

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 2

- (Exam 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
    
```

▼
 CloudAppEvents
 DeviceFileEvents
 DeviceProcessEvents

▼
 avg()
 count()
 sum()

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

```

| where TimeStamp > ago(2d)

| summarize activityCount =
ActionType, AccountDisplayName
| where activityCount > 5
    
```

▼
 CloudAppEvents
 DeviceFileEvents
 DeviceProcessEvents

▼
 avg()
 count()
 sum()

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 4

- (Exam Topic 1)

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.

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

Answer Area

Internal threat: ▼

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

External threat: ▼

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 5

- (Exam Topic 2)

You need to add notes to the events to meet the Azure Sentinel requirements.

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

Actions		Answer Area
Add a bookmark and map an entity.		
From Azure Monitor, run a Log Analytics query.		
Add the query to favorites.	⬅	⬆
Select a query result.	➡	⬇
From the Azure Sentinel workspace, run a Log Analytics query.		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated
 Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

NEW QUESTION 6

- (Exam Topic 2)

You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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

NOTE: Each correct selection is worth one point.

Log Analytics workspace to use:

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

Windows security events to collect:

	▼
All Events	
Common	
Minimal	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

NEW QUESTION 7

- (Exam Topic 2)

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:

	▼
Add a security extension	
Configure app connectors	
Configure log collectors	

From Azure Sentinel in the Azure portal:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel>

NEW QUESTION 8

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security information Model (ASIM) parse from a built-in unified ASIM parser.

What should you create in Workspace1?

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

Answer: A

NEW QUESTION 9

- (Exam Topic 3)

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

You need to deploy the log forwarder.

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

Actions

Answer Area

- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.
- Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.
- Download and install the Log Analytics agent.
- Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog>

NEW QUESTION 10

- (Exam Topic 3)

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 10

- (Exam Topic 3)

You have an Azure subscription. You need to delegate permissions to meet the following requirements:

- > Enable and disable Azure Defender.
- > Apply security recommendations to resource.

The solution must use the principle of least privilege.

Which Azure Security Center 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

- Security Admin
- Resource Group Owner
- Subscription Contributor
- Subscription Owner

Enable and disable Azure Defender:

Apply security recommendations to a resource:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

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

NEW QUESTION 14

- (Exam Topic 3)

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 15

- (Exam Topic 3)

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

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

NOTE: Each correct selection is worth one point.

```

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

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert>

NEW QUESTION 16

- (Exam Topic 3)

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

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

NOTE: Each correct selection is worth one point.

Actions	Answer area
Select Pricing & settings.	
Select Security alerts.	
Select IP as the entity type and specify the IP address.	<div style="text-align: center;"> ⏪ ⏩ </div>
Select Azure Resource as the entity type and specify the ID.	<div style="text-align: center;"> ⏪ ⏩ </div>
Select Suppression rules, and then select Create new suppression rule.	<div style="text-align: center;"> ⏪ ⏩ </div>
Select Security policy.	<div style="text-align: center;"> ⏪ ⏩ </div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 19

- (Exam Topic 3)

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled. You need to ensure that the Fusion rule can generate alerts.

What should you do?

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

Answer: B

Explanation:

Reference:

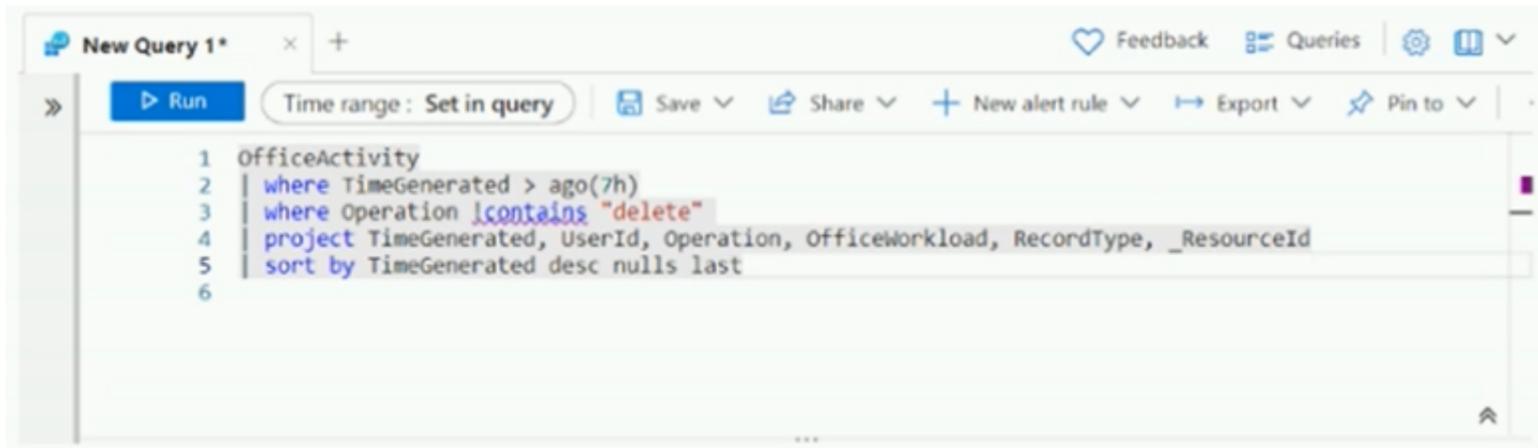
<https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources>

