

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

HOTSPOT - (Topic 1)

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

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

NOTE: Each correct selection is worth one point.

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

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

	▼
0	
1	
2	
3	

Query element required to correlate data between tenants:

	▼
extend	
project	
workspace	

NEW QUESTION 2

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

Internal threat:

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

External threat:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Internal threat:

Add resource locks to the key vault.

Modify the access policy settings for the key vault.

Modify the role-based access control (RBAC) settings for the key vault.

External threat:

Implement Azure Firewall.

Modify the Key Vault firewall settings.

Modify the network security groups (NSGs).

NEW QUESTION 3

- (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 4

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

- A. executive
- B. sales
- C. marketing

Answer: B

Explanation:

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

NEW QUESTION 5

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

Actions

Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

Provide global administrator credentials to the litware.com Azure AD tenant.

Install the sensor on DC1.

Install the standalone sensor on DC1.

Answer Area

⬅️

➡️

⬆️

⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Step 1: log in to <https://portal.atp.azure.com> as a global admin
Step 2: Create the instance
Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor.

NEW QUESTION 6

HOTSPOT - (Topic 2)

You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Log Analytics workspace to use:

	▼
A new Log Analytics workspace in the East US Azure region	
Default workspace created by Azure Security Center	
LA1	

Windows security events to collect:

	▼
All Events	
Common	
Minimal	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Log Analytics workspace to use:

	▼
A new Log Analytics workspace in the East US Azure region	
Default workspace created by Azure Security Center	
LA1	

Windows security events to collect:

	▼
All Events	
Common	
Minimal	

NEW QUESTION 7

HOTSPOT - (Topic 2)

You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Log Analytics workspace to use:

	▼
A new Log Analytics workspace in the East US Azure region	
Default workspace created by Azure Security Center	
LA1	

Windows security events to collect:

	▼
All Events	
Common	
Minimal	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Log Analytics workspace to use:

	▼
A new Log Analytics workspace in the East US Azure region	
Default workspace created by Azure Security Center	
LA1	

Windows security events to collect:

	▼
All Events	
Common	1
Minimal	

NEW QUESTION 8

- (Topic 2)

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Onboarding settings from Device management in Microsoft Defender Security Center
- B. Cloud App Security anomaly detection policies
- C. Advanced features from Settings in Microsoft Defender Security Center
- D. the Cloud Discovery settings in Cloud App Security

Answer: CD

Explanation:

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/mde-govern>

NEW QUESTION 9

- (Topic 2)

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

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 10

- (Topic 3)

You need to 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 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:

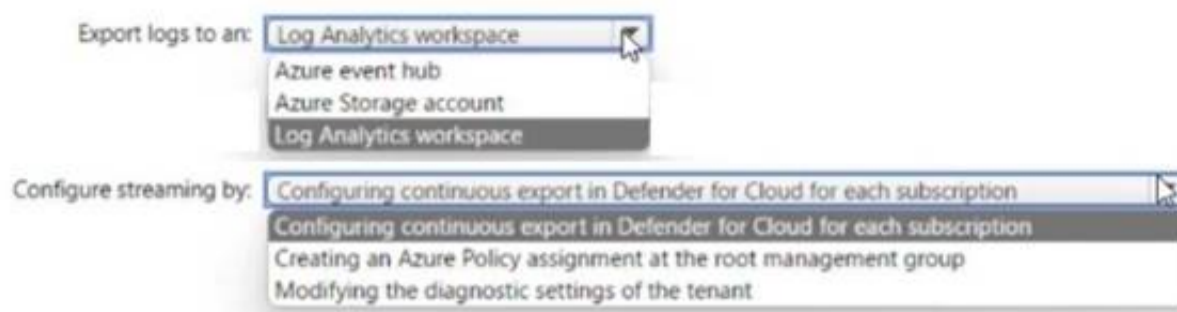
<https://docs.microsoft.com/en-us/azure/sentinel/roles>

