

Exam Questions SC-200

Microsoft Security Operations Analyst

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



NEW QUESTION 1

- (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 2

- (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

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 3

- (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 4

- (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:

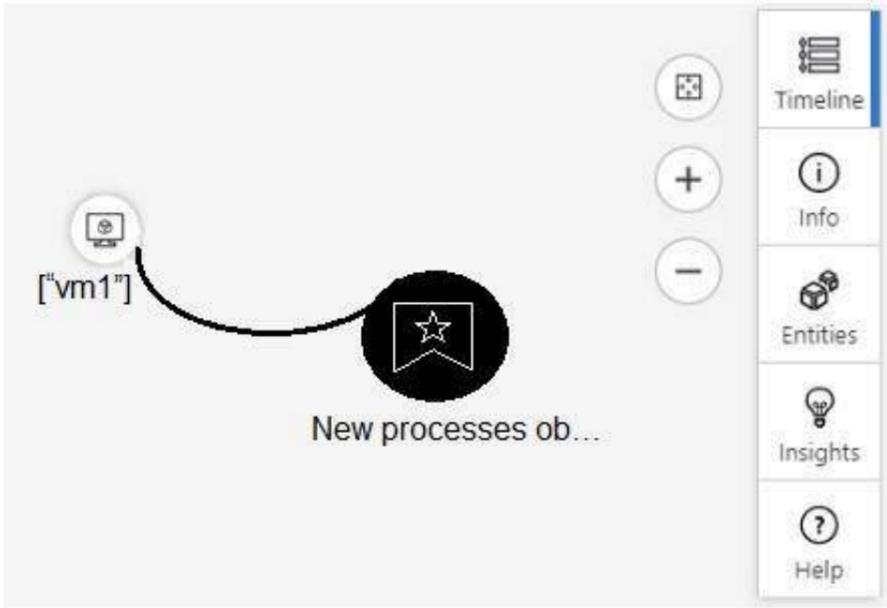
Reference:

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

NEW QUESTION 5

- (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 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 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 7

- (Exam Topic 3)

You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
 NOTE: Each correct selection is worth one point.

- A. user
- B. resource group
- C. IP address
- D. computer

Answer: CD

NEW QUESTION 8

- (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	Answer Area
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 .	

- 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 9

- (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 10

- (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 10

- (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 12

- (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-to-trigger>

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 20

- (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 21

- (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

|

	▼	FileName, SHA256
extend		
join		
project		
union		

) on SHA256

|

	▼	Timestamp, FileName, SHA256, DeviceName, DeviceId,
extend		
join		
project		
union		

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 26

.....

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