Exam Questions SC-200

Microsoft Security Operations Analyst

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

NEW QUESTION 1
- (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

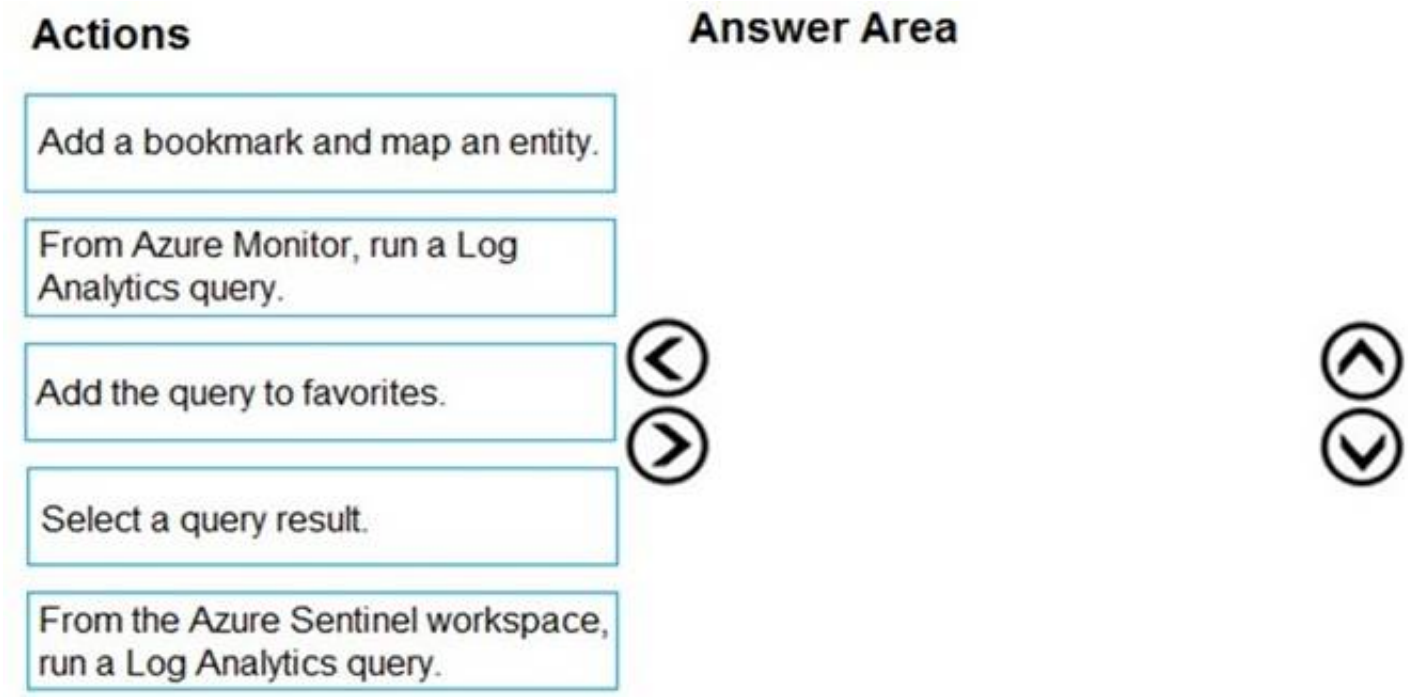
NEW QUESTION 2
- (Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Answer: B

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

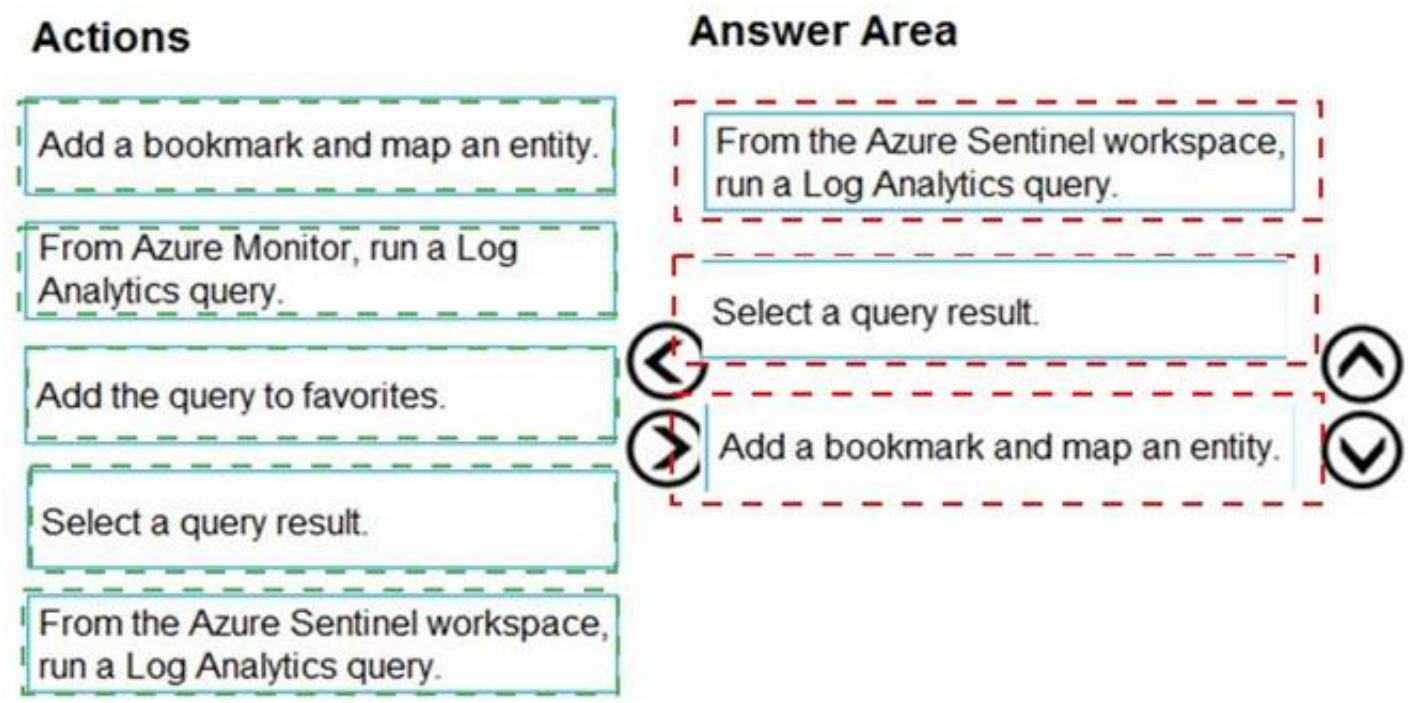
NEW QUESTION 3
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 4
- (Topic 2)
You need to modify the anomaly detection policy settings to meet the Microsoft Defender for Cloud Apps requirements and resolve the reported problem.
Which policy should you modify?

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

Answer: D

NEW QUESTION 5
HOTSPOT - (Topic 2)
You need to configure the Microsoft Sentinel integration to meet the Microsoft Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 6
- (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

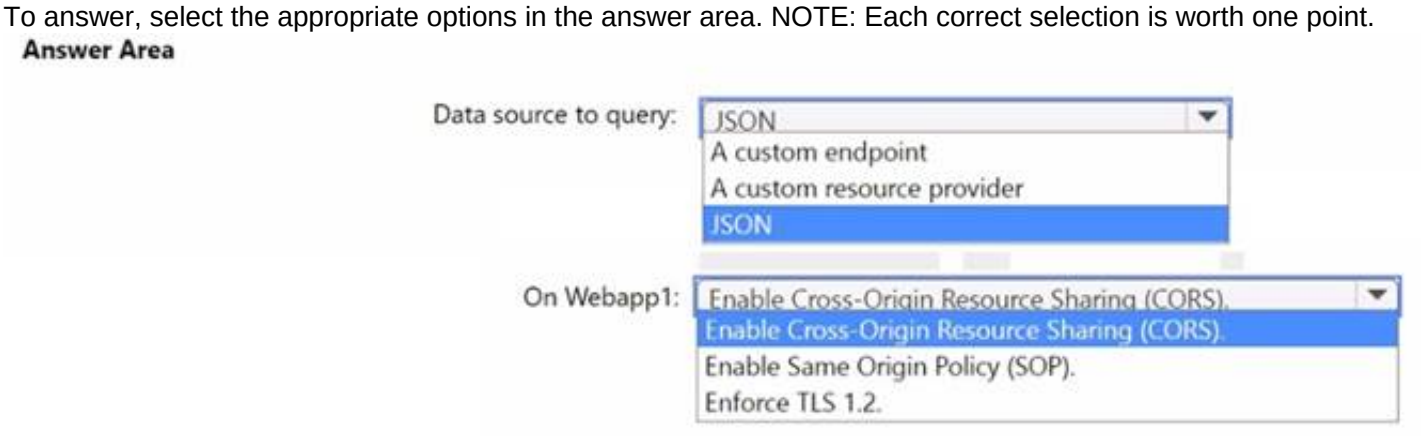
NEW QUESTION 7
- (Topic 2)
You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

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

Answer: C

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

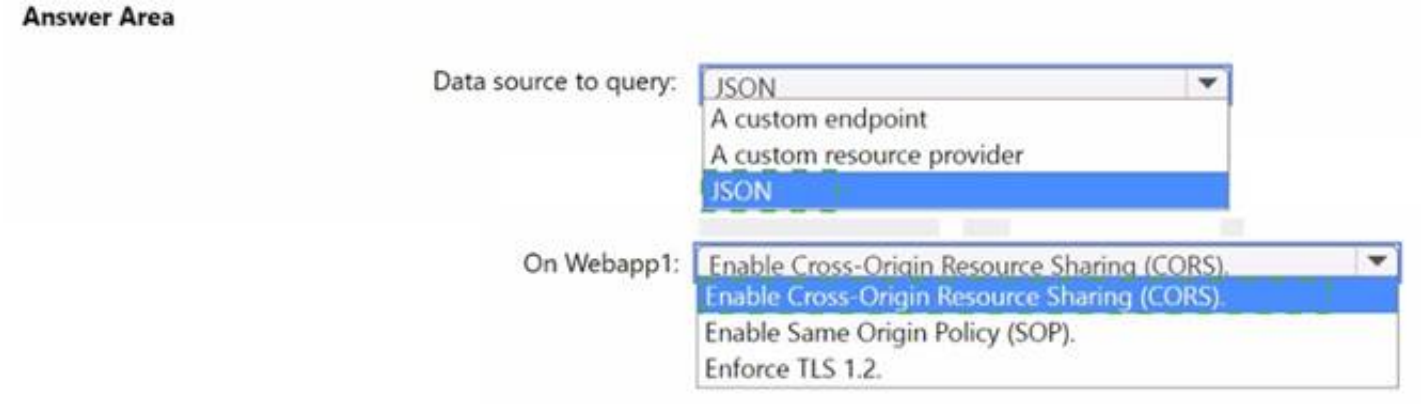
NEW QUESTION 8
HOTSPOT - (Topic 3)
You need to implement the query for Workbook1 and Webapp1. The solution must meet the Microsoft Sentinel requirements. How should you configure the query?
To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 9
- (Topic 3)
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

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

Answer: D

NEW QUESTION 10
- (Topic 3)
You need to implement the Defender for Cloud requirements. What should you configure for Server2?

A. the Microsoft Antimalware extension
B. an Azure resource lock
C. an Azure resource tag
D. the Azure Automanage machine configuration extension for Windows

Answer: D

NEW QUESTION 10
- (Topic 3)
You need to ensure that the processing of incidents generated by rulequery1 meets the Microsoft Sentinel requirements.
What should you create first?

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

Answer: A

NEW QUESTION 15
- (Topic 3)
You need to implement the Defender for Cloud requirements. Which subscription-level role should you assign to Group1?

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

Answer: B

NEW QUESTION 16
- (Topic 3)
You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

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

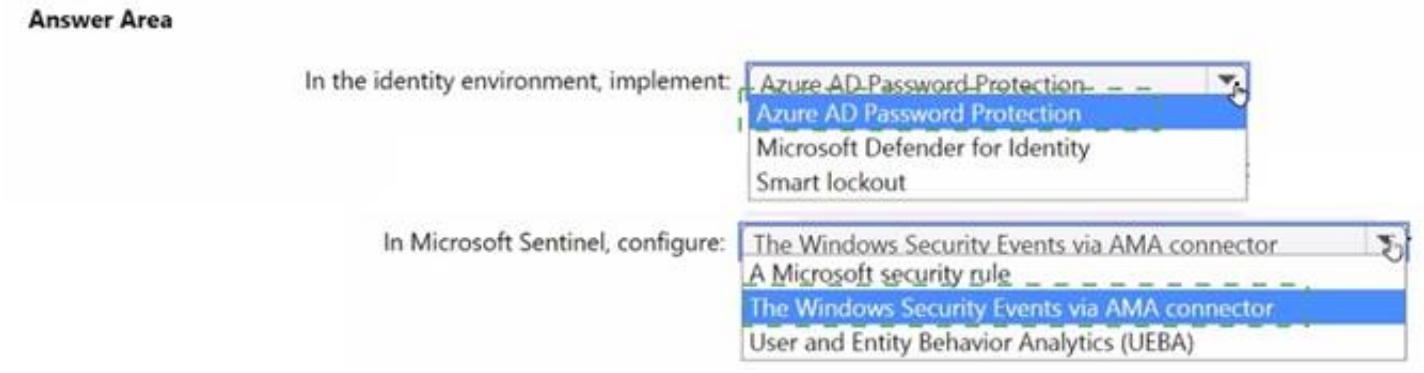
Answer: D

NEW QUESTION 17
HOTSPOT - (Topic 3)
You need to monitor the password resets. The solution must meet the Microsoft Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 19
- (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 22
- (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 23
HOTSPOT - (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.
You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  [ ▼ ]  kind=inner AlertEvidence on DeviceId
| project AlertId
| join AlertInfo on AlertId
|  [ ▼ ]  AlertId, Timestamp, Title, Severity, Category
```

[▼] options: extend / join / project

[▼] options: project / summarize / take

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: join An inner join.
This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.
This query uses the DeviceInfo table to check if a potentially compromised user (<account- name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

