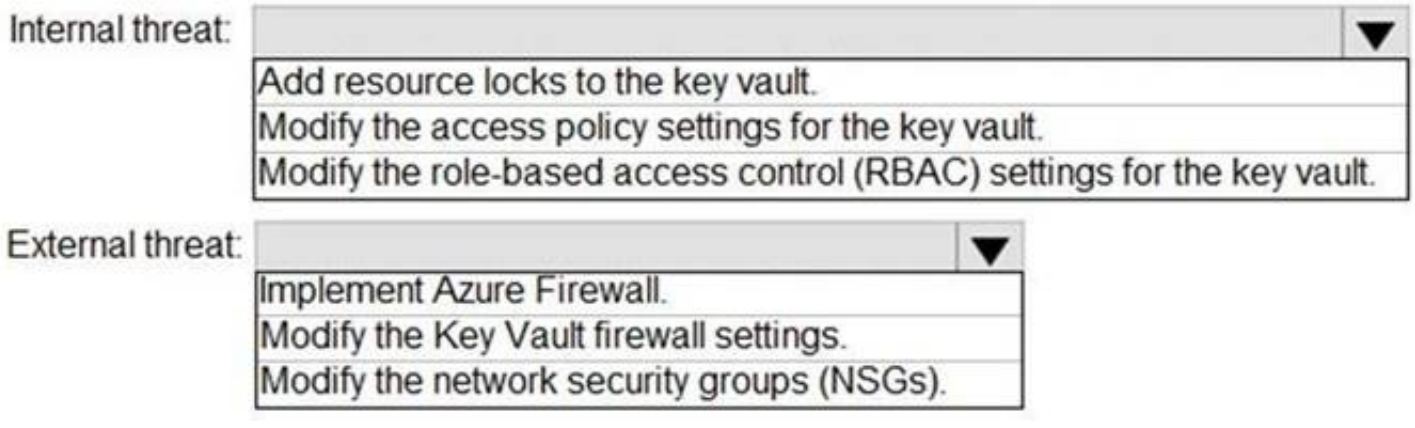
Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

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

Answer Area

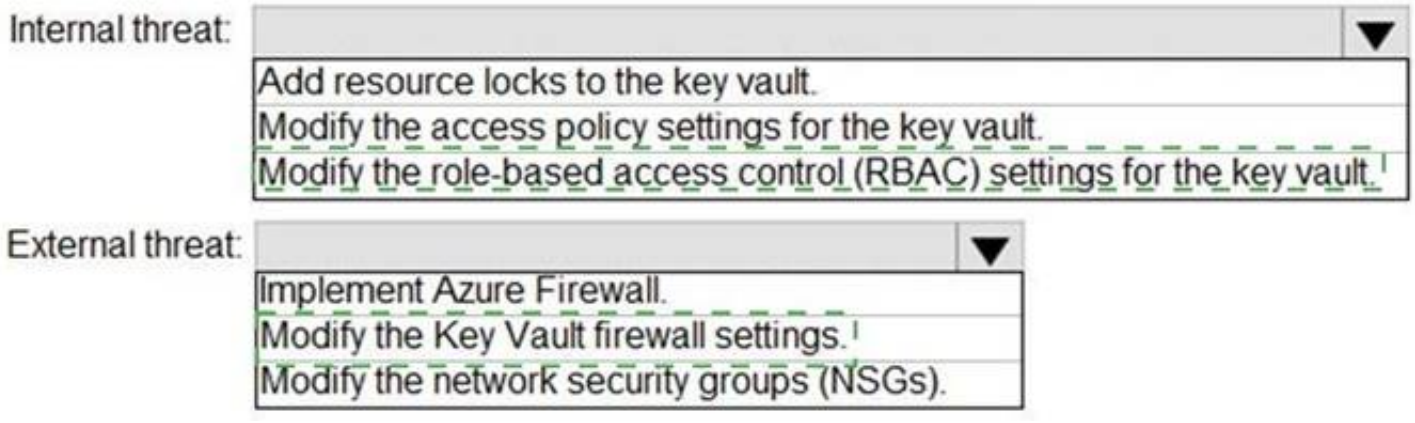


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



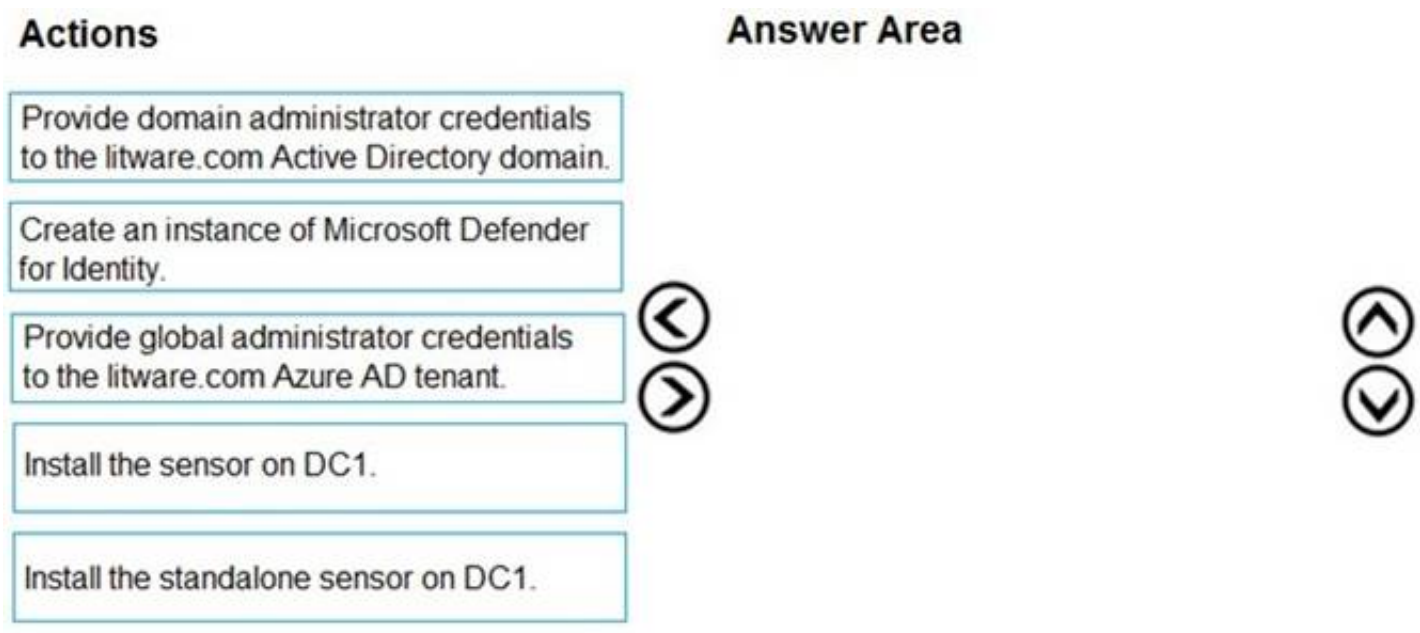
NEW QUESTION 2
- (Topic 1)
You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

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

Answer: B

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

NEW QUESTION 3
DRAG DROP - (Topic 2)
You need to configure DC1 to meet the business requirements.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

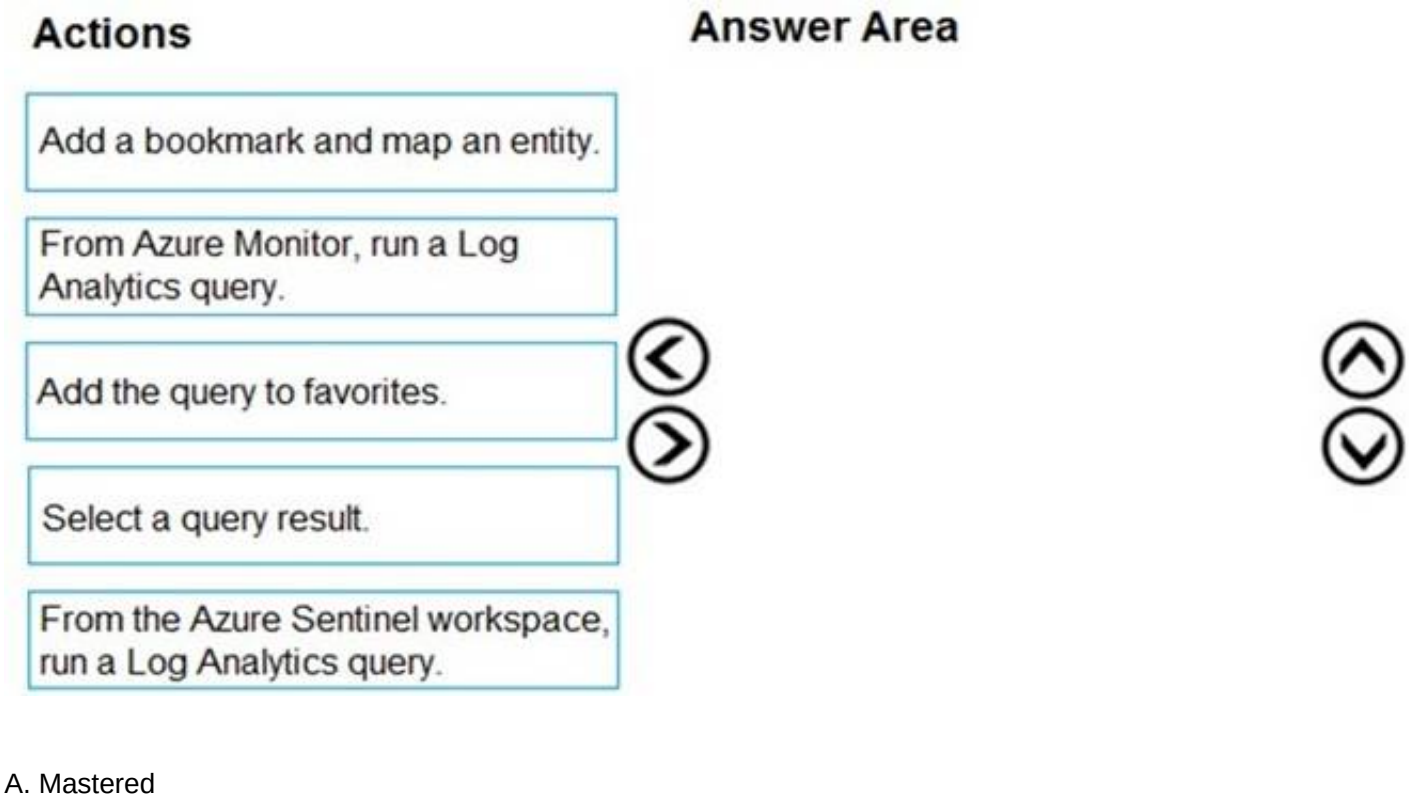


A. Mastered
B. Not Mastered

Answer: A

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

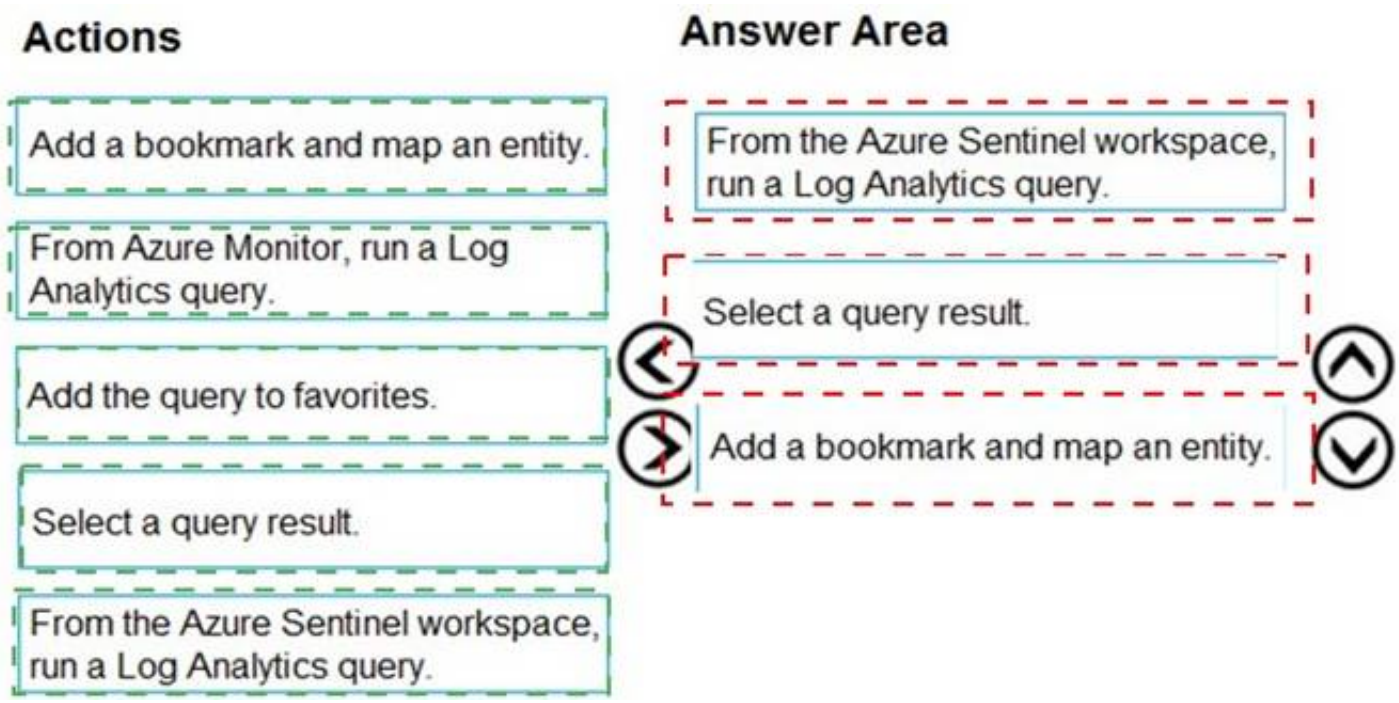
NEW QUESTION 4
DRAG DROP - (Topic 2)
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 5
- (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 6
- (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 7
- (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 8
- (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 9
- (Topic 3)
You need to ensure that the configuration of HuntingQuery1 meets the Microsoft Sentinel requirements.

