

Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst



NEW QUESTION 1

HOTSPOT - (Topic 1)

You need to create an advanced hunting query to investigate the executive team issue.

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 TimeStamp > ago(2d)
```

```
| summarize activityCount =
```

ActionType, AccountDisplayName

```
| where activityCount > 5
```

by FolderPath, FileName,

avg()
count()
sum()

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```
| where TimeStamp > ago(2d)
```

```
| summarize activityCount =
```

ActionType, AccountDisplayName

```
| where activityCount > 5
```

by FolderPath, FileName,

avg()
count()
sum()

NEW QUESTION 2

- (Topic 1)

You need to remediate active attacks to meet the technical requirements. What should you include in the solution?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 3

- (Topic 1)

The issue for which team can be resolved by using Microsoft Defender for Office 365?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 4

- (Topic 1)

You need to complete the query for failed sign-ins to meet the technical requirements. Where can you find the column name to complete the where clause?

- A. Security alerts in Azure Security Center
- B. Activity log in Azure
- C. Azure Advisor
- D. the query windows of the Log Analytics workspace

Answer: D

NEW QUESTION 5

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:

Windows security events to collect:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Log Analytics workspace to use:

Windows security events to collect:

NEW QUESTION 6

- (Topic 2)

You need to implement the Azure Information Protection requirements. What should you configure first?

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

Answer: D

Explanation:

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

NEW QUESTION 7

- (Topic 3)

You need to implement the scheduled rule for incident generation based on rulequery1. What should you configure first?

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

Answer: D

NEW QUESTION 8

- (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 9

- (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 10

- (Topic 4)

You have a custom analytics rule to detect threats in Azure Sentinel.

You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.

What is a possible cause of the issue?

- A. There are connectivity issues between the data sources and Log Analytics.
- B. The number of alerts exceeded 10,000 within two minutes.
- C. The rule query takes too long to run and times out.
- D. Permissions to one of the data sources of the rule query were modified.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 10

- (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

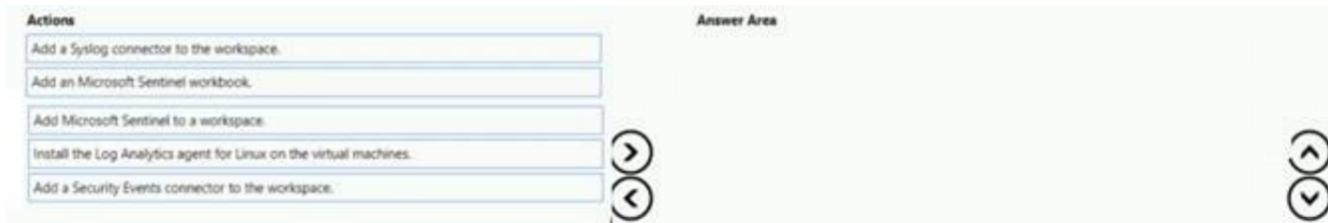
NEW QUESTION 13

DRAG DROP - (Topic 4)

You have an Azure subscription that contains 100 Linux virtual machines.

You need to configure Microsoft Sentinel to collect event logs from the virtual machines. Which three actions should you perform in sequence? To answer, move the appropriate

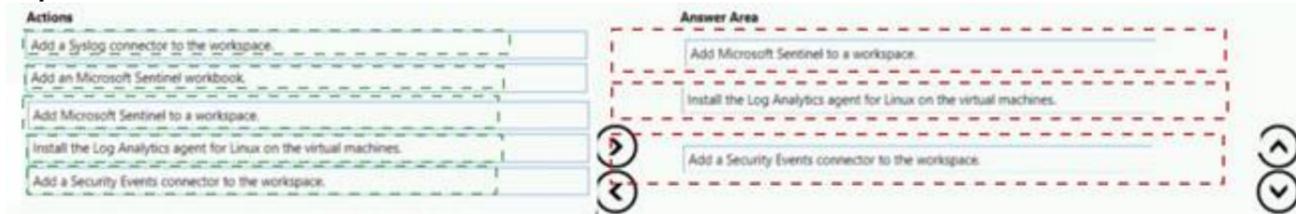
actions from the list of actions to the answer area and arrange them in the correct order.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 18

- (Topic 4)

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant. You need to identify all the changes made to Domain Admins group during the past 30 days. What should you use?

- A. the Azure Active Directory Provisioning Analysis workbook
- B. the Overview settings of Insider risk management
- C. the Modifications of sensitive groups report in Microsoft Defender for Identity
- D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Answer: C

NEW QUESTION 22

- (Topic 4)

You have the resources shown in the following Table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to enable Microsoft Defender for Servers on each resource. Which resources will require the installation of the Azure Arc agent?