```
DeviceInfo
//Query for devices that the potentially compromised account has logged onto
| where LoggedOnUsers contains '<account-name>'
| distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables
| join kind=inner AlertEvidence on DeviceId
| project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
```

DeviceInfo LoggedOnUsers AlertEvidence "project AlertID" Box 2: project

NEW QUESTION 24
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 26
- (Topic 4)
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

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

Answer: B

NEW QUESTION 27
- (Topic 4)
You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector. You need to customize which details will be included when an alert is created for a specific event. What should you do?

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

Answer: D

NEW QUESTION 31
- (Topic 4)
You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

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

Answer: B

Explanation:

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

NEW QUESTION 36
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.
You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

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

Answer: A

NEW QUESTION 41
- (Topic 4)
You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.
What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

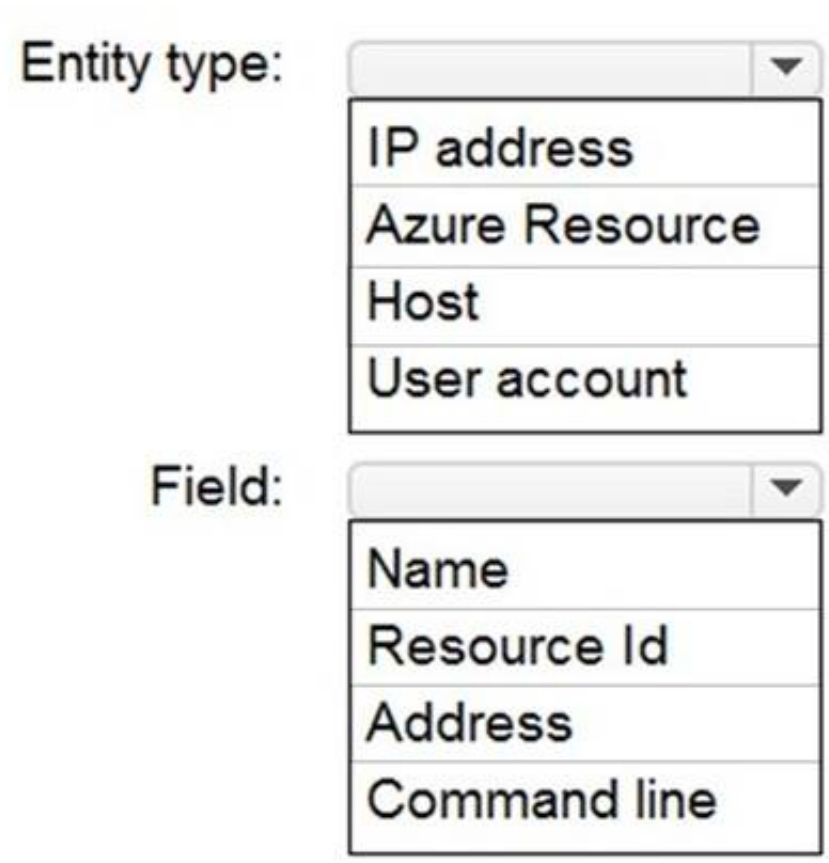
A. the Threat Protection Status report in Microsoft Defender for Office 365

B. the mailbox audit log in Exchange
C. the Safe Attachments file types report in Microsoft Defender for Office 365
D. the mail flow report in Exchange

Answer: A

Explanation:
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

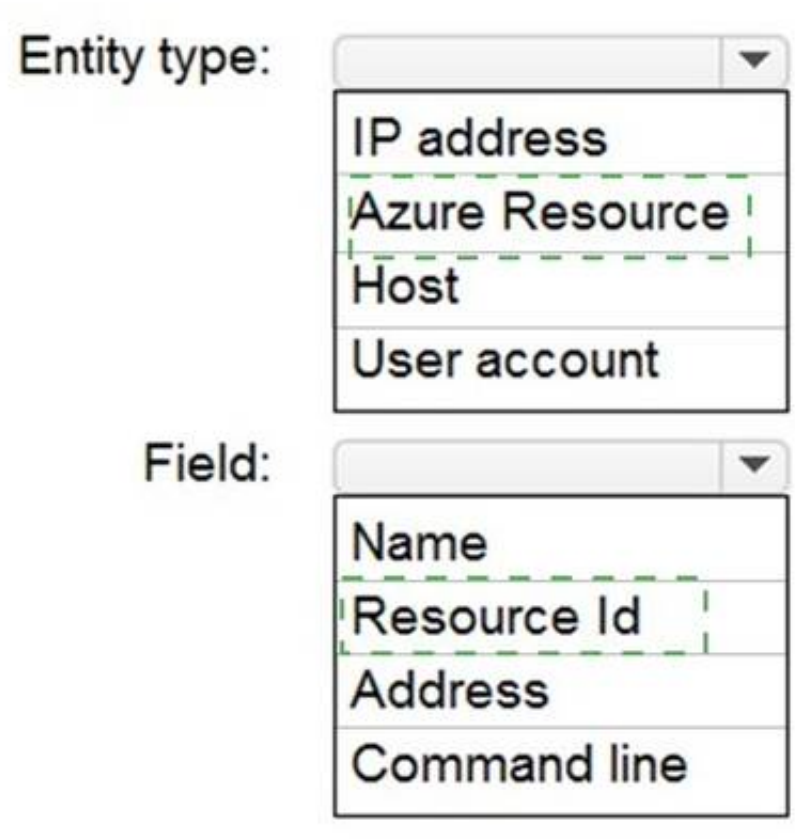
NEW QUESTION 44
HOTSPOT - (Topic 4)
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

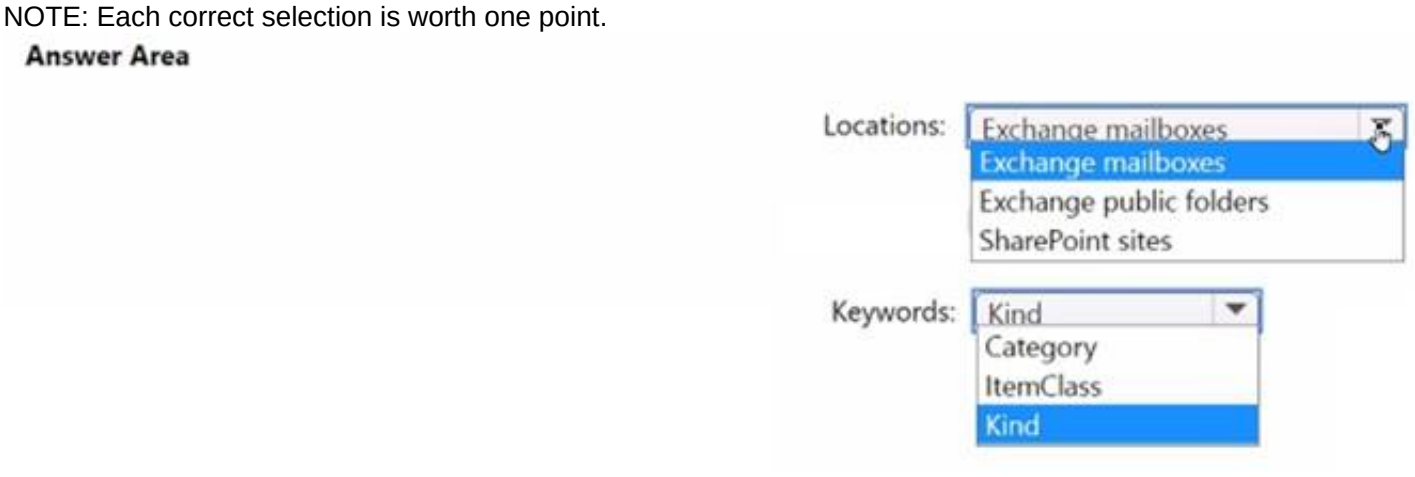


NEW QUESTION 48
- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
• App name: App1
• IP address: 192.168.1.2
• Computer name: Device1
• Used client 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 51
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.
How should you configure the content search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 54
- (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 55

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 60
- (Topic 4)
Your company has an on-premises network that uses Microsoft Defender for Identity.
The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.
You need remediate the security risk. What should you do?

A. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.
B. Modify the properties of the computer objects listed as exposed entities.
C. Disable legacy protocols on the computers listed as exposed entities.
D. Enforce LDAP signing on the computers listed as exposed entities.

Answer: B

Explanation:
To remediate the security risk associated with unsecure Kerberos delegation, you should modify the properties of the computer objects listed as exposed entities. Specifically, you should set the Kerberos delegation settings to either 'Trust this computer for delegation to any service' or 'Trust this computer for delegation to specified services only'. This will ensure that the computer is not allowed to use Kerberos delegation to access other computers on the network. Reference: https://docs.microsoft.com/en- us/windows/security/identity-protection/microsoft-defender-for-identity/configure-kerberos- delegation