NEW QUESTION 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

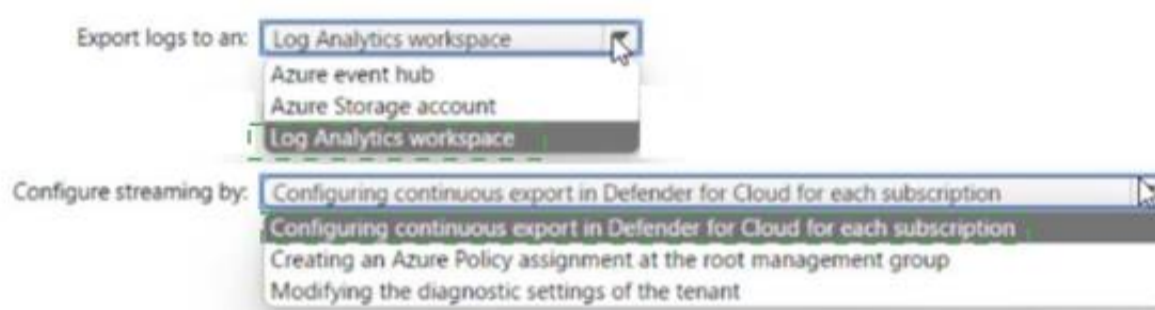


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 17

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
```

extend

join

project

```
| project AlertId
```

```
| join AlertInfo on AlertId
```

```
|  AlertId, Timestamp, Title, Severity, Category
```

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 22

DRAG DROP - (Topic 4)

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

Actions

Add a Syslog connector to the workspace.

Add an Microsoft Sentinel workbook.

Add Microsoft Sentinel to a workspace.

Install the Log Analytics agent for Linux on the virtual machines.

Add a Security Events connector to the workspace.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Add a Syslog connector to the workspace.

Add an Microsoft Sentinel workbook.

Add Microsoft Sentinel to a workspace.

Install the Log Analytics agent for Linux on the virtual machines.

Add a Security Events connector to the workspace.

Answer Area

Add Microsoft Sentinel to a workspace.

Install the Log Analytics agent for Linux on the virtual machines.

Add a Security Events connector to the workspace.

NEW QUESTION 26

- (Topic 4)

You have an Azure subscription that uses Microsoft Sentinel. You detect a new threat by using a hunting query. You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort. What should you do?

- A. Create a playbook.
- B. Create a watchlist.
- C. Create an analytics rule.
- D. Add the query to a workbook.

Answer: A

Explanation:

By creating an analytics rule, you can set up a query that will automatically run and alert you when the threat is detected, without having to manually run the query. This will help minimize administrative effort, as you can set up the rule once and it will run on a schedule, alerting you when the threat is detected. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-rule>

NEW QUESTION 30

- (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 32

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace that contains a custom workbook.
You need to query the number of daily security alerts. The solution must meet the following requirements:

- Identify alerts that occurred during the last 30 days.
- Display the results in a timechart.

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

Answer Area

SecurityAlert

| where TimeGenerated >= ago(30d)

|

lookup
project
summarize

 count() by ProviderName,

bin
make series
range

 (TimeGenerated, 1d)

| render timechart

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

SecurityAlert

| where TimeGenerated >= ago(30d)

|

lookup
project
summarize

 count() by ProviderName,

bin
make series
range

 (TimeGenerated, 1d)

| render timechart

NEW QUESTION 34

- (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 37

HOTSPOT - (Topic 4)
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2. You have the hunting query shown in the following exhibit.

Run Time range : Set in query Save Share + New alert rule Export Pin to Format query

1 AuditLogs
2 where TimeGenerated >ago(7d)
3 where OperationName == "Add user"
4 project AddedTime = TimeGenerated, user = tostring(TargetResources[0].userPrincipalName)
5 join (AzureActivity
6 where OperationName == "Create role assignment"
7 project OperationName, RoleAssignmentTime = TimeGenerated, user = Caller) on user
8 project-away user1
9

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.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User3.	<input type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	<input type="radio"/>	<input checked="" type="radio"/>
The query will identify the creation of User3.	<input checked="" type="radio"/>	<input type="radio"/>
The query will identify the creation of User5.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 40

HOTSPOT - (Topic 4)

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

View the window

You need to test LA1 in Security Center.

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

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered

When an Azure Security Center Alert is created or triggered

When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations

Workflow automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Set the LA1 trigger to:

When an Azure Security Center Recommendation is created or triggered

When an Azure Security Center Alert is created or triggered

When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

Recommendations

Workflow automation

NEW QUESTION 43

- (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 48

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

|

	▼
extend	
join	
project	
union	

 FileName, SHA256

) on SHA256

|

	▼
extend	
join	
project	
union	

 Timestamp, FileName, SHA256, DeviceName, DeviceId,

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 50

- (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 53

HOTSPOT - (Topic 4)

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

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

NOTE: Each correct selection is worth one point.

```

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

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

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

```

NEW QUESTION 55

- (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 60

- (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 61

- (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 63

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.

▼

AzureActivity
BehaviorAnalytics
SecurityEvent