NEW QUESTION 20

- (Exam Topic 3)

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: C

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 24

- (Exam Topic 3)

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 25

- (Exam Topic 3)

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices. Which three actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Answer: ACD

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manag>

NEW QUESTION 29

- (Exam Topic 3)

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 31

- (Exam Topic 3)

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 35

- (Exam Topic 3)

You create a custom analytics rule to detect threats in Azure Sentinel. You discover that the rule fails intermittently.

What are two possible causes of the failures? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. The rule query takes too long to run and times out.
- B. The target workspace was deleted.
- C. Permissions to the data sources of the rule query were modified.
- D. There are connectivity issues between the data sources and Log Analytics

Answer: AD

NEW QUESTION 37

- (Exam Topic 3)

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

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

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center. Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 38

- (Exam Topic 3)

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 42

- (Exam Topic 3)

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 44

- (Exam Topic 3)

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 48

- (Exam Topic 3)

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

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort

Which blade should you use in the Microsoft 365 Defender portal?

- A. Advanced hunting
- B. Threat analytics
- C. Incidents & alerts
- D. Learning hub

Answer: B

Explanation:

To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender-threat-analyti>

NEW QUESTION 49

- (Exam Topic 3)

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

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

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

Actions

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:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

NEW QUESTION 54

- (Exam Topic 3)

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 58

- (Exam Topic 3)

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 60

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

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

NOTE: Each correct selection is worth one point.

```

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

```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: AzureActivity

The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: |

'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous. The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

```

| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner ( AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous\_Listing\_O

```

NEW QUESTION 65

- (Exam Topic 3)

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 69

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the

stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You are configuring Microsoft Defender for Identity integration with Active Directory. From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit. Solution: From 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 73

- (Exam Topic 3)

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 78

- (Exam Topic 3)

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

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 81

- (Exam Topic 3)

You have the following SQL query.

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

Answer Area

Statements	Yes	No
The <code>username</code> field is set as the account entity.	<input type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="radio"/>
The <code>IPList</code> variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
The <code>username</code> field is set as the account entity.	<input type="radio"/>	<input type="checkbox"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="checkbox"/>
The <code>IPList</code> variable is set as the IP address entity.	<input type="radio"/>	<input type="checkbox"/>

NEW QUESTION 84

- (Exam Topic 3)

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

Answer Area

- SW1
- CEF1
- Server1
- Server2

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:

Graphical user interface, text Description automatically generated

Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog>

NEW QUESTION 85

- (Exam Topic 3)

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

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

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

Answer: C

Explanation:

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

NEW QUESTION 87

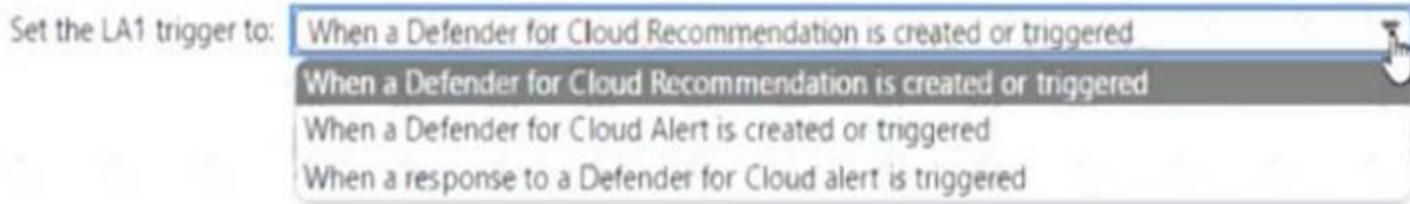
- (Exam Topic 3)

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.

