



---

MICROSOFT  
**SC-200**  
Security Operations Analyst  
(SC-200) Exam Questions & Answers

---

Total Questions: **05**

[Click Here to Get All Microsoft Exam Questions →](#)

<https://itexamsquiz.com/product/sc-200-practice-tests/>

## About ITExamsQuiz

At ITExamsQuiz, we believe every IT professional deserves access to high-quality exam preparation without breaking the bank. Our expert team curates accurate, up-to-date study material for a wide range of certification exams.

With ITExamsQuiz you get expert-vetted study material, real exam insights, and a fair shot at success.

- ✓ **Lifetime Free Updates**
- ✓ **Money-Back Guarantee**
- ✓ **100% Verified Questions**
- ✓ **24/7 Support via Email**

### Doubt Support

We resolve 400+ doubts every day with an average rating of 4.8/5.

<https://itexamsquiz.com>

✉ [support@itexamsquiz.com](mailto:support@itexamsquiz.com)

★ ★ ★ ★ ★ **Logan**

I passed with 920/1000! More than 45 questions were from your PDFs. Highly recommended!

★ ★ ★ ★ ★ **Hailey**

Updated material and correct answers. Passed AZ-900 on first attempt. Thank you ITExamsQuiz!

★ ★ ★ ★ ★ **Brandon**

Amazing accuracy. Out of 52 questions, 50 were from your dumps. Passed with 870 marks!

★ ★ ★ ★ ★ **Madison**

Customer support is very responsive. The PDFs are super accurate. Will recommend to friends!

### Question: 1

ITExamsQuiz

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

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

✓ **Answer: B**

**Explanation:**

<https://itexamsquiz.com> | ACE YOUR EXAM

### Question: 2

ITExamsQuiz

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:**

**Question: 3**

ITExamsQuiz

**HOTSPOT**

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:

External threat:

**Answer:**

**Answer Area**

Internal threat:

External threat:

**Explanation:**

**Question: 4**

ITExamsQuiz

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:**

**Question: 5**

ITExamsQuiz

**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.

	▼
CloudAppEvents	
DeviceFileEvents	
DeviceProcessEvents	

| where TimeStamp > ago(2d)

| summarize activityCount =

ActionType, AccountDisplayName

| where activityCount > 5

	▼
avg()	
count()	
sum()	

by FolderPath, FileName,

**Answer:**

```
CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

| where TimeStamp > ago(2d)

| summarize activityCount = count() by FolderPath, FileName,
| where activityCount > 5
```

Explanation:

**Thank you for trying the SC-200 Exam Dumps PDF Demo**

**Practice smarter with our updated SC-200 PDF Questions**

If you want to buy our premium Practice Questions, please follow the link below and get started now!

<https://itexamsquiz.com/product/sc-200-practice-tests/>