# Zertifizierung der SC-200 mit umfassenden Garantien zu bestehen


P.S. Kostenlose 2026 Microsoft SC-200 Prüfungsfragen sind auf Google Drive freigegeben von It-Pruefung verfügbar: https://drive.google.com/open?id=1WCx9FdU6ZjFHSYSV5P6xCbCiVmUoQy5N

Die Konkurrenz in unserer Gesellschaft wird immer heftiger. Unsere It-Pruefung ist noch bei vielen Prüfungskandidaten sehr beliebt, weil wir immer vom Standpunkt der Teilnehmer die Softwaren entwickeln. Z.B. die gut gekaufte Microsoft SC-200 Prüfungssofteware wird von unserem professionellem Team entwickelt mit großer Menge Forschung der Microsoft SC-200 Prüfung. Obwohl wir eine volle Rückerstattung für die Verlust des Tests versprechen, bestehen fast alle Kunde Microsoft SC-200, die unsere Produkte benutzen. Was beweist die Vertrauenswürdigkeit und die Effizienz unserer Microsoft SC-200 Prüfungsunterlagen.

Die Microsoft SC-200 Prüfung ist eine wichtige Zertifizierung für Sicherheitsfachleute, die mit Microsoft-Technologien arbeiten. Der Erwerb dieser Zertifizierung zeigt ein starkes Verständnis für Sicherheitsoperationen und die Fähigkeit, effektive Sicherheitsmaßnahmen in einer Microsoft-Umgebung umzusetzen. Mit der zunehmenden Nachfrage nach qualifizierten Sicherheitsfachleuten kann diese Zertifizierung dazu beitragen, Karrieremöglichkeiten und Gehaltsaussichten zu verbessern.

Die Microsoft SC-200-Zertifizierungsprüfung ist ein wichtiger Berechtigungsnachweis für Sicherheitsfachleute, die mit Microsoft-Produkten und -dienstleistungen arbeiten. Das Bestehen der Prüfung zeigt, dass der Kandidat über das Wissen und die Fähigkeiten verfügt, um Microsoft -Umgebungen vor Cyber -Bedrohungen zu schützen. Um sich auf die Prüfung vorzubereiten, sollten Kandidaten Erfahrung in Sicherheitsvorgängen haben und mit Microsoft 365 Defender, Azure Defender und Azure Sentinel vertraut sein. Microsoft bietet mehrere Ressourcen an, um den Kandidaten dabei zu helfen, sich auf die Prüfung vorzubereiten, und das

Bestehen der Prüfung erhält dem Kandidaten die Zertifizierung von Microsoft Security Operations Analyst.

**>> SC-200 Unterlage <<**

## SC-200 PDF, SC-200 Deutsch Prüfung

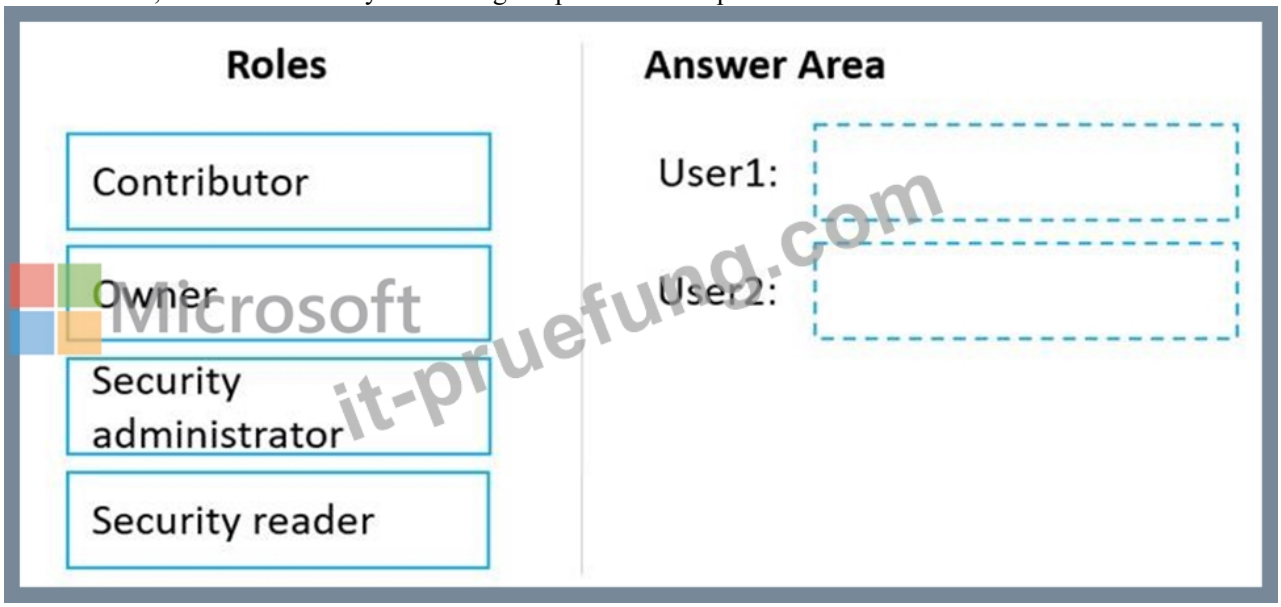
Die It-Pruefung Website hat guten Ruf bei Microsoft SC-200 Zertifizierungsprüfungen. Das ist auch die Tatsche, die viele Leute kennen. Die It-Pruefung sind nach Ihren starken Dumps gut anerkannt. Wenn Sie die als das Vorbereitungsgerät benutzen, können Sie gute Ergebnisse für die Microsoft SC-200 Zertifizierungsprüfung bekommen. Downloaden Sie kostlose Demo, dann können Sie wissen, dass diese Auswahl richtig ist.