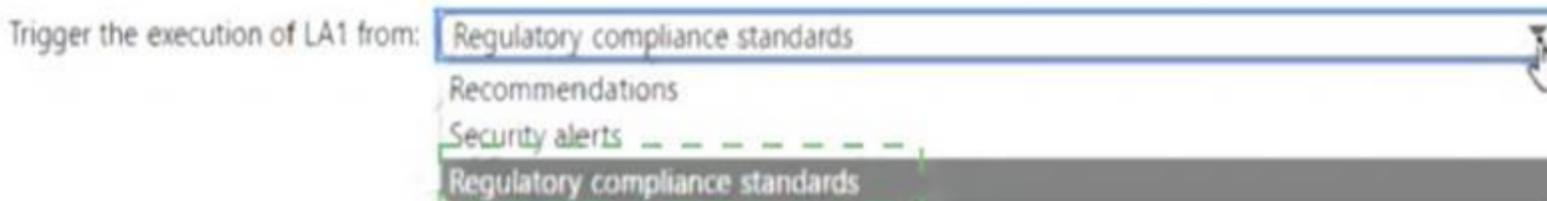
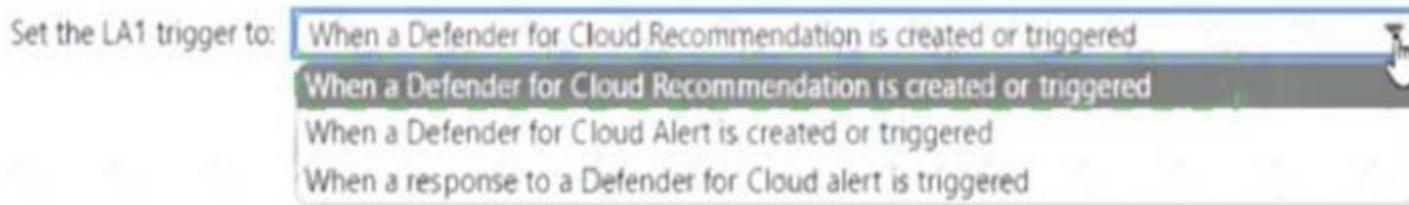
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 92

- (Exam Topic 3)

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses. You determine that 99% of the alerts are legitimate sign-ins from your corporate offices. You need to prevent alerts for legitimate sign-ins from known locations.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Override automatic data enrichment.
- B. Add the IP addresses to the corporate address range category.

- C. Increase the sensitivity level of the impossible travel anomaly detection policy.
- D. Add the IP addresses to the other address range category and add a tag.
- E. Create an activity policy that has an exclusion for the IP addresses.

Answer: AD

NEW QUESTION 94

- (Exam Topic 3)

You have an Azure Sentinel deployment.

You need to query for all suspicious credential access activities.

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

Actions

Answer Area

- From Azure Sentinel, select **Hunting**.
- Select **Run All Queries**.
- Select **New Query**.
- Filter by tactics.
- From Azure Sentinel, select **Notebooks**.



- A. Mastered
- B. Not Mastered

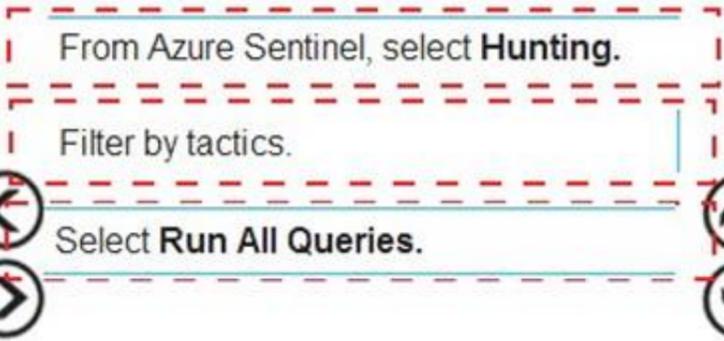
Answer: A

Explanation:

Actions

Answer Area

- From Azure Sentinel, select **Hunting**.
- Select **Run All Queries**.
- Select **New Query**.
- Filter by tactics.
- From Azure Sentinel, select **Notebooks**.



NEW QUESTION 98

- (Exam Topic 3)

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.

What should you configure in Security Center to enable the email notifications?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 103

- (Exam Topic 3)

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.

