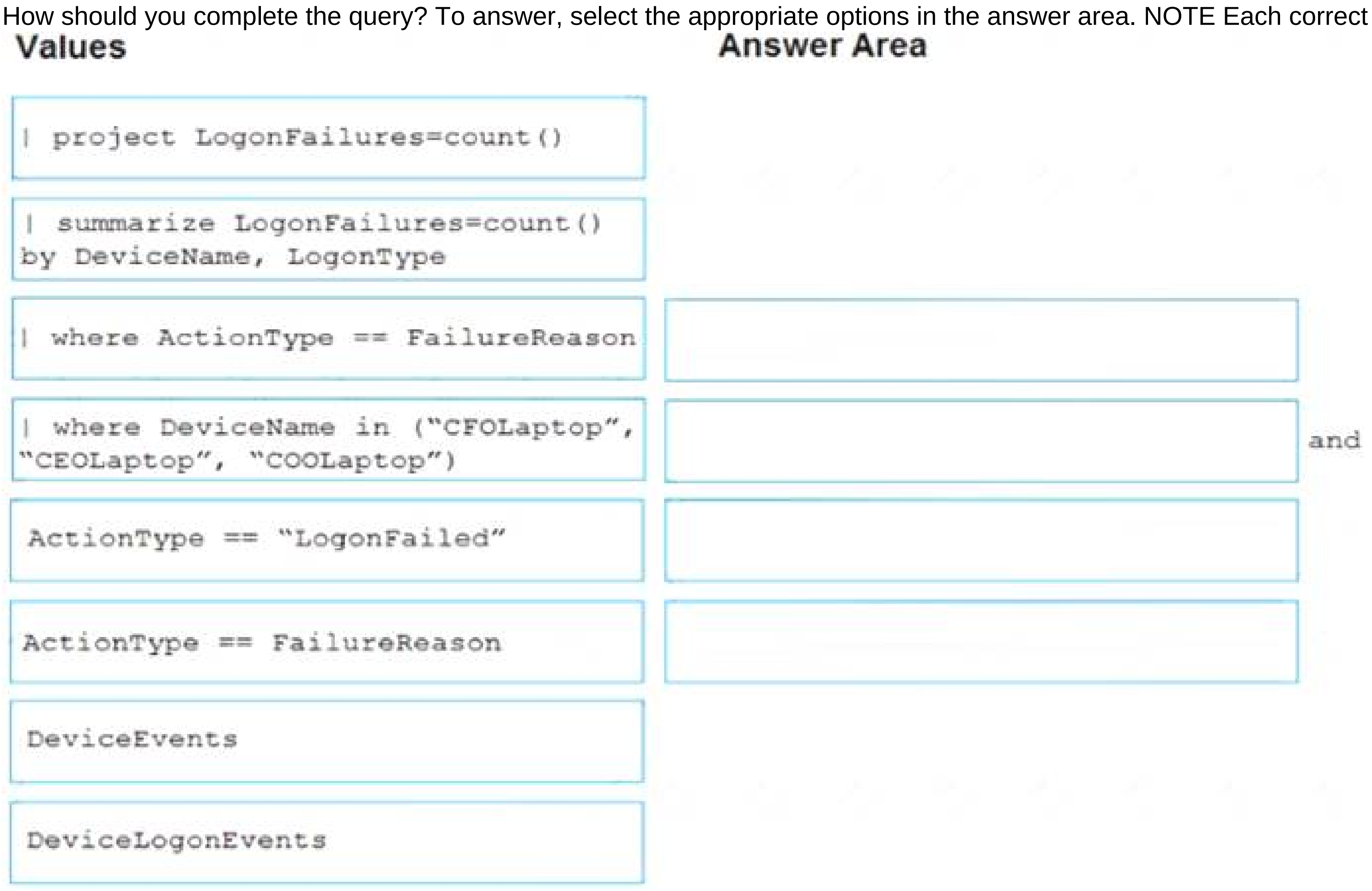
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

