

# Exam Questions SC-200

Microsoft Security Operations Analyst

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



### 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)

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 3

- (Exam Topic 1)

The issue for which team can be resolved by using Microsoft Defender for Office 365?

- A. executive
- B. marketing
- C. security
- D. sales

**Answer:** B

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide>

#### NEW QUESTION 4

- (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 5

- (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 6

- (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 7

- (Exam Topic 3)

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?

- A. Azure Sentinel Responder
- B. Logic App Contributor
- C. Azure Sentinel Contributor
- D. Azure Sentinel Reader

**Answer:** A

**Explanation:**

Reference:

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

### 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 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 9

- (Exam Topic 3)

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

The screenshot shows the Microsoft Cloud App Security portal. The 'Discovered apps' tab is active, displaying a list of apps. The 'Launchpad' app is highlighted, showing a score of 1 and a risk factor of 13. The interface includes a sidebar with navigation options like Dashboard, Discover, Investigate, and Control. The main area displays a list of discovered apps with columns for App, Score, Traffic, Upload, Transac., Users, IP addr, Last se, and Actions.

App	Score	Traffic	Upload	Transac.	Users	IP addr	Last se	Actions
Applied Innovations Hosting services	1	866 KB	-	12	11	8	Apr 20...	✓ ⚙ ⋮
StatusCake Website monitoring	1	939 KB	-	13	13	7	Apr 20...	✓ ⚙ ⋮
Usersnap Productivity	1	1 MB	-	15	15	10	Apr 20...	✓ ⚙ ⋮
CopperEgg Website monitoring	1	866 KB	-	12	12	8	Apr 20...	✓ ⚙ ⋮
Launchpad Code-hosting	1	939 KB	-	13	13	7	Apr 20...	✓ ⚙ ⋮

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.



## Actions

## Answer Area

Tag the app as **Unsanctioned**.

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

Select the app.

Tag the app as **Sanctioned**.

Generate a block script.



- A. Mastered
- B. Not Mastered

**Answer:** A

### Explanation:

Reference:

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

### NEW QUESTION 10

- (Exam Topic 3)

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a livestream
- B. Add a data connector
- C. Create an analytics rule
- D. Create a hunting query.
- E. Create a bookmark.

**Answer:** BD

### Explanation:

Reference:

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

### NEW QUESTION 10

- (Exam Topic 3)

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Add a playbook.
- B. Associate a playbook to an incident.
- C. Enable Entity behavior analytics.
- D. Create a workbook.
- E. Enable the Fusion rule.

**Answer:** AB

### NEW QUESTION 11

- (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

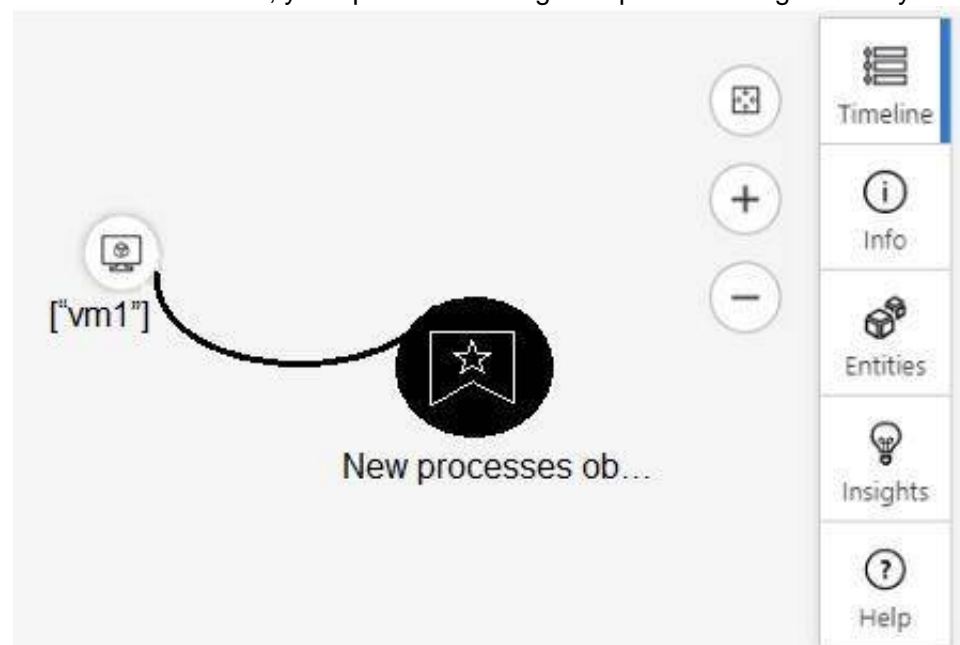
### Explanation:

Reference:  
<https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts>

NEW QUESTION 12

- (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 15

- (Exam Topic 3)

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually. You deploy Azure Sentinel. You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

- A. Add a new scheduled query rule.
- B. Add a data connector to Azure Sentinel.
- C. Configure a custom Threat Intelligence connector in Azure Sentinel.
- D. Modify the trigger in the logic app.

Answer: B

NEW QUESTION 19

- (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 Mitigate the threat section.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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

NEW QUESTION 22

- (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 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 28

- (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 32**

- (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 36**

- (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 39**

- (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

| 

	▼
extend	
join	
project	
union	

 FileName, SHA256

) on SHA256

| 

	▼
extend	
join	
project	
union	

 Timestamp, FileName, SHA256, DeviceName, DeviceId,

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 41**

.....

## 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