```

| 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()
bin()
count()

```

    ) 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 64

- (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 66

- (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 69

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, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles	Answer Area
Resource Group Owner	Enable and disable advanced features of Microsoft Defender for Cloud: <input type="text"/>
Security Admin	Apply security recommendations to a resource: <input type="text"/>
Subscription Contributor	
Subscription Owner	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Roles

Resource Group Owner

Security Admin

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable advanced features of Microsoft Defender for Cloud:

Security Admin

Apply security recommendations to a resource:

Subscription Contributor

NEW QUESTION 70

HOTSPOT - (Topic 4)

You need to create a query for a workbook. The query must meet the following requirements:

? List all incidents by incident number.

? Only include the most recent log for each incident.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

SecurityIncident

▼

project

sort

summarize

▼

arg_max

limit

top

(LasModifiedTime,*) by IncidentNumber

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

SecurityIncident

▼

project

sort

summarize

▼

arg_max

limit

top

(LasModifiedTime,*) by IncidentNumber

NEW QUESTION 73

HOTSPOT - (Topic 4)

You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).

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

Answer Area

To the AD DS domain controllers, deploy:

The Azure Connected Machine agent

Microsoft Defender for Identity sensors

The Azure Connected Machine agent

The Azure Monitor agent

For Sentinel1, configure:

The Audit Logs data source

The Audit Logs data source

The Security Events data source

The Signin Logs data source

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

To the AD DS domain controllers, deploy:

The Azure Connected Machine agent

Microsoft Defender for Identity sensors

The Azure Connected Machine agent

The Azure Monitor agent

For Sentinel1, configure:

The Audit Logs data source

The Audit Logs data source

The Security Events data source

The Signin Logs data source

NEW QUESTION 77

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

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

Answer: A

NEW QUESTION 81

- (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 85

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

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

and

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 89

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

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 93

- (Topic 4)
You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Microsoft Sentinel bookmarks
