

# SC-200<sup>Q&As</sup>

Microsoft Security Operations Analyst

**Pass Microsoft SC-200 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.certbus.com/sc-200.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



### QUESTION 1

#### DRAG DROP

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.

Select and Place:

#### Actions

#### Answer Area

From Device Inventory, search for the CVE.
Open the Threat Protection report.
From Threat & Vulnerability Management, select <b>Weaknesses</b> , and search for the CVE.
From Advanced hunting, search for cveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.
Create the remediation request.
Select <b>Security recommendations</b> .



Correct Answer:

### Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Advanced hunting, search for cveId in the DeviceTvmSoftwareInventoryVulnerabilitites table.

### Answer Area

- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- Select **Security recommendations**.
- Create the remediation request.

### QUESTION 2

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.

Correct Answer: AB

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

### QUESTION 3

DRAG DROP

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.

Select and Place:

### Actions

From Azure Sentinel, select **Hunting**.

Select **Run All Queries**.

Select **New Query**.

Filter by tactics.

From Azure Sentinel, select **Notebooks**.

### Answer Area



Correct Answer:

### Actions

Select **New Query**.

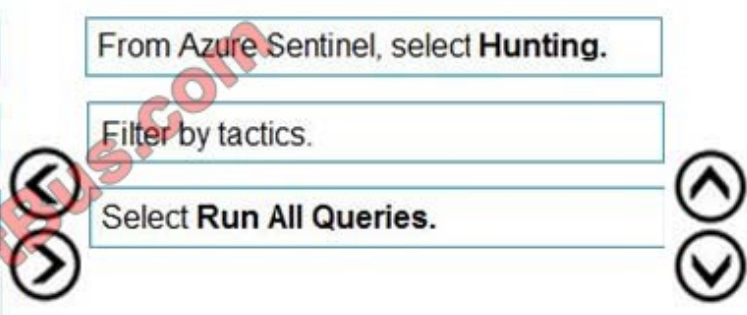
From Azure Sentinel, select **Notebooks**.

### Answer Area

From Azure Sentinel, select **Hunting**.

Filter by tactics.

Select **Run All Queries**.



## QUESTION 4

### HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

Correct Answer:

## Answer Area

Create the rule of type:

	▼
Fusion	
Microsoft incident creation	
Scheduled	

Configure the playbook to include:

	▼
Diagnostics settings	
A service principal	
A trigger	

QUESTION 5

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

Correct Answer: C

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations>

#### QUESTION 6

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

Correct Answer: CD



### QUESTION 7

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

Correct Answer: C

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

---

### QUESTION 8

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

Correct Answer: C

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

---

### QUESTION 9

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.

Correct Answer: BD

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

### QUESTION 10

#### HOTSPOT

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.

Hot Area:

### 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"/>

Correct Answer:



## Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	<input checked="" type="radio"/>	<input type="radio"/>
Both virtual machines have management ports exposed directly to the internet.	<input type="radio"/>	<input checked="" 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 checked="" type="radio"/>	<input type="radio"/>

### QUESTION 11

#### HOTSPOT

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.

Hot Area:

### Answer Area

```

| where TimeStamp > ago(2d)
| summarize activityCount =
ActionType, AccountDisplayName
| where activityCount > 5
    
```

▼  
 CloudAppEvents  
 DeviceFileEvents  
 DeviceProcessEvents

▼  
 avg()  
 count()  
 sum()

by FolderPath, FileName,

Correct Answer:

## Answer Area

```
| where TimeStamp > ago(2d)
| summarize activityCount =
ActionType, AccountDisplayName
| where activityCount > 5
```

CloudAppEvents  
DeviceFileEvents  
DeviceProcessEvents

avg()  
count()  
sum()

by FolderPath, FileName,

### QUESTION 12

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

Correct Answer: A

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

[SC-200 VCE Dumps](#)

[SC-200 Study Guide](#)

[SC-200 Exam Questions](#)

To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

## Try our product !

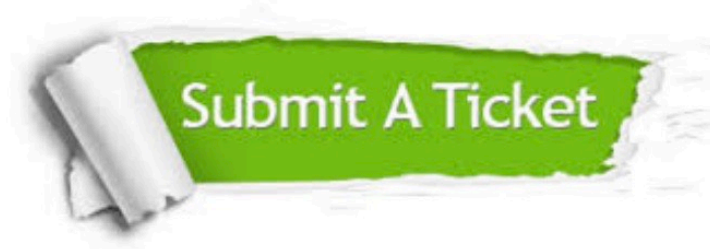
100% Guaranteed Success  
100% Money Back Guarantee  
365 Days Free Update  
Instant Download After Purchase  
24x7 Customer Support  
Average 99.9% Success Rate  
More than 800,000 Satisfied Customers Worldwide  
Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.  
You can view Vendor list of All Certification Exams offered:

<https://www.certbus.com/allproducts>

## Need Help

Please provide as much detail as possible so we can best assist you.  
To update a previously submitted ticket:



 <p><b>One Year Free Update</b> Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p><b>Money Back Guarantee</b> To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.  
All trademarks are the property of their respective owners.  
Copyright © certbus, All Rights Reserved.