

SC-200 Dumps

Microsoft Security Operations Analyst

<https://www.certleader.com/SC-200-dumps.html>



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.

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

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



```
| summarize activityCount =
```

	▼
avg()	
count()	
sum()	

```
by FolderPath, FileName,
```

```
ActionType, AccountDisplayName
```



```
| where activityCount > 5
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

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



```
| summarize activityCount =
```

	▼
avg()	
count()	
sum()	

```
by FolderPath, FileName,
```

```
ActionType, AccountDisplayName
```



```
| where activityCount > 5
```

NEW QUESTION 3

- (Exam Topic 1)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 4

- (Exam Topic 2)

You need to create the analytics rule 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.

Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

NEW QUESTION 5

- (Exam Topic 2)

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.

Which two configurations should you modify? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: CD

Explanation:

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

Reference:

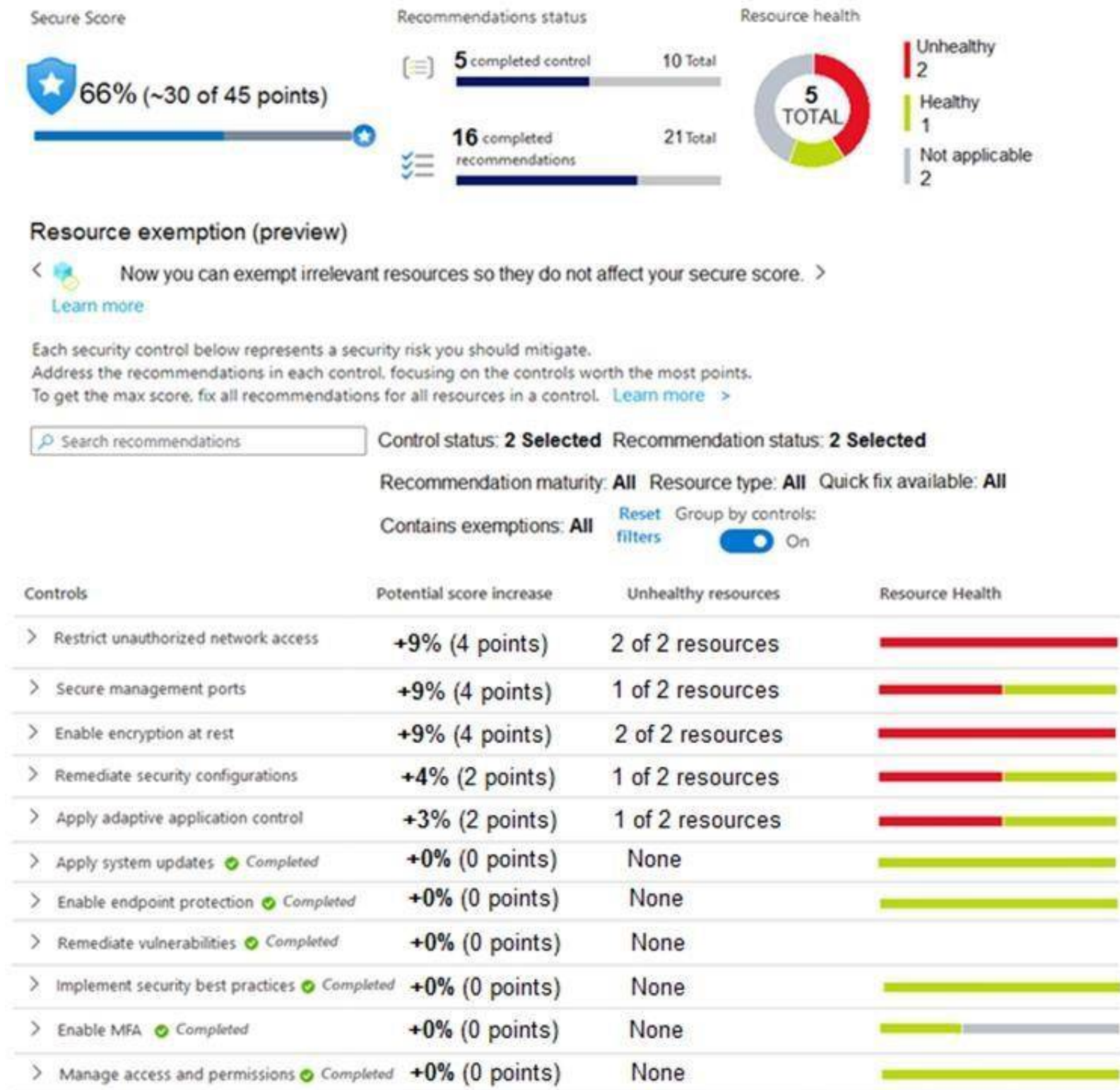
<https://docs.microsoft.com/en-us/cloud-app-security/mde-govern>

NEW QUESTION 6

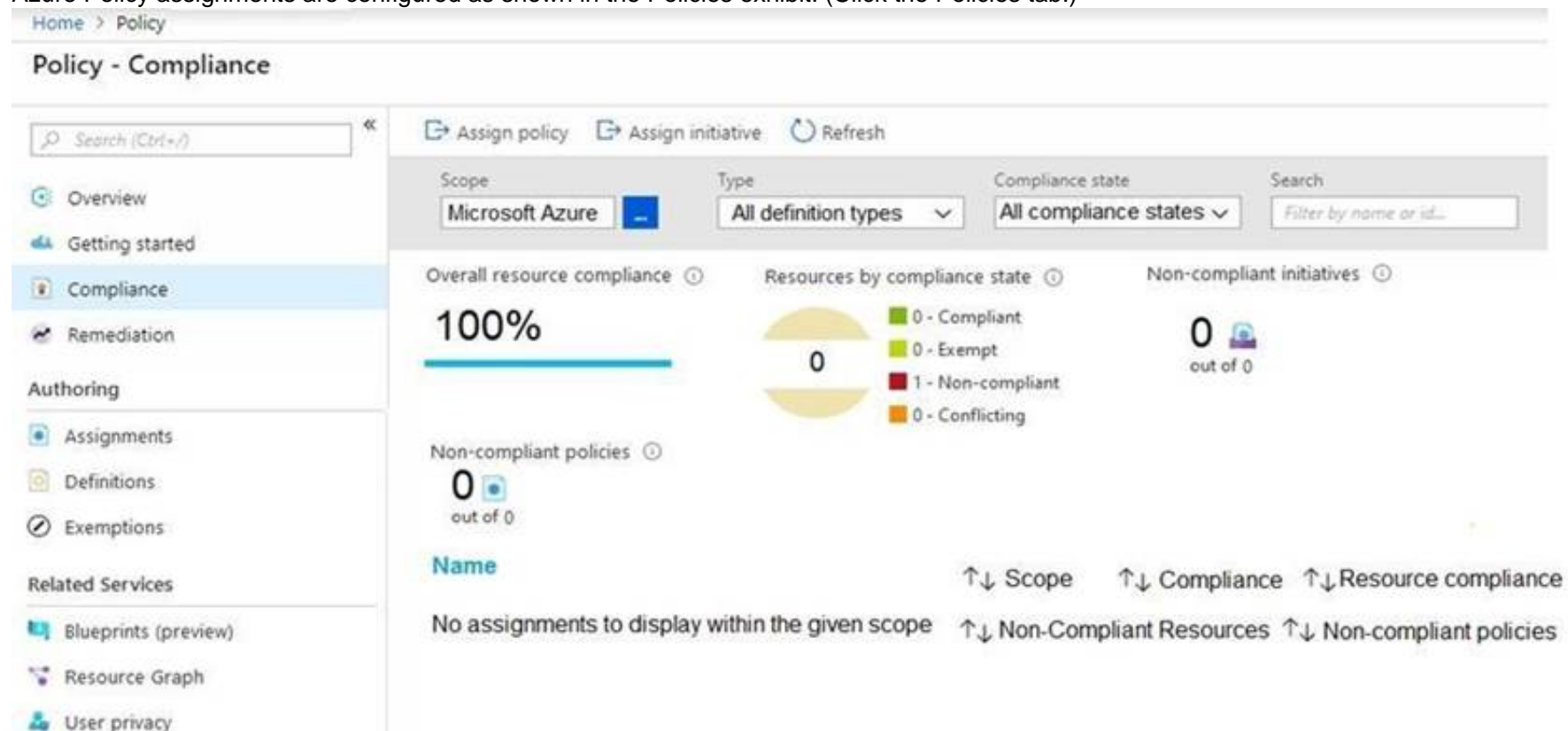
- (Exam Topic 3)

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



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



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

Answer Area

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac> <https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1>

NEW QUESTION 7

- (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 8

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named Workspaces

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

What should you create in Workspace1?

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

Answer: D

Explanation:

To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in

the Microsoft Sentinel workspace. An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used. Reference: <https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule>

NEW QUESTION 9

- (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 10

- (Exam Topic 3)

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 10

- (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 14

- (Exam Topic 3)

You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.

You need to create a query that will be used to display a bar graph. What should you include in the query?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 18