- B. Azure Automation runbooks
- C. Microsoft Sentinel automation rules
- D. Microsoft Sentinel playbooks
- E. Azure Functions apps

Answer: CE

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

NEW QUESTION 94

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.

Actions

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

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

Enable Azure Defender for the subscription.

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

Run the executable file and specify the appropriate arguments.

Rename the executable file as AlertTest.exe.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

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

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

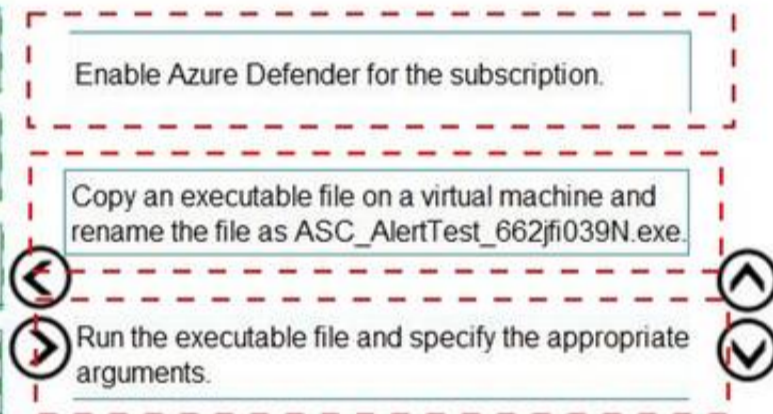
Enable Azure Defender for the subscription.

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

Run the executable file and specify the appropriate arguments.

Rename the executable file as AlertTest.exe.

Answer Area



NEW QUESTION 97

- (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

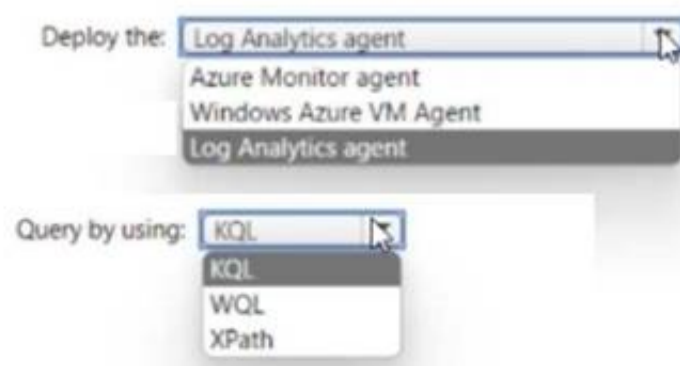
Answer: C

NEW QUESTION 100

HOTSPOT - (Topic 4)

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

Answer Area



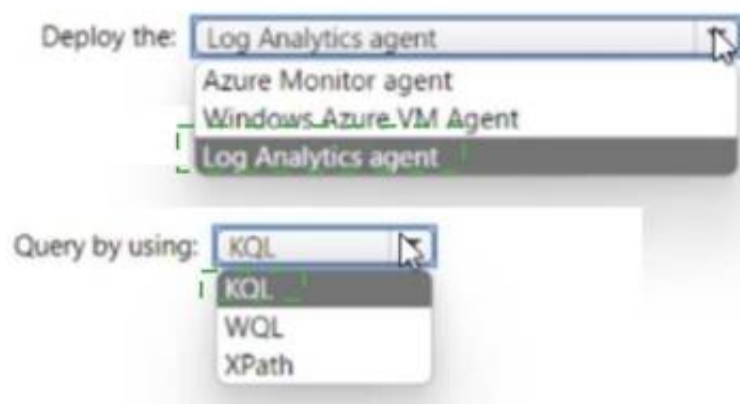
- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 101

- (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 Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 105

- (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 110

DRAG DROP - (Topic 4)

Your company deploys Azure Sentinel.

You plan to delegate the administration of Azure Sentinel to various groups. You need to delegate the following tasks:

? Create and run playbooks

? Create workbooks and analytic rules.

The solution must use the principle of least privilege.

Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

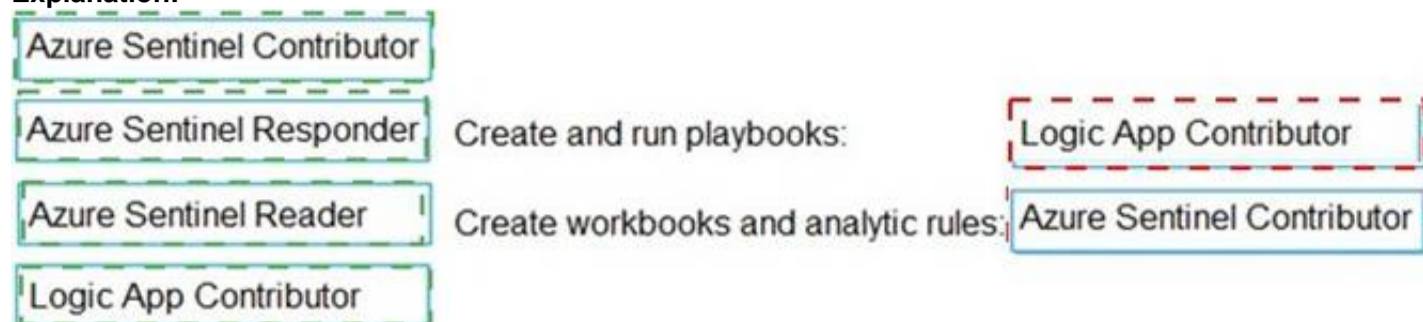
NOTE: Each correct selection is worth one point.

Azure Sentinel Contributor	
Azure Sentinel Responder	Create and run playbooks:
Azure Sentinel Reader	Create workbooks and analytic rules:
Logic App Contributor	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 112

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.)



Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >
[Learn more](#)

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

Control status: **2 Selected**

Recommendation status: **2 Selected**

Recommendation maturity: **All**

Resource type: **All**

Quick fix available: **All**

Contains exemptions: **All**

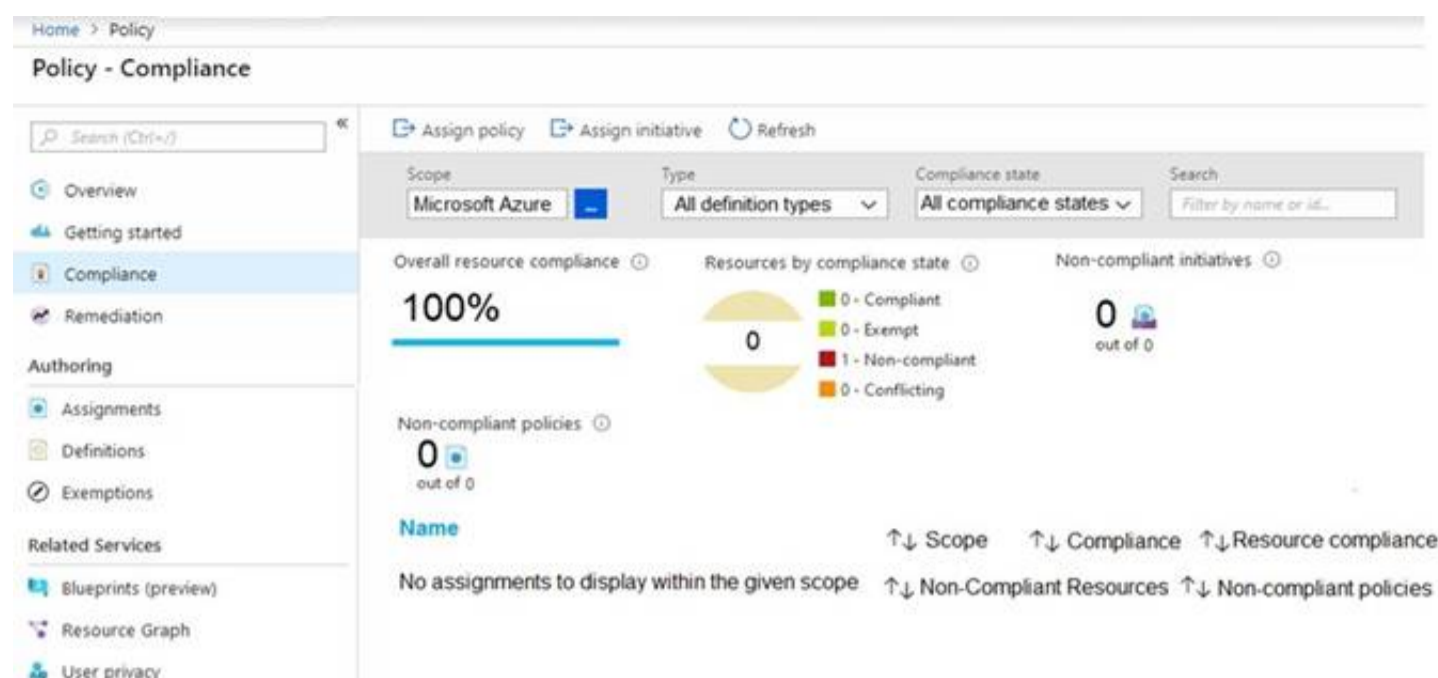
[Reset filters](#)

Group by controls:

☒ On

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

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.	<input type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input type="radio"/>	<input type="radio"/>