NEW QUESTION 39
- (Exam Topic 3)
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 41
- (Exam Topic 3)
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
```

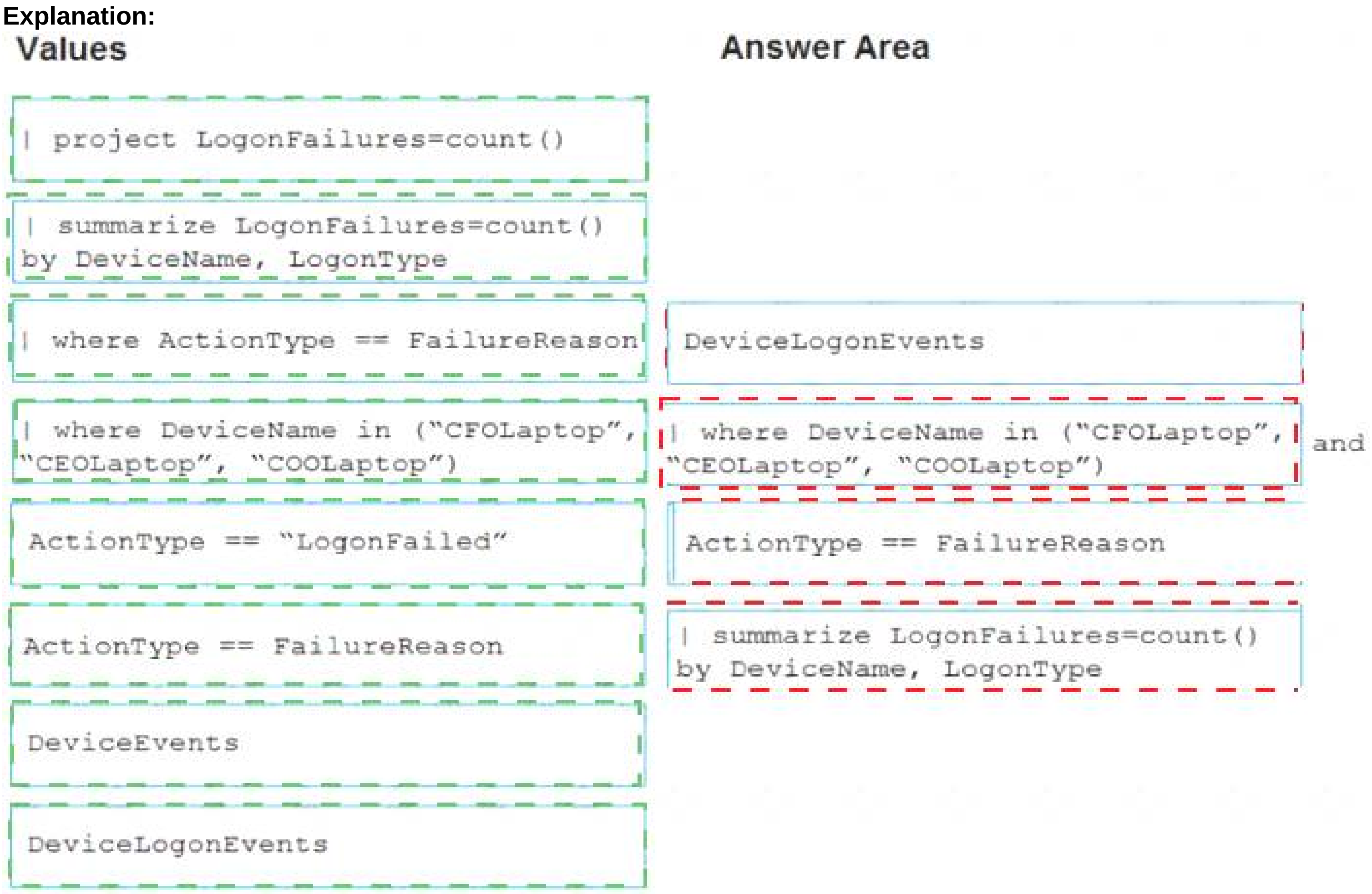
Answer Area

and

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Values

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

Answer Area

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

NEW QUESTION 45
- (Exam Topic 3)
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

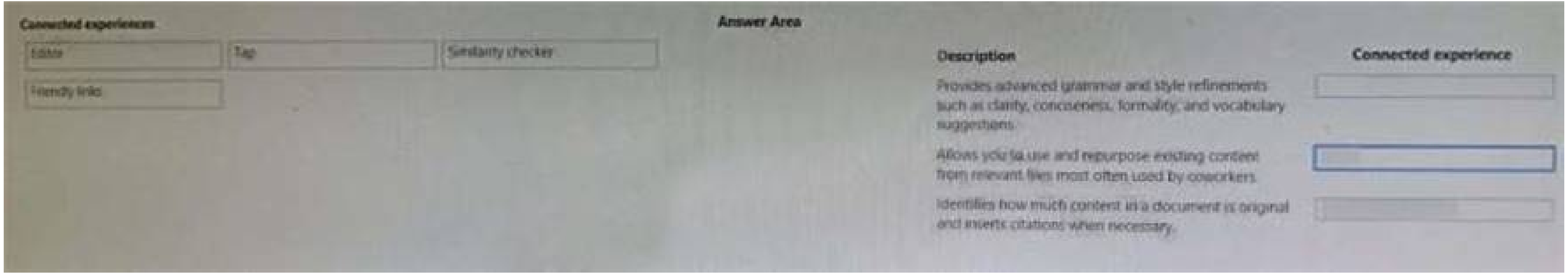
Answer: B

NEW QUESTION 47
- (Exam Topic 3)
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: A

NEW QUESTION 48
- (Exam Topic 3)
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



Connected experiences

Editor | Tap | Similarity checker

Friendly links

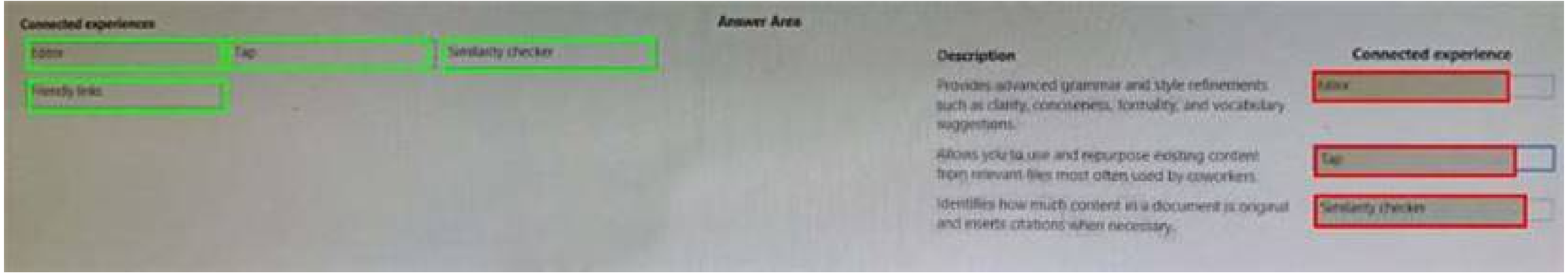
Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Connected experiences

Editor | Tap | Similarity checker

Friendly links

Answer Area

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

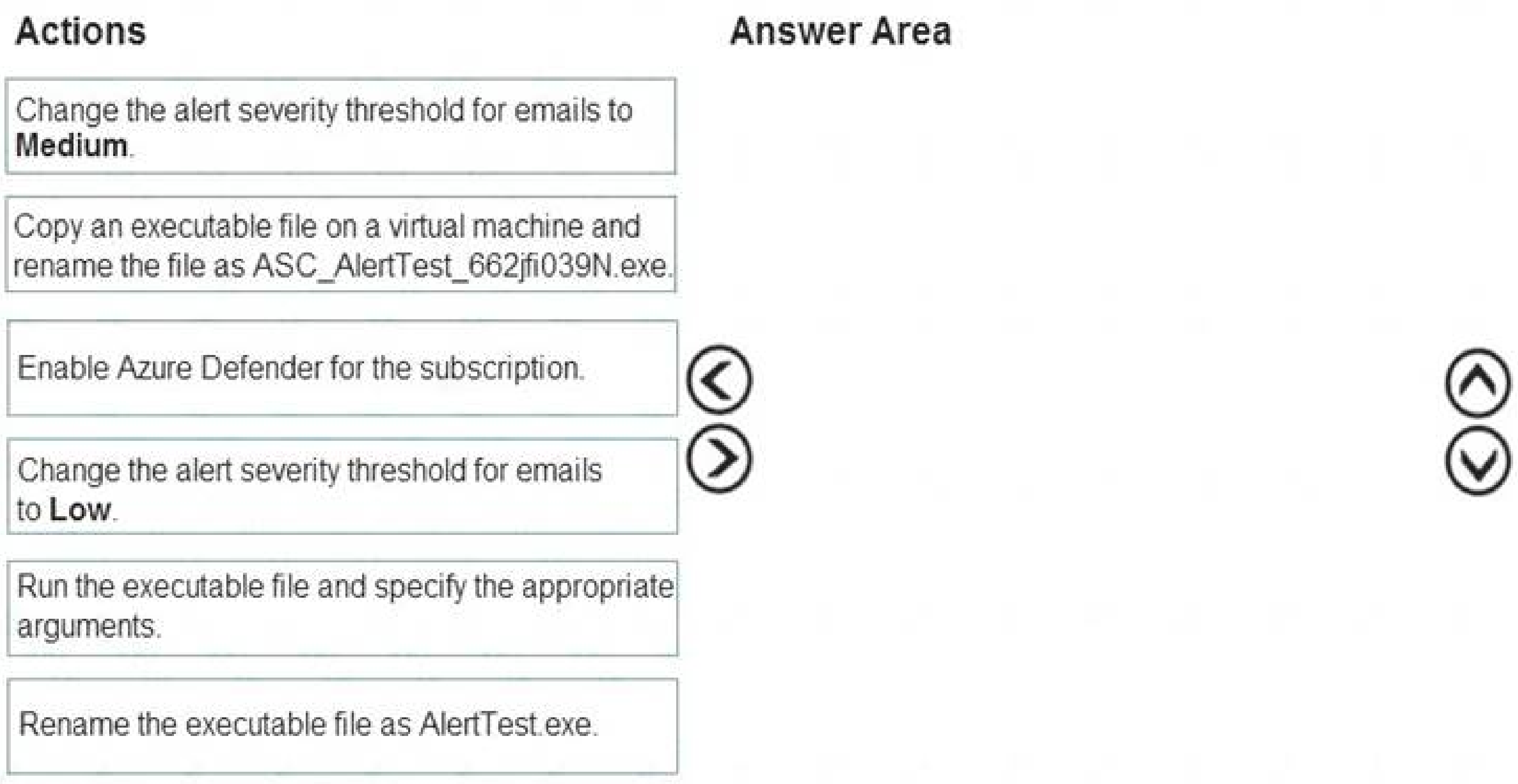
NEW QUESTION 53
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.
You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort
Which blade should you use 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-analyti

NEW QUESTION 56
- (Exam Topic 3)
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



Actions

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

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

Enable Azure Defender for the subscription.

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

Run the executable file and specify the appropriate arguments.

Rename the executable file as AlertTest.exe.

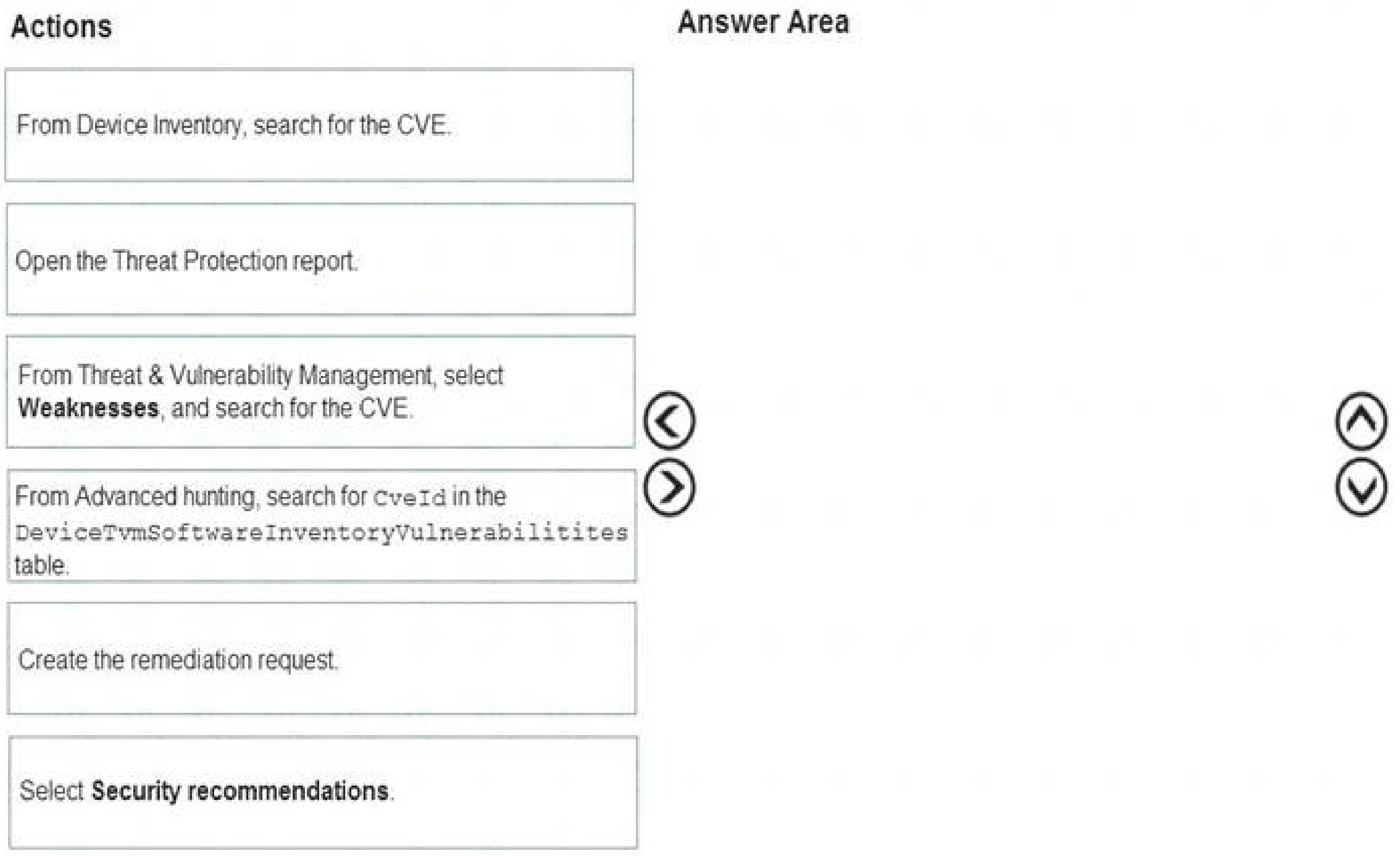
Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 58
- (Exam Topic 3)
You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

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

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

Create the remediation request.

Select **Security recommendations**.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps

NEW QUESTION 60
- (Exam Topic 3)

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 65
- (Exam Topic 3)
Your company deploys the following services:

- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

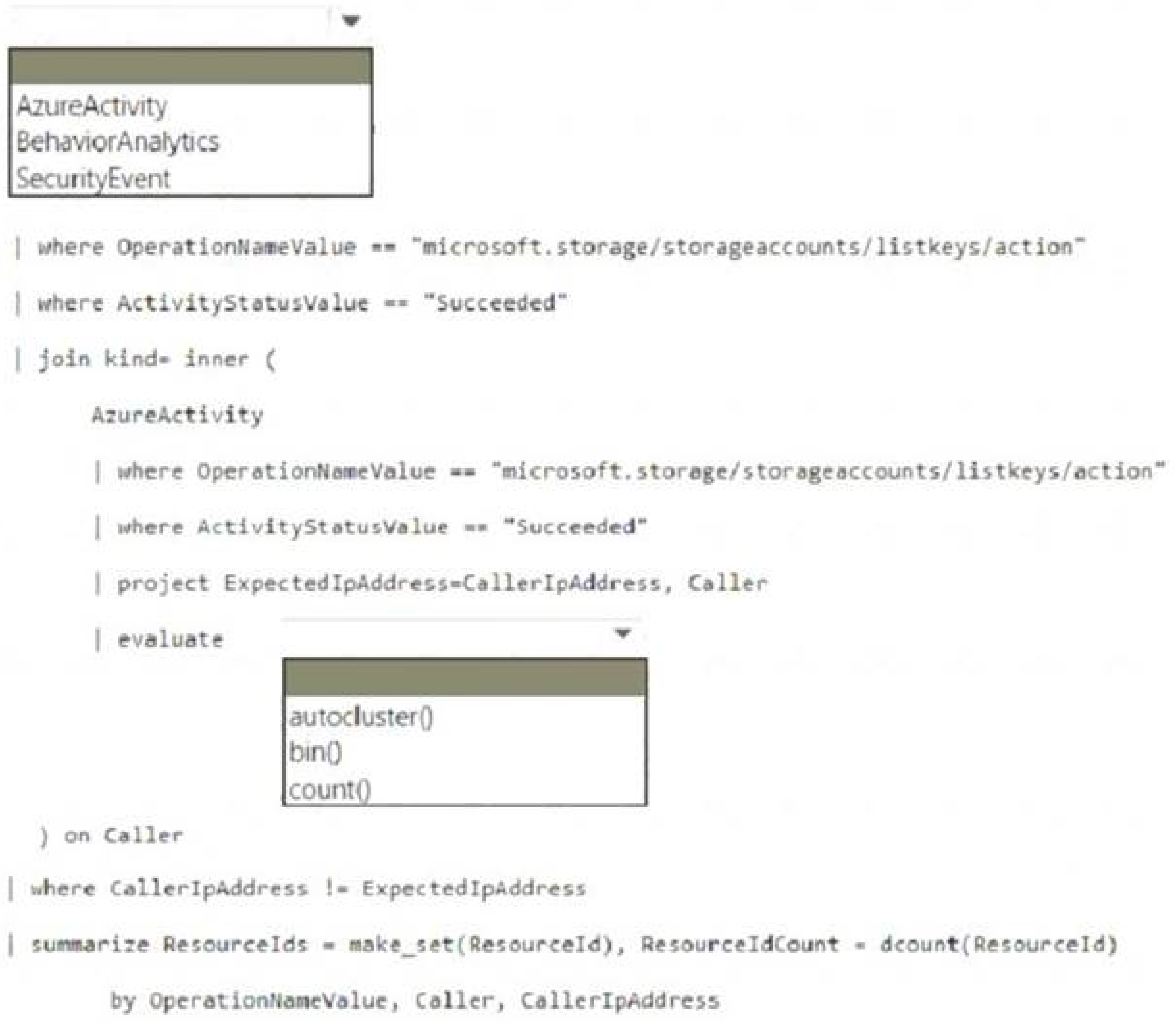
You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.
Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)
B. the Active remediation actions role in Microsoft Defender for Endpoint
C. the Security Administrator role in Azure Active Directory (Azure AD)
D. the Security Reader role in Azure Active Directory (Azure AD)

Answer: BD

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

NEW QUESTION 68
- (Exam Topic 3)
You have a Microsoft Sentinel workspace named sws1.
You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
    | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
    | where ActivityStatusValue == "Succeeded"
    | project ExpectedIpAddress=CallerIpAddress, Caller
    | evaluate
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
      by OperationNameValue, Caller, CallerIpAddress
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: AzureActivity
The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:
Box 2: autocluster()
Example: description: |
'Listing of storage keys is an interesting operation in Azure which might expose additional
secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this
type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.
The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned
clusters of expected activities and activity which is not expected is returned.' AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_O

NEW QUESTION 72
- (Exam Topic 3)
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 73
- (Exam Topic 3)
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 76
- (Exam Topic 3)
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

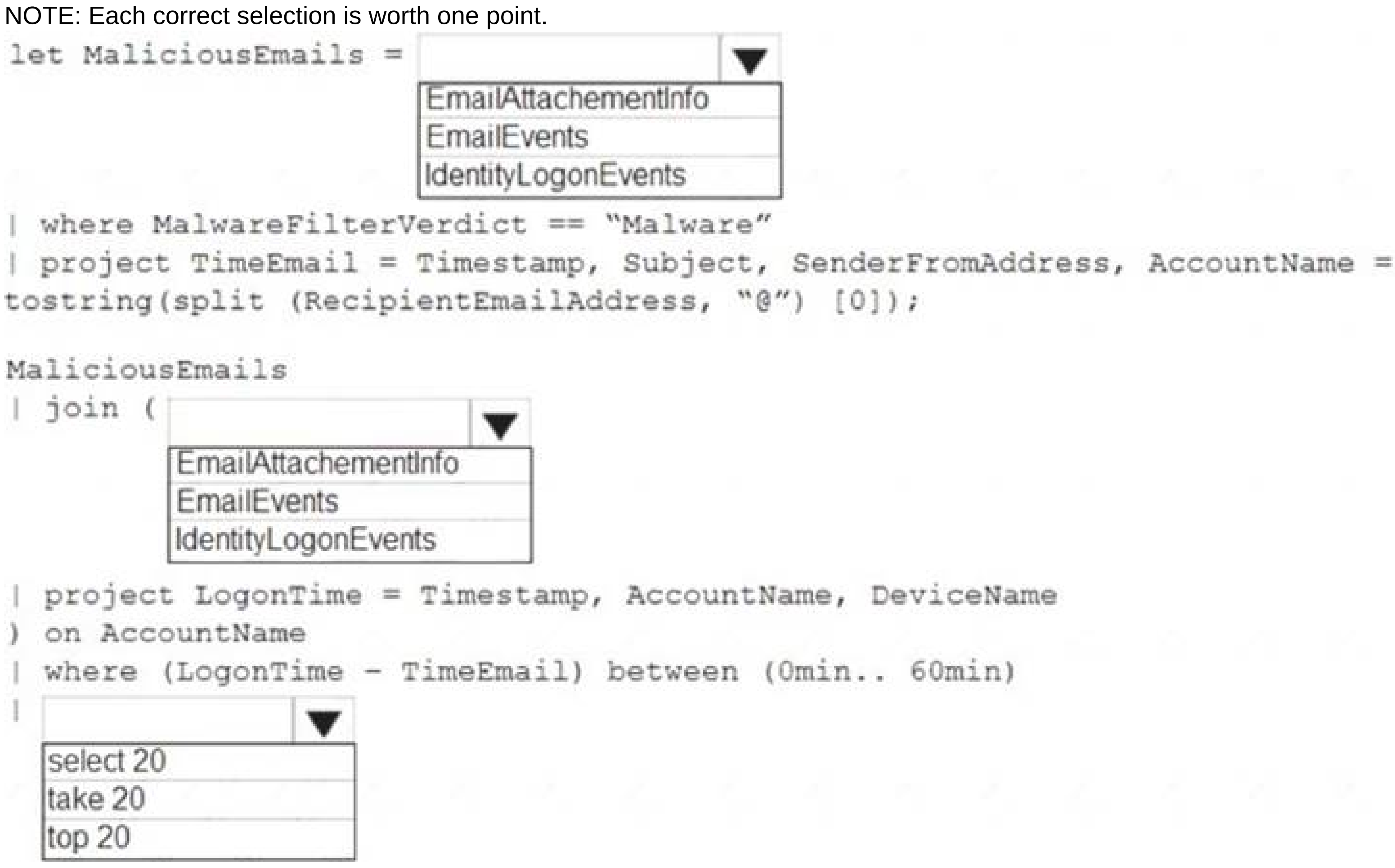
NEW QUESTION 78
- (Exam Topic 3)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1. You need to identify which blobs were deleted. What should you review?

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

Answer: A

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

NEW QUESTION 79
- (Exam Topic 3)
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.



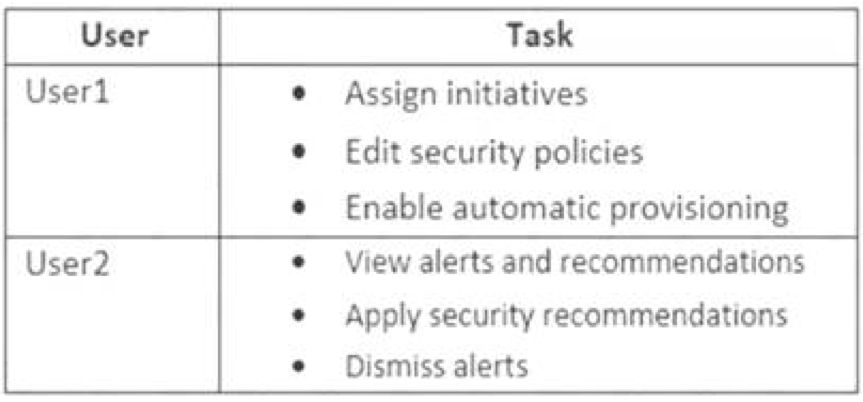
```
let MaliciousEmails = [ ▼ ]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress,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