What should you do?

A. Add HuntingQuery1 to a livestream.
B. Create a watch list.
C. Create an Azure Automation rule.
D. Add HuntingQuery1 to favorites.

Answer: D

NEW QUESTION 10
- (Topic 4)
You use Azure Sentinel.
You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: BC

Explanation:
B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.
C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

NEW QUESTION 10
- (Topic 4)
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

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

Answer: A

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

NEW QUESTION 11
- (Topic 4)
Your company uses Azure Security Center and Azure Defender.
The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

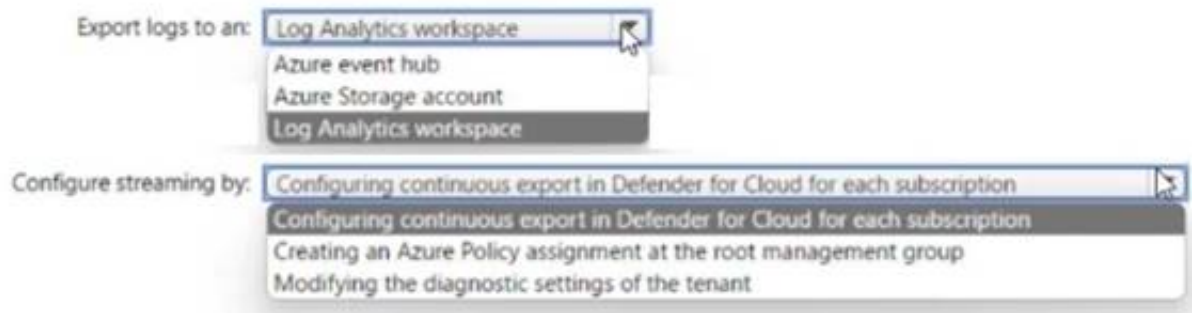
A. Security solutions
B. Security policy
C. Pricing & settings
D. Security alerts
E. Azure Defender

Answer: C

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

NEW QUESTION 14
HOTSPOT - (Topic 4)
You have 100 Azure subscriptions that have enhanced security features m Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud togs to a syslog server. The solution must minimize administrative effort What should you do? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point

Answer Area

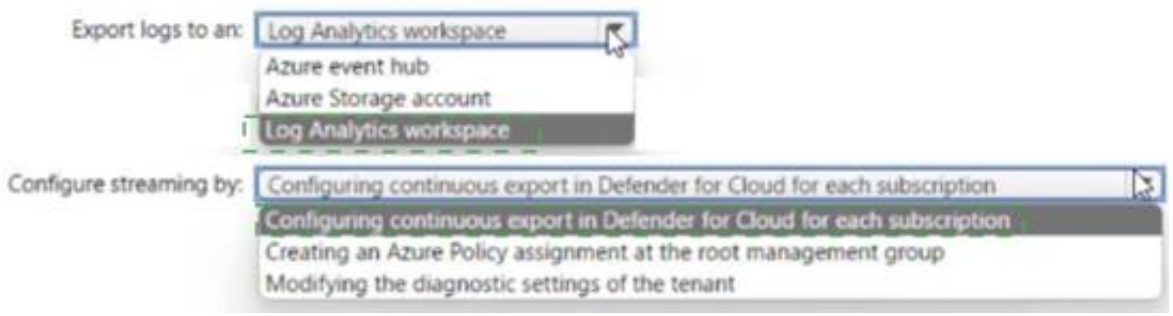


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 16
- (Topic 4)
You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery
B. Replace
C. Block and Enable redirect
D. Monitor and Enable redirect

Answer: A

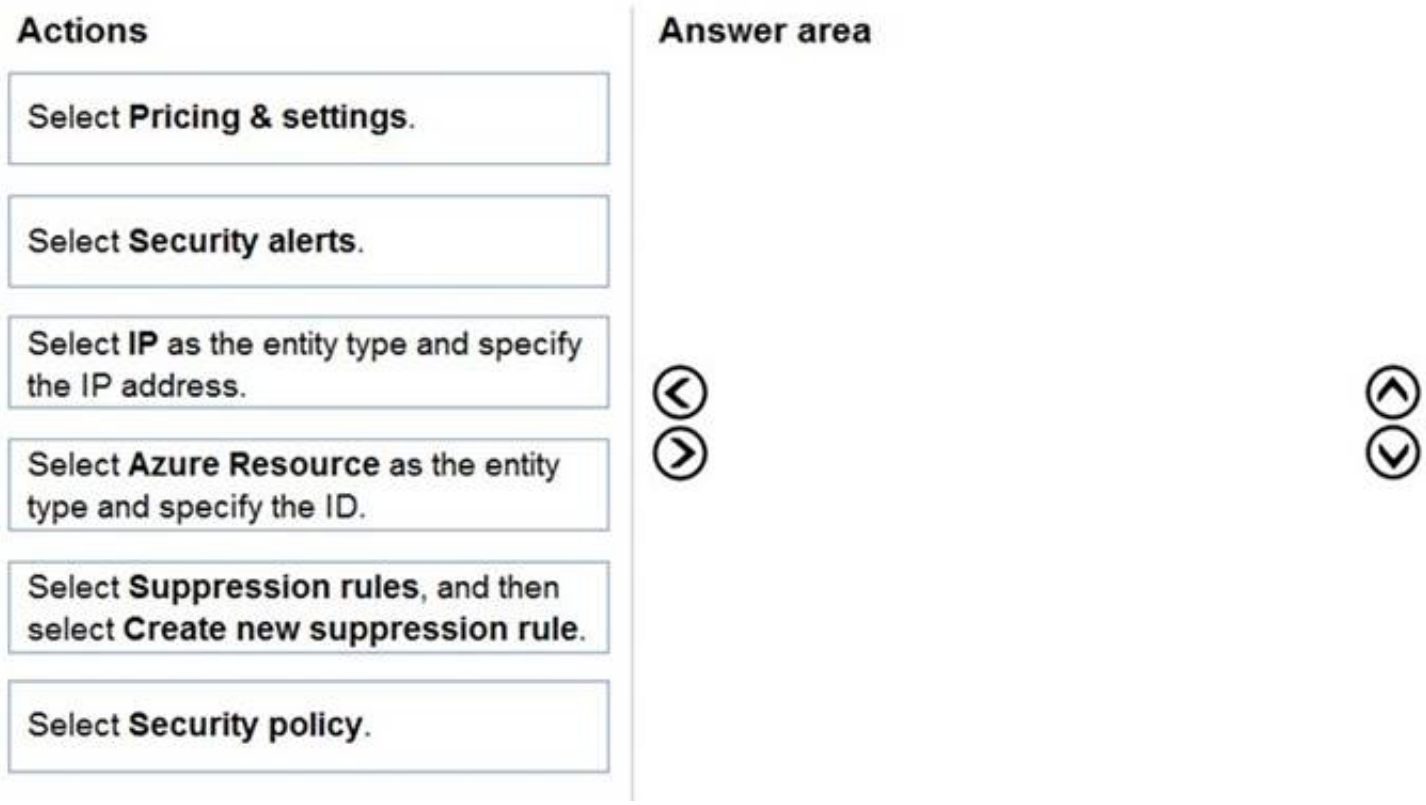
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

NEW QUESTION 20
- (Topic 4)
You use Microsoft Sentinel.
You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point

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

Answer: DE

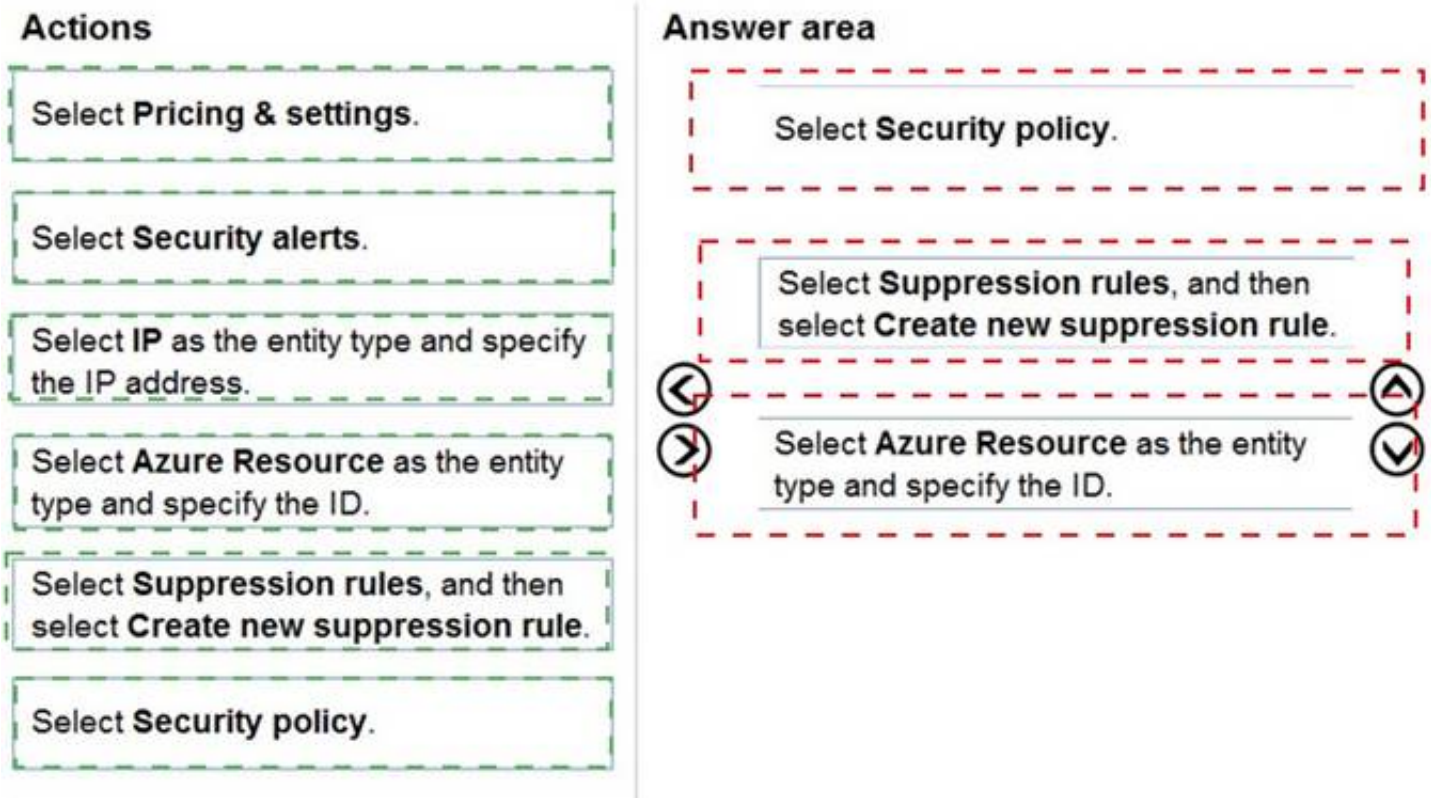
NEW QUESTION 22
DRAG DROP - (Topic 4)
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 26
- (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

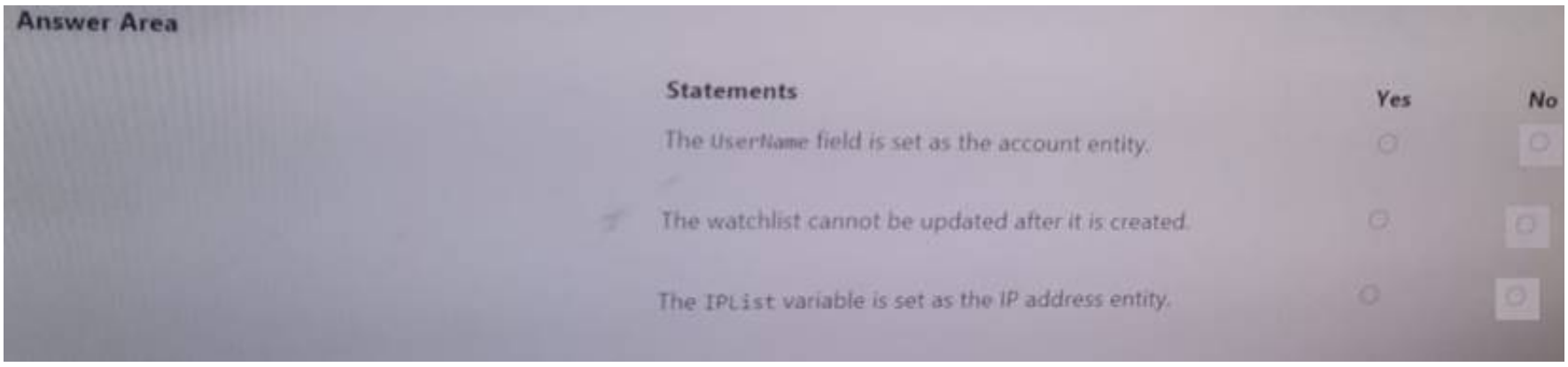
NEW QUESTION 31
- (Topic 4)
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert 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 34
HOTSPOT - (Topic 4)
You have the following SQL query.