- 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.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" type="radio"/>
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 115

- (Topic 4)

You need to ensure that you can run hunting queries to meet the Microsoft Sentinel requirements. Which type of workspace should you create?

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

Answer: D

NEW QUESTION 117

DRAG DROP - (Topic 4)

You have the resources shown in the following table.

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

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

Resources

SW1
CEF1
Server1
Server2

Answer Area

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

From the Log Analytics agent, disable Syslog synchronization.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Resources

SW1
CEF1
Server1
Server2

Answer Area

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

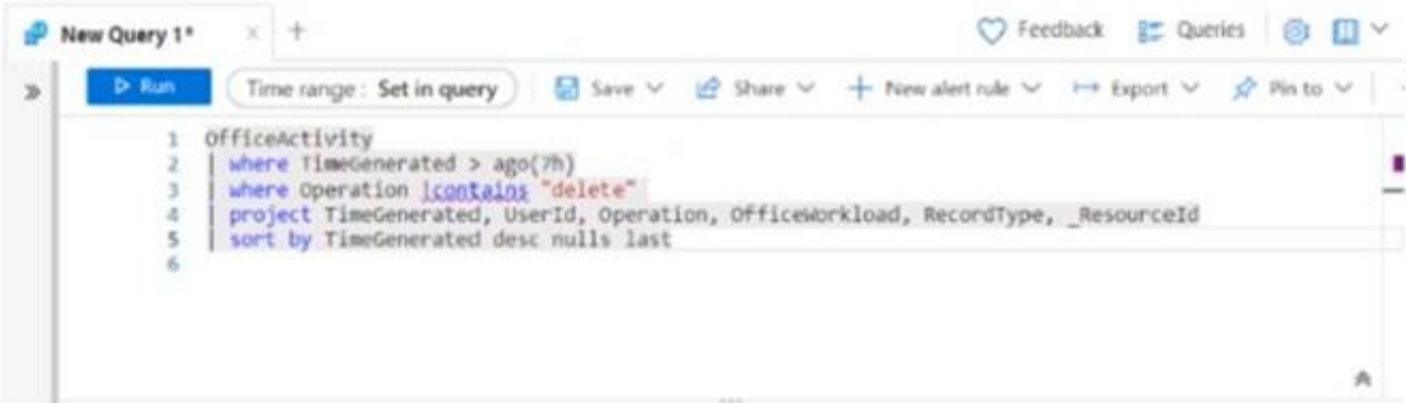
From the Log Analytics agent, disable Syslog synchronization.

Server1

CEF1

NEW QUESTION 120

- (Topic 4)
You have a Microsoft Sentinel workspace.
You have a query named Query1 as shown in the following exhibit.



You plan to create a custom parser named Parser 1. You need to use Query1 in Parser1. What should you do first?

- A. Remove line 2.
- B. In line 4. remove the TimeGenerated predicate.
- C. Remove line 5.
- D. In line 3, replace the 'contains operator with the !has operator.

Answer: A

Explanation:

This can be confirmed by referring to the official Microsoft documentation on creating custom log queries in Azure Sentinel, which states that the “has” operator should not be used in the query, and that it is unnecessary.
 Reference: <https://docs.microsoft.com/en-us/azure/sentinel/query-custom-logs>

NEW QUESTION 125

- (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 130

HOTSPOT - (Topic 4)

You have a Microsoft Sentinel workspace

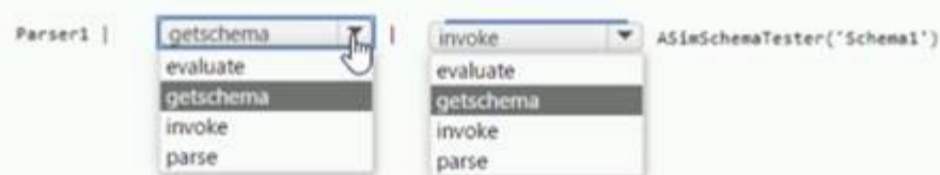
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

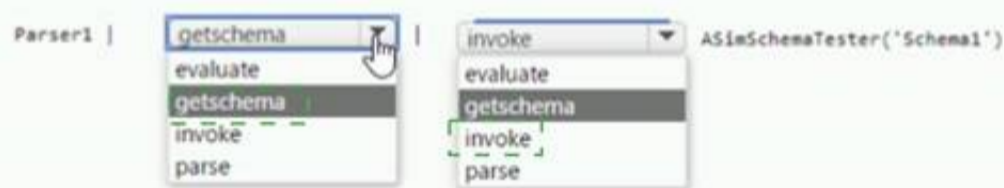


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 132

- (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 137

- (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 142

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

Group1: Security Admin
 Contributor
 Owner
 Security Admin
 Security Assessment Contributor

Group2: Contributor
 Contributor
 Owner
 Security Admin
 Security Assessment Contributor

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Group1: Security Admin
 Contributor
 Owner
 Security Admin
 Security Assessment Contributor

Group2: Contributor
 Contributor
 Owner
 Security Admin
 Security Assessment Contributor

NEW QUESTION 145

- (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 148

- (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 149

- (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 152

- (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 (IAM) role for Defender for Cloud.