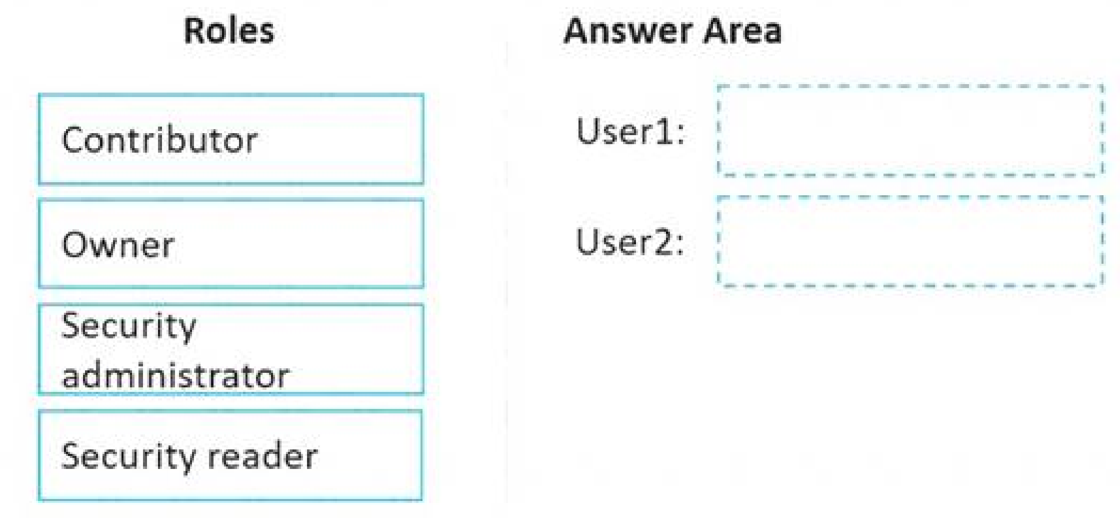
Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view