- A. Server 3 only
- B. Server1 and Server4 only
- C. Server 1, Server2, and Server4 only
- D. Server 1, Server2, Server3, and Server4

Answer: B

NEW QUESTION 27

HOTSPOT - (Topic 4)

You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

How should you configure the content search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Locations: 
 Exchange mailboxes
 Exchange public folders
 SharePoint sites

Keywords: 
 Kind
 Category
 ItemClass
 Kind

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Locations: 
 Exchange mailboxes
 Exchange public folders
 SharePoint sites

Keywords: 
 Kind
 Category
 ItemClass
 Kind

NEW QUESTION 28

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": " ,
    "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'), ' ,
          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 29

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 30

- (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 32

- (Topic 4)

Your company deploys the following services:

? Microsoft Defender for Identity

? Microsoft Defender for Endpoint

? Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.

Which two roles should assign to the analyst? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 34

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

▼		▼		(LasModifiedTime,*) by IncidentNumber
project		arg_max		
sort		limit		
summarize		top		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

SecurityIncident

▼		▼		(LasModifiedTime,*) by IncidentNumber
project		arg_max		
sort		limit		
summarize		top		

NEW QUESTION 38

- (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 40

- (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://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal>

NEW QUESTION 42

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.

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Microsoft Teams:

	▼
Custom	
Office 365	
Security Events	
Syslog	

Linux virtual machines in Azure:

	▼
Custom	
Office 365	
Security Events	
Syslog	

NEW QUESTION 43

- (Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have Linux virtual machines on Amazon Web Services (AWS). You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 44

- (Topic 4)

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.34.32- 171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

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

Answer: D

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference: [1] <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence-manage-indicators>

NEW QUESTION 49

- (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 53

HOTSPOT - (Topic 4)

You have an Microsoft Sentinel workspace named SW1.

You plan to create a custom workbook that will include a time chart.

You need to create a query that will identify the number of security alerts per day for each provider.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName,
|
```

render

materialize

project

render

bin

bin

series_add

series_fill_linear

take

(TimeGenerated, 1d)

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