- (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 20

- (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 24

- (Exam Topic 3)

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-world>

NEW QUESTION 29

- (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 Azure Identity Protection, you configure the sign-in risk policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 32

- (Exam Topic 3)

You create an Azure subscription.

You enable Microsoft Defender for Cloud for the subscription.

You need to use Defender for Cloud to protect on-premises computers. What should you do on the on-premises computers?

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

Answer: C

Explanation:

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

NEW QUESTION 37

- (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 38

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

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

NOTE: Each correct selection is worth one point.

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty (
    (DeviceId)
    (RecipientEmailAddress)
    (SenderFromAddress)
    (SHA256)
)

| join (
    DeviceFileEvents
    | project FileName, SHA256
) on (
    (DeviceId)
    (RecipientEmailAddress)
    (SenderFromAddress)
    (SHA256)
)

| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view>

NEW QUESTION 42

- (Exam Topic 3)

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

User	Task
User1	<ul style="list-style-type: none"> Assign initiatives Edit security policies Enable automatic provisioning
User2	<ul style="list-style-type: none"> View alerts and recommendations Apply security recommendations Dismiss alerts

The solution must use the principle of least privilege.

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

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

Roles	Answer Area
<div>Contributor</div>	User1: <div></div>
<div>Owner</div>	User2: <div></div>
<div>Security administrator</div>	
<div>Security reader</div>	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Owner

Only the Owner can assign initiatives. Box 2: Contributor

Only the Contributor or the Owner can apply security recommendations.

Reference:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions>

NEW QUESTION 46

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online. You delete users from the subscription.

You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.

What should you use?

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

Answer: C

Explanation:

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

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