NEW QUESTION 82
- (Exam Topic 3)
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.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

NEW QUESTION 87
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add each account as a Sensitive account. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 92
- (Exam Topic 3)
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-c https://docs.microsoft.com/en-us/azure/security-

center/workflow-automation

NEW QUESTION 94
- (Exam Topic 3)
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack. Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only
B. a URL/domain indicator that has Action set to Alert and block
C. a file hash indicator that has Action set to Alert and block
D. a certificate indicator that has Action set to Alert and block

Answer: C

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

NEW QUESTION 98
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

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

Answer: C

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

NEW QUESTION 102
- (Exam Topic 3)
You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.
You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.
Which two actions should you perform? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.
B. Create a Microsoft incident creation rule based on Azure Security Center.
C. Create a Microsoft Cloud App Security connector.
D. Create an Azure AD Identity Protection connector.

Answer: AD

Explanation:
To use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity, you should perform the following two actions:
> Create an Azure AD Identity Protection connector. This will allow you to monitor suspicious activities in your Azure AD tenant and detect malicious sign-ins.
> Create a custom rule based on the Office 365 connector templates. This will allow you to monitor and detect anomalous activities in the Microsoft 365 subscription.
Reference: https://docs.microsoft.com/en-us/azure/sentinel/fusion-rules

NEW QUESTION 104
- (Exam Topic 3)
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?

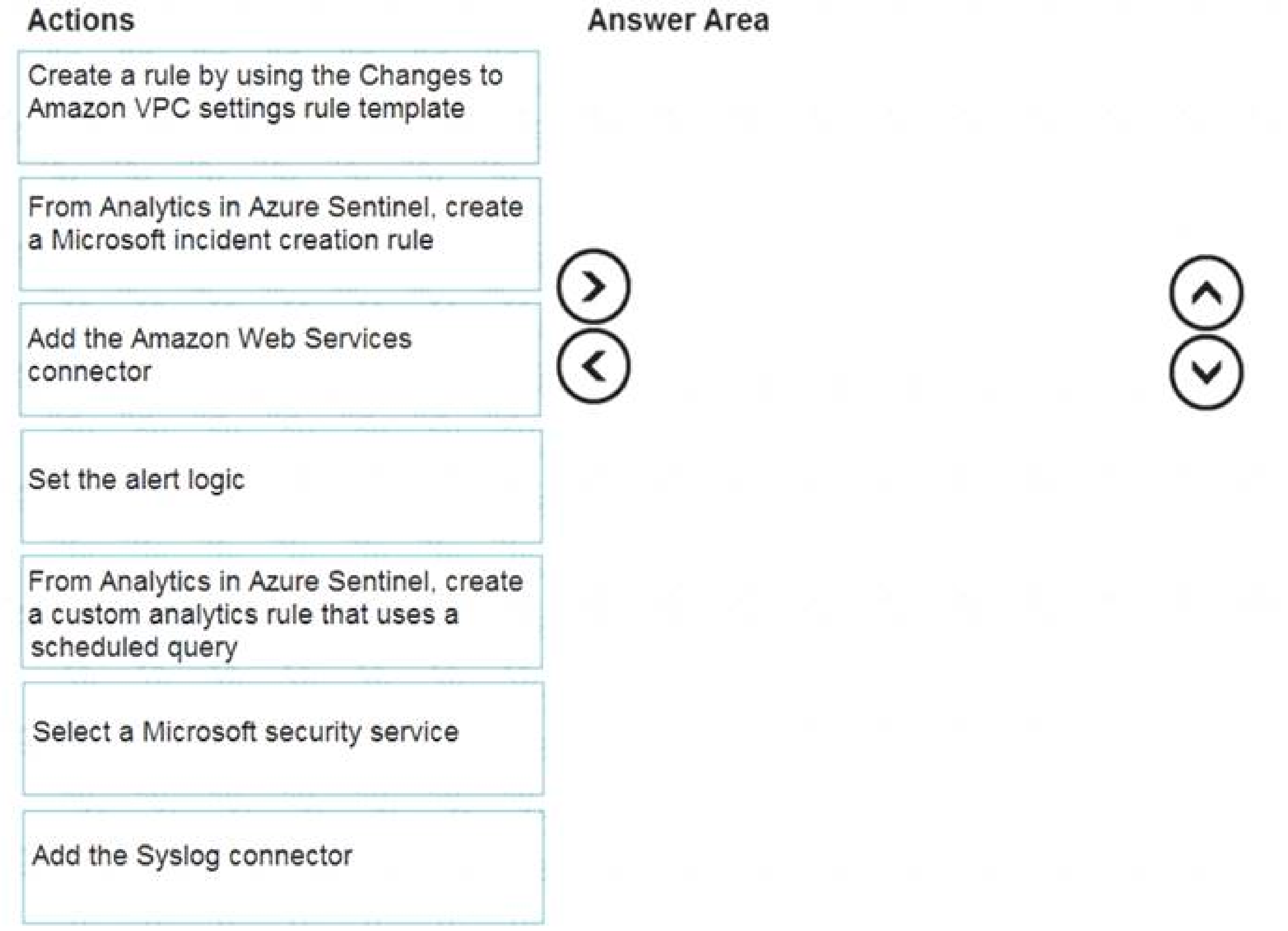
A. at the subscription level
B. at the workspace level
C. at the resource level

Answer: A

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

NEW QUESTION 108
- (Exam Topic 3)

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.



