



**Microsoft**

**Exam Questions SC-200**

Microsoft Security Operations Analyst

#### 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 2)

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

- A. Activity from suspicious IP addresses
- B. Activity from anonymous IP addresses
- C. Impossible travel
- D. Risky sign-in

**Answer:** C

#### Explanation:

Reference:

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

#### 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 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 5

- (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 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 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 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)

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 10**

- (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 10**

- (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 15

- (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 18

- (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

From Azure Sentinel, select Hunting.

Select Run All Queries.

Select New Query.

Filter by tactics.

From Azure Sentinel, select Notebooks.

Answer Area

- 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 21

- (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 form the list of actions to the answer area and arrange them in the correct order.



## Actions

## Answer Area

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.



- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Reference:

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

### NEW QUESTION 23

- (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 25

- (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 29

- (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.

## Values

## Answer Area

project LogonFailures=count()	
summarize LogonFailures=count() by DeviceName, LogonType	
where ActionType == FailureReason	
where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")	
ActionType == "LogonFailed"	

and

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

## Values

## Answer Area

project LogonFailures=count()	summarize LogonFailures=count() by DeviceName, LogonType
summarize LogonFailures=count() by DeviceName, LogonType	where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")
where ActionType == FailureReason	where ActionType == FailureReason
where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")	ActionType == "LogonFailed"
ActionType == "LogonFailed"	project LogonFailures=count()

and

### NEW QUESTION 31

- (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-whe>

NEW QUESTION 32

- (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 35

- (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

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.

Answer Area

<

>

↑

↓

- A. Mastered  
B. Not Mastered

Answer: A

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

NEW QUESTION 37

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-200 Practice Test Here](#)**