NEW QUESTION 64
- (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 68
- (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

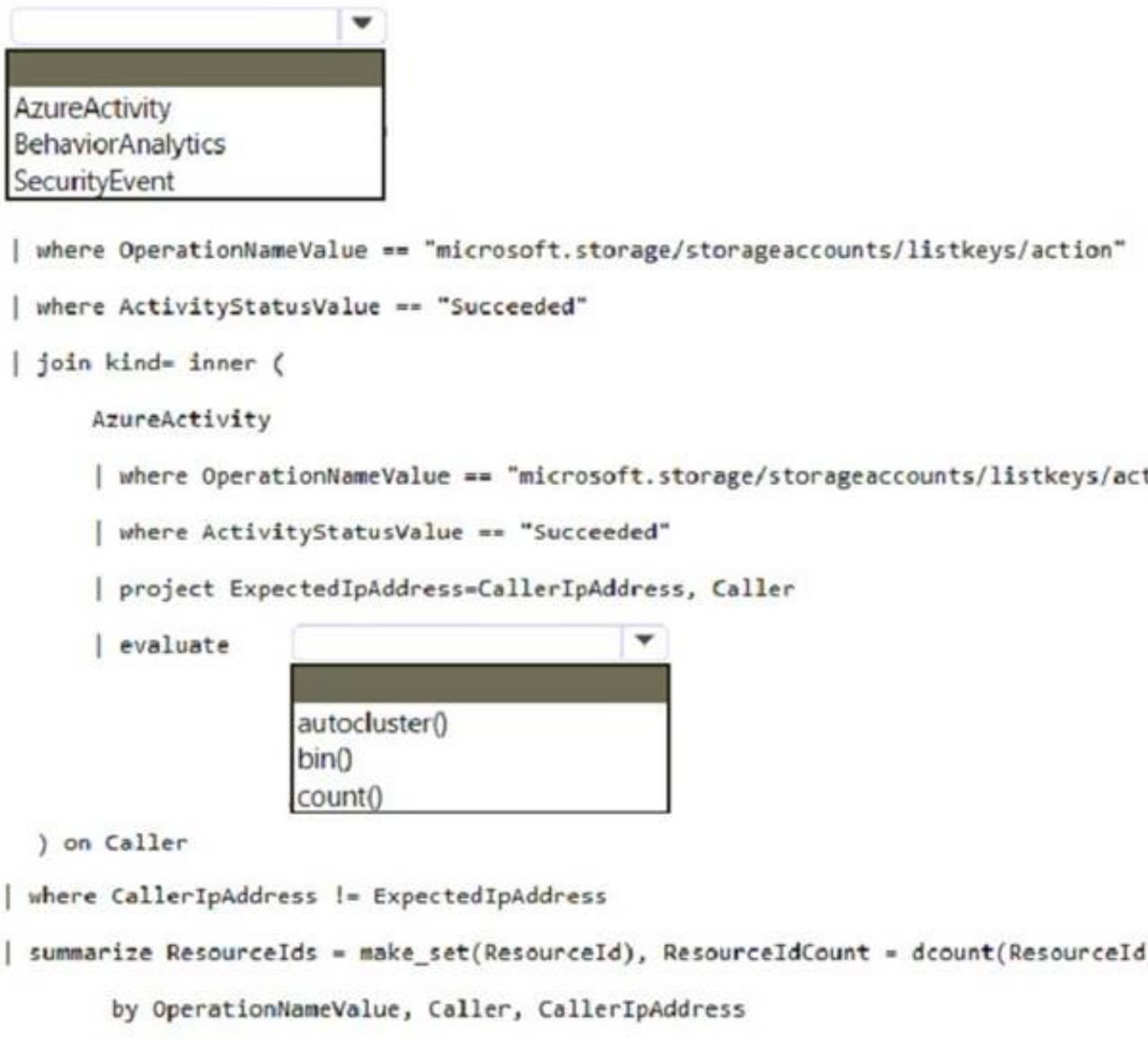
Explanation:
You can use alerts suppression rules to suppress false positives or other unwanted
security alerts from Defender for Cloud.
Note: To create a rule directly in the Azure portal:
* 1. From Defender for Cloud's security alerts page:
Select the specific alert you don't want to see anymore, and 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 73
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You have a GitHub account named Account1 that contains 10 repositories.
You need to ensure that Defender for Cloud can assess the repositories in Account1. What should you do first in the Microsoft Defender for Cloud portal?

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

Answer: A

NEW QUESTION 77
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 79
- (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 83
- (Topic 4)
You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

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

Answer: C

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

NEW QUESTION 88
- (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online. You delete users from the subscription.
You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.
What should you use?

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

Answer: C

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

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

NEW QUESTION 92
- (Topic 4)
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?

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

Answer: B

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

NEW QUESTION 93
- (Topic 4)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

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

Answer: D

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

NEW QUESTION 94
- (Topic 4)
You need to correlate data from the SecurityEvent Log Anarytks table to meet the Microsoft Sentinel requirements for using UEBA. Which Log Analytics table should you use?

A. SentwlAuoNt
B. AADRiskyUsers
C. IdentityOirectoryEvents
D. Identityinfo

Answer: C

NEW QUESTION 99
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

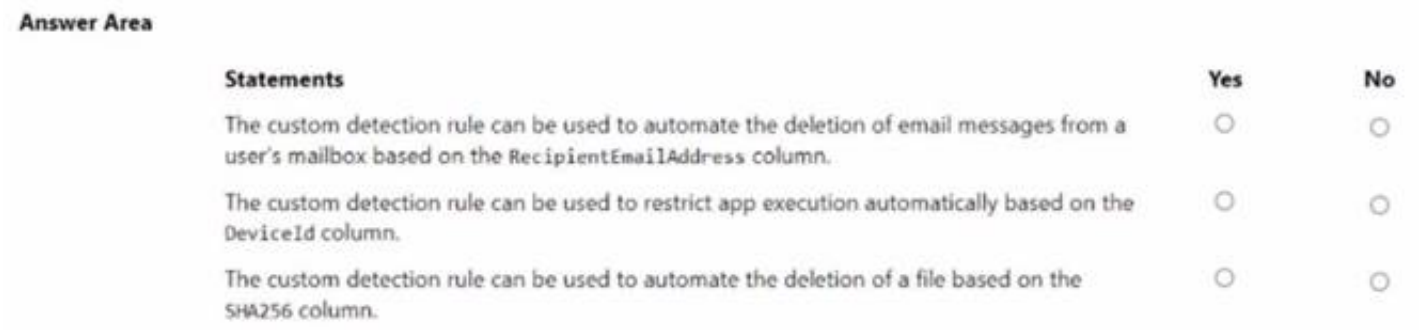
Answer: A

Explanation:

NEW QUESTION 102
HOTSPOT - (Topic 4)
You have a custom detection rule that includes the following KQL query.

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

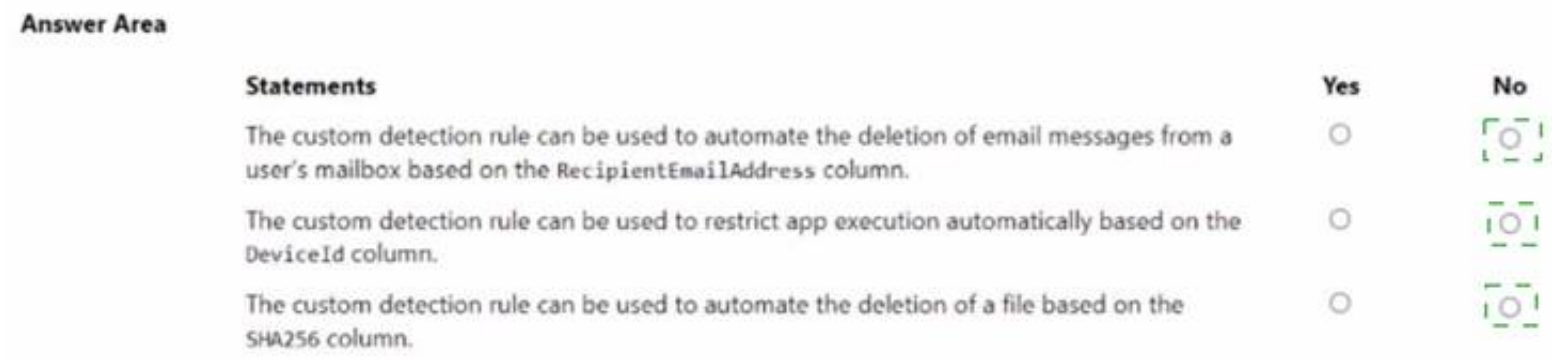
For each of the following statements, select Yes if True. Otherwise select No. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 106
- (Topic 4)
You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

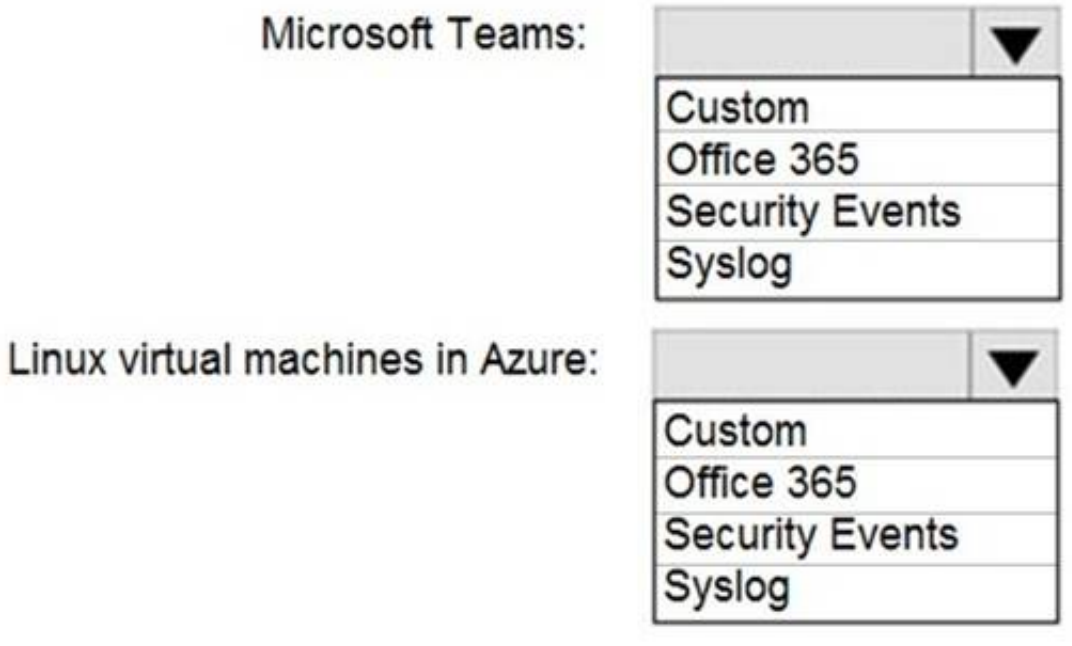
A. Key Vault firewalls and virtual networks
B. Azure Active Directory (Azure AD) permissions
C. role-based access control (RBAC) for the key vault
D. the access policy settings of the key vault

Answer: A

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

NEW QUESTION 111
HOTSPOT - (Topic 4)
You deploy Azure Sentinel.

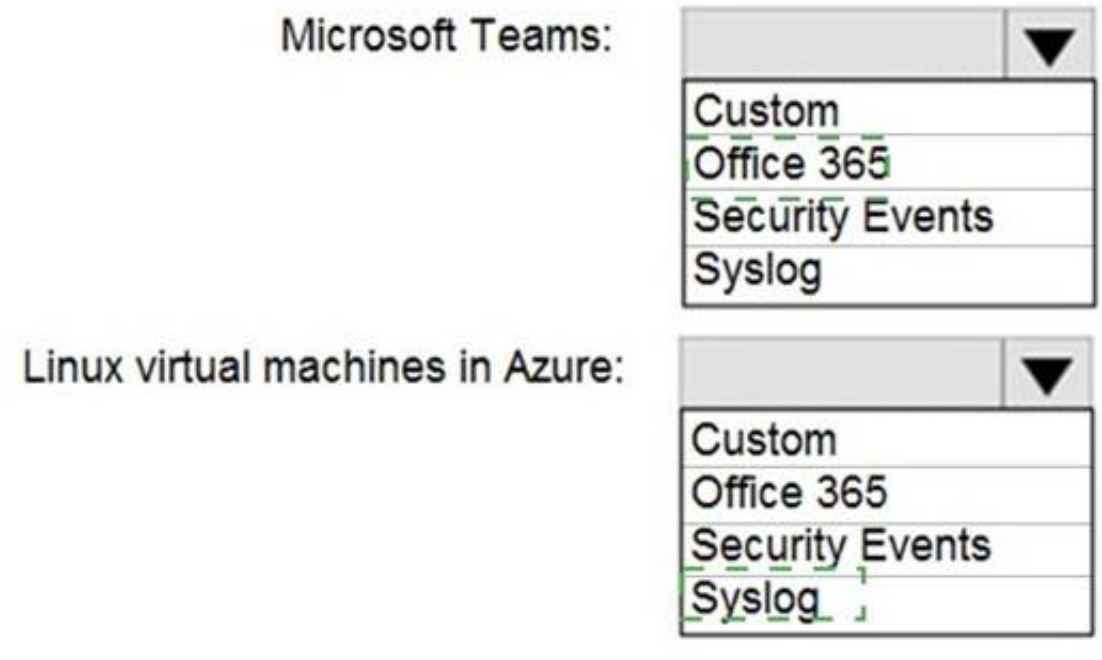
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct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



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 112