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

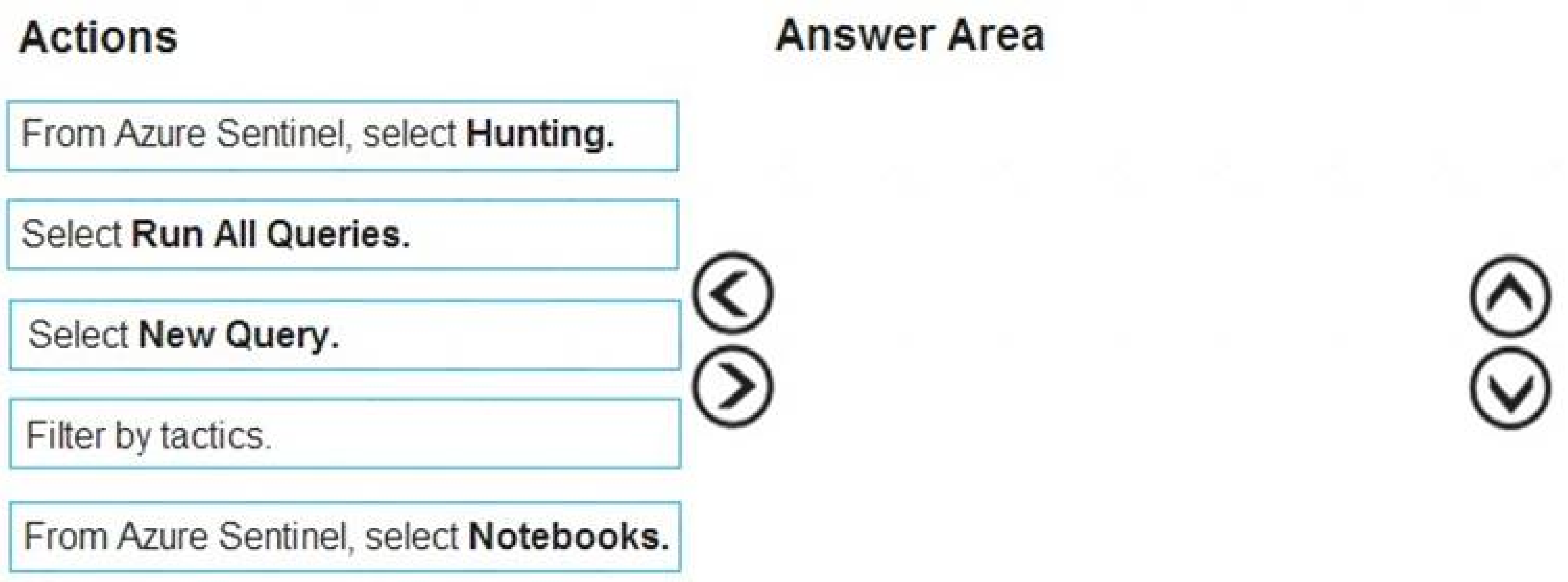
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION 110
- (Exam Topic 3)
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

From Azure Sentinel, select **Hunting.**

Select **Run All Queries.**

Select **New Query.**

Filter by tactics.

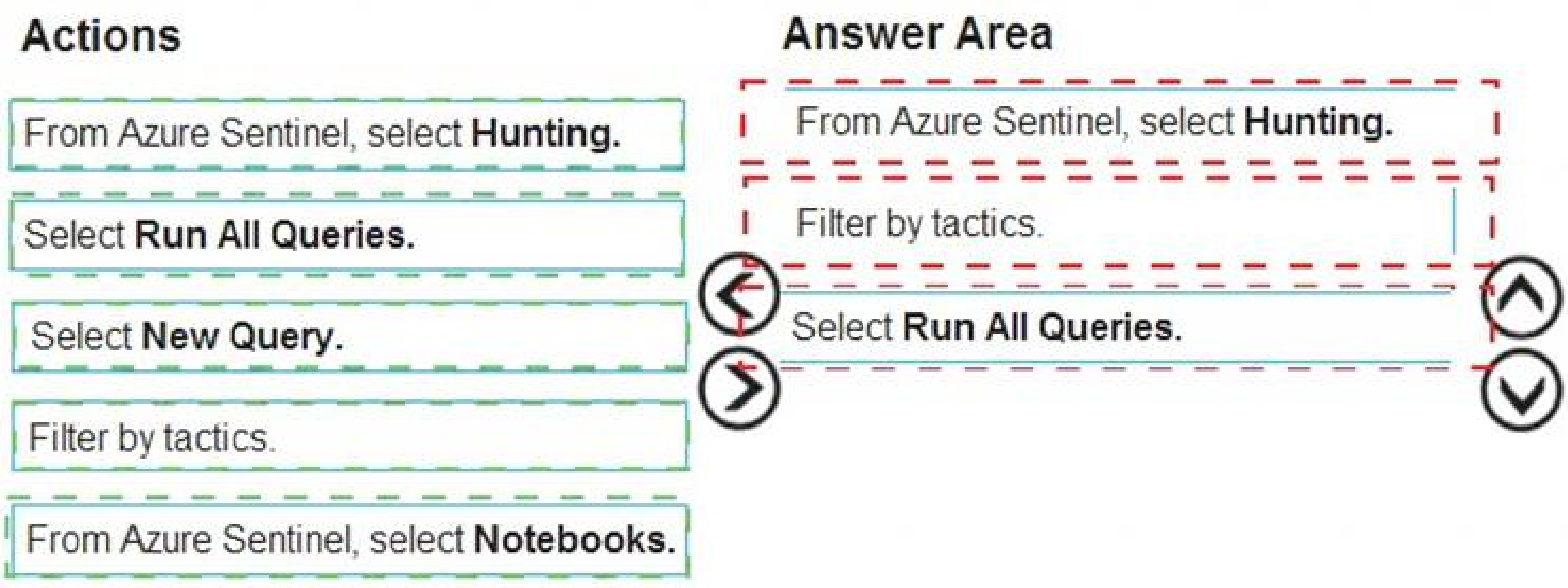
From Azure Sentinel, select **Notebooks.**

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:



Actions

From Azure Sentinel, select **Hunting.**

Select **Run All Queries.**

Select **New Query.**

Filter by tactics.

From Azure Sentinel, select **Notebooks.**

Answer Area

From Azure Sentinel, select **Hunting.**

Filter by tactics.

Select **Run All Queries.**

NEW QUESTION 114
- (Exam Topic 3)
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 115
- (Exam Topic 3)
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 120
- (Exam Topic 3)
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 122
- (Exam Topic 3)
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.

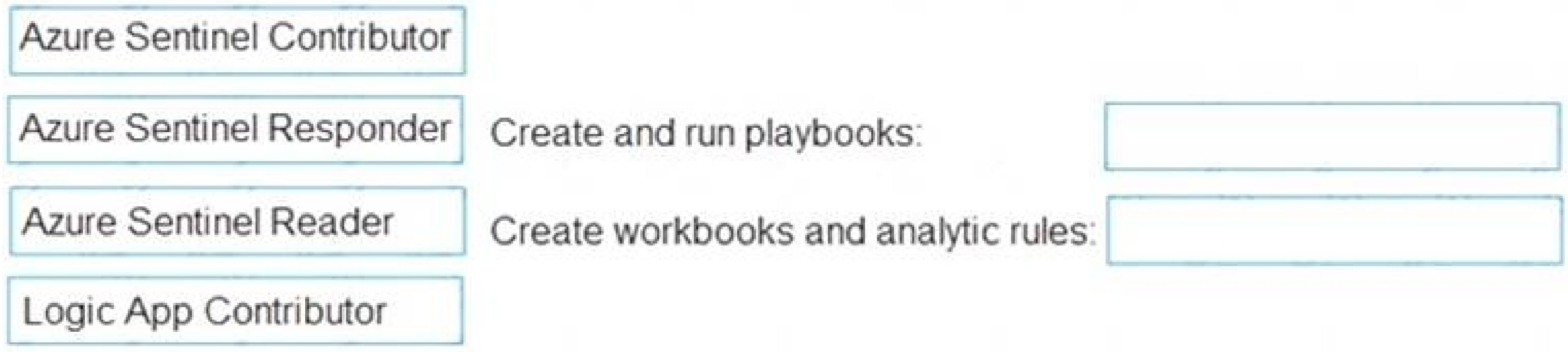
Answer: B

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

NEW QUESTION 126
- (Exam Topic 3)
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:
A picture containing graphical user interface Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION 130
- (Exam Topic 3)
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