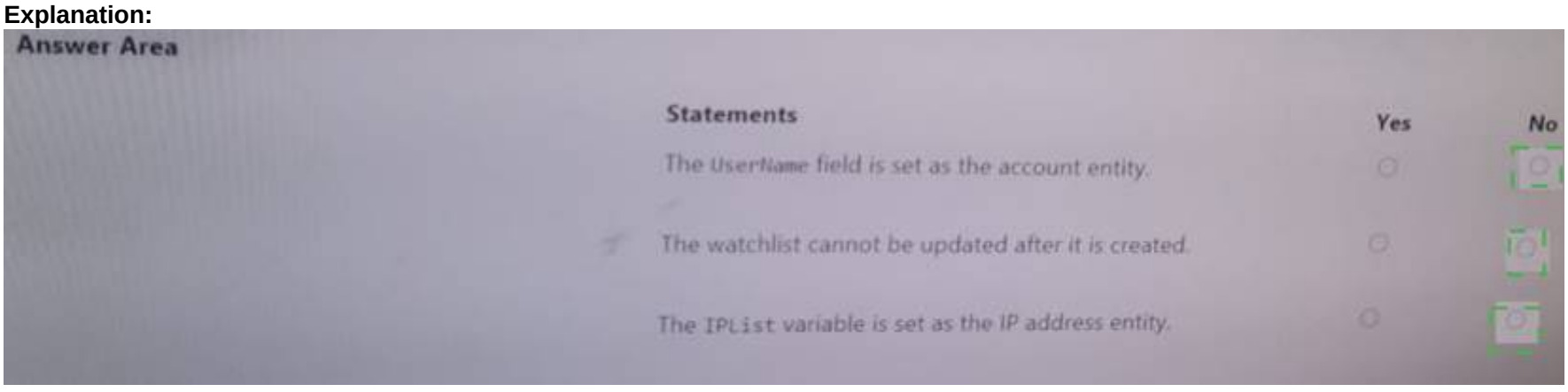
```
let IPList = _GetWatchlist('Bad_IPs');
Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID == 3
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
   | where SourceIP in (IPList) or DestinationIP in (IPList)
   | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
   | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 35
- (Topic 4)
You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
? Microsoft Excel macros that download scripts from untrusted websites
? Users that open executable attachments in Microsoft Outlook
? Outlook rules and forms exploits
What should you use?

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

Answer: B

Explanation:

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

NEW QUESTION 40
- (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 livestream from a query. 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 44
- (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:

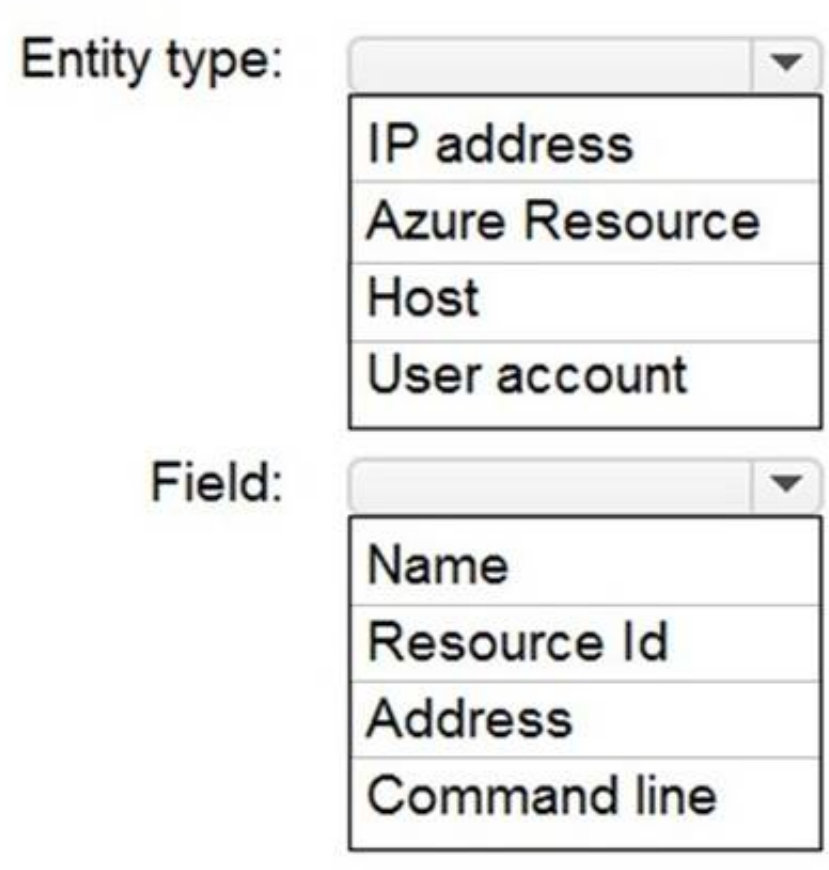
Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

NEW QUESTION 46
- (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

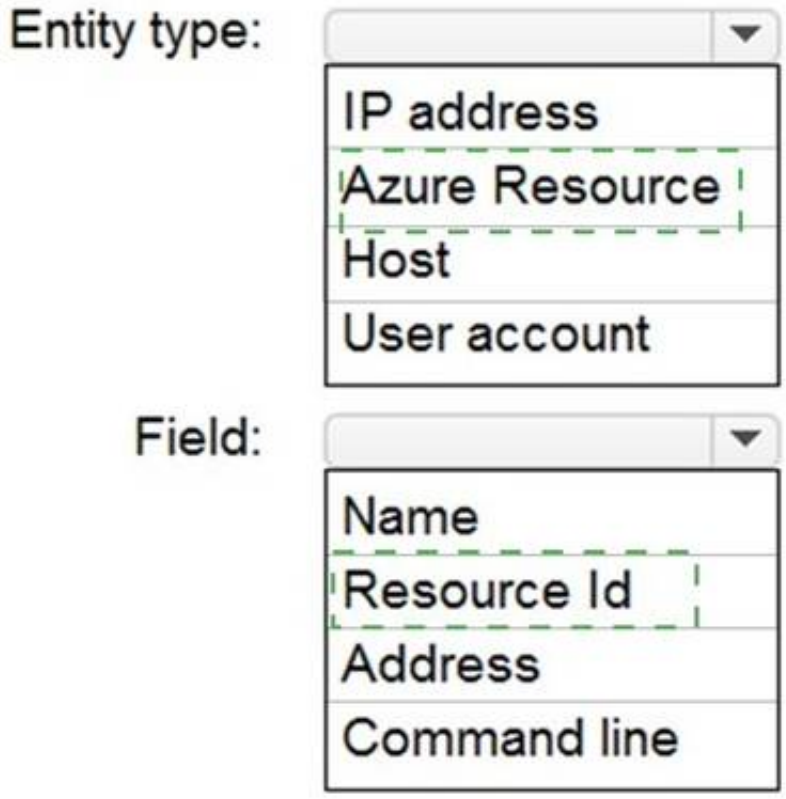
NEW QUESTION 47
HOTSPOT - (Topic 4)
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



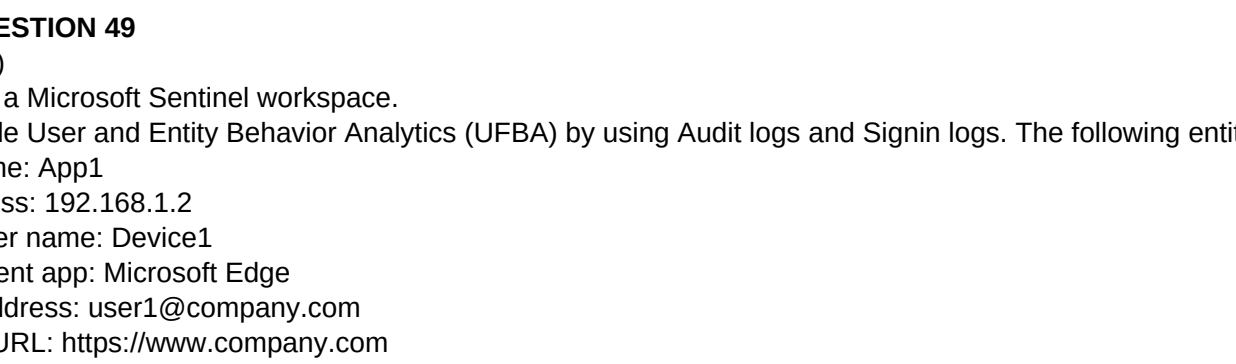
NEW QUESTION 49
- (Topic 4)
You have a Microsoft Sentinel workspace.
You enable User and Entity Behavior Analytics (UFBA) by using Audit logs and Signin logs. The following entities are detected in the Azure AD tenant:
• App name: App1
• IP address: 192.168.1.2
• Computer name: Device1
• Used client 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 50
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:
• Identify alerts that occurred during the last 30 days.
• Display the results in a timechart.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

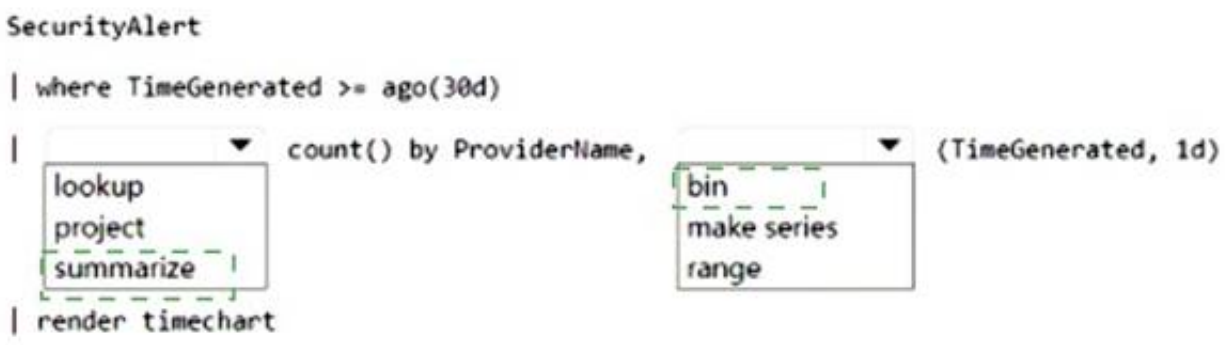


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



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

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

Answer: B

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

NEW QUESTION 56
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains two users named User! and User2. You have the hunting query shown in the following exhibit.

The users perform the following anions:
• User1 assigns User2 the Global administrator role.
• User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
• User2 creates a new user named User4 and assigns the user the Security reader role.
• User2 creates a new user named User5 and assigns the user the Security operator role. 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
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

NEW QUESTION 57
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct answer is worth one point.

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

Answer: BC

NEW QUESTION 58
- (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 63
- (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 67
- (Topic 4)
You have a custom Microsoft Sentinel workbook named Workbooks.
You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.
What should you do?

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

Answer: B

NEW QUESTION 69
- (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 71
- (Topic 4)
You have a Microsoft Sentinel workspace.
You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.
What are two ways to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

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

Answer: AD

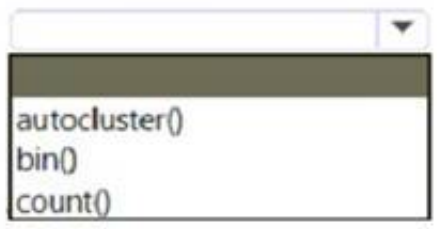
NEW QUESTION 73
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT) VM access for the virtual machines in RG1. The solution must meet the following
• Limit the maximum request time to two hours.
• Limit protocol access to Remote Desktop Protocol (RDP) only.
• Minimize administrative effort. What should you use?

A. Azure AD Privileged Identity Management (PIM)
B. Azure Policy
C. Azure Front Door
D. Azure Bastion

Answer: A

NEW QUESTION 78
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.