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 115
- (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 120
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
You need to add threat indicators for all the IP addresses in a range of 171.23.3432- 171.2334.63. The solution must minimize administrative effort.
What should you do in the Microsoft 365 Defender portal?

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

Answer: D

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

NEW QUESTION 122
- (Topic 4)
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

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

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

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

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

Answer: BC

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

NEW QUESTION 124
- (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?

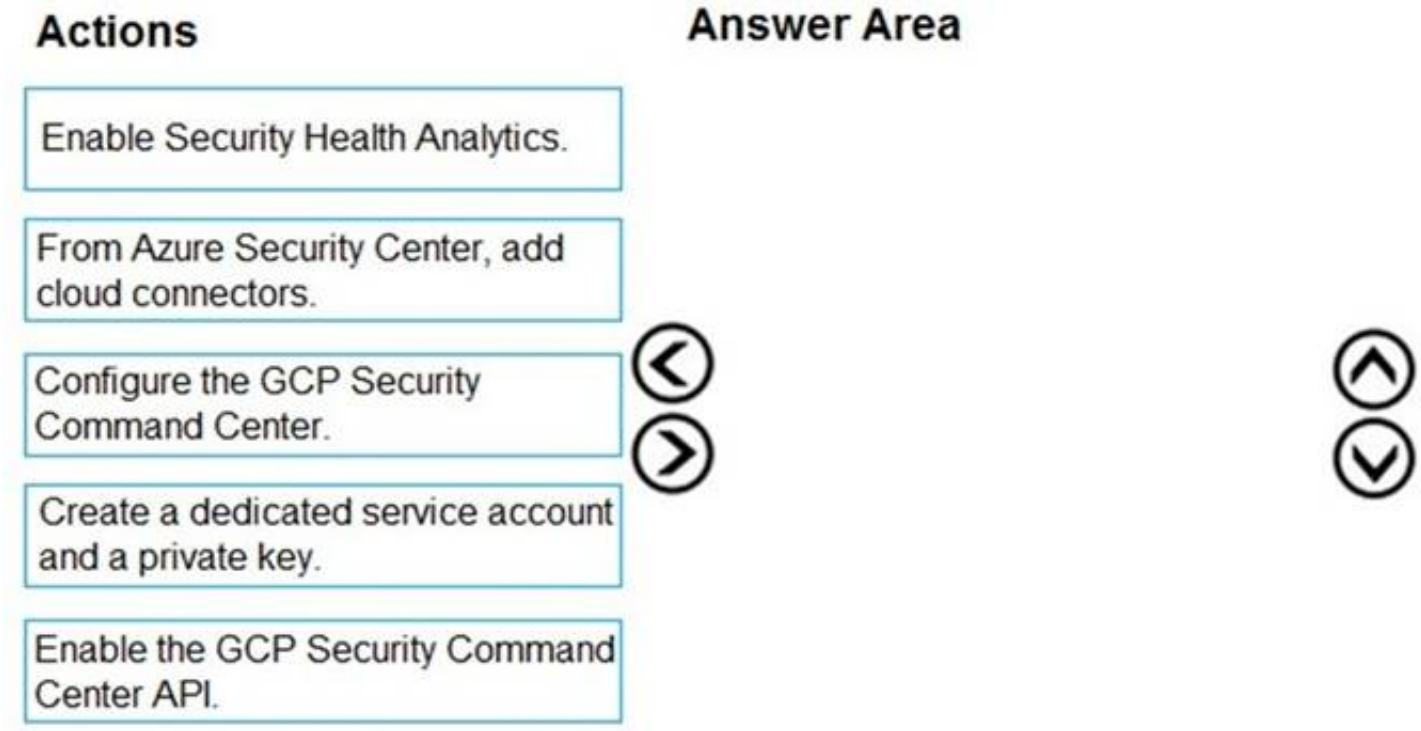
A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

Answer: A

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

NEW QUESTION 126
DRAG DROP - (Topic 4)
You have resources in Azure and Google cloud.

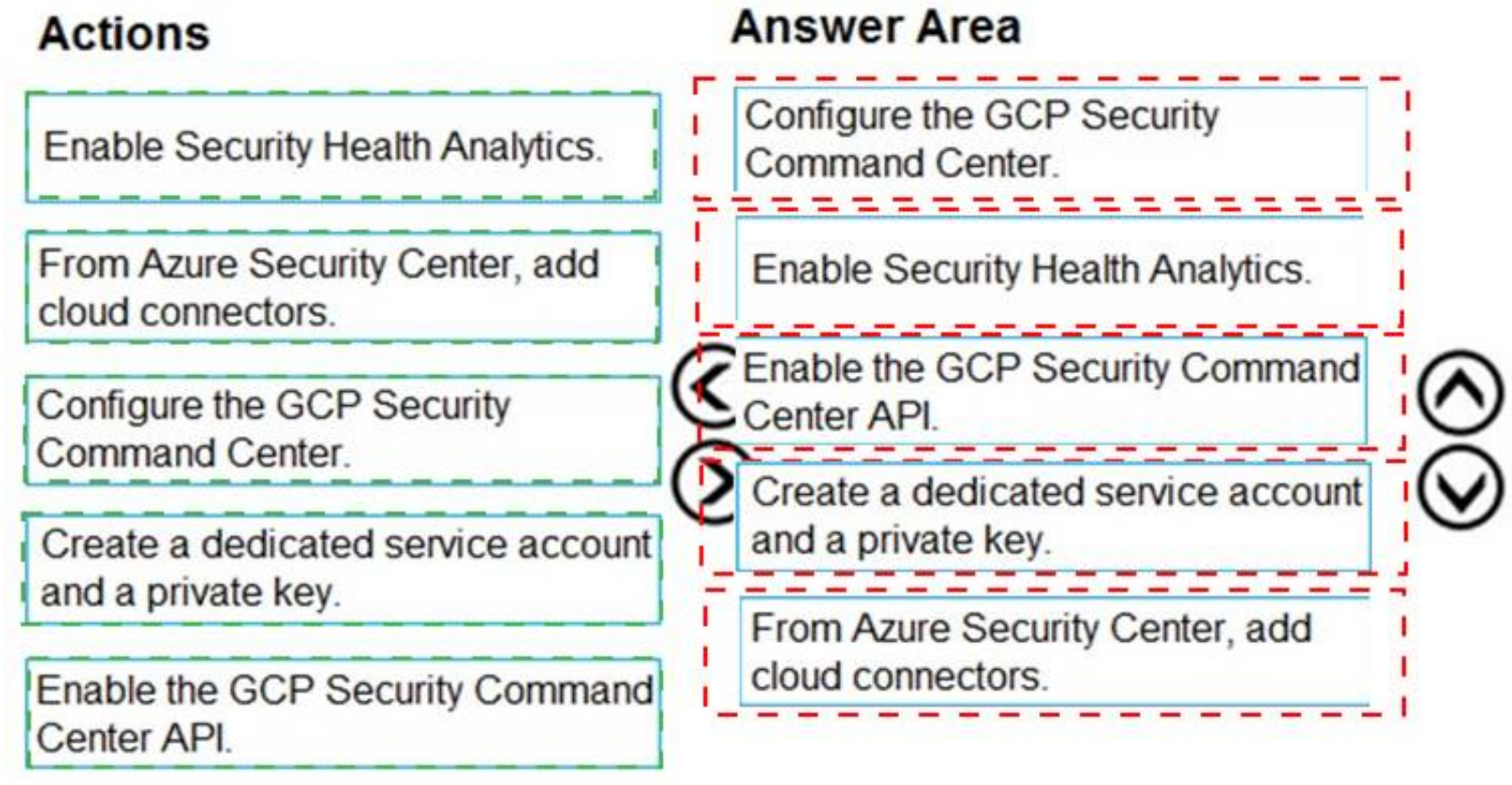
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



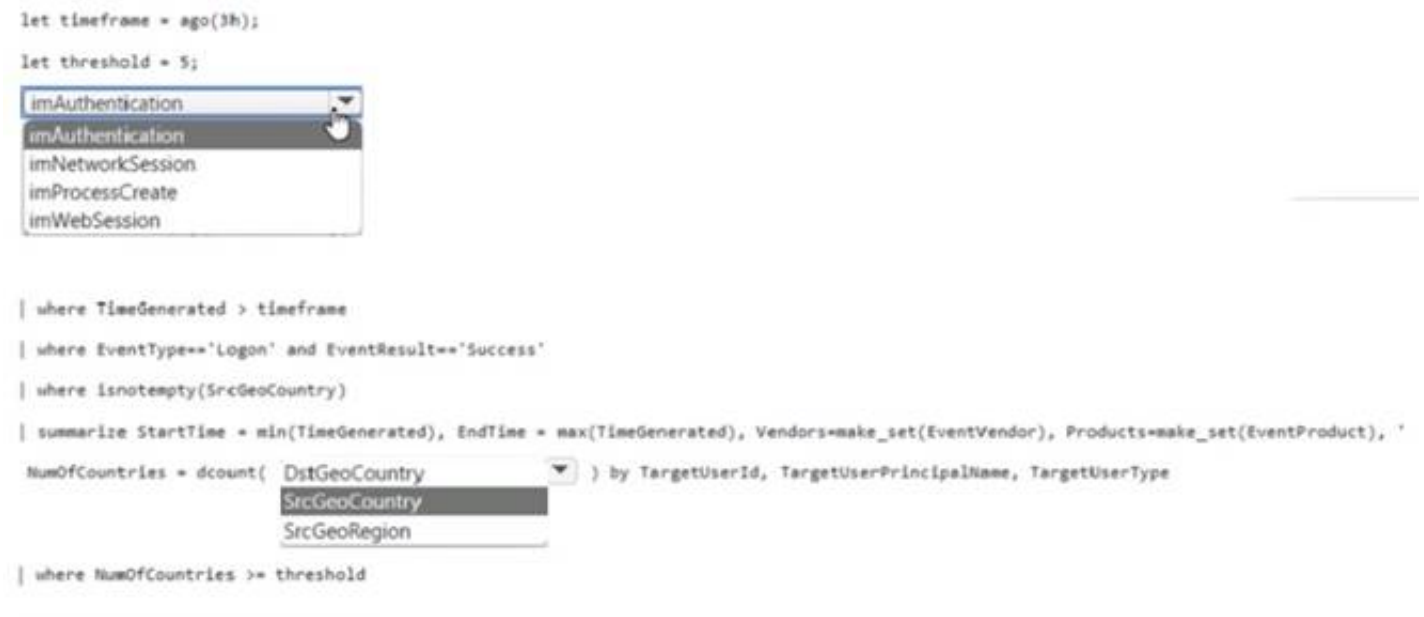
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 130
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace.
You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.
How should you complete the query? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point

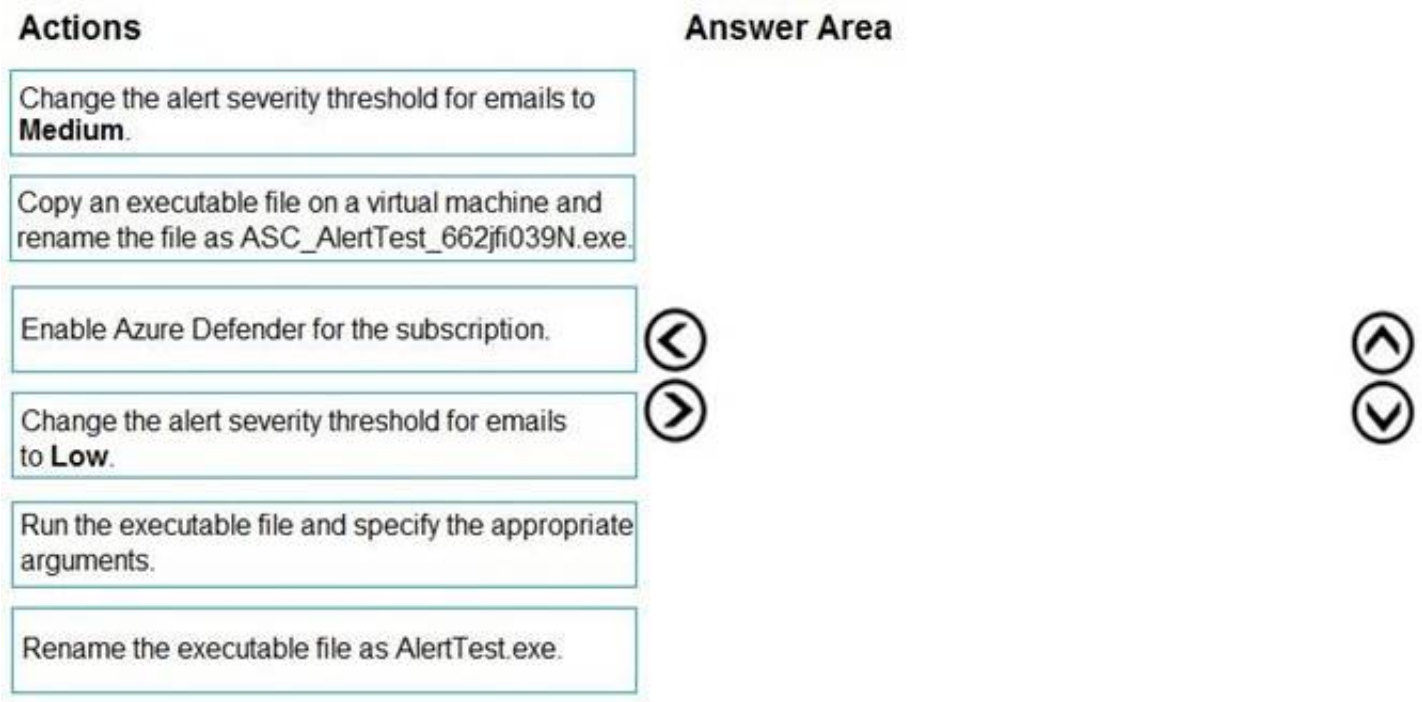


A. Mastered
B. Not Mastered

Answer: A

Explanation:

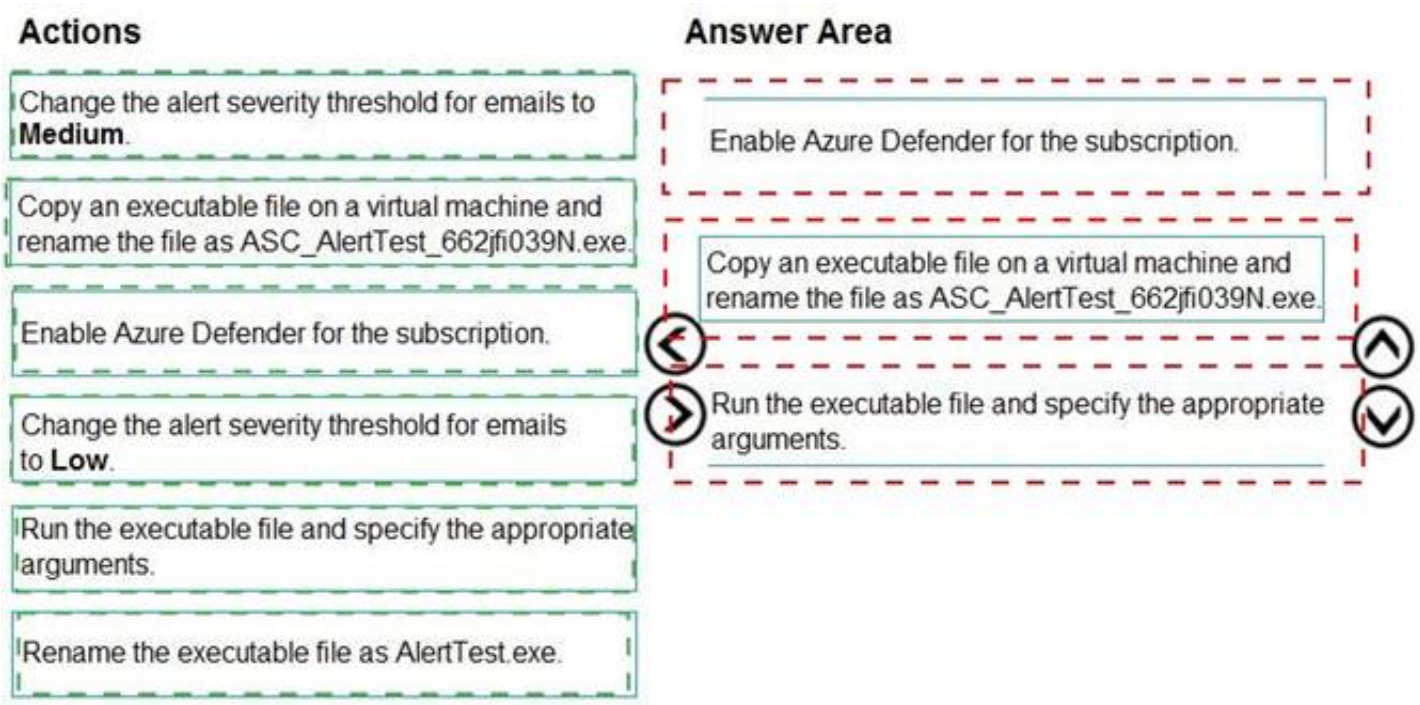
NEW QUESTION 133
DRAG DROP - (Topic 4)
DRAG DROP
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 136
- (Topic 4)
You need to identify which mean time metrics to use to meet the Microsoft Sentinel requirements. Which workbook should you use?

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

Answer: C

NEW QUESTION 138
HOTSPOT - (Topic 4)
You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 140
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.
How should you complete The KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area


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


NEW QUESTION 144
- (Topic 4)
Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely. What should you include in the solution?

A. a fraud alert
B. a user risk policy
C. a named location
D. a sign-in user policy

Answer: C

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

NEW QUESTION 149
- (Topic 4)

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

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

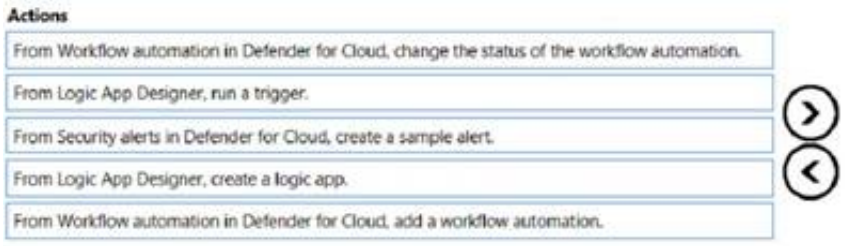
Answer: D

NEW QUESTION 153
- (Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned an Azure Active Directory Premium Plan 2 license
You need to identify whether the identity of User1 was compromised during the last 90 days.
What should you use?

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

Answer: B

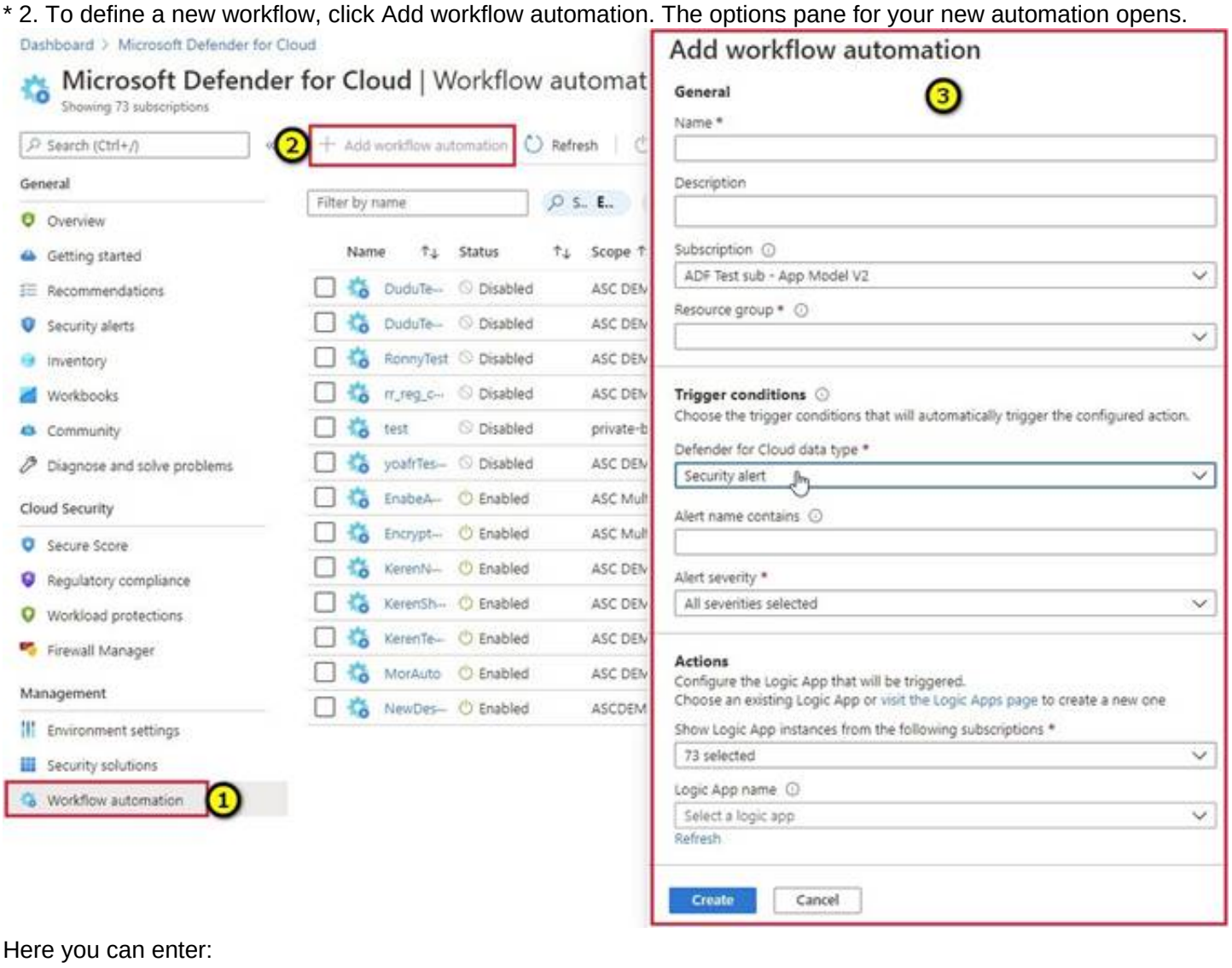
NEW QUESTION 158
DRAG DROP - (Topic 4)
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

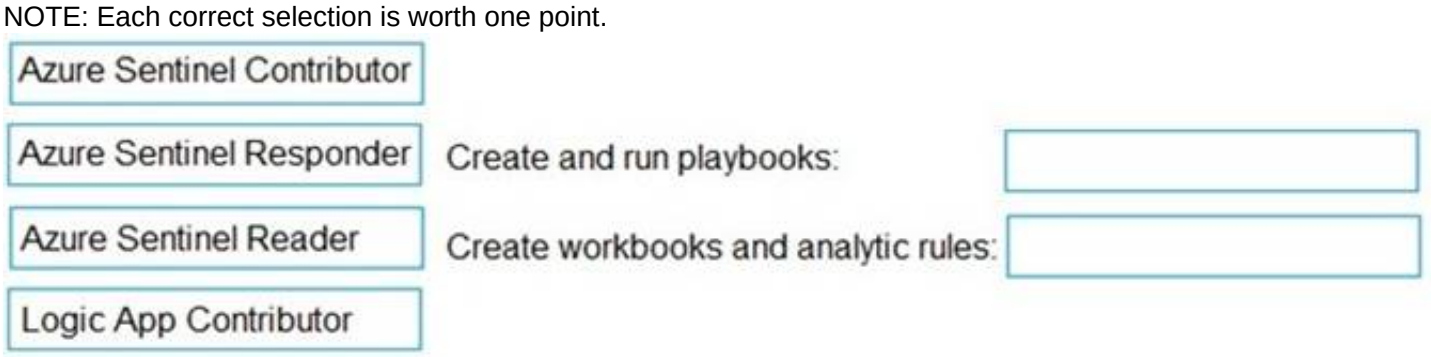
Explanation:
Step 1: From Logic App Designer, create a logic app.
Create a logic app and define when it should automatically run
* 1. From Defender for Cloud's sidebar, select Workflow automation.