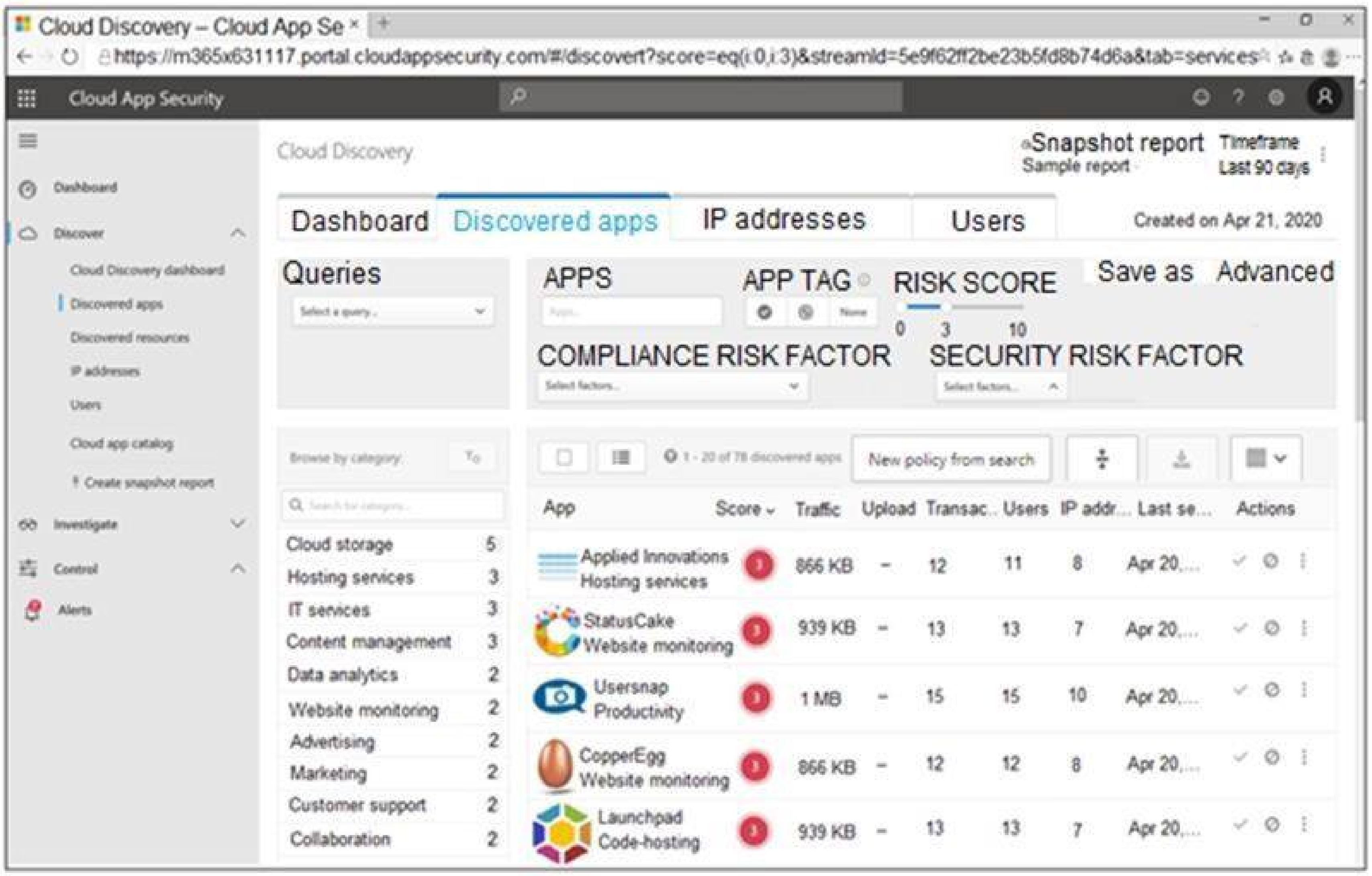
NEW QUESTION 131
- (Exam Topic 3)
A company uses Azure Sentinel.
You need to create an automated threat response. What should you use?

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

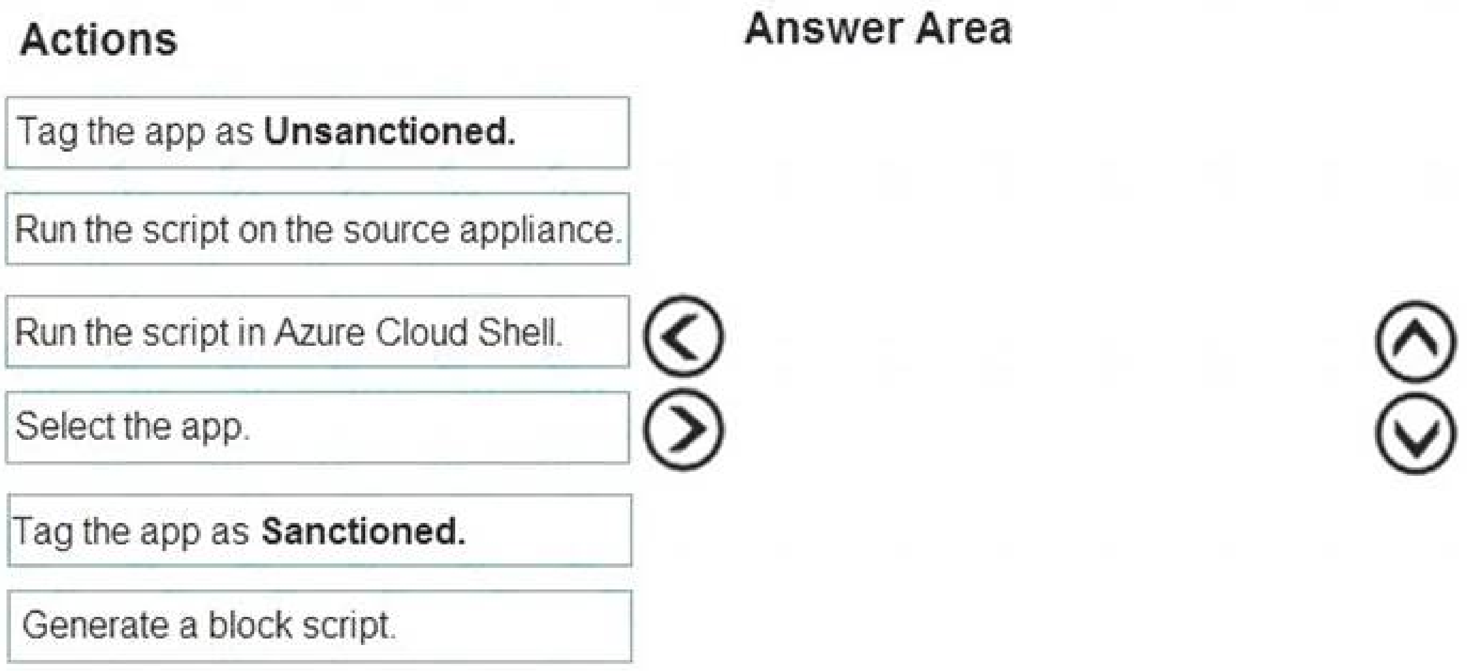
NEW QUESTION 132
- (Exam Topic 3)
You open the Cloud App Security portal as shown in the following exhibit.



Cloud storage	5
Hosting services	3
IT services	3
Content management	3
Data analytics	2
Website monitoring	2
Advertising	2
Marketing	2
Customer support	2
Collaboration	2

App	Score	Traffic	Upload	Transac..	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	-	12	11	8	Apr 20,...	
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20,...	
Usersnap Productivity	3	1 MB	-	15	15	10	Apr 20,...	
CopperEgg Website monitoring	3	866 KB	-	12	12	8	Apr 20,...	
Launchpad Code-hosting	3	939 KB	-	13	13	7	Apr 20,...	

You need to remediate the risk for the Launchpad app.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Tag the app as **Unsanctioned.**

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned.**

Generate a block script.