```
| 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
```

NEW QUESTION 82
- (Topic 4)
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook
B. a notebook
C. a livestream
D. a bookmark

Answer: C

Explanation:
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

NEW QUESTION 84
DRAG DROP - (Topic 4)
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
• Enable and disable advanced features of Microsoft Defender for Cloud.
• Apply security recommendations to a resource. The solution must use the principle of least privilege.
Which Microsoft Defender for Cloud role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, mote than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 86
- (Topic 4)
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 Microsoft Defender for Cloud.
C. Create a Microsoft Cloud App Security connector.
D. Create an Azure AD Identity Protection connector.

Answer: AB

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 90
- (Topic 4)
You are investigating an incident in Azure Sentinel that contains more than 127 alerts. You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator. What should you do to provide the alerts to the administrator?

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

Answer: D

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

NEW QUESTION 91
- (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

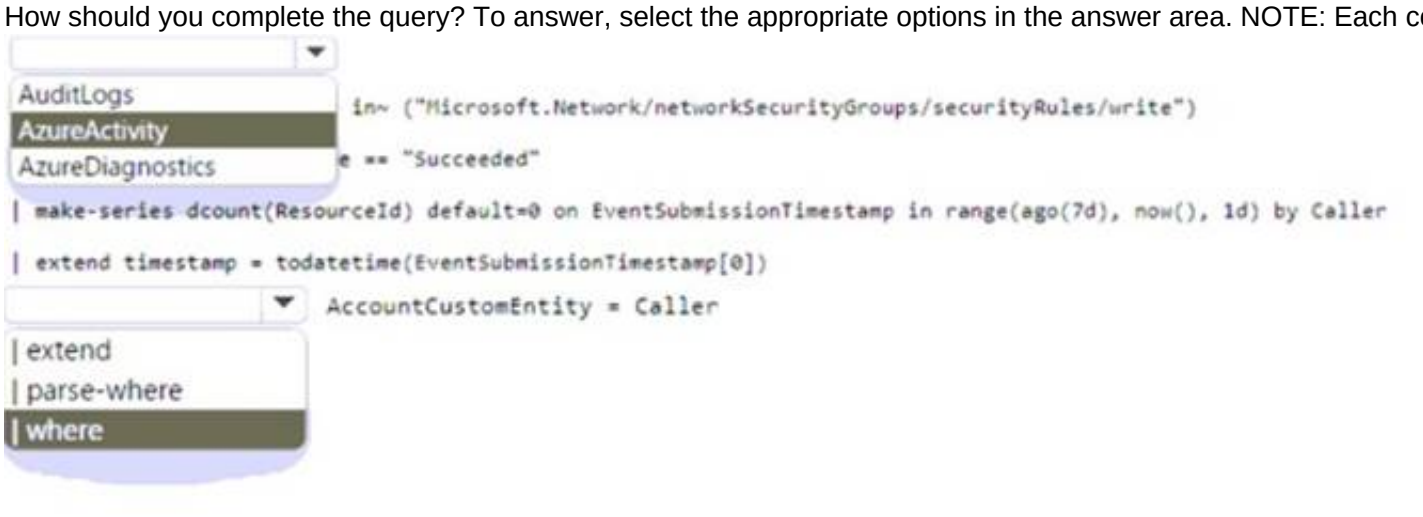
NEW QUESTION 95
HOTSPOT - (Topic 4)
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 99
HOTSPOT - (Topic 4)
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:
• Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
• Automatically associates the security principal with an Microsoft Sentinel entity
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 103
HOTSPOT - (Topic 4)
You have a custom detection rule that includes the following KQL query.

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

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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 108
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 111
- (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

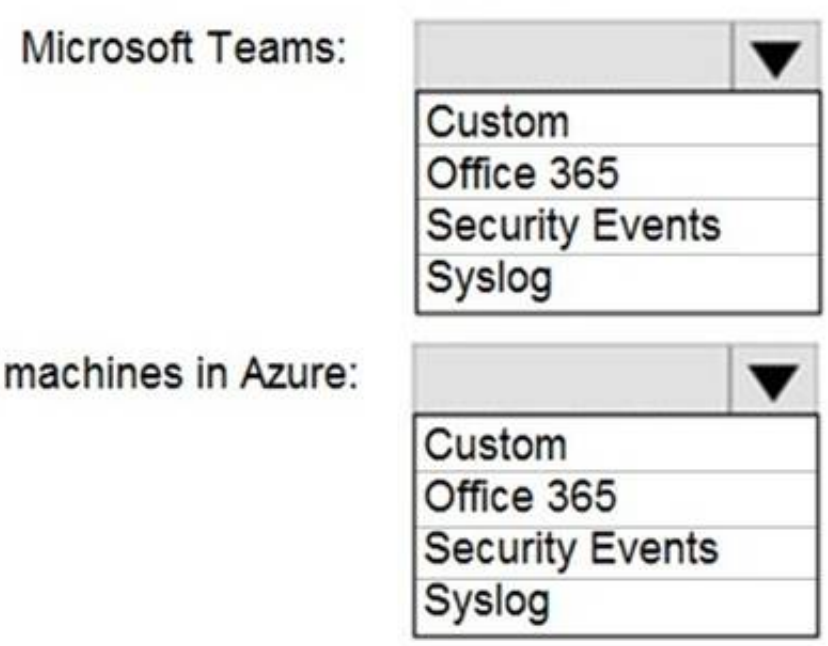
NEW QUESTION 113
- (Topic 4)
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.
To which service should you export the alerts?

A. Azure Cosmos DB
B. Azure Event Grid
C. Azure Event Hubs
D. Azure Data Lake

Answer: C

Explanation:
Reference: https://docsmicrosoftcom/en-us/azure/security-center/continuous-export?tabs=azure-portal

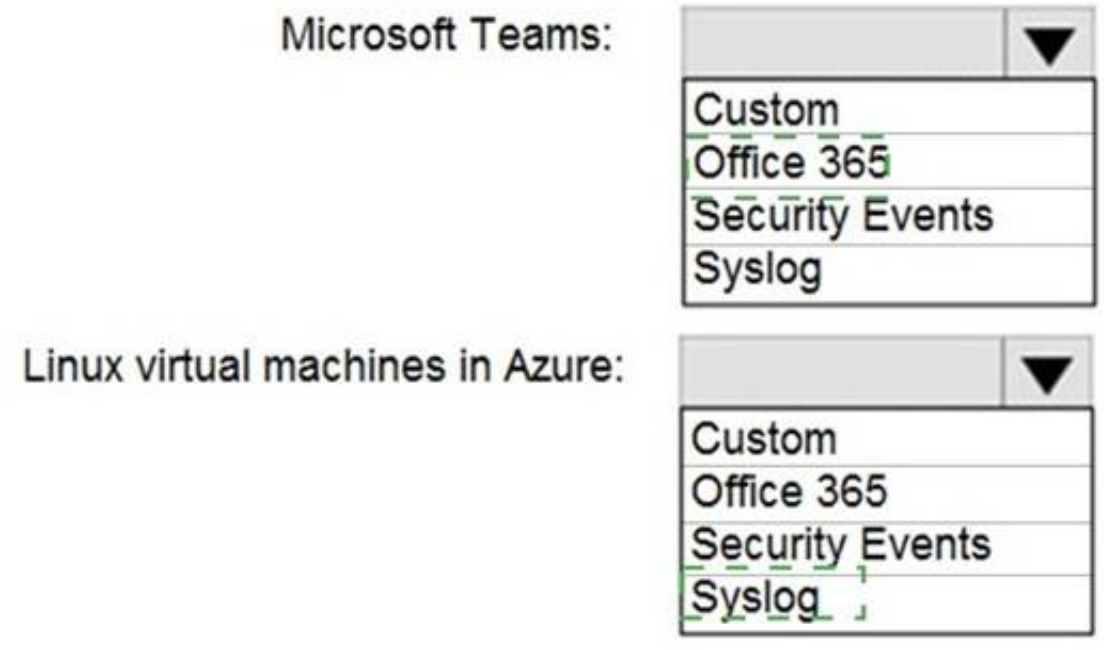
NEW QUESTION 114
HOTSPOT - (Topic 4)
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select 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 115
- (Topic 4)
You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: A

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

NEW QUESTION 117
- (Topic 4)
You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region. You need to ensure that you can use scheduled analytics rules in the existing Azure
Sentinel deployment to generate alerts based on queries to LogsWest. What should you do first?