* 2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.
The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
The Logic App that will run when your trigger conditions are met.
* 3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.
* 4. Etc.
Step 2: From Logic App Designer, run a trigger. Manually trigger a Logic App
You can also run Logic Apps manually when viewing any security alert or recommendation.
Step 3: From Workflow automation in Defender for cloud, add a workflow automation. Configure workflow automation at scale using the supplied policies
Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.

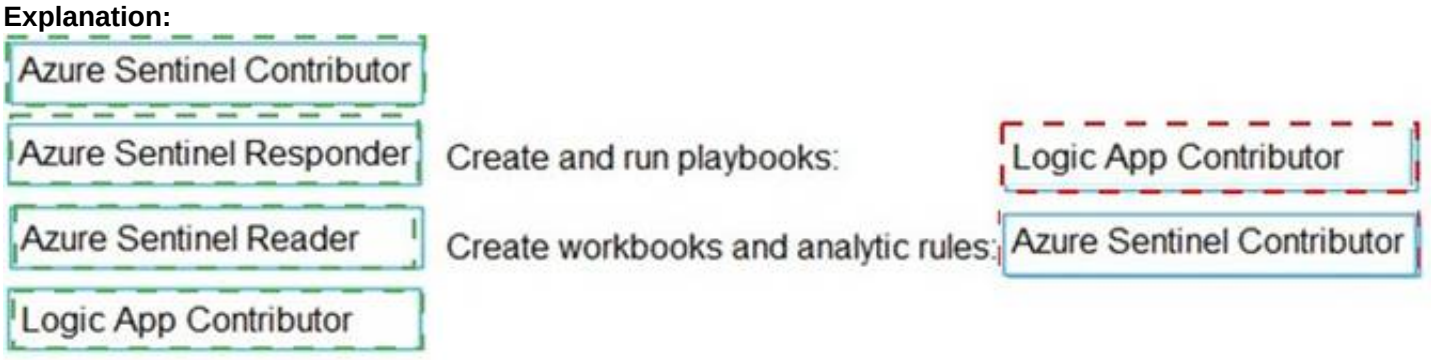
NEW QUESTION 161
DRAG DROP - (Topic 4)
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups. You need to delegate the following tasks:
? Create and run playbooks
? Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



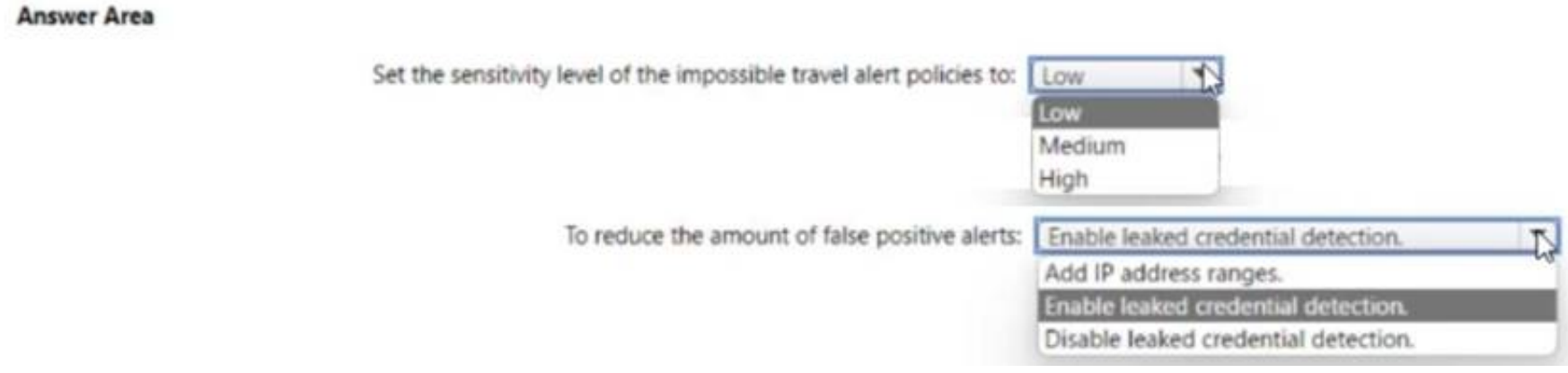
NEW QUESTION 165
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

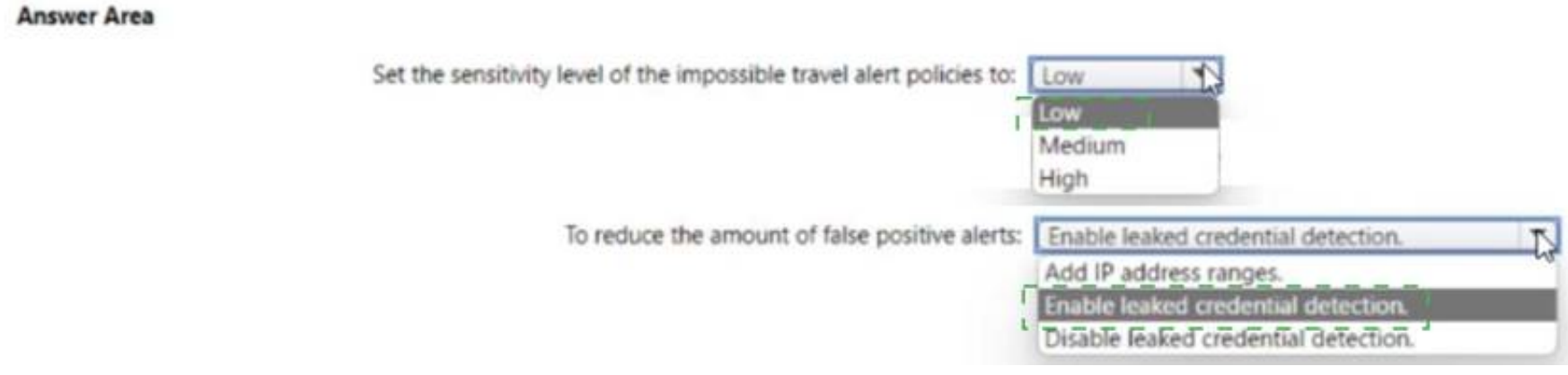
NEW QUESTION 170
HOTSPOT - (Topic 4)
You need to meet the Microsoft Defender for Cloud Apps requirements
What should you do? To answer. select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 171
- (Topic 4)
You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.
You need to create a query that will be used to display the time chart. What should you include in the query?

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

Answer: B

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

NEW QUESTION 176
- (Topic 4)
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

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

Answer: A

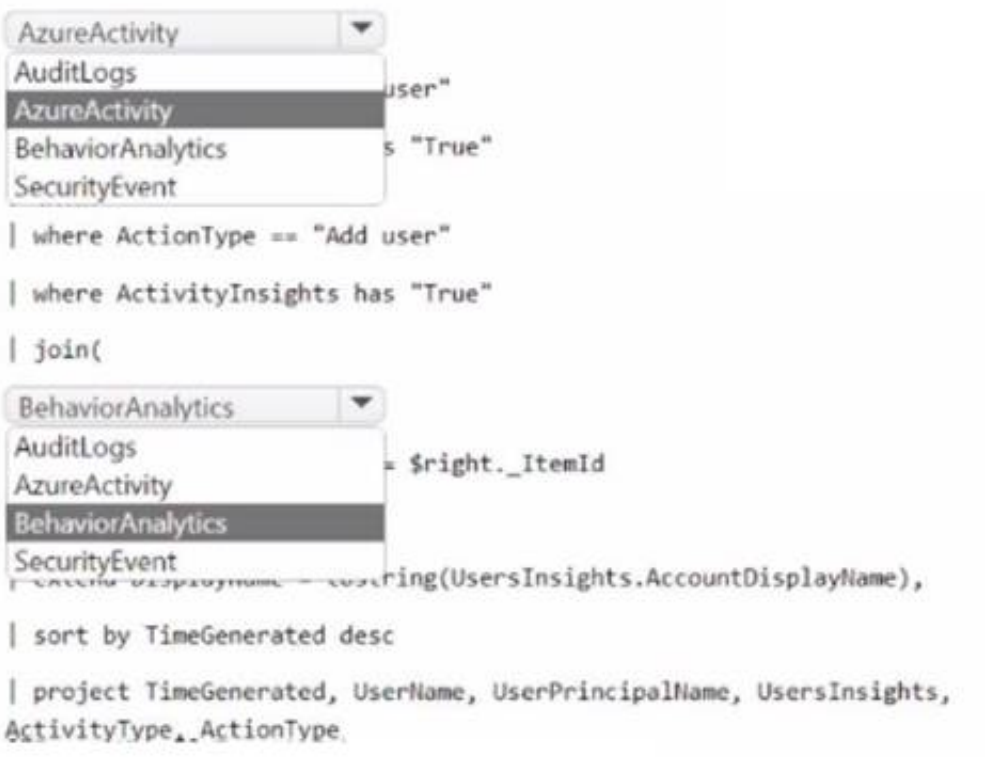
NEW QUESTION 177
- (Topic 4)
You need to meet the Microsoft Sentinel requirements for App1. What should you configure for App1?

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

Answer: B

NEW QUESTION 182
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

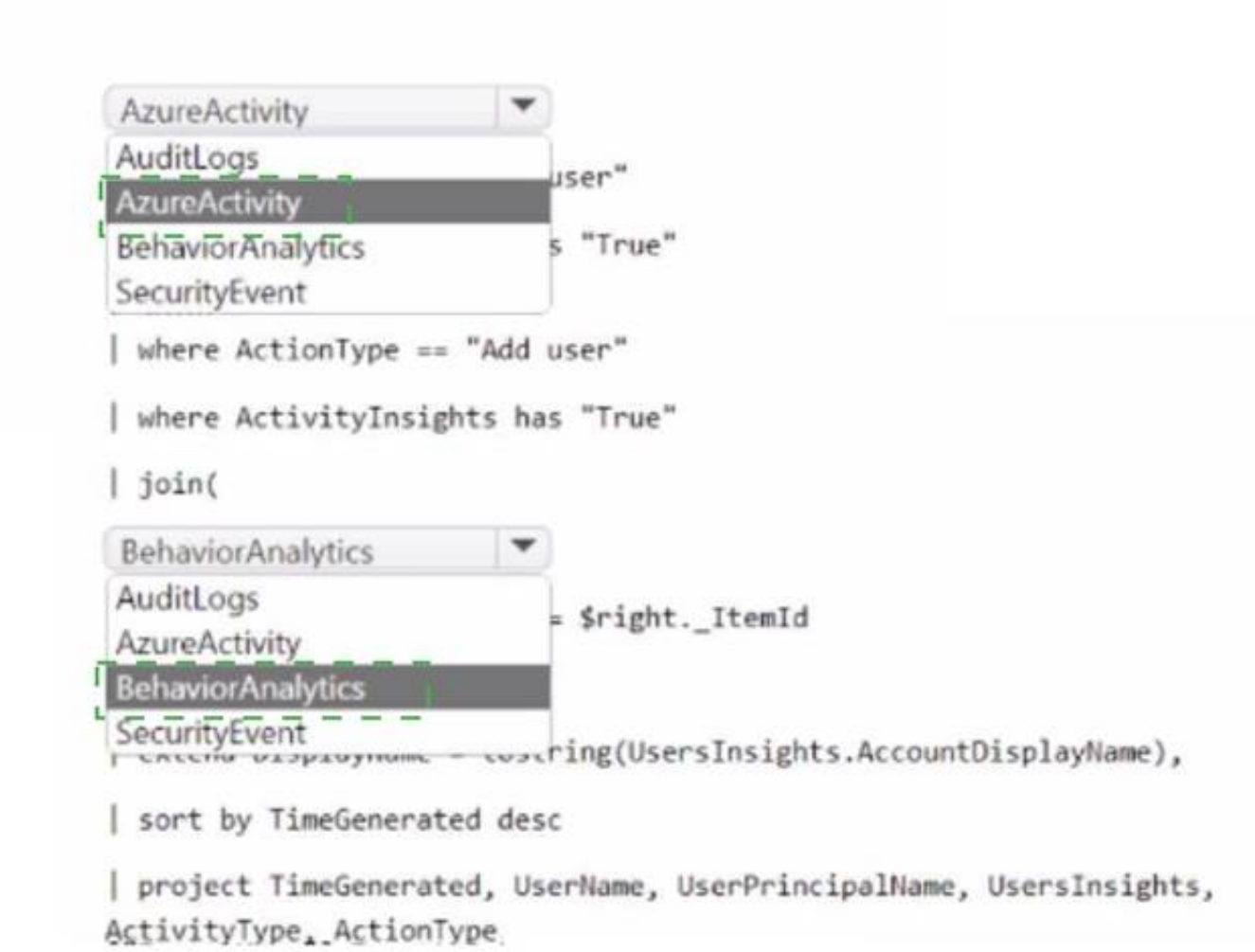


A. Mastered
B. Not Mastered

Answer: A

Explanation:

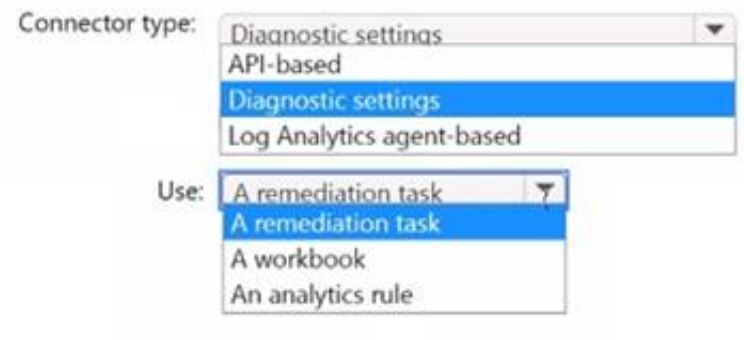
Answer Area



NEW QUESTION 184
HOTSPOT - (Topic 4)
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.

Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

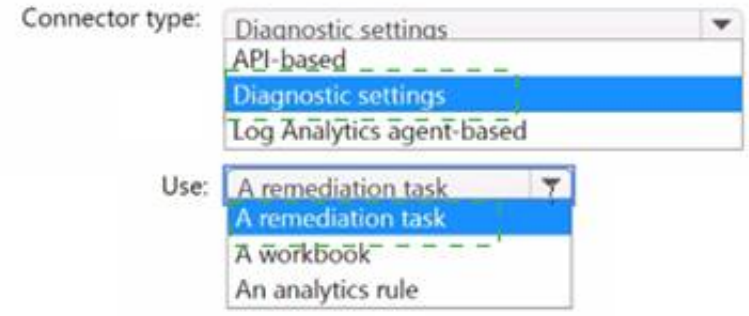


A. Mastered
B. Not Mastered

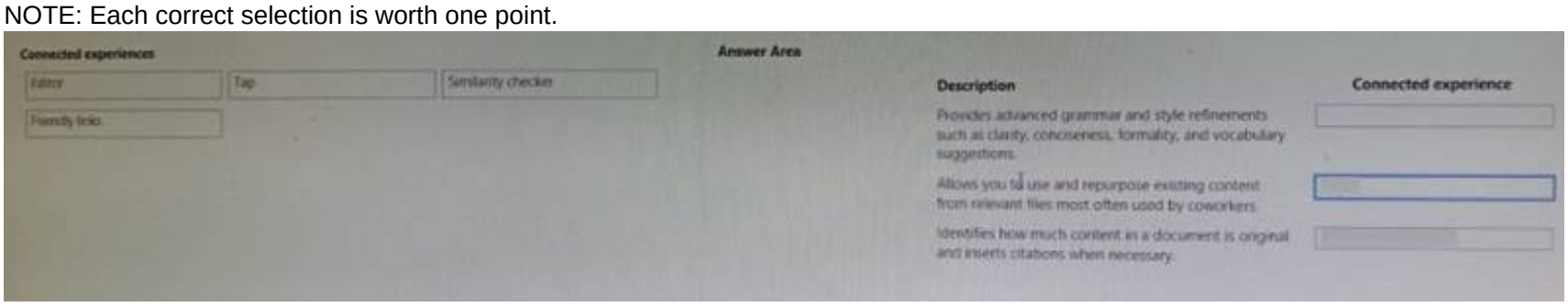
Answer: A

Explanation:

Answer Area



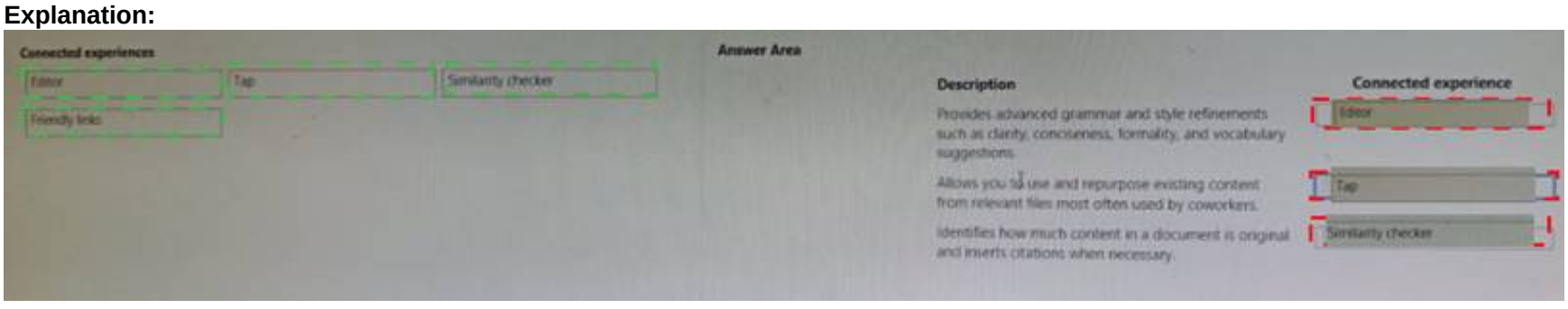
NEW QUESTION 185
DRAG DROP - (Topic 4)
A company wants to analyze by using Microsoft 365 Apps.
You need to describe the connected experiences the company can use.
Which connected experiences should you describe? To answer, drag the appropriate connected experiences to the correct description. Each connected experience may be used once, more than once, or not at all. You may need to drag the split between panes or scroll to view content.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 189
- (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 191
- (Topic 4)
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

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

Answer: A

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

NEW QUESTION 193
- (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 194
- (Topic 4)
You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

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

Answer: D

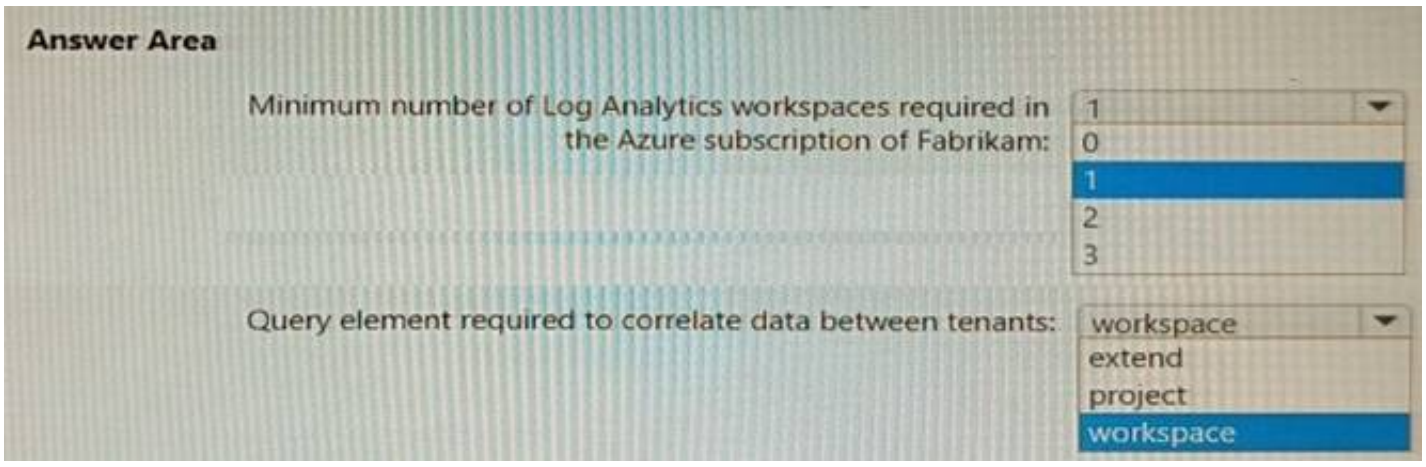
NEW QUESTION 199