```
SecurityAlert
| where TimeGenerated >= ago(30d)
| summarize count() by ProviderName,
|
```

render

materialize

project

render

bin

bin

series_add

series_fill_linear

take

(TimeGenerated, 1d)

NEW QUESTION 58

DRAG DROP - (Topic 4)

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Answer Area

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.

- Configure the GCP Security Command Center.
- Enable Security Health Analytics.
- Enable the GCP Security Command Center API.
- Create a dedicated service account and a private key.
- From Azure Security Center, add cloud connectors.



NEW QUESTION 59

- (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 62

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

Answer Area

- 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Answer Area

- 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.

- Enable Azure Defender for the subscription.
- 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.



NEW QUESTION 67

- (Topic 4)

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

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

Answer: DE

NEW QUESTION 71

HOTSPOT - (Topic 4)

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 73

- (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 74

- (Topic 4)

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

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a scheduled query rule for a data connector. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 77

- (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 80

- (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 84

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.

Actions

- Configure the Suppress similar alerts settings.
- Configure the Mitigate the threat settings.
- Filter by alert title.
- Select **Take action**.
- Configure the Prevent future attacks settings.
- Configure the Trigger automated response settings.

➤

➤

Answer Area

- 1
- 2
- 3

- 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 88

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 style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;"> > < </div> <div style="text-align: center;"> ↑ ↓ </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 90

- (Topic 4)

Your company uses Microsoft Sentinel

A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

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

Answer: A

Explanation:

The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac>

NEW QUESTION 92

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.

Minimize costs for daily ingested data:

- Use a commitment tier.
- Apply a daily cap.
- Use a commitment tier.
- Use the Pay-As-You-Go (PAYG) model.

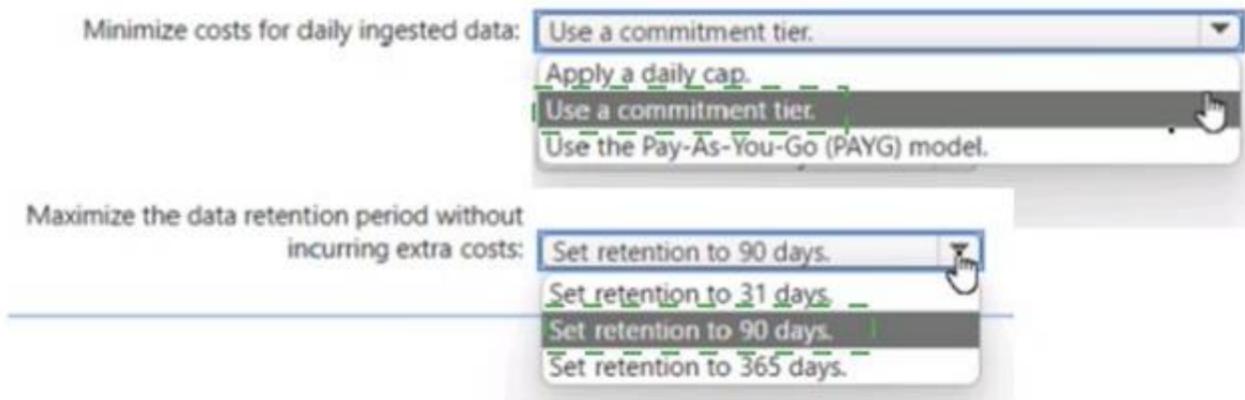
Maximize the data retention period without incurring extra costs:

- Set retention to 90 days.
- Set retention to 31 days.
- Set retention to 90 days.
- Set retention to 365 days.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 93

- (Topic 4)

You have a playbook in Azure Sentinel.

When you trigger the playbook, it sends an email to a distribution group.

You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.

What should you do?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 96

- (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 98

- (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 103

HOTSPOT - (Topic 4)

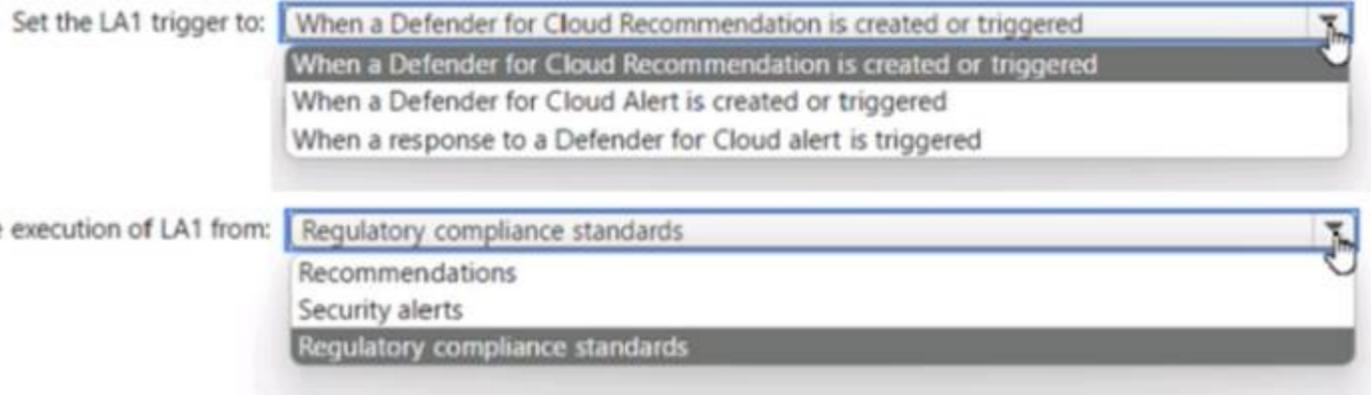
You have an Azure subscription that has Azure Defender enabled for all supported resource types.

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.

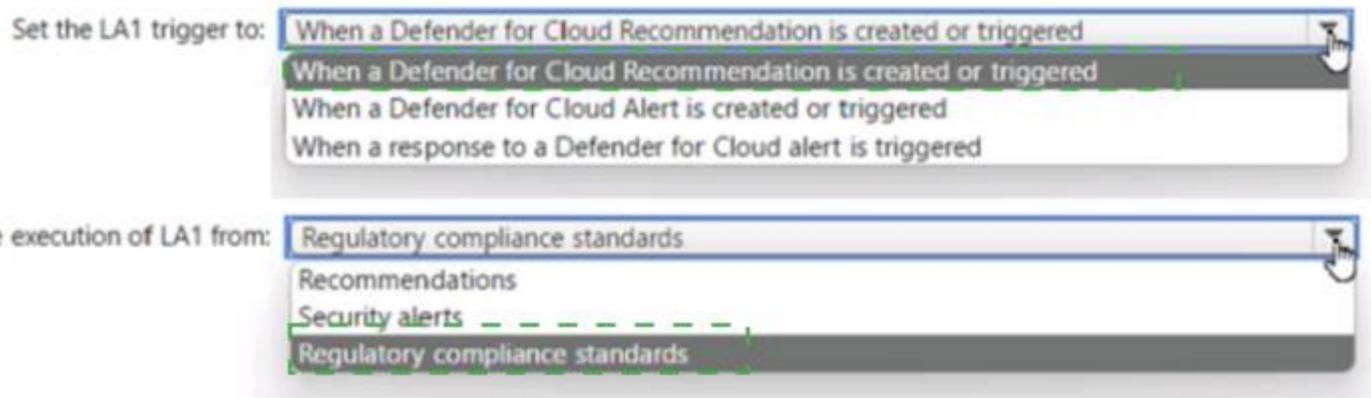
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 106

- (Topic 4)

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

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

Answer: A

NEW QUESTION 109

- (Topic 4)

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. What should you do?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 112

- (Topic 4)

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

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

D. the Azure Pipelines agent

Answer: C

NEW QUESTION 116

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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

100% Actual & Verified — Instant Download, Please Click
[Order The SC-200 Practice Test Here](#)