NEW QUESTION 47

- (Exam Topic 3)

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AC

Explanation:

Reference:

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

NEW QUESTION 49

- (Exam Topic 3)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a playbook.
B. Associate a playbook to an incident.

- C. Enable Entity behavior analytics.
- D. Create a workbook.
- E. Enable the Fusion rule.

Answer: AB

Explanation:

Reference:

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

NEW QUESTION 53

- (Exam Topic 3)

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

- A. Create an Azure Policy assignment.
- B. Modify the Workload protections settings in Defender for Cloud.
- C. Create an alert rule in Azure Monitor.
- D. Modify the alert settings in Defender for Cloud.

Answer: D

Explanation:

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.

Note: To create a rule directly in the Azure portal:

* 1. From Defender for Cloud's security alerts page:

Select the specific alert you don't want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

* 2. In the new suppression rule pane, enter the details of your new rule.

Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.

Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.

* 3. Enter details of the rule.

* 4. Save the rule.

Reference: <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules>

NEW QUESTION 54

- (Exam Topic 3)

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 56

- (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.

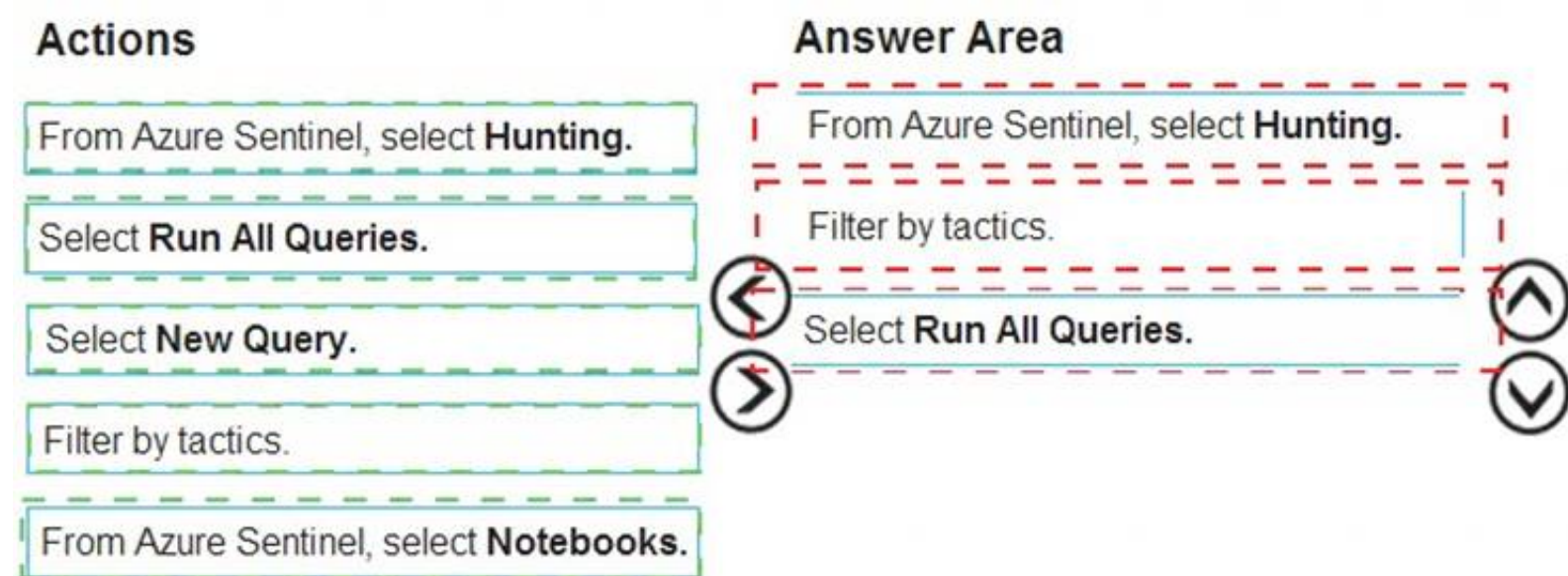
From Azure Sentinel, select **Notebooks**.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 61

- (Exam Topic 3)

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account. You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements.

- Ensure that failed sign-in alerts are generated for other accounts.
- Minimize administrative effort

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

Answer: A

Explanation:

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

NEW QUESTION 64

- (Exam Topic 3)

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.

You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 65

- (Exam Topic 3)

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1. You receive an alert for suspicious use of PowerShell on VM1.

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

- > The modification of local group memberships
- > The purging of event logs

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Step 1: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights. Incident Insights

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address Account Host