- (Topic 4)
A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

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

Answer: A

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

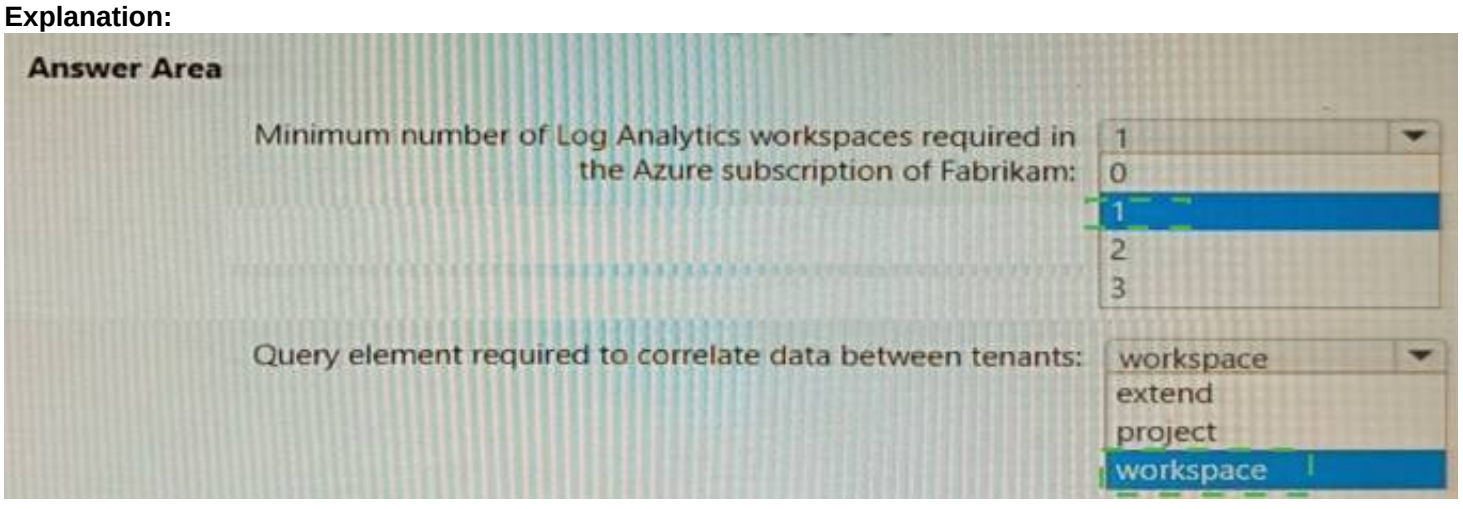
NEW QUESTION 200
HOTSPOT - (Topic 4)
You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 204
- (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

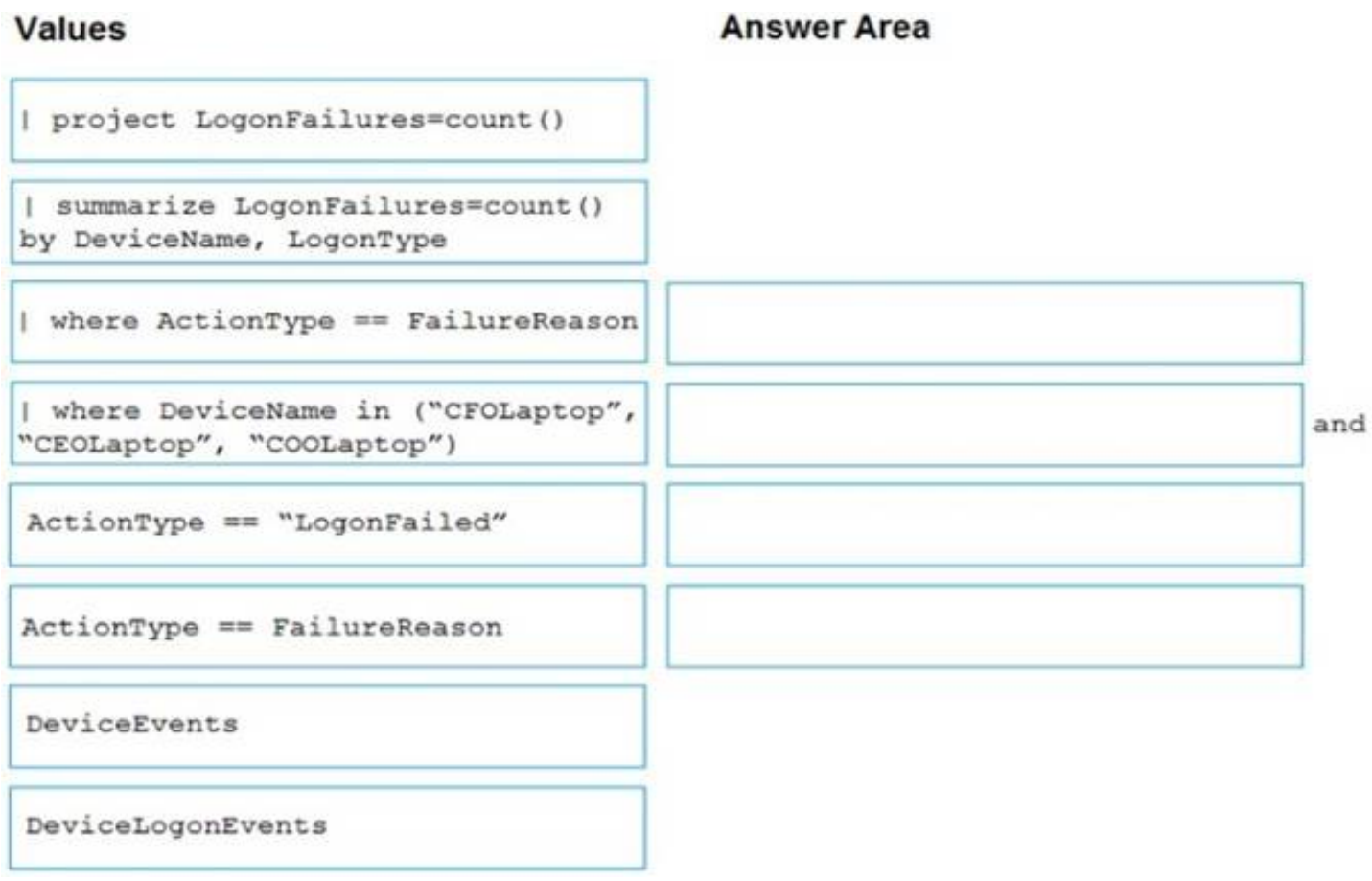
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION 207
- (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

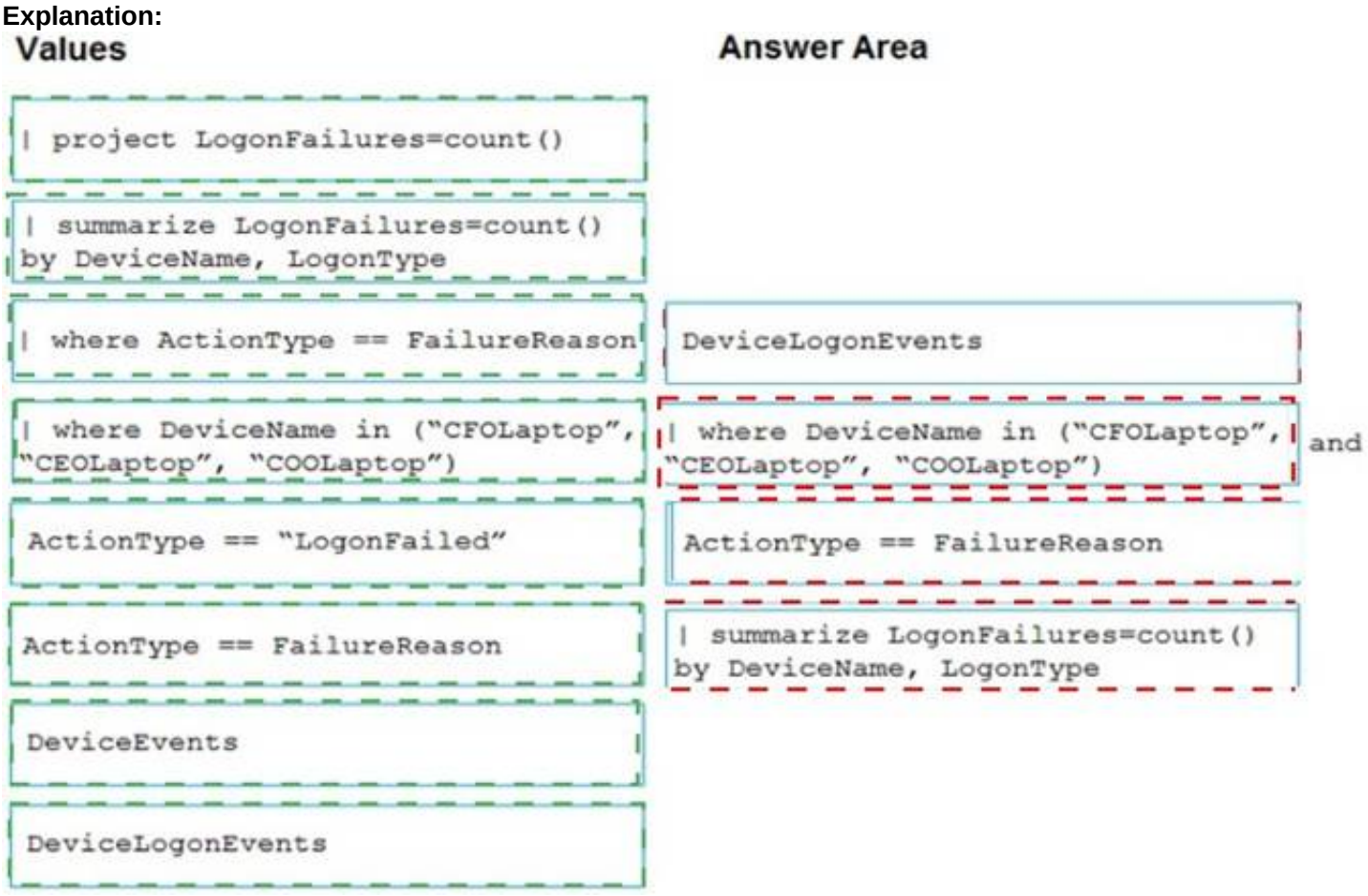
NEW QUESTION 209
DRAG DROP - (Topic 4)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 212
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

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

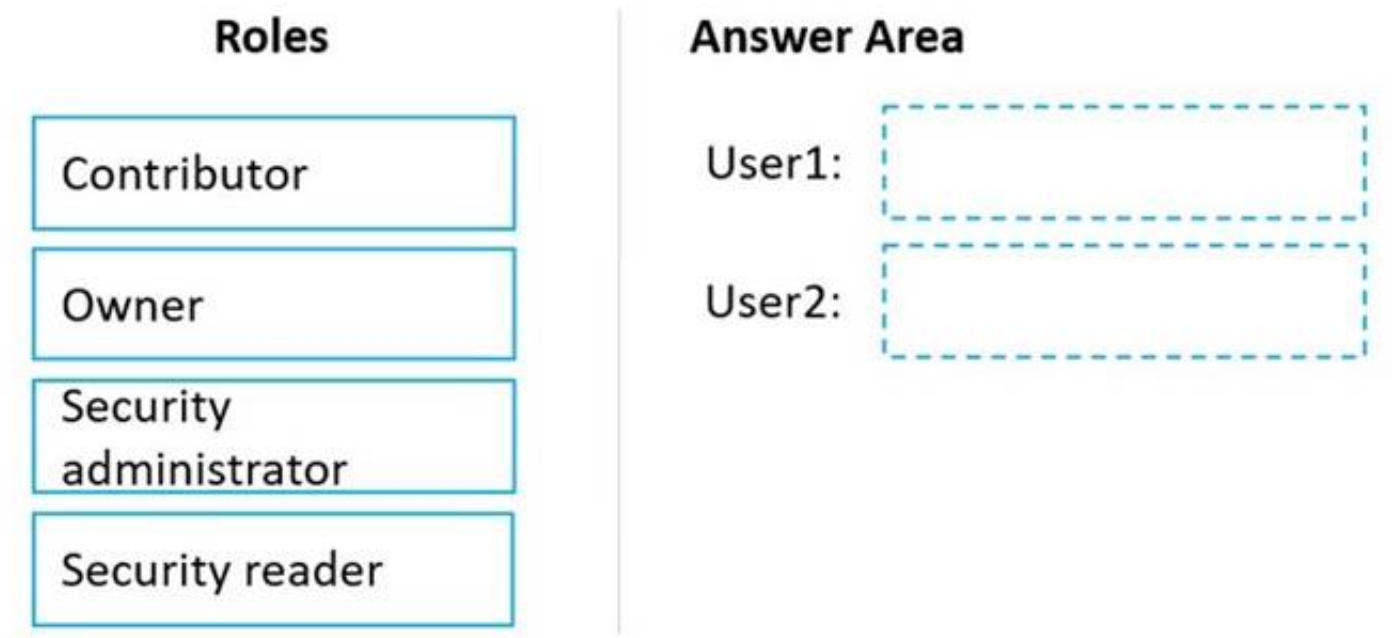
Answer: D

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

NEW QUESTION 216
DRAG DROP - (Topic 4)
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

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

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 218
- (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

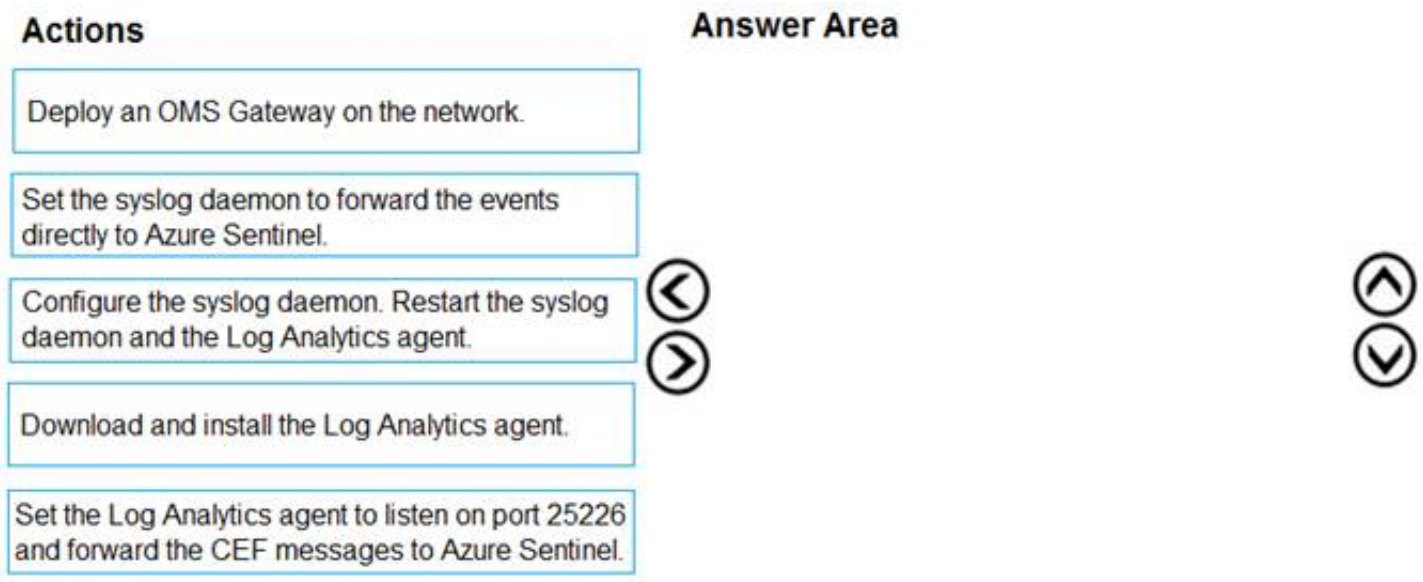
NEW QUESTION 221
- (Topic 4)
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

Answer: BE

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

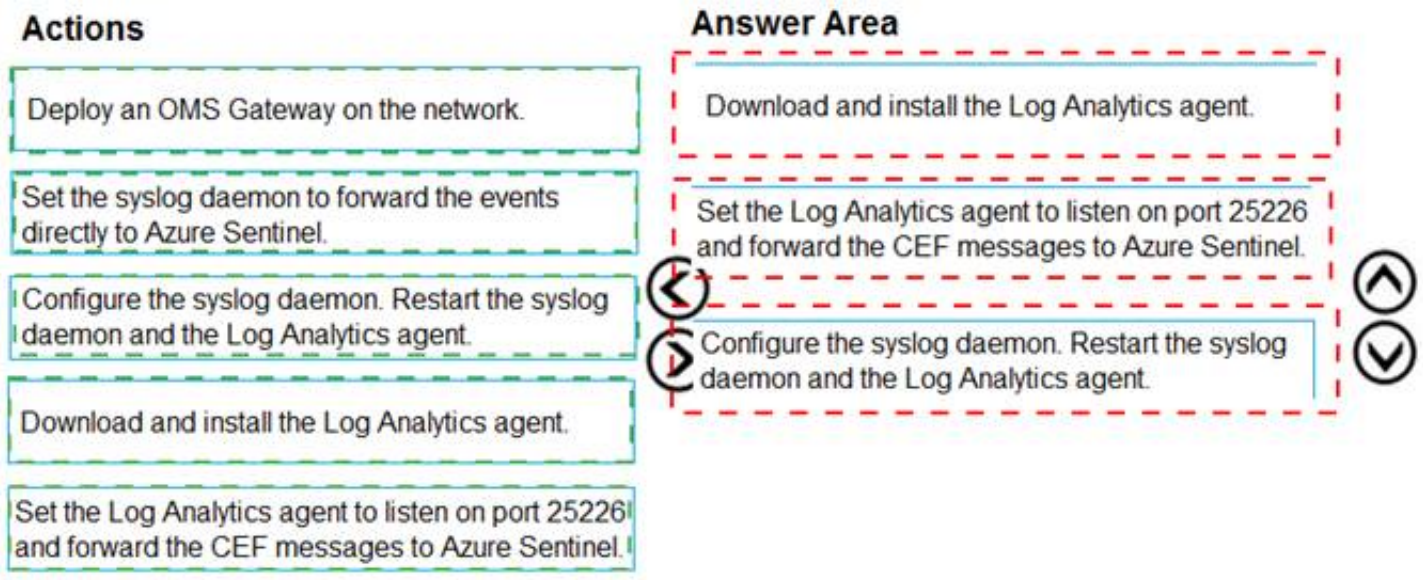
NEW QUESTION 222
DRAG DROP - (Topic 4)
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 227
- (Topic 4)
You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.
You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.
What should you do first?

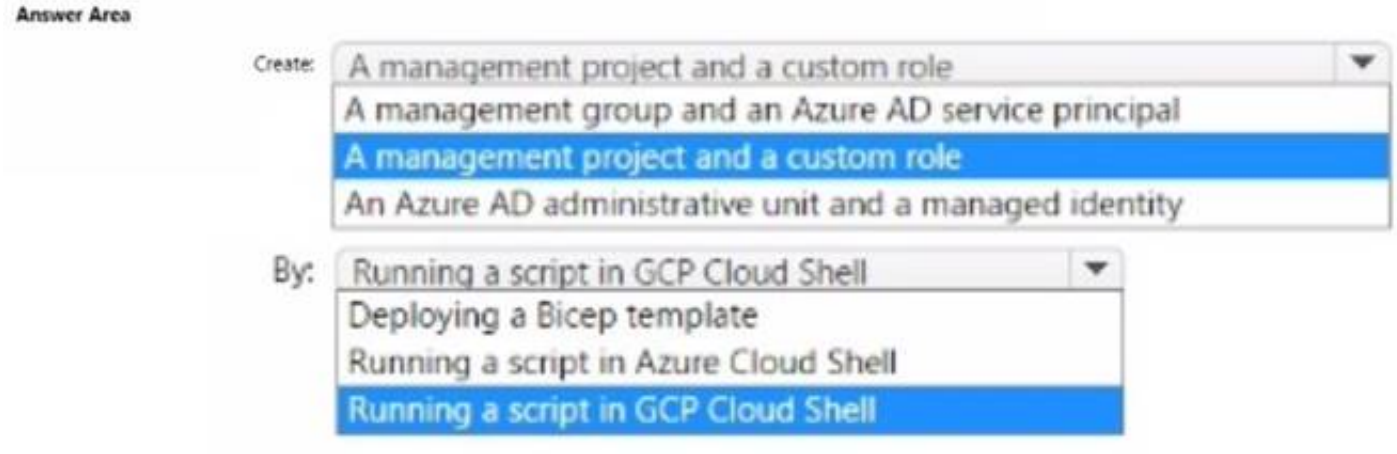
A. From Azure Security Center, add a workflow automation.
B. On VM1, run the Get-MPThreatCatalog cmdlet.
C. On VM1 trigger a PowerShell alert.
D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Answer: C

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

NEW QUESTION 232

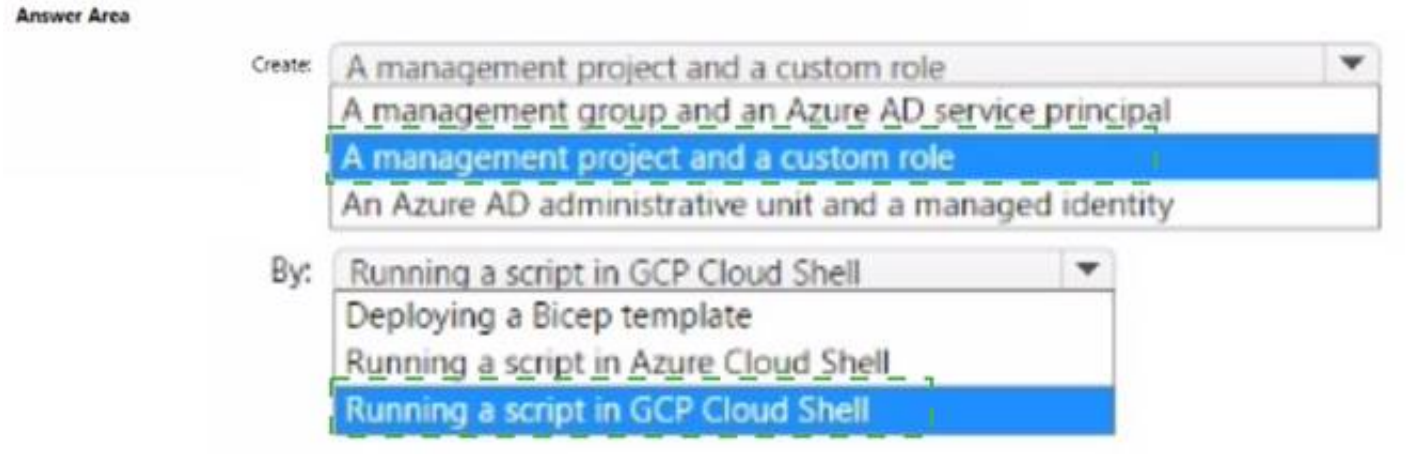
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud. You create a Google Cloud Platform (GCP) organization named GCP1.
You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded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



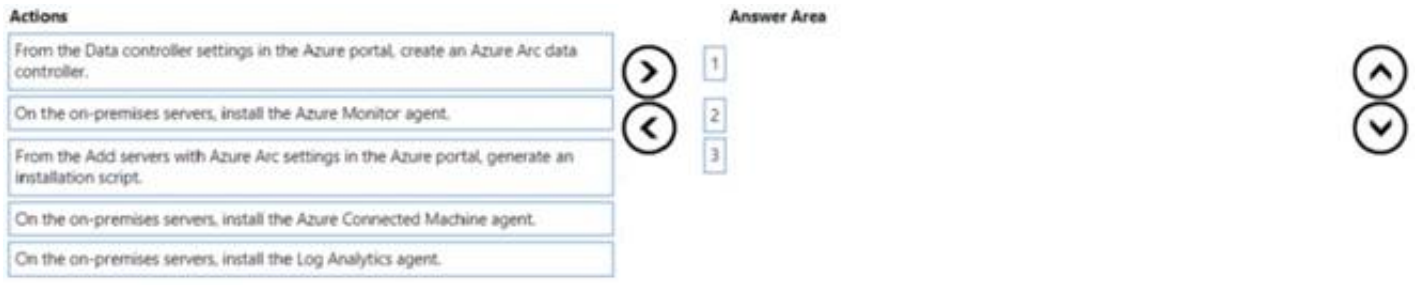
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 236
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 241
- (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 245
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You 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 246
- (Topic 4)
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

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

Answer: D

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

NEW QUESTION 250
- (Topic 4)
You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

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

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

Answer: AE

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

NEW QUESTION 253
- (Topic 4)

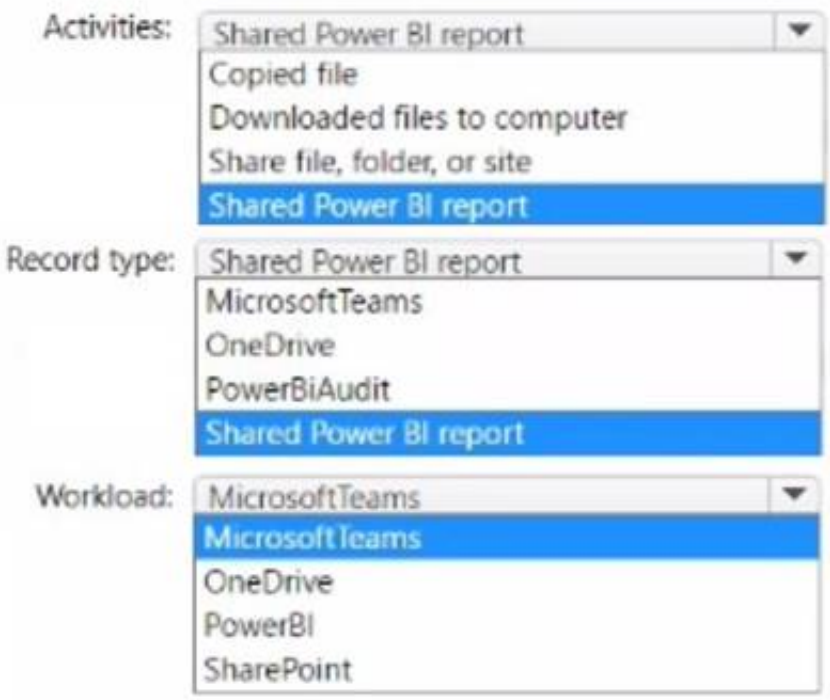
You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.
You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the fallowing requirements:
• Minimize administrative effort
• Minimize the parsing required to read log data What should you configure?

A. REST API integration
B. a SysJog connector
C. a Log Analytics Data Collector API
D. a Common Event Format (CEF) connector

Answer: B