- C. Configure AWS Security Hub.
- D. Deploy the AWS Systems Manager (SSM) agent

Answer: D

NEW QUESTION 155

HOTSPOT - (Topic 4)

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

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

NOTE: Each correct selection is worth one point.

Answer Area

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

1
0
1
2
3

Query element required to correlate data between tenants:

workspace
extend
project
workspace

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

1
0
1
2
3

Query element required to correlate data between tenants:

workspace
extend
project
workspace

NEW QUESTION 159

- (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 163

DRAG DROP - (Topic 4)

You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point

Values

| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

ActionType == FailureReason

DeviceEvents

DeviceLogonEvents

Answer Area

and

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Values

| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType == FailureReason

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

ActionType == "LogonFailed"

ActionType == FailureReason

DeviceEvents

DeviceLogonEvents

Answer Area

DeviceLogonEvents

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

and

ActionType == FailureReason

| summarize LogonFailures=count()
by DeviceName, LogonType

NEW QUESTION 166

- (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 168

DRAG DROP - (Topic 4)

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions		Answer Area
Enable Microsoft Defender for Cloud's enhanced security features for the subscription.	<div> <div>></div> <div><</div> </div>	<div> <div>^</div> <div>v</div> </div>
Change the alert severity threshold for emails to Medium .		
Rename the executable file as AlertTest.exe.		
Change the alert severity threshold for emails to Low .		
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.		
Run the executable file and specify the appropriate arguments.		

A. Mastered

B. Not Mastered

Answer: A

Explanation:

To validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server, you should perform the following three actions in sequence:

? Copy an executable file on a virtual machine and rename the file as

ASC_AlertTest_662jfi039N.exe

? Run the executable file and specify the appropriate arguments

? Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

These actions will simulate a malicious activity on the virtual machine and generate an alert in Defender for Cloud. You can then verify the alert details and response recommendations in the Azure portal. For more information, see Alert validation - Microsoft Defender for Cloud.

NEW QUESTION 172

- (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 suppress 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 175

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.