URL

Step 3: From the details pane of the incident, select Investigate. Choose a single incident and click View full details or Investigate. Reference:

<https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview> <https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases>

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 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 74

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 77

- (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 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

- A. Create an import file that contains the IP address of 171.23.34.32/27. Select 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 rang
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-intellige>

NEW QUESTION 79

- (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 84

- (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 88

- (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.	<input type="radio"/>	<input type="radio"/>
The watchlist cannot be updated after it is created.	<input type="radio"/>	<input type="radio"/>
The IPList variable is set as the IP address entity.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 93

- (Exam Topic 3)

You have a Microsoft Sentinel workspace that contains an Azure AD data connector. You need to associate a bookmark with an Azure AD-related incident.

What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content

NOTE: Each correct selection is worth one point.

Blades

Hunting blade

Incident blade

Logs blade

Answer Area

Create a bookmark by using the:

Blade

Associate a bookmark with the incident by using the:

Blade

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You can use the Logs blade or incident blade to create a bookmark of an Azure AD-related incident. Once the bookmark is created, you can associate it with the incident by using the incident blade. This allows you to quickly and easily access important information related to the incident in the future.

NEW QUESTION 96

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment. How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

|

	▼
extend	
join	
project	
union	

 (

DeviceFileEvents

|

	▼
extend	
join	
project	
union	

 FileName, SHA256

) on SHA256

|

	▼
extend	
join	
project	
union	

 Timestamp, FileName, SHA256, DeviceName, DeviceId,

NetworkMessageId, SenderFromAddress, RecipientEmailAddress

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36>

NEW QUESTION 99

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your SC-200 Exam with Our Prep Materials Via below:

<https://www.certleader.com/SC-200-dumps.html>