NEW QUESTION 254
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.
User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.
You need to identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 257
- (Topic 4)
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 260
- (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The

solution must minimize development effort.
What should you use to create the visuals?

A. plotly
B. TensorFlow
C. msticpy
D. matplotlib

Answer: C

Explanation:
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:
Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX. Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
Visualization tools using event timelines, process trees, and geo mapping.
Advanced analyses, such as time series decomposition, anomaly detection, and clustering.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started https://msticpy.readthedocs.io/en/latest/

NEW QUESTION 264
- (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 265
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report.
Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 268
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 273
- (Topic 4)
You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.
You need to create a new near-real-time (NRT) analytics rule that will use the playbook. What should you configure for the rule?

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

Answer: B

NEW QUESTION 278
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

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

Answer: C

Explanation:
Reference:

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

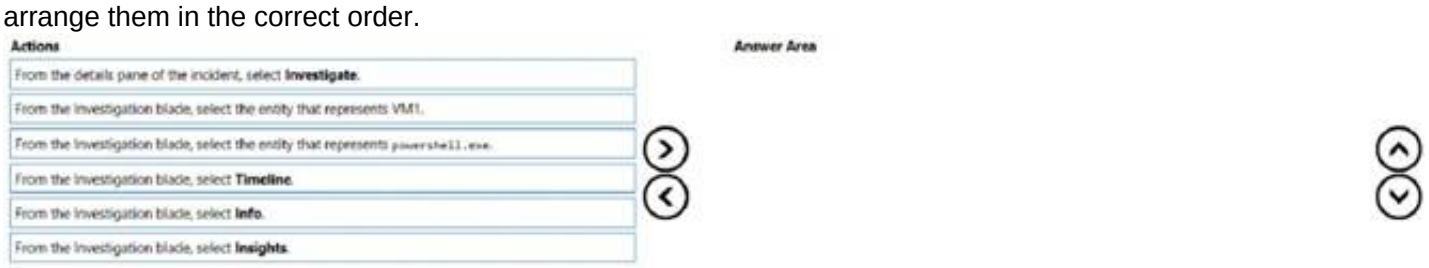
NEW QUESTION 279
HOTSPOT - (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.
You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.
Which roles should you assign to Used? To answer select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 283
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.
You receive an alert for suspicious use of PowerShell on VM1.
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:
? The modification of local group memberships
? The purging of event logs
Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: From the Investigation blade, select Insights
The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.
Step 2: From the Investigation blade, select the entity that represents VM1.
The Investigation Insights workbook is broken up into 2 main sections, Incident Insights
and Entity Insights.
Incident Insights

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.
Entity Insights
The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:
IP Address Account Host
URL
Step 3: From the details pane of the incident, select Investigate. Choose a single incident and click View full details or Investigate.

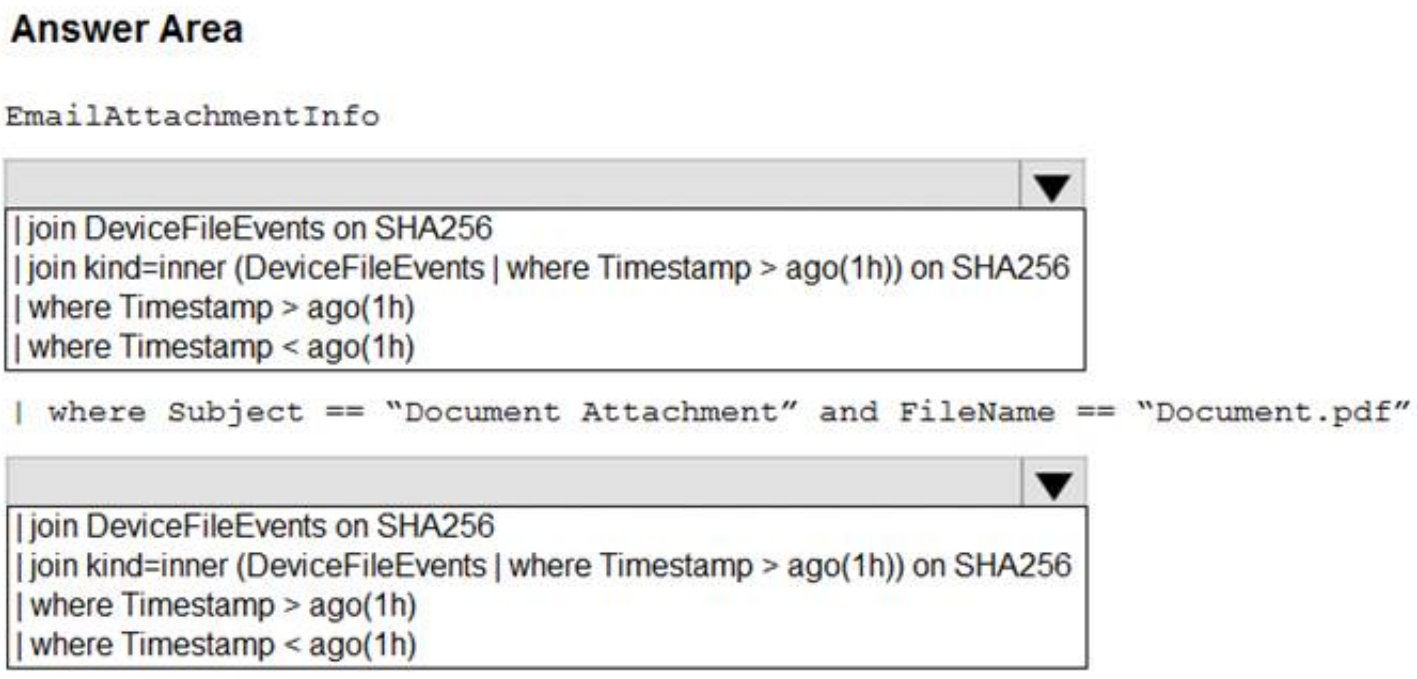
NEW QUESTION 286
DRAG DROP - (Topic 4)
You have a Microsoft Sentinel workspace that contains an Azure AD data connector. You need to associate a bookmark with an Azure AD-related incident.
What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content
NOTE: Each correct selection is worth one point.

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 287
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription.
You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:
• Only show emails sent during the last hour.
• Optimize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