A. Deploy Azure Data Catalog to the West US Azure region.
B. Modify the workspace settings of the existing Azure Sentinel deployment
C. Add Microsoft Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

Answer: C

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

NEW QUESTION 118
HOTSPOT - (Topic 4)
You have an Microsoft Sentinel workspace named SW1.
You plan to create a custom workbook that will include a time chart.
You need to create a query that will identify the number of security alerts per day for each provider.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 119
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 120
- (Topic 4)
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: C

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 122
- (Topic 4)
You have a Microsoft Sentinel workspace.
You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.
You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.
• Ensure that failed sign-in alerts are generated for other accounts.
• Minimize administrative effort What should do?

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

Answer: A

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

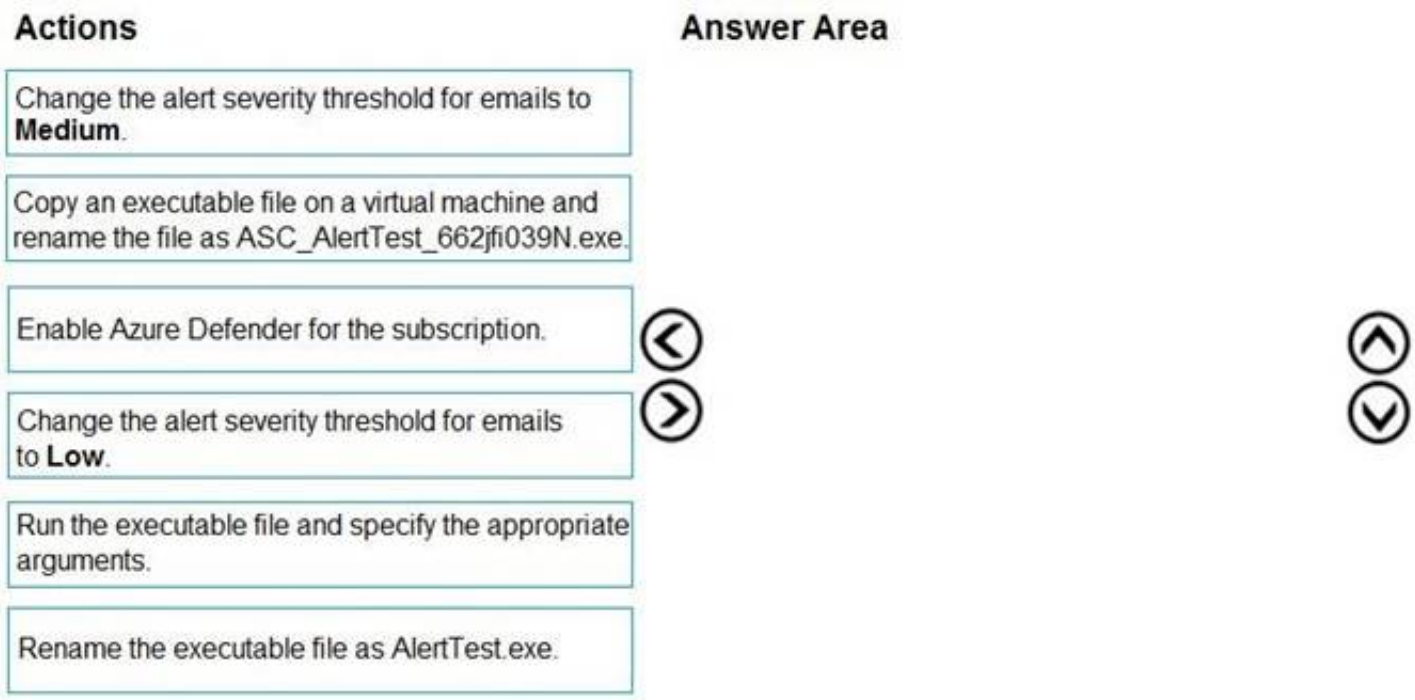
NEW QUESTION 127
- (Topic 4)
You have 50 Microsoft Sentinel workspaces.
You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.
Which page should you use in the Azure portal?

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

Answer: D

NEW QUESTION 131
DRAG DROP - (Topic 4)

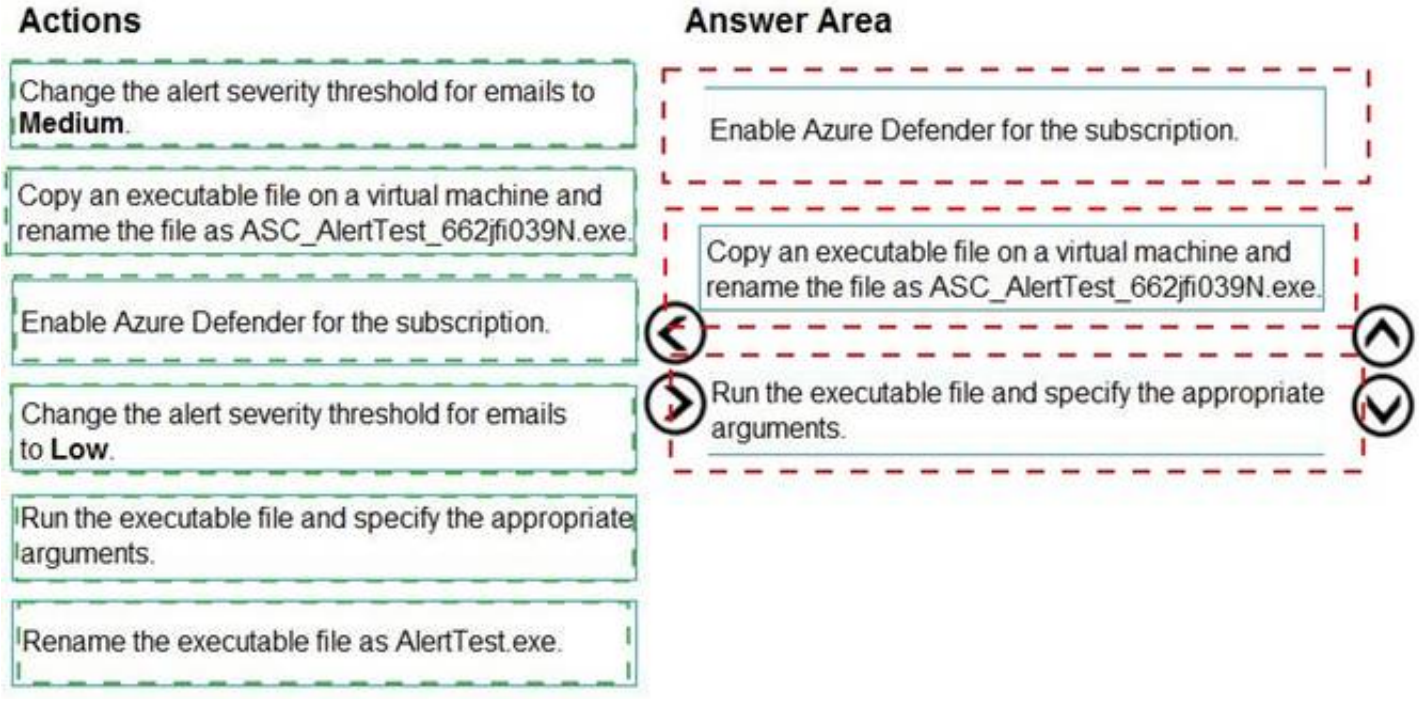
DRAG DROP
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions 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:



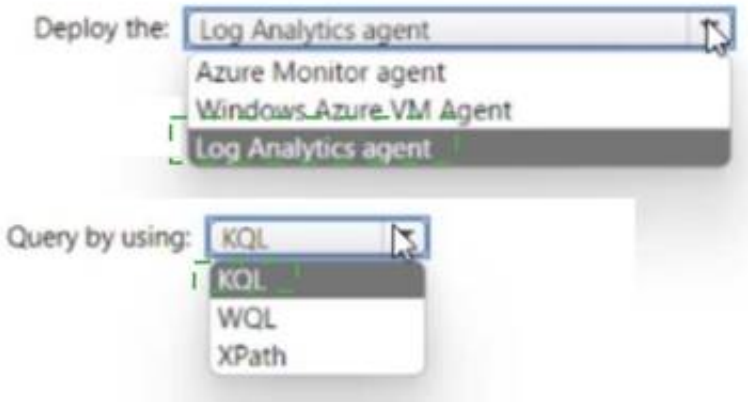
NEW QUESTION 133
HOTSPOT - (Topic 4)
You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 137
- (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

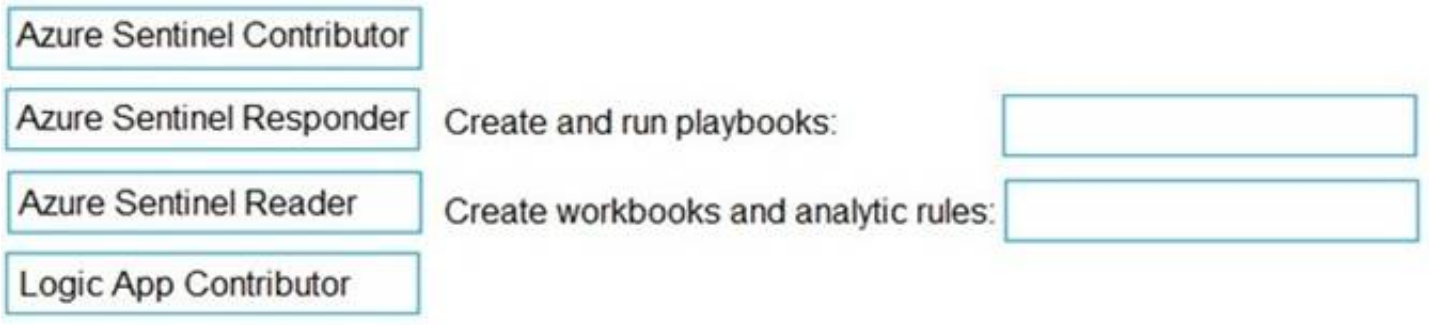
NEW QUESTION 139
- (Topic 4)
You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

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

Answer: C

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

NEW QUESTION 143
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

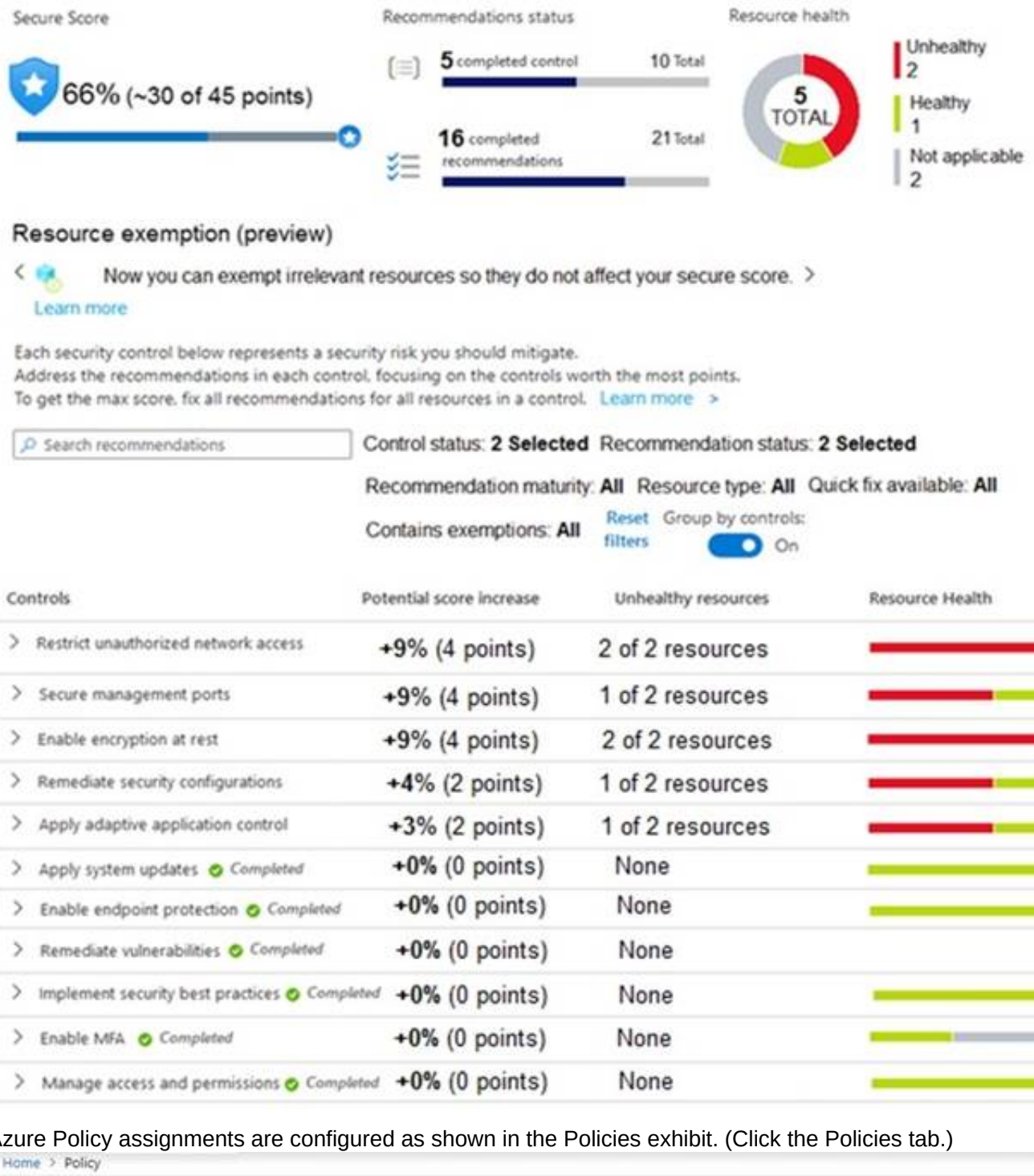
Explanation:

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

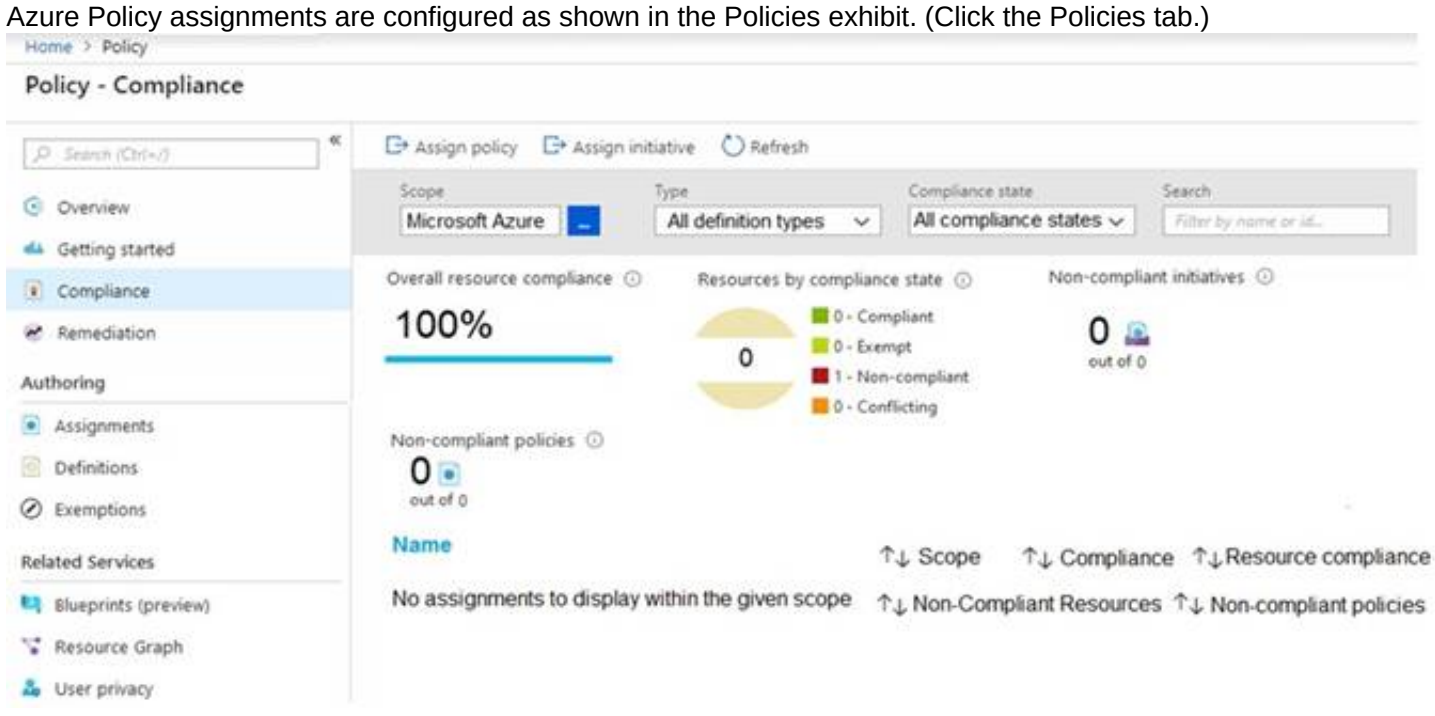
Create and run playbooks: Logic App Contributor

Create workbooks and analytic rules: Azure Sentinel Contributor

NEW QUESTION 145
HOTSPOT - (Topic 4)
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



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



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

Answer Area

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 147
DRAG DROP - (Topic 4)
You have the resources shown in the following table.

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

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

Resources

- SW1
- CEF1
- Server1
- Server2

Answer Area

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

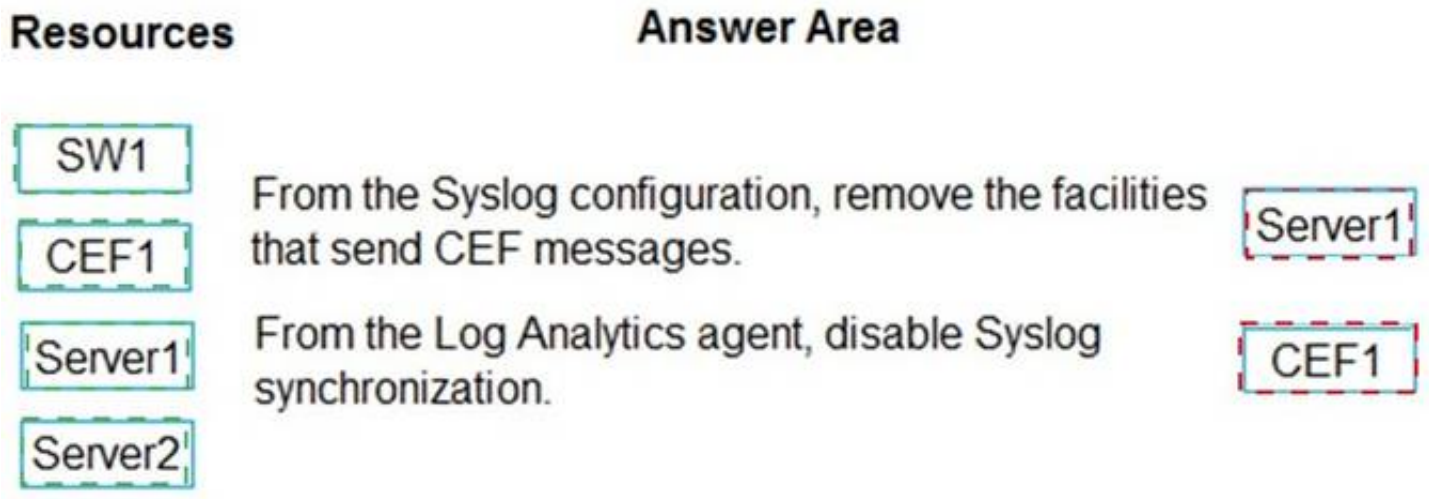