Answer Area

Create: A management project and a custom role
 A management group and an Azure AD service principal
 A management project and a custom role
 An Azure AD administrative unit and a managed identity

By: Running a script in GCP Cloud Shell
 Deploying a Bicep template
 Running a script in Azure Cloud Shell
 Running a script in GCP Cloud Shell

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Create: A management project and a custom role
 A management group and an Azure AD service principal
 A management project and a custom role
 An Azure AD administrative unit and a managed identity

By: Running a script in GCP Cloud Shell
 Deploying a Bicep template
 Running a script in Azure Cloud Shell
 Running a script in GCP Cloud Shell

NEW QUESTION 178

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.

Actions

From the Data controller settings in the Azure portal, create an Azure Arc data controller.

On the on-premises servers, install the Azure Monitor agent.

From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

Answer Area

1
2
3

1
2
3

- 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 182

HOTSPOT - (Topic 4)

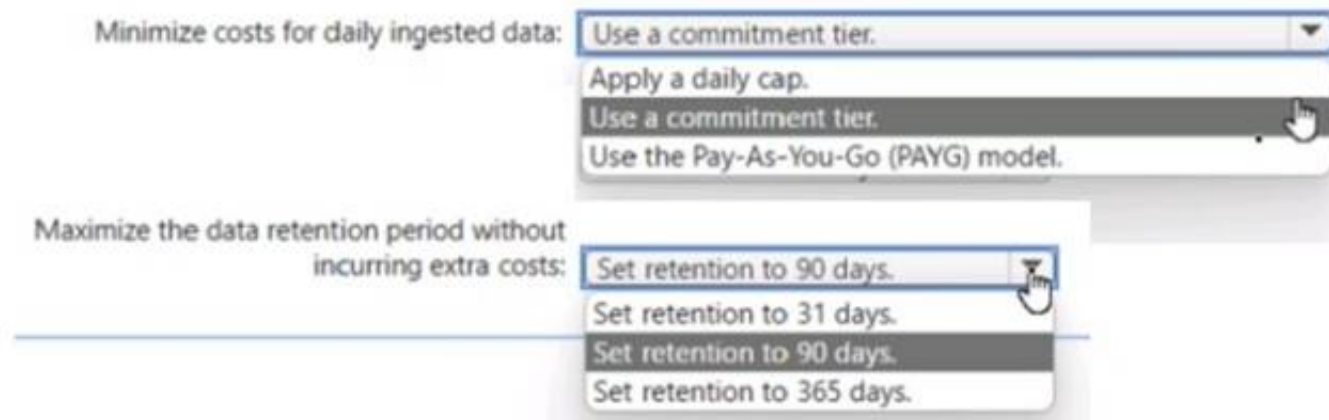
You have an Azure subscription.

You plan to implement an Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

You need to configure storage for the workspace. The solution must meet the following requirements:

- Minimize costs for daily ingested data.
- Maximize the data retention period without incurring extra costs.

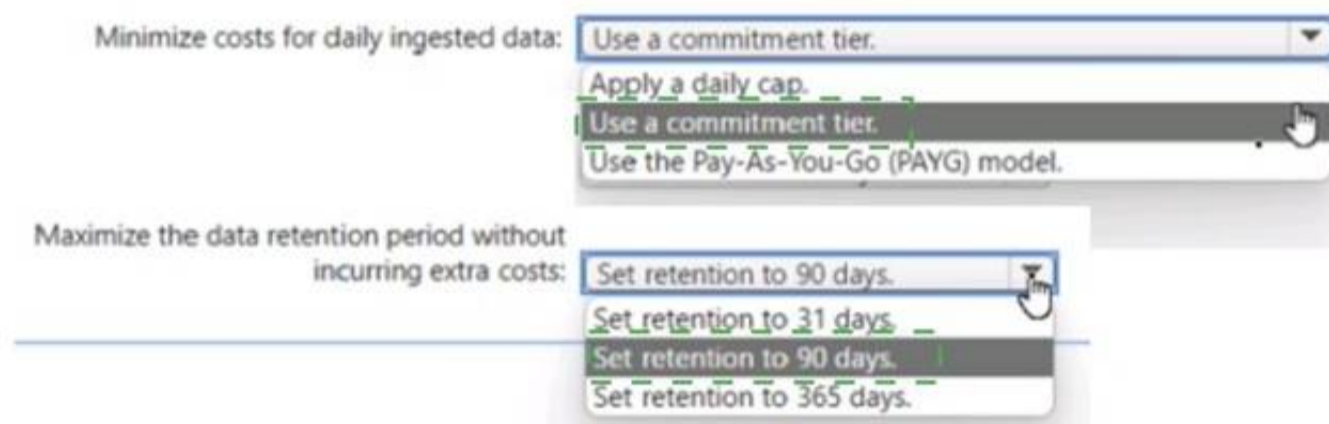
What should you do for each requirement? To answer, select the appropriate options in the answer area. NOTE Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 183

HOTSPOT - (Topic 4)

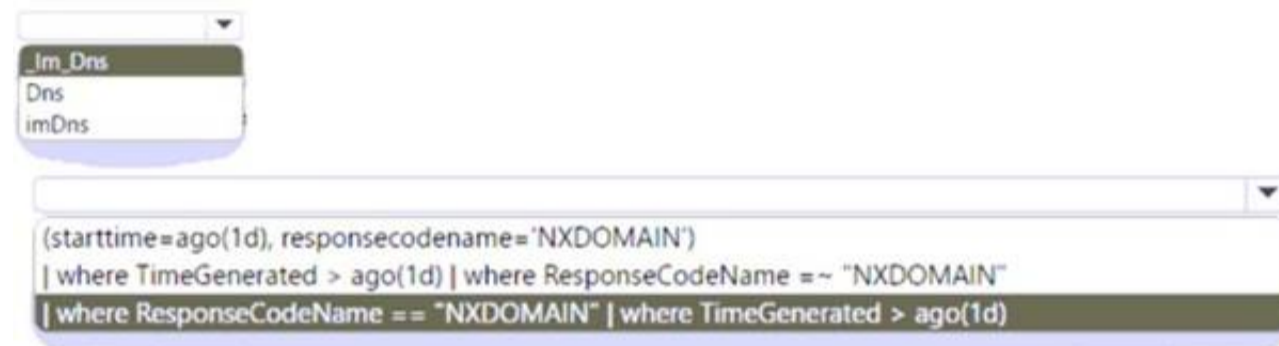
You have a Microsoft Sentinel workspace named Workspaces You configure Workspace1 to c

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

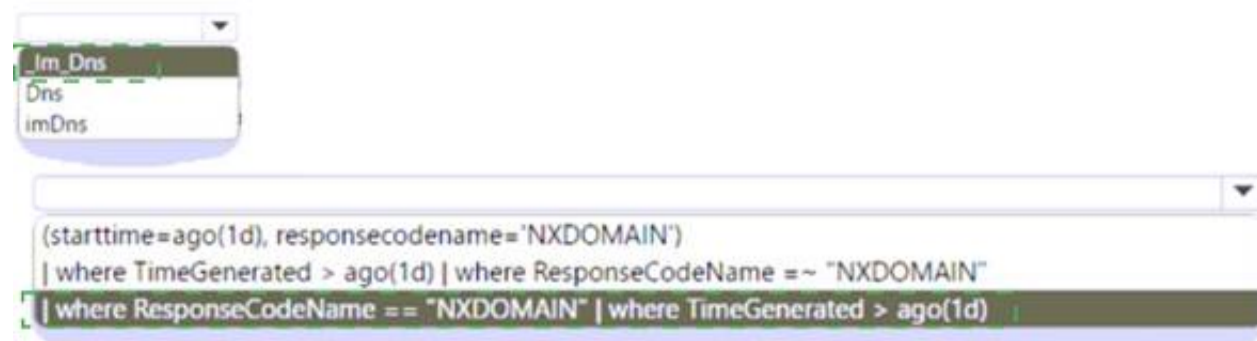
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 185

- (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 following 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 188

- (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 191

HOTSPOT - (Topic 4)

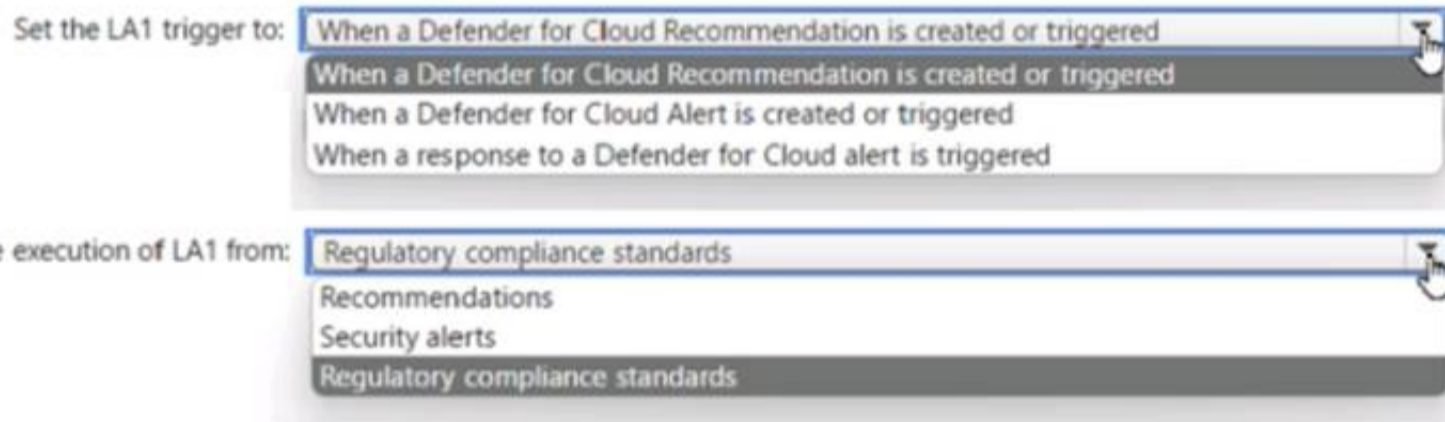
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

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 192

- (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 193

DRAG DROP - (Topic 4)

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

? The modification of local group memberships

? The purging of event logs

Which three actions should you perform in sequence in the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions	Answer Area
From the details pane of the incident, select Investigate .	
From the investigation blade, select the entity that represents VM1.	
From the investigation blade, select the entity that represents powershell.exe.	
