

SC-200 Dumps

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (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 2

- (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 the accounts to an Active Directory group and add the group as a Sensitive group. 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 3

- (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 4

- (Exam Topic 3)

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?

- A. Modify the access control settings for the key vault.
- B. Enable the Key Vault firewall.
- C. Create an application security group.
- D. Modify the access policy for the key vault.

Answer: B

Explanation:

Reference:

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

NEW QUESTION 5

- (Exam Topic 3)

You open the Cloud App Security portal as shown in the following exhibit.

You need to remediate the risk for the Launchpad app.

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery>

NEW QUESTION 6

- (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 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.)

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.

- 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)

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 9

- (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.

- 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 10

- (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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10

- (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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 11

- (Exam Topic 3)

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Answer: BCE

Explanation:

Reference:

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

NEW QUESTION 13

- (Exam Topic 3)

You are investigating an incident by using Microsoft 365 Defender.

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 16

- (Exam Topic 3)

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.

Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

NEW QUESTION 19

- (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.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 23

- (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.

- 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 28

.....

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>