From the Log Analytics agent, disable Syslog synchronization. [ ]

A. Mastered

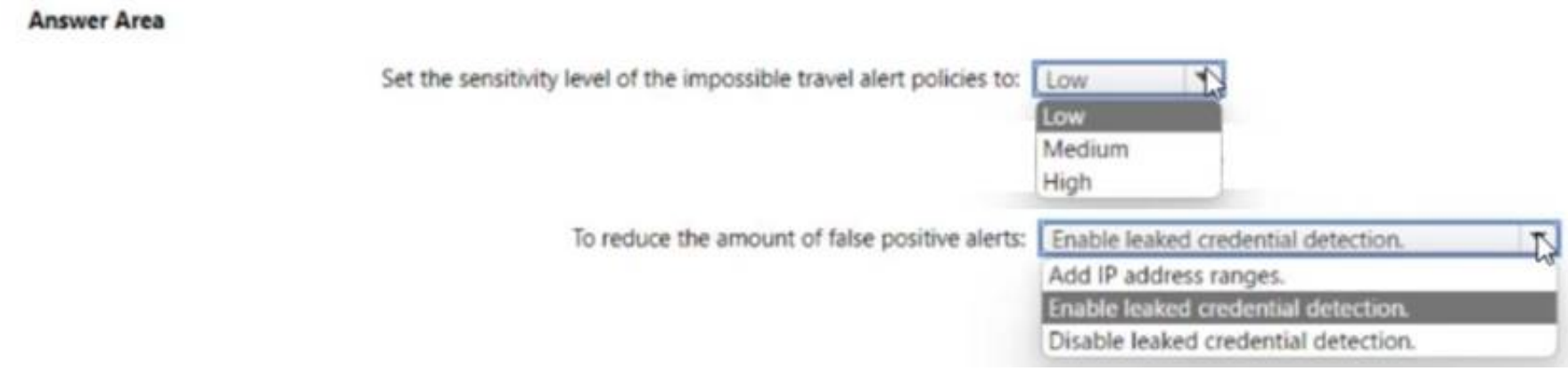
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 152
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 154
- (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 159
- (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 162
- (Topic 4)
You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

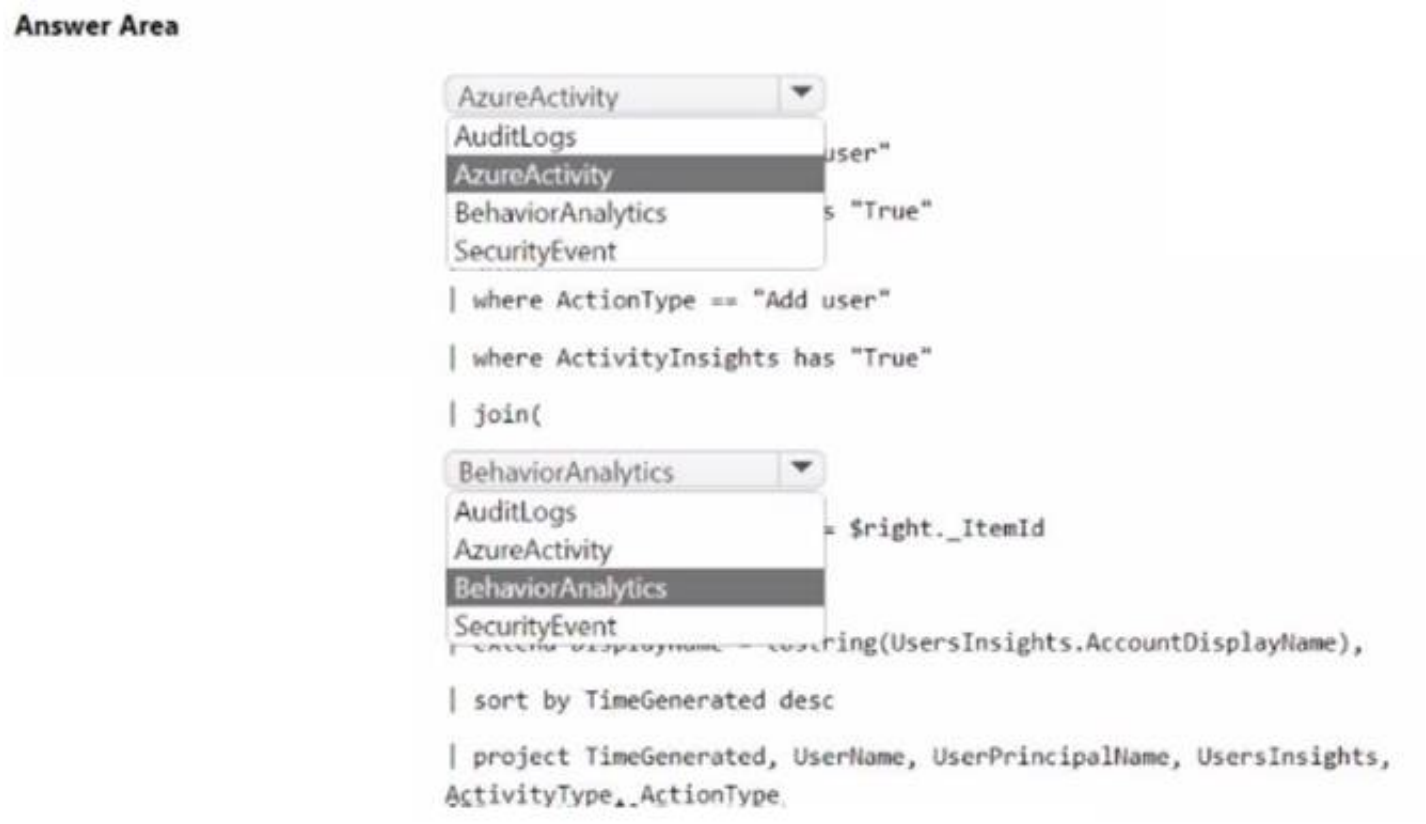
A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

Answer: C

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

NEW QUESTION 166
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

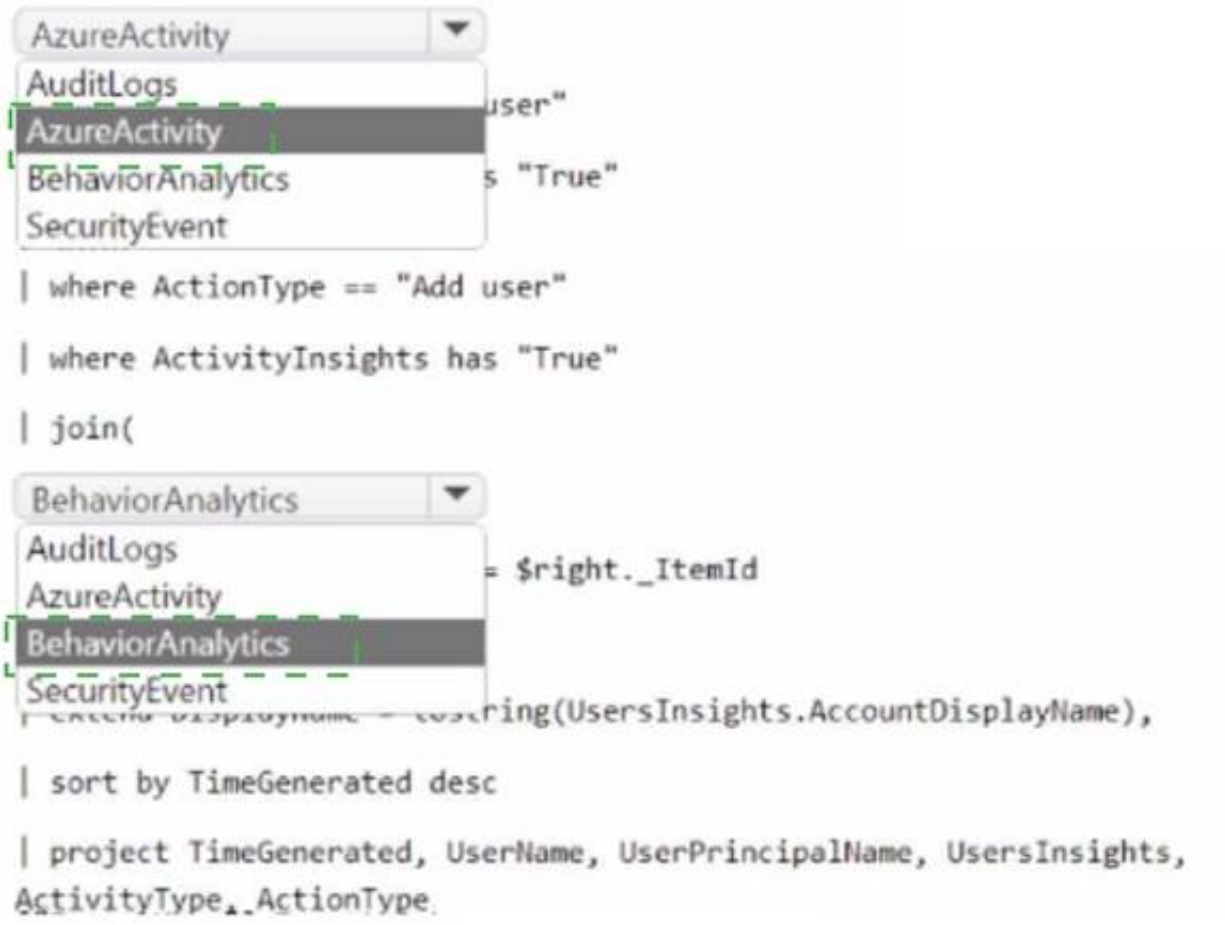


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 170
HOTSPOT - (Topic 4)
You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group? 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 171
- (Topic 4)
You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.
You enable agentless scanning.
You need to prevent Server1 from being scanned. The solution must minimize administrative effort.
What should you do?

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

Answer: D

NEW QUESTION 173
- (Topic 4)
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address
D. computer

Answer: CD

NEW QUESTION 175
- (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 176
- (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 178
- (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 181
- (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 186
HOTSPOT - (Topic 4)
You have the following KQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

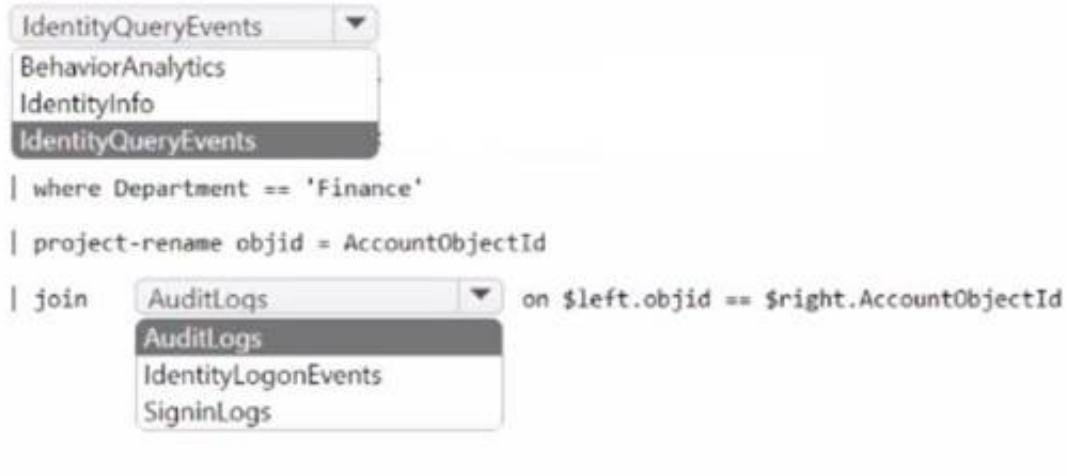
NEW QUESTION 187
- (Topic 4)
You have an Azure subscription that uses resource type for Cloud. You need to filter the security alerts view to show the following alerts:
• Unusual user accessed a key vault
• Log on from an unusual location
• Impossible travel activity Which severity should you use?

A. Informational
B. Low
C. Medium
D. High

Answer: C

NEW QUESTION 191
HOTSPOT - (Topic 4)
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.
You need to identify all the interactive authentication attempts by the users in the finance department of your company.
How should you complete the KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

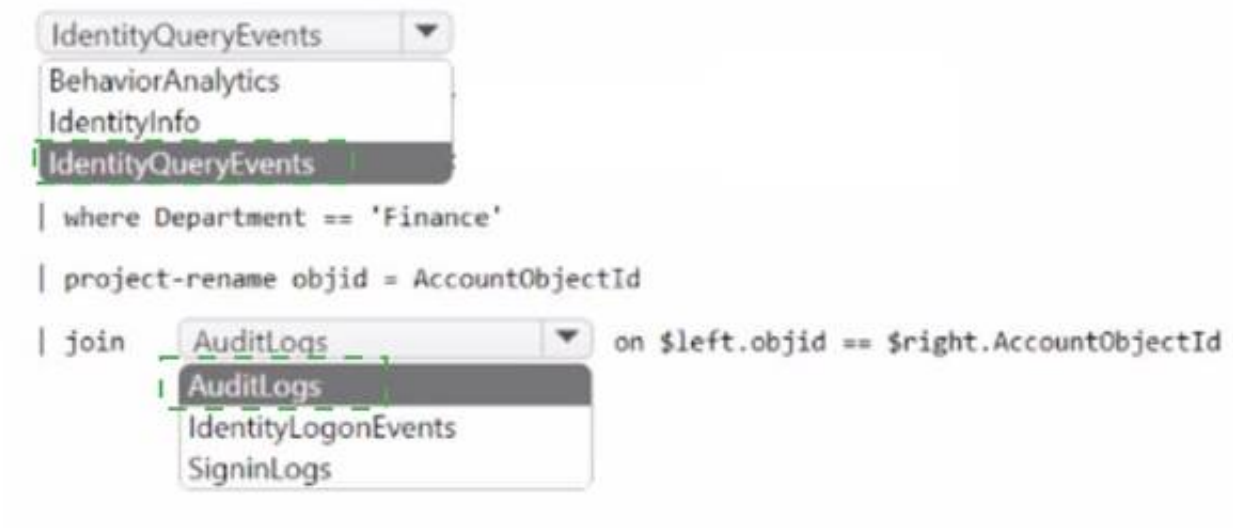


A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 192
- (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

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

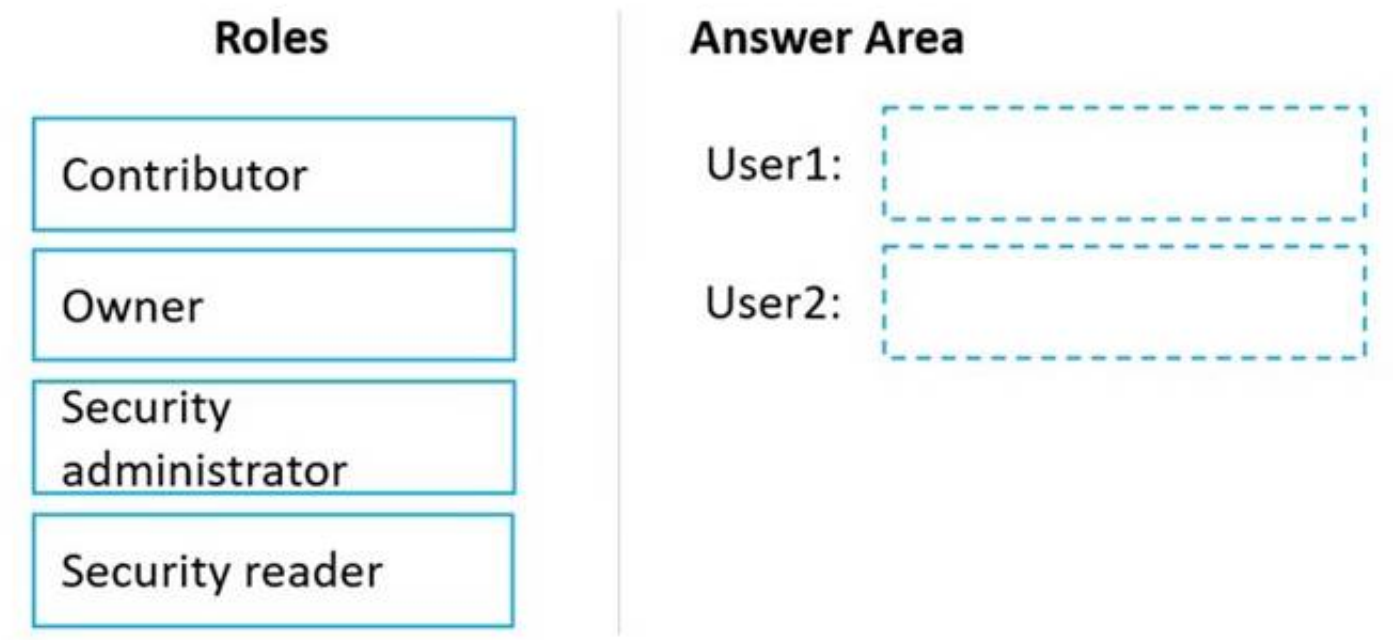
Answer: D

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

NEW QUESTION 197
DRAG DROP - (Topic 4)
You 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

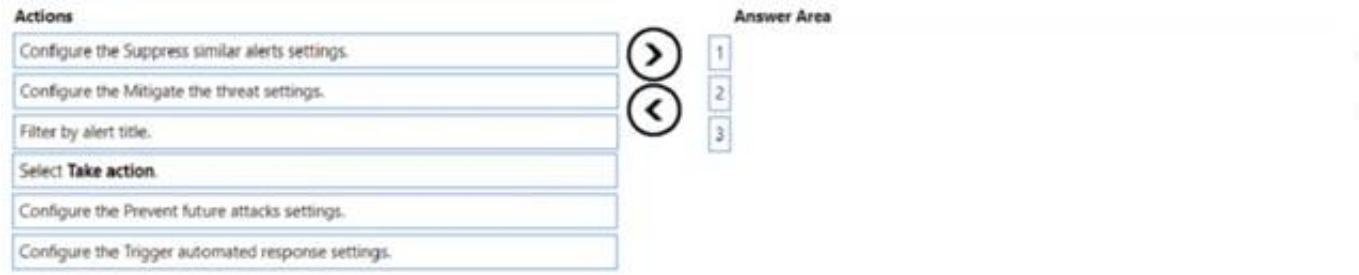
Answer: A

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 198
DRAG DROP - (Topic 4)
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.

Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.
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

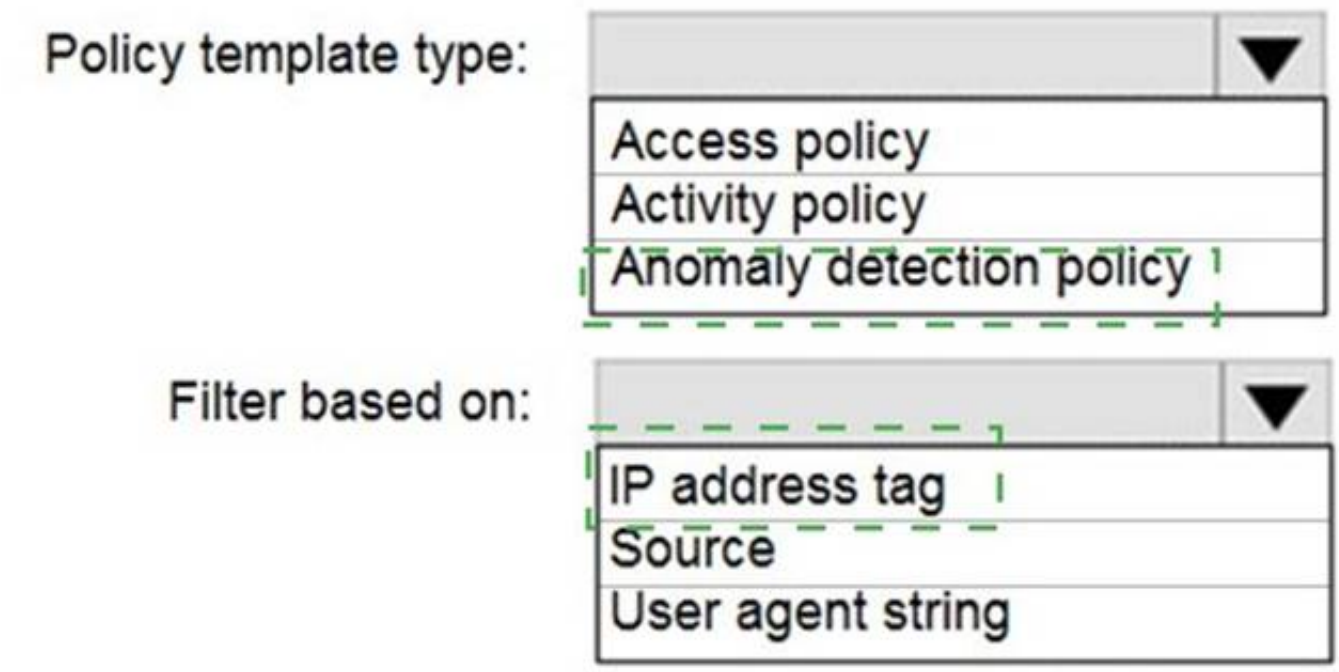
Explanation:
