

SC-200 Dumps

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (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 2

- (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 3

- (Exam Topic 1)

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

- A. just-in-time (JIT) access
- B. Azure Defender
- C. Azure Firewall
- D. Azure Application Gateway

Answer: B

Explanation:

Reference:

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

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 3)

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:

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

NEW QUESTION 6

- (Exam Topic 3)

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

- A. notebooks in Azure Sentinel
- B. Microsoft Cloud App Security
- C. Azure Monitor
- D. hunting queries in Azure Sentinel

Answer: A

Explanation:

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

NEW QUESTION 7

- (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.)



Resource exemption (preview)

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

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

Search recommendations: Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** [Reset filters](#) Group by controls: On

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

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

Home > Policy

Policy - Compliance

Search (Ctrl+):

Assign policy Assign initiative Refresh

Scope: Microsoft Azure Type: All definition types Compliance state: All compliance states Search: Filter by name or id...

Overall resource compliance: **100%**

Resources by compliance state: 0 (0 - Compliant, 0 - Exempt, 1 - Non-compliant, 0 - Conflicting)

Non-compliant initiatives: 0 out of 0

Non-compliant policies: 0 out of 0

Name ↑↓ Scope ↑↓ Compliance ↑↓ Resource compliance

No assignments to display within the given scope ↑↓ Non-Compliant Resources ↑↓ Non-compliant policies

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 8

- (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 Prevent future attacks section.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

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

NEW QUESTION 9

- (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 . | <input type="radio"/> |
| Filter by tactics. | <input type="radio"/> |
| From Azure Sentinel, select Notebooks . | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

Answer Area

From Azure Sentinel, select **Hunting**.

Filter by tactics.

Select **Run All Queries**.



NEW QUESTION 10

- (Exam Topic 3)

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

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

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps>

NEW QUESTION 10

- (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 Azure Security Center. You need to test LA1 in Security Center.

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

Answer Area

Set the LA1 trigger to:

| |
|--|
| ▼ |
| When an Azure Security Center Recommendation is created or triggered |
| When an Azure Security Center Alert is created or triggered |
| When a response to an Azure Security Center alert is triggered |

Trigger the execution of LA1 from:

| |
|---------------------|
| ▼ |
| Recommendations |
| Workflow automation |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

[https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when](https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-to-trigger)

NEW QUESTION 15

- (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 20

.....

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>