

# SC-200 Schulungsmaterialien & SC-200 Dumps Prüfung & SC-200 Studienguide



Laden Sie die neuesten ZertFragen SC-200 PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter:  
<https://drive.google.com/open?id=1Co1EeXemHAJmcZdGNzslfDz2CnoilZd5>

Sorgen Sie noch um die Vorbereitung der Microsoft SC-200 Prüfung? Aber solange Sie diesen Blog sehen, können Sie sich doch beruhigen, weil Sie der professionellste und der autoritativste Lieferant gefunden haben. Unsere Produkte haben viele Angestellten geholfen, die in IT-Firmen arbeiten, die Microsoft SC-200 Zertifizierungsprüfung zu bestehen. Die Gründe sind einfach. Da unsere Prüfungsunterlagen sind am neusten und am umfassendsten! Außerdem bieten wir einjährige kostenlose Aktualisierung nach Ihrem Kauf der Prüfungsunterlagen der Microsoft SC-200 . Keine Sorge bei der Vorbereitung!

Die Microsoft SC-200 Zertifizierungsprüfung ist eine ausgezeichnete Wahl für Sicherheitsfachleute, die ihre Karriere im Bereich der Cybersicherheit vorantreiben möchten. Sie umfasst eine breite Palette von Themen im Zusammenhang mit Sicherheitsoperationen und bewertet die Fähigkeiten des Kandidaten, Microsoft-Sicherheitstechnologien zur Sicherung der IT-Umgebung ihrer Organisation zu nutzen. Durch den Erwerb dieser Zertifizierung können Einzelpersonen ihre technischen Fähigkeiten und Kenntnisse demonstrieren und sich im Arbeitsmarkt einen Vorteil verschaffen.

>> SC-200 Deutsch Prüfungsfragen <<

## SC-200 Übungstest: Microsoft Security Operations Analyst & SC-200 Brandumps Prüfung

Wenn Sie die Schulungsunterlagen zur Microsoft SC-200 Zertifizierungsprüfung aus ZertFragen haben, können Durcheinander entwirren und nervöse Stimmung vertreiben. Die Schulungsunterlagen zur Microsoft SC-200 Zertifizierungsprüfung von ZertFragen sind die genaueste Lehrbücher auf dem aktuellen Markt, mit denen die Bestehensrate für die Microsoft SC-200 Zertifizierungsprüfung fast 100% betragen kann. Wenn Sie ZertFragen wählen, gehen Sie dann auf dem Weg zum Erfolg.

## Microsoft Security Operations Analyst SC-200 Prüfungsfragen mit Lösungen (Q277-Q282):

### 277. Frage

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a Windows device named Device1.

You detect malicious activity on Device1.

You initiate a live response session on Device1.

You need to perform the following actions:

\* Download a file from the live response library.

\* Stop a process that is running on Device1.

Which live response command should you run for each action? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Antwort:**

Begründung:

Explanation:

### 278. Frage

You have 100 Azure subscriptions that have enhanced security features in Microsoft Defender for Cloud enabled. All the subscriptions are linked to a single Azure AD tenant. You need to stream the Defender for Cloud logs to a syslog server. The solution must minimize administrative effort. What should you do? To answer, select the appropriate options in the answer area.  
NOTE: Each correct selection is worth one point.

**Antwort:**

Begründung:

Explanation:

### 279. Frage

Hotspot Question

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You plan to investigate suspicious activity in the subscription by using Microsoft Graph activity logs.

You need to search for requests to delete resources from the subscription and identify the users that initiated the requests.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Antwort:**

Begründung:

### 280. Frage

You have an Azure subscription that contains two users named User1 and User2 and a Microsoft Sentinel workspace named workspace1. You need to ensure that the users can perform the following tasks in workspace1:

\* User1 must be able to dismiss incidents and assign incidents to users.

\* User2 must be able to modify analytics rules.

The solution must use the principle of least privilege.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

**Antwort:**

Begründung:

Explanation:

### 281. Frage

You have 500 on-premises Windows 11 devices that use Microsoft Defender for Endpoint. You enable Network device discovery. You need to create a hunting query that will identify discovered network devices and return the identity of the onboarded device that discovered each network device.

Which built-in function should you use?

- A. next ()
- B. SeenBy ()
- C. current\_cluster,endpoint()
- **D. DeviceFromIP ()**

**Antwort: D**