* A. Configure the Trigger automated response settings in the Azure Security Center or Azure Logic App,
* B. Filter by alert title (e.g. "Suspicious process executed").
* C. Select "Take action" (e.g. "Mitigate the threat").

NEW QUESTION 202
HOTSPOT - (Topic 4)
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

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

Answer: C

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

NEW QUESTION 206
- (Topic 4)
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a playbook that will run automatically in response to an Microsoft Sentinel alert.
What should you create first?

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

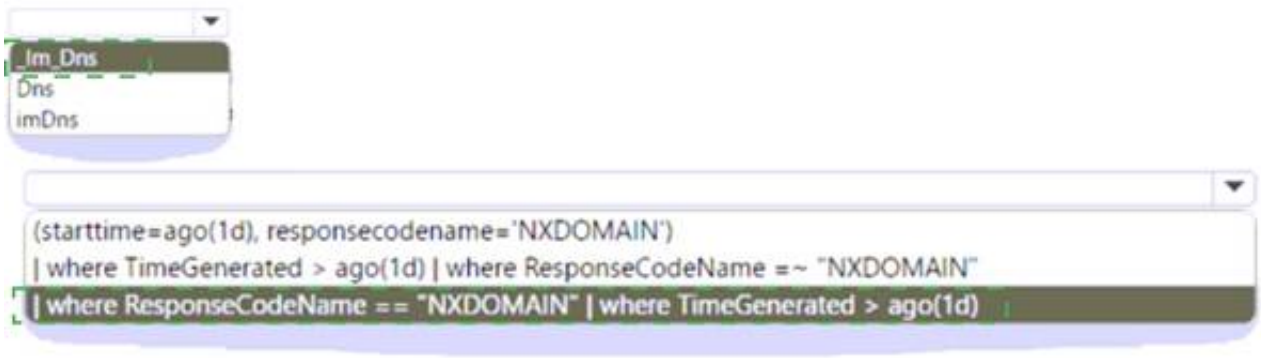
Answer: D

NEW QUESTION 207
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c
ollect DNS events and deploy the Advanced Security information Model (ASIM) unifying parser for the DNS schema.
You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.
How should you complete the query? To answer, select the appropriate options in the answer area
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 210
- (Topic 4)
You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations
B. Devices
C. Evidence and Response
D. Alerts

Answer: C

Explanation:
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate- incidents

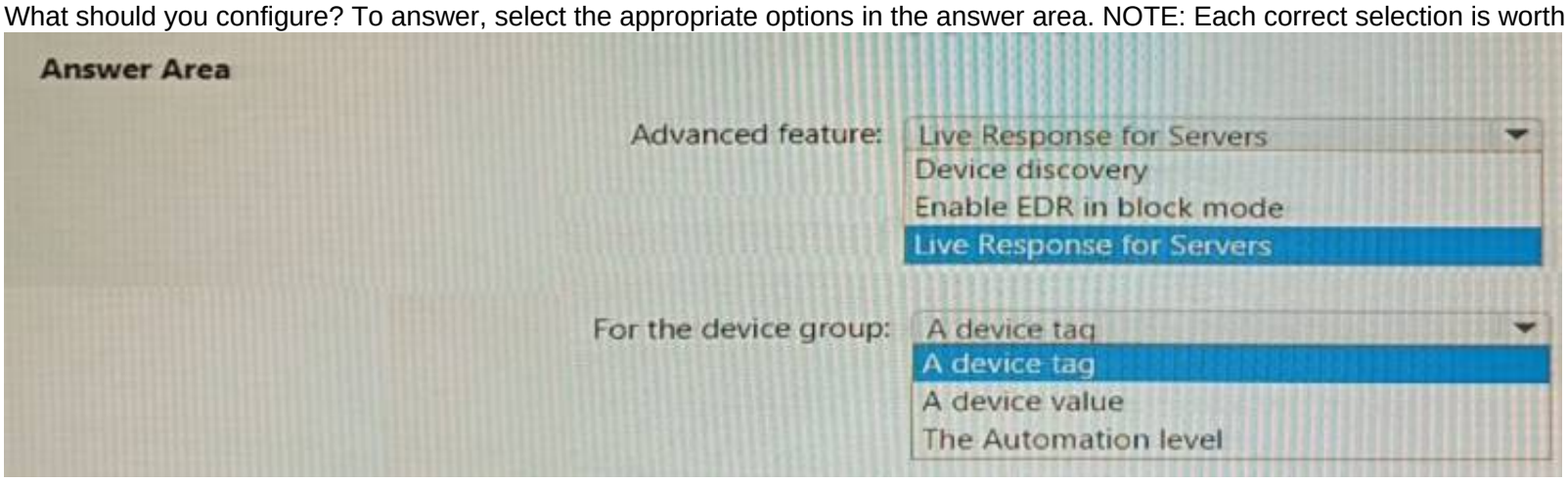
NEW QUESTION 212
- (Topic 4)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Answer: AB

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

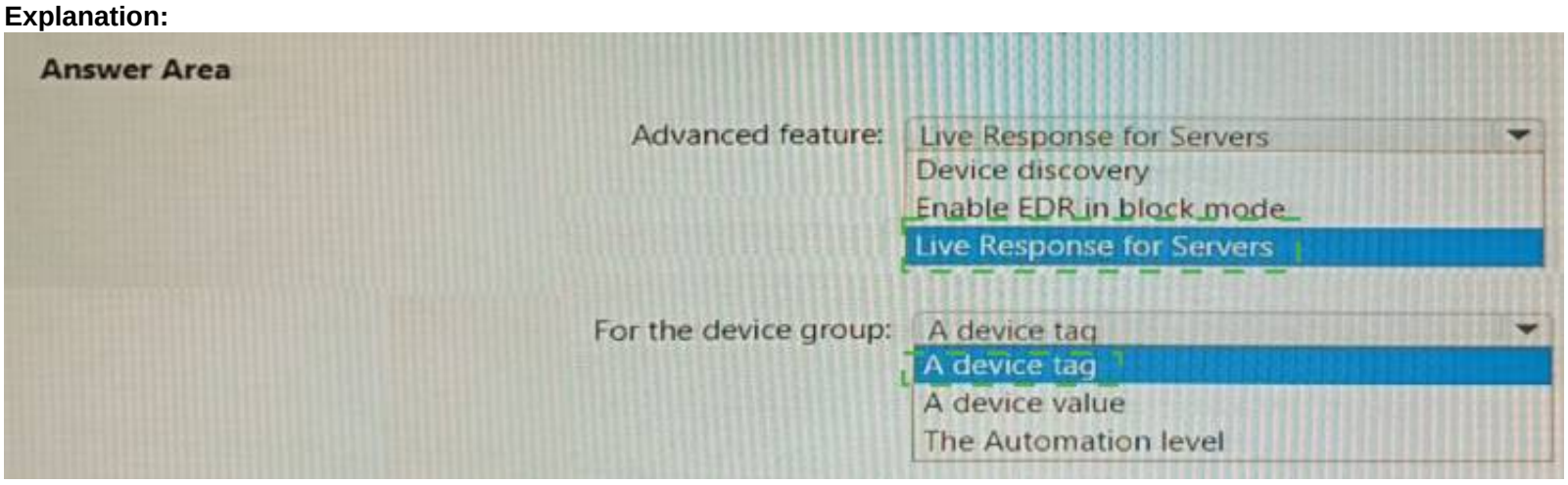
NEW QUESTION 217
HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender for Endpoint.
You need to ensure that you can initiate remote shell connections to Windows servers by using the Microsoft 365 Defender portal.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



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

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

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

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

Answer: AE

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

NEW QUESTION 222
- (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

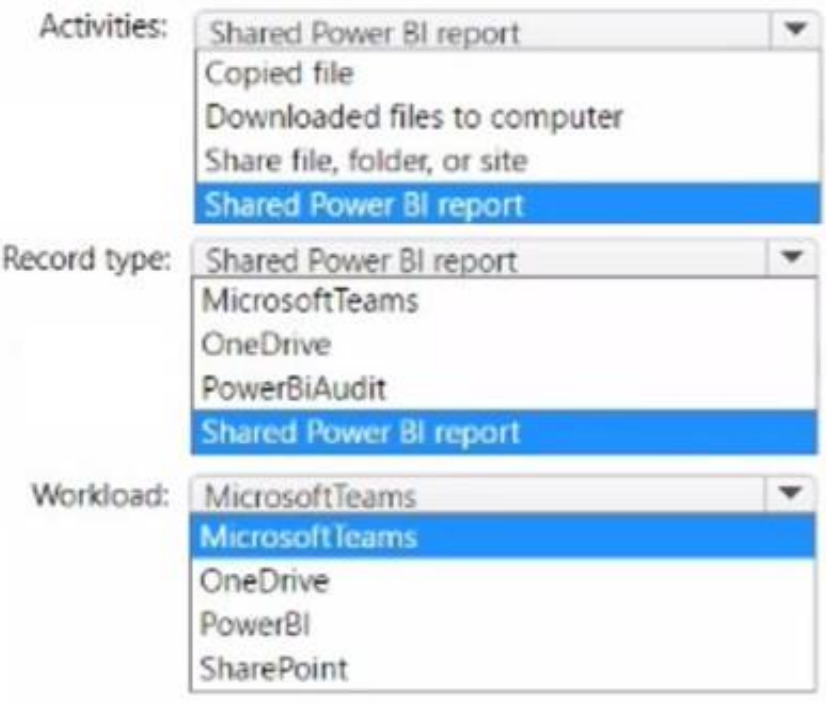
• Minimize the parsing required to read log data What should you configure?

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 223
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

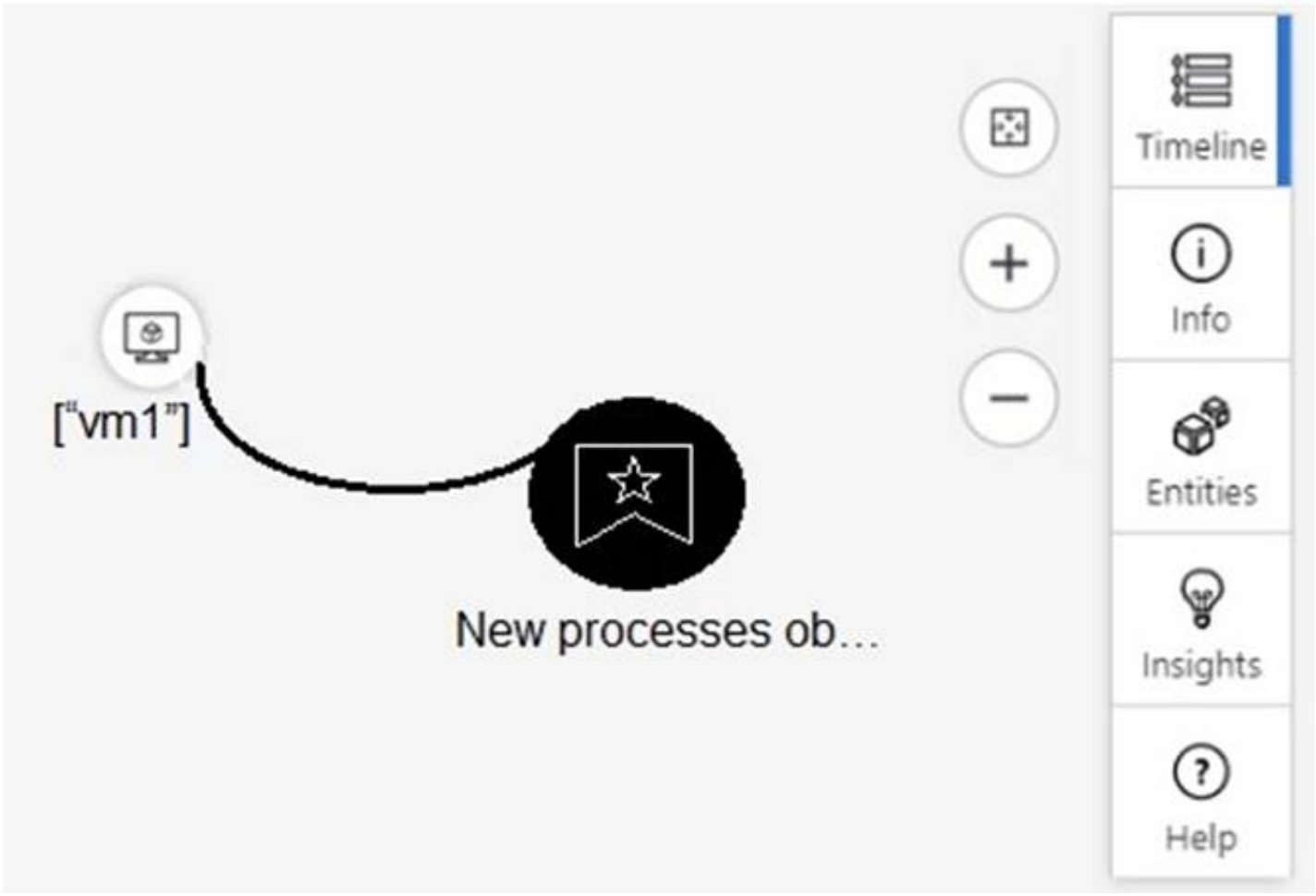


A. Mastered
B. Not Mastered

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 226
HOTSPOT - (Topic 4)
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

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

- Entities
- Info
- Insights
- Timeline

A. Mastered
B. Not Mastered

Answer: A

Explanation:

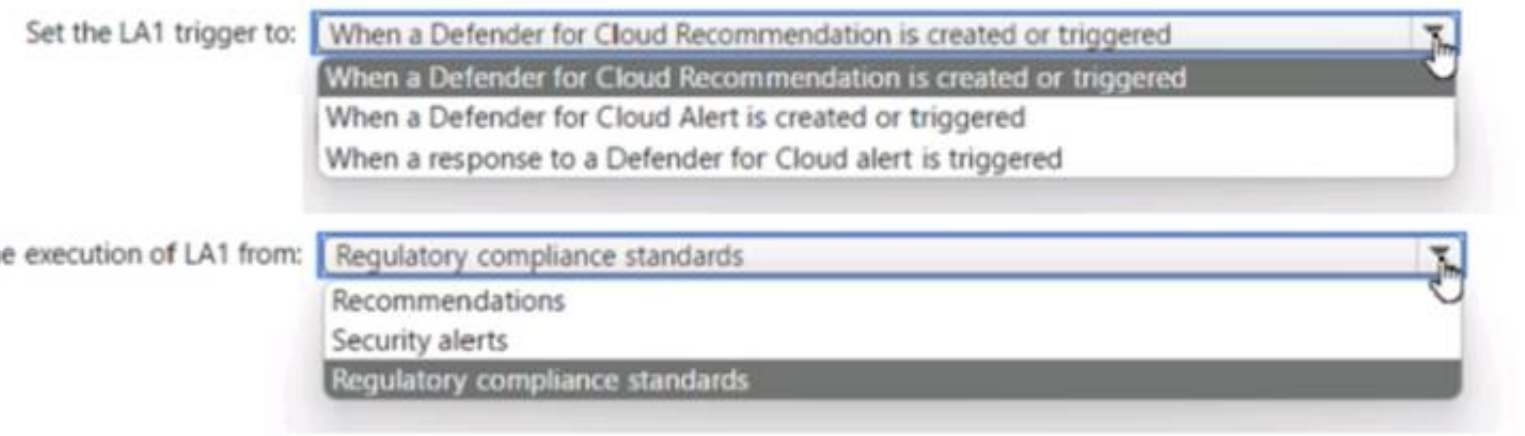
If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

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

- Entities
- Info
- Insights
- Timeline

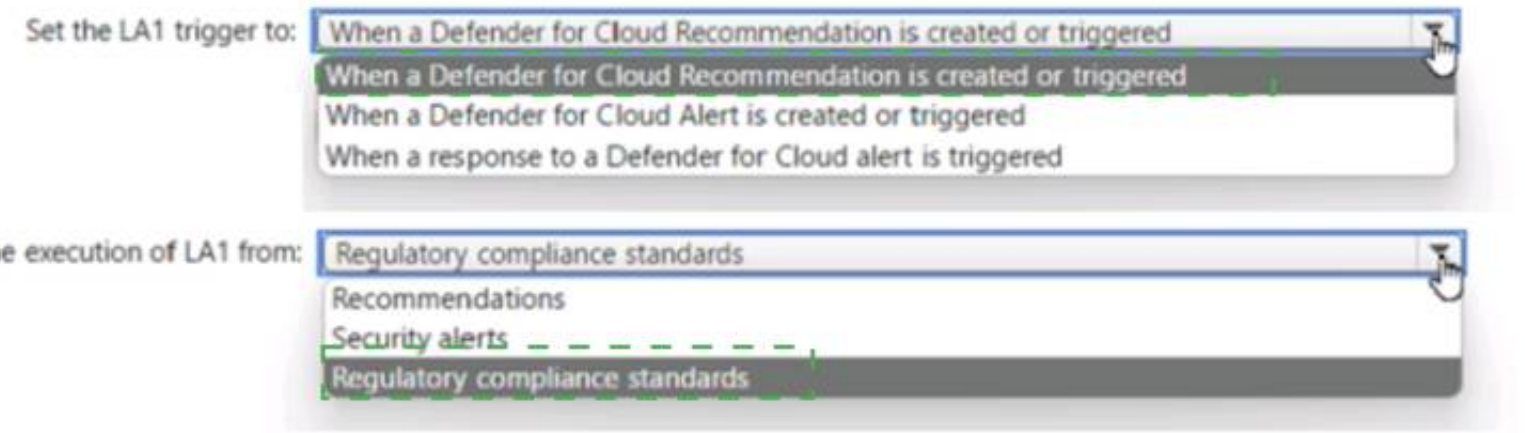
NEW QUESTION 230
HOTSPOT - (Topic 4)
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.
You need to test LA1 in Defender for Cloud.
