

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (Exam Topic 2)

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements. Which role should you assign?

- A. Automation Operator
- B. Automation Runbook Operator
- C. Azure Sentinel Contributor
- D. Logic App Contributor

Answer: C

Explanation:

Reference:

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

NEW QUESTION 2

- (Exam Topic 2)

You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

- A. From Set rule logic, turn off suppression.
- B. From Analytics rule details, configure the tactics.
- C. From Set rule logic, map the entities.
- D. From Analytics rule details, configure the severity.

Answer: C

Explanation:

Reference:

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

NEW QUESTION 3

- (Exam Topic 2)

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

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

Answer: D

Explanation:

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

NEW QUESTION 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)

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 8

- (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 9

- (Exam Topic 3)

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. `cp /bin/echo ./asc_alerttest_662jfi039n`
- B. `./alerttest testing eicar pipe`
- C. `cp /bin/echo ./alerttest`
- D. `./asc_alerttest_662jfi039n testing eicar pipe`

Answer: AD

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux>

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.

- 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 a custom analytics rule to detect threats in Azure Sentinel.

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

What is a possible cause of the issue?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 14

- (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 16

- (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: BDE

Explanation:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

NEW QUESTION 19

- (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.

- 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-whe>

NEW QUESTION 23

- (Exam Topic 3)

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.

What should you do?

- A. In workspace1, install a solution.
- B. In sub1, register a provider.
- C. From Security Center, create a Workflow automation.
- D. In workspace1, create a workbook.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

NEW QUESTION 27

.....

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