From the investigation blade, select Timeline .	
From the investigation blade, select Info .	
From the investigation blade, select Insights .	

- 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 195

- (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 198

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 202

- (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 204

- (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 206

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.

Answer Area

Configure the connector to use:

Role to assign to the credentials:

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Configure the connector to use:

Role to assign to the credentials:

NEW QUESTION 210

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 214

HOTSPOT - (Topic 4)

You use Azure Sentinel to monitor irregular Azure activity.
 You create custom analytics rules to detect threats as shown in the following exhibit.

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

General Set rule logic Incident settings Automated response Review and create

Define the logic for your new analytics rule.

Rule query

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

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

[View query results >](#)

Map entities

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

Entity Type	Column
Account	<div>Choose column ▼ Add</div>
Host	<div>Choose column ▼ Add</div>
IP	<div>Choose column ▼ Add</div>
URL	<div>Choose column ▼ Add</div>
FileHash	<div>Choose column ▼ Add</div>

Query scheduling

Run query every *

5 ✓

Minutes ▼

Lookup data from the last * ⓘ

5

Hours ▼

Alert threshold

Generate alert when number of query results *

Is greater than ▼

2 ✓

Event grouping

Configure how rule query results are grouped into alerts

- ☒ Group all events into a single alert
- ☐ Trigger an alert for each event

Suppression

Stop running query after alert is generated ⓘ

On Off

Stop running query for *

5 ✓

Hours ▼

[Previous](#)

[Next : Incident settings >](#)

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

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

NOTE: Each correct selection is worth one point.

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

▼

0 alerts

1 alert

2 alerts

3 alerts

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

▼

0 alerts

1 alert

2 alerts

3 alerts

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 219

- (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 220

- (Topic 4)

You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege. Which role should you assign to SecAdmin1?

- A. the Security Reader role for the subscription
- B. the Contributor for the subscription
- C. the Contributor role for RG1
- D. the Owner role for RG1

Answer: C

NEW QUESTION 222

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 223

.....

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