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 233
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 238
- (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 242
- (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

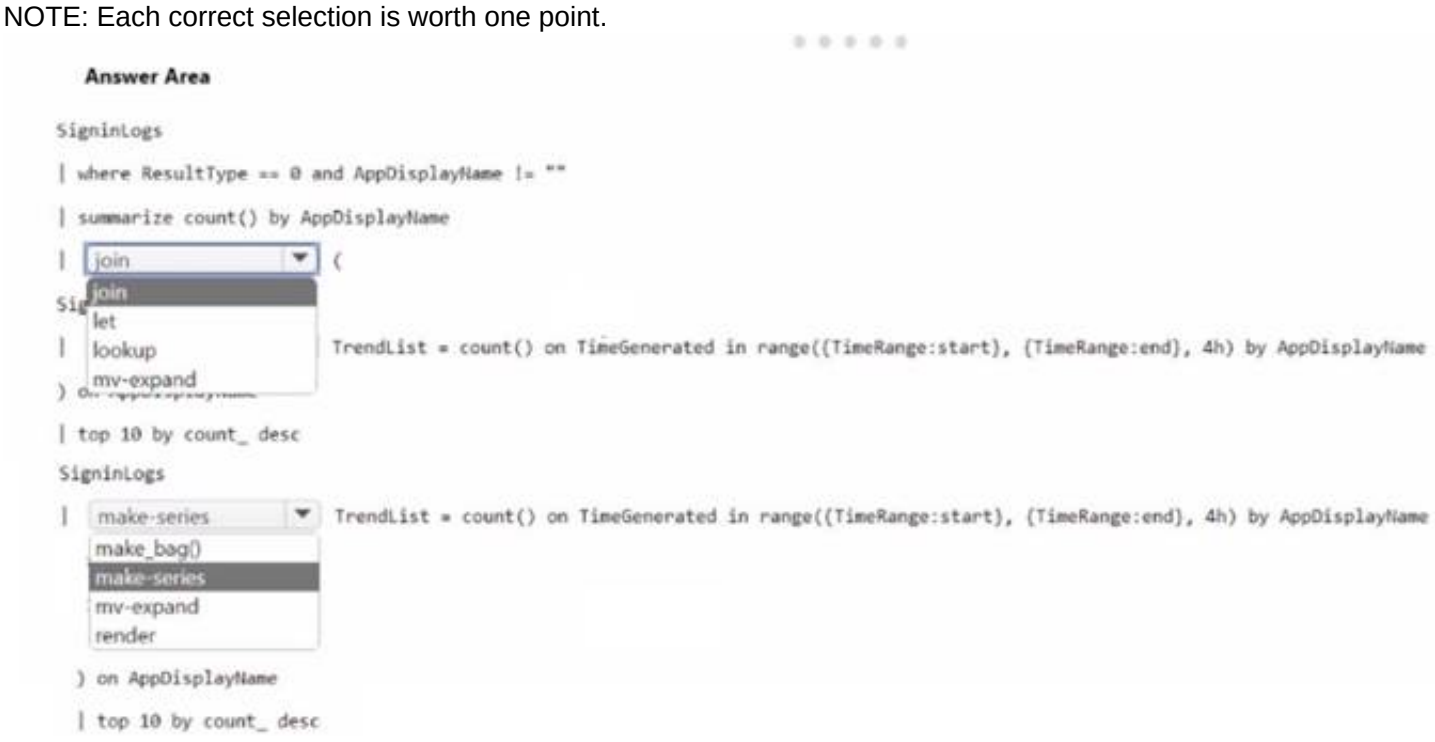
NEW QUESTION 247
- (Topic 4)
You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.
B. Create an Azure logic appthat has a manual trigger
C. Create an Azure logic app that has an Azure Security Center alert trigger.
D. Create an Azure logic appthat has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

Answer: AC

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

NEW QUESTION 250
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 254
- (Topic 4)
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

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

Answer: D

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

NEW QUESTION 259
- (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 260
- (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 261
- (Topic 4)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 262
- (Topic 4)
You have a Microsoft Sentinel workspace that contains the following incident. Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident. What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Answer: A

Explanation:
Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.

NEW QUESTION 266
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.

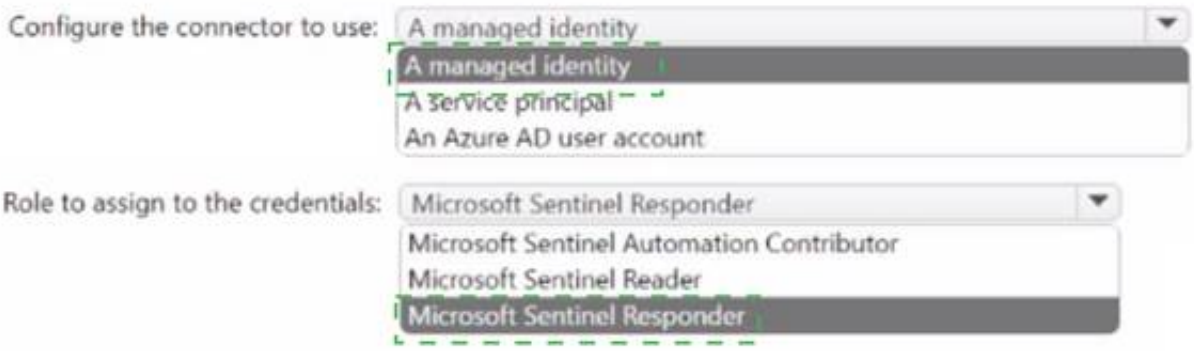
NEW QUESTION 267
HOTSPOT - (Topic 4)
You have a Microsoft Sentinel workspace named sws1.
You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:
• Minimize administrative effort.
• Use the principle of least privilege.
How should you configure the credentials? 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

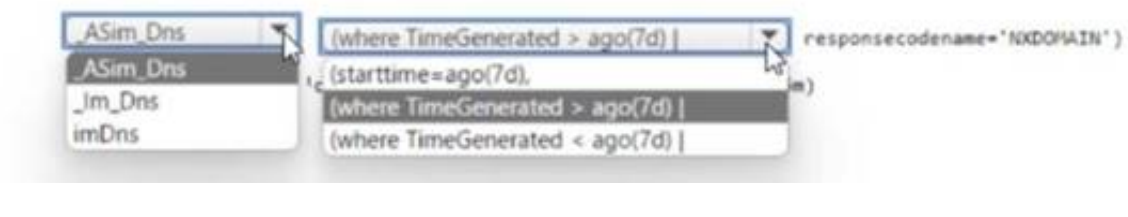
Explanation:

Answer Area



NEW QUESTION 268
HOTSPOT - (Topic 4)
You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query?
To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 272
- (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 275
HOTSPOT - (Topic 4)
You are informed of an increase in malicious email being received by users.
You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.
How should you complete the query? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point.

```
let MaliciousEmails = [                    ▼]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [                                 ▼]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [                                        ▼]
   select 20
   take 20
   top 20
```

A. Mastered

B. Not Mastered

Answer: A

Explanation:

```
let MaliciousEmails = [                    ▼]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [                                 ▼]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [                                        ▼]
   select 20
   take 20
   top 20
```

NEW QUESTION 278

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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