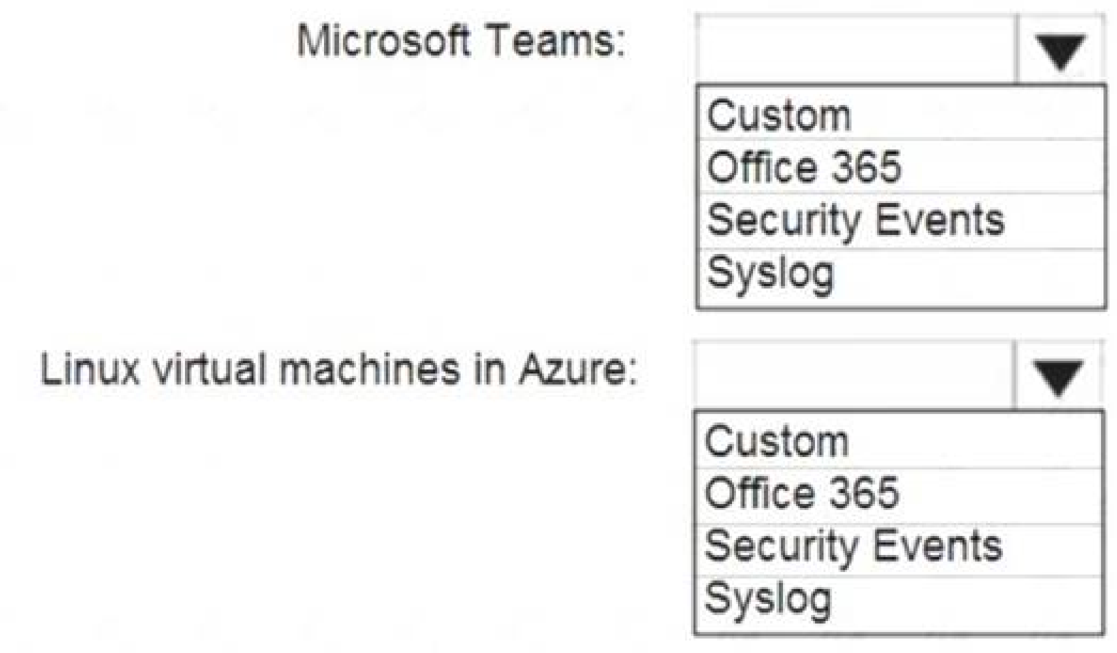
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

NEW QUESTION 136
- (Exam Topic 3)
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:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365 https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION 139
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

A. Yes
B. No

Answer: B

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

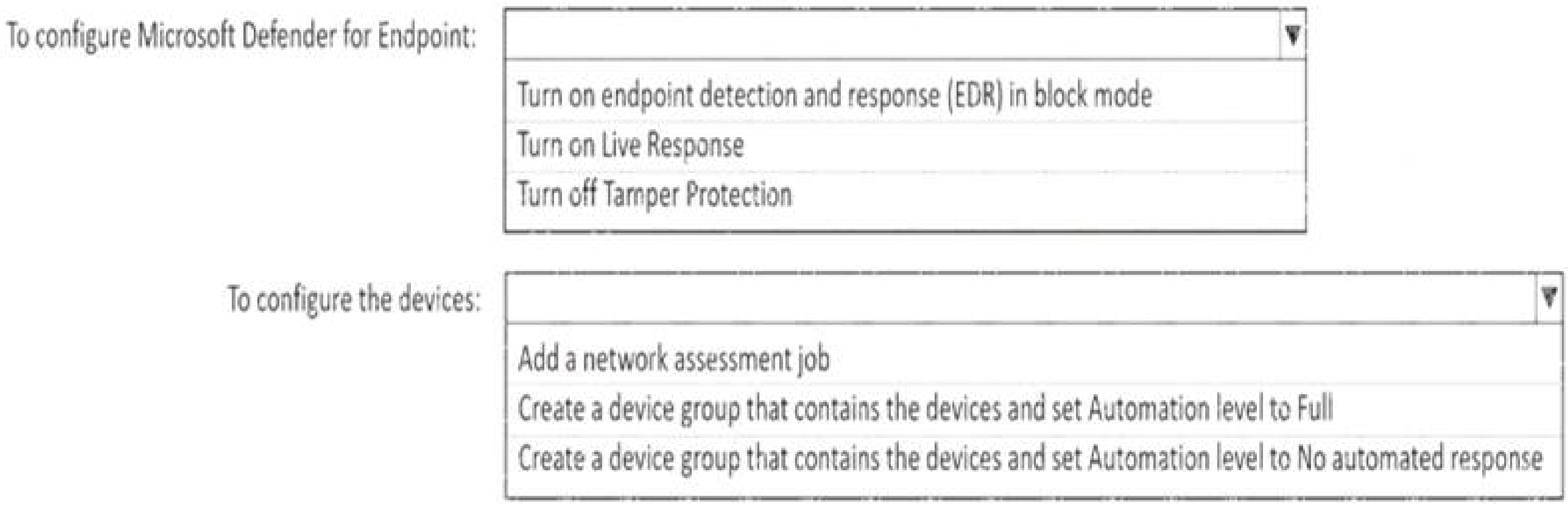
NEW QUESTION 141
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct 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 146
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



To configure Microsoft Defender for Endpoint:

- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:

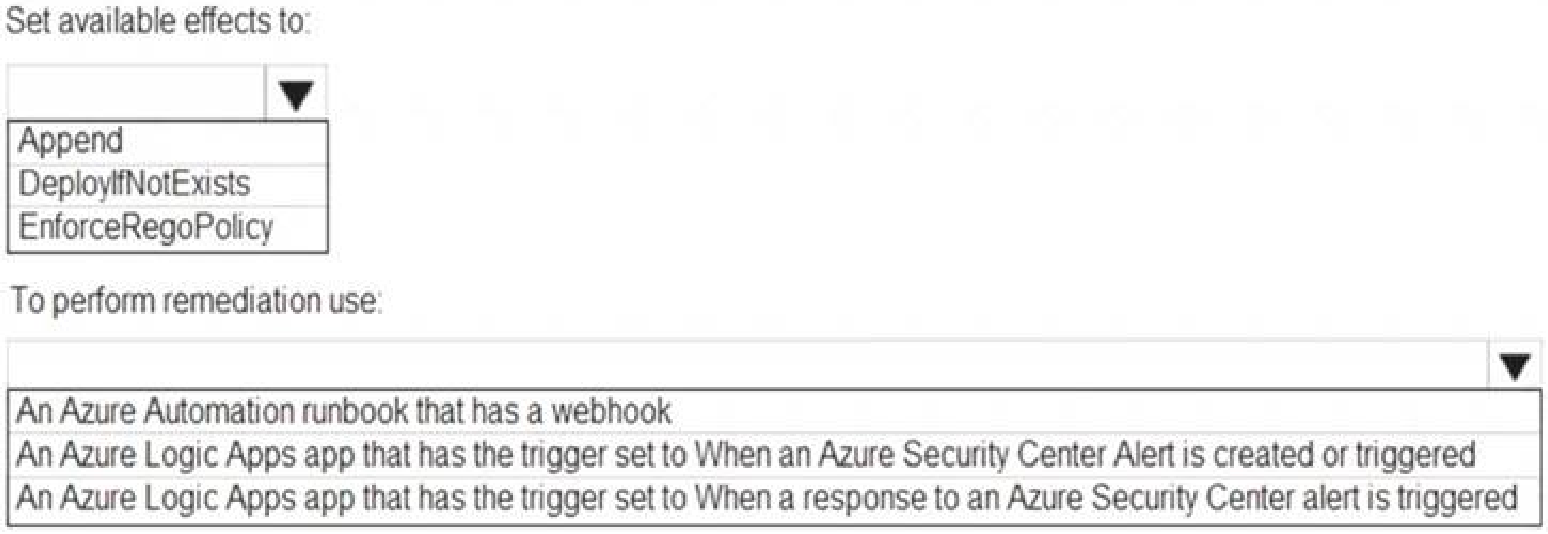
- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365- https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw

NEW QUESTION 151
- (Exam Topic 3)
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:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 155
- (Exam Topic 3)
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

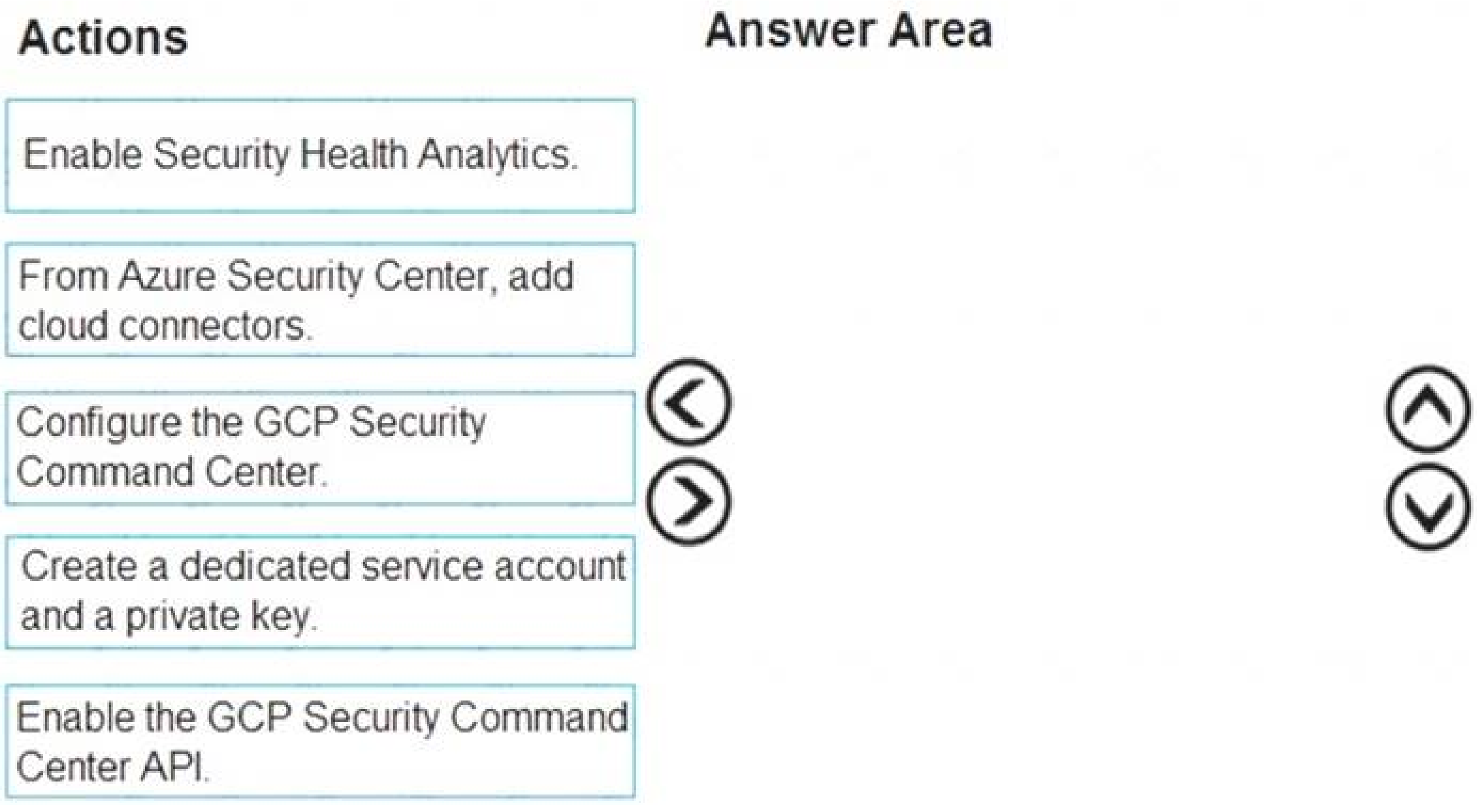
NEW QUESTION 157
- (Exam Topic 3)
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