You are troubleshooting an issue on the virtual machines.

In Security Center, you need to view the alerts generated by the virtual machines during the last five days. What should you do?

- A. Change the rule expiration date of the suppression rule.
- B. Change the state of the suppression rule to Disabled.
- C. Modify the filter for the Security alerts page.
- D. View the Windows event logs on the virtual machines.

Answer: B

Explanation:

Reference:

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

NEW QUESTION 107

- (Exam Topic 3)

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 110

- (Exam Topic 3)

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

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

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 114

- (Exam Topic 3)

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 171.23.34.32-171.23.34.63. 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 171.23.34.32-171.23.34.63.
- 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: C

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>

NEW QUESTION 115

- (Exam Topic 3)

Your company deploys Azure Sentinel.

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

- > Create and run playbooks
- > Create workbooks and analytic rules.

The solution must use the principle of least privilege.

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

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

NOTE: Each correct selection is worth one point.

Azure Sentinel Contributor

Azure Sentinel Responder

Azure Sentinel Reader

Logic App Contributor

Create and run playbooks:

Create workbooks and analytic rules:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A picture containing graphical user interface Description automatically generated

Reference:

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

NEW QUESTION 120

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advance Security information Model (ASIM) parse from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 125

- (Exam Topic 3)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender. You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft 365 Defender portal?

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

Answer: C

Explanation:

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents>

NEW QUESTION 128

- (Exam Topic 3)

A company uses Azure Sentinel.

You need to create an automated threat response. What should you use?

- A. a data connector
- B. a playbook
- C. a workbook
- D. a Microsoft incident creation rule

Answer: B

Explanation:

Reference:

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

NEW QUESTION 130

- (Exam Topic 3)

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: C

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 131

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To configure Microsoft Defender for Endpoint:

<input type="checkbox"/> Turn on endpoint detection and response (EDR) in block mode <input type="checkbox"/> Turn on Live Response <input type="checkbox"/> Turn off Tamper Protection

To configure the devices:

<input type="checkbox"/> Add a network assessment job <input type="checkbox"/> Create a device group that contains the devices and set Automation level to Full <input type="checkbox"/> Create a device group that contains the devices and set Automation level to No automated response
--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Turn on Live Response

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 : Add a network assessment job

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-> <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw>

NEW QUESTION 136

- (Exam Topic 3)

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually. You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 140

- (Exam Topic 3)

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.

You need to identify all the changes made to sensitivity labels during the past seven days. What should you use?

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

Answer: C

Explanation:

Labeling activities are available in Activity explorer. For example:
 Sensitivity label applied

This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label. It is captured at the time of save in Office native applications and web applications.

It is captured at the time of occurrence in Azure Information protection add-ins.

Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter. Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-event>

NEW QUESTION 145

- (Exam Topic 3)

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



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

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

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

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

- Entities
- Info
- Insights
- Timeline

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-d>

NEW QUESTION 150

- (Exam Topic 3)

You have the following KQL query.

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

Statements

Yes

No

The `username` field is set as the account entity.

The watchlist cannot be updated after it is created.

The `IPList` variable is set as the IP address entity.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

Yes

No

The `username` field is set as the account entity.

The watchlist cannot be updated after it is created.

The `IPList` variable is set as the IP address entity.

NEW QUESTION 152

- (Exam Topic 3)

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.

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 doount(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	Choose column <input type="button" value="Add"/>
Host	Choose column <input type="button" value="Add"/>
IP	Choose column <input type="button" value="Add"/>
URL	Choose column <input type="button" value="Add"/>
FileHash	Choose column <input type="button" value="Add"/>

Query scheduling

Run query every *

Lookup data from the last *

Alert threshold

Generate alert when number of query results

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 *

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

Reference:

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

NEW QUESTION 156

- (Exam Topic 3)

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 161

- (Exam Topic 3)

You have the following advanced hunting query in Microsoft 365 Defender.

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

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

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

Answer: AE

Explanation:

Reference:

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

NEW QUESTION 165

- (Exam Topic 3)

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1. You need to configure just in time (JIT) VM access for the virtual machines in RG1. The solution must meet the following

- Limit the maximum request time to two hours.
- Limit protocol access to Remote Desktop Protocol (RDP) only.
- Minimize administrative effort. What should you use?

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

Answer: A

NEW QUESTION 167

- (Exam Topic 3)

You use Azure Sentinel.

You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

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

Answer: A

Explanation:

Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources. Reference:

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

NEW QUESTION 172

.....

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