```
EmailAttachmentInfo
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ]
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ]
```

NEW QUESTION 288
- (Topic 4)
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

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

Answer: C

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

NEW QUESTION 293
- (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 296
- (Topic 4)
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center. What should you do?

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

Answer: B

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

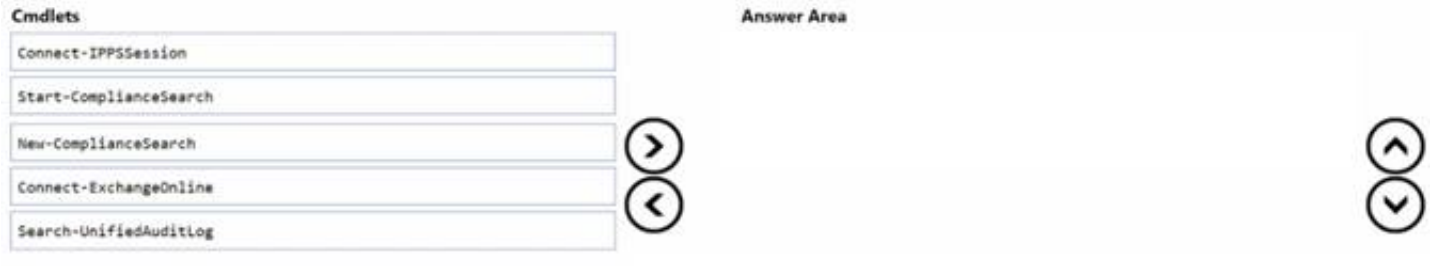
NEW QUESTION 299
- (Topic 4)
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).
You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

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

Answer: C

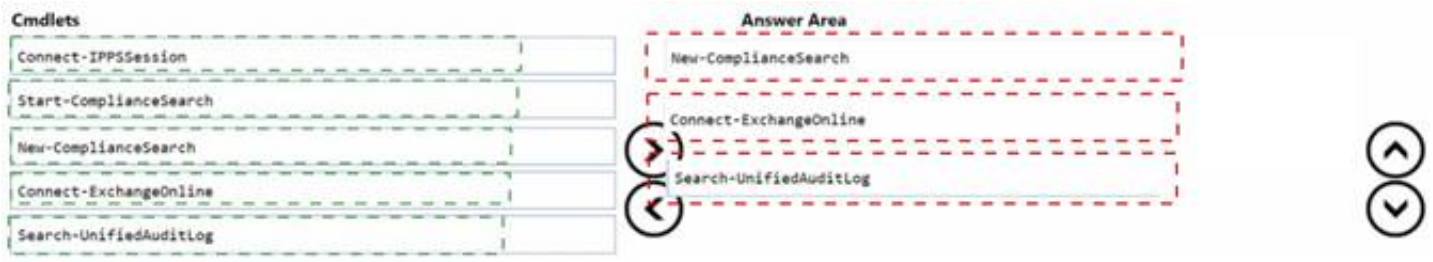
NEW QUESTION 301
DRAG DROP - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online. You need to identify phishing email messages.
Which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

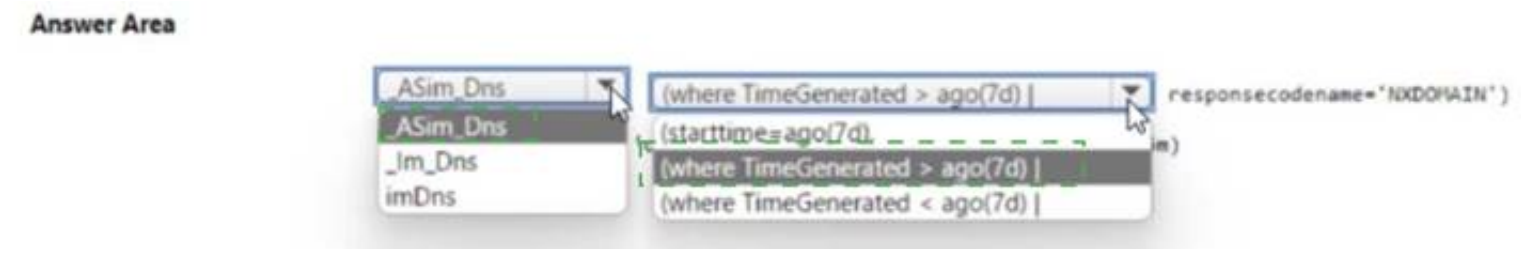


NEW QUESTION 305
HOTSPOT - (Topic 4)
You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query?
To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 309
- (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 310
- (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 311
- (Topic 4)
You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

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

Answer: B

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

NEW QUESTION 312
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-200 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-200 Product From:

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

Money Back Guarantee

SC-200 Practice Exam Features:

* SC-200 Questions and Answers Updated Frequently

* SC-200 Practice Questions Verified by Expert Senior Certified Staff

* SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year