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-event

NEW QUESTION 158
- (Exam Topic 3)
You have resources in Azure and Google cloud.
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Answer Area

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

NEW QUESTION 161
- (Exam Topic 3)
You have the following environment:
- Azure Sentinel
- A Microsoft 365 subscription
- Microsoft Defender for Identity
- An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.
You deploy Microsoft Defender for Identity by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified in Active Directory. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.
B. Modify the permissions of the Domain Controllers organizational unit (OU).
C. Configure auditing in the Microsoft 365 compliance center.

D. Configure Windows Event Forwarding on the domain controllers.

Answer: AD

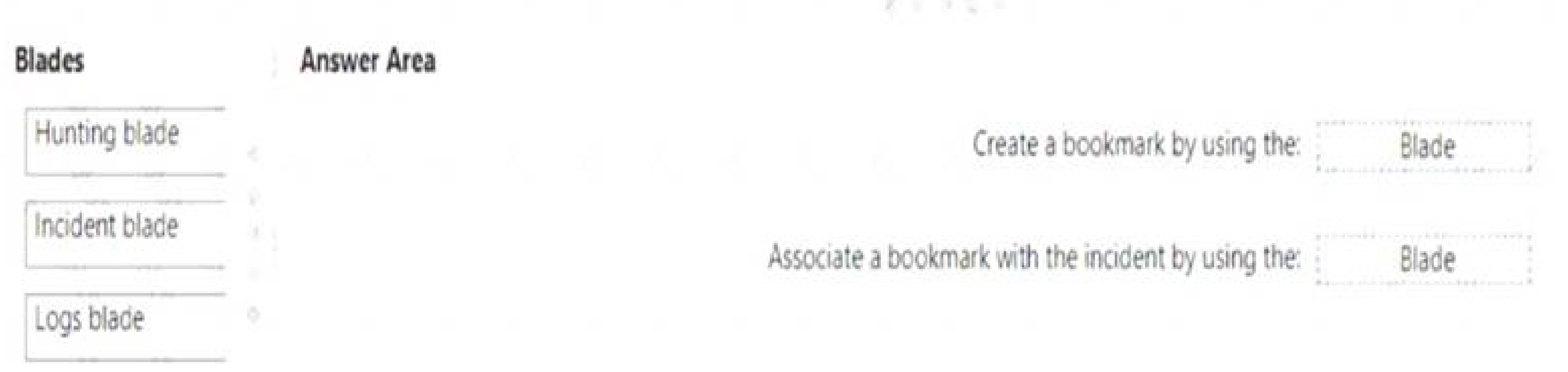
Explanation:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

NEW QUESTION 166
- (Exam Topic 3)
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 170
- (Exam Topic 3)
You have a Microsoft Sentinel workspace that contains an Azure AD data connector. You need to associate a bookmark with an Azure AD-related incident. What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content
NOTE: Each correct selection is worth one point.



Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the: Blade

Associate a bookmark with the incident by using the: Blade

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 173
- (Exam Topic 3)
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 178
- (Exam Topic 3)
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

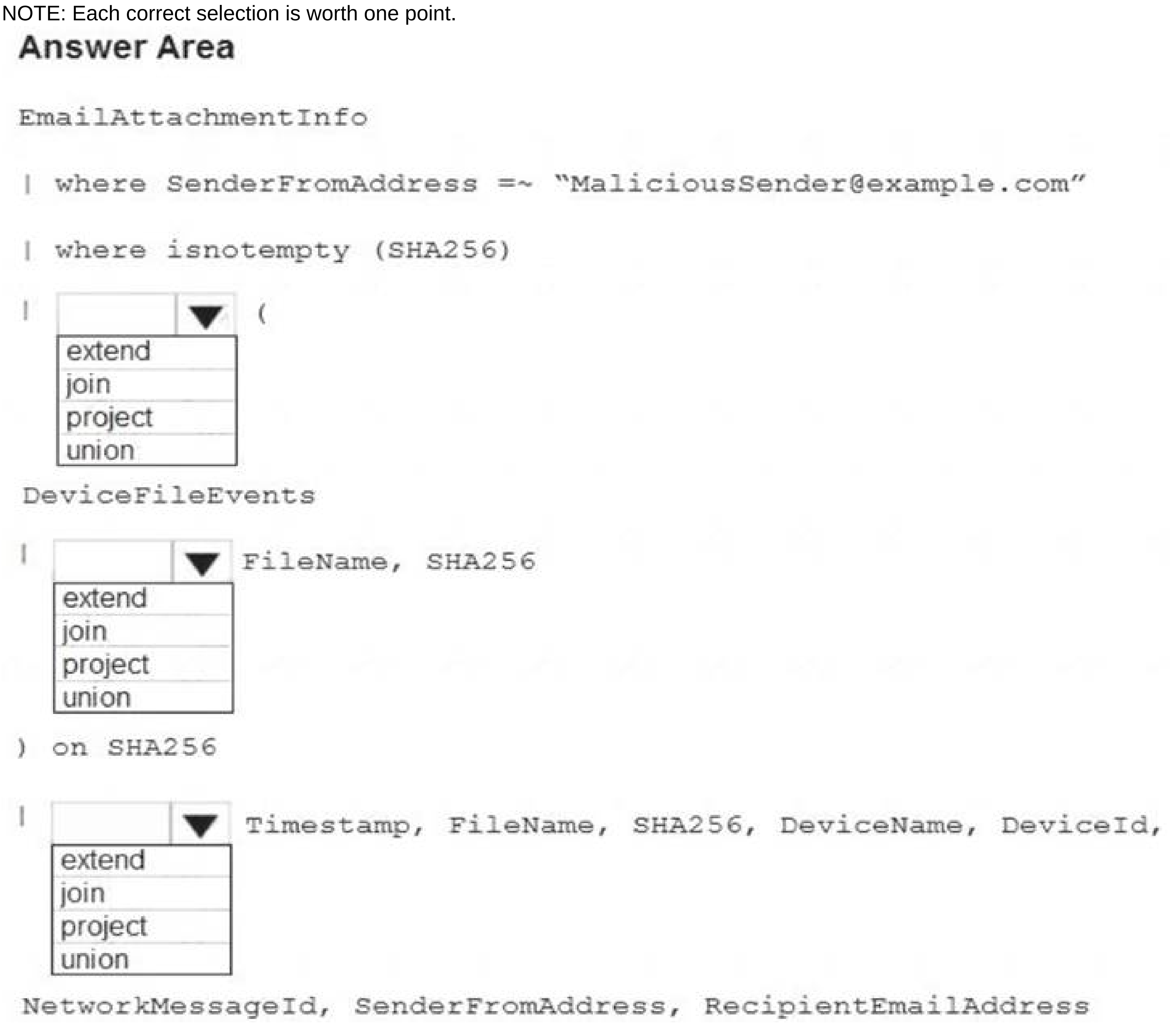
NEW QUESTION 179
- (Exam Topic 3)
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

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 181
- (Exam Topic 3)
You have a Microsoft 365 E5 subscription.
You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment. How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36

NEW QUESTION 184
- (Exam Topic 3)
You use Azure Sentinel.
You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Contributor
B. Security Administrator
C. Azure Sentinel Responder
D. Logic App Contributor

Answer: A

Explanation:
Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources. Reference: https://docs.microsoft.com/en-us/azure/sentinel/roles

NEW QUESTION 185
......