## Microsoft Security Operations Analyst SC-200 Prüfungsfragen mit Lösungen (Q165-Q170):

**165. Frage**
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

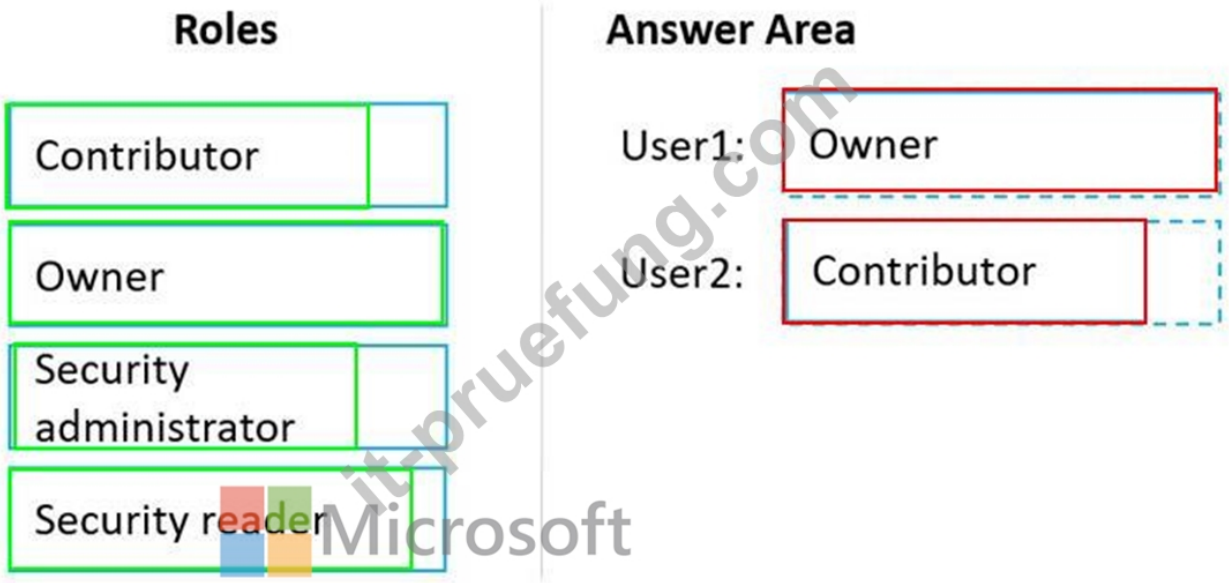
| User | Task |
|---|---|
| User1 | • Assign initiatives<br>• Edit security policies<br>• Enable automatic provisioning |
| User2 | • View alerts and recommendations<br>• Apply security recommendations<br>• Dismiss alerts |

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.



**Antwort:**

Begründung:




.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

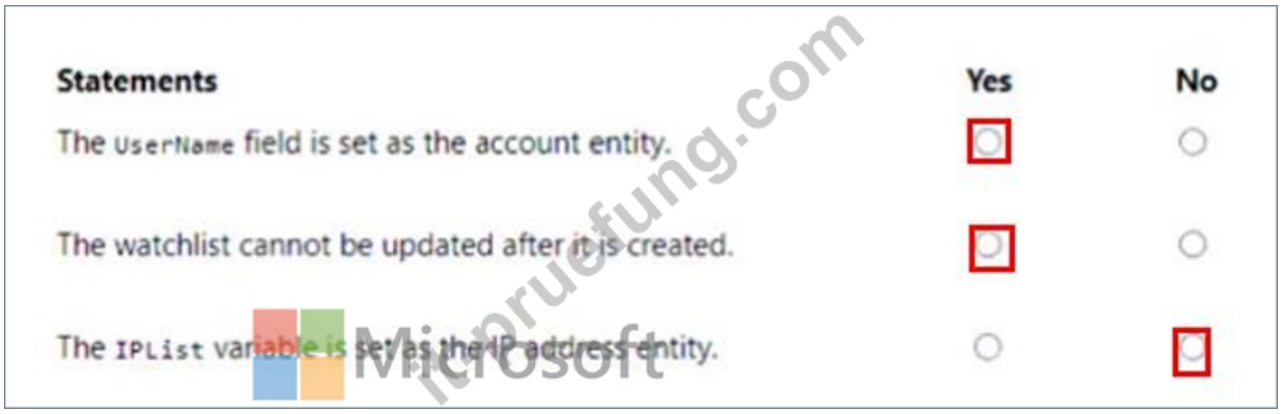
**166. Frage**
You have the following KQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

| Statements | Yes | No |
|---|---|---|
| The `UserName` field is set as the account entity. | ○ | ○ |
| The watchlist cannot be updated after it is created. | ○ | ○ |
| The `IPList` variable is set as the IP address entity. | ○ | ○ |

**Antwort:**

Begründung:




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

**Antwort: A,D**

Begründung:
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/sentinel/livestream

**168. Frage**
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. computer
- B. IP address
- C. user
- D. resource group

**Antwort: A,B**

**169. Frage**
You have an Azure subscription that contains the users shown in the following table.

| Name | Role |
|---|---|
| User1 | Security administrator |
| User2 | Security reader |
| User3 | Contributor |

You need to delegate the following tasks:
* Enable Microsoft Defender for Servers on virtual machines.
* Review security recommendations and enable server vulnerability scans.
The solution must use the principle of least privilege.
Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user 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:
Task
User
Enable Microsoft Defender for Servers on virtual machines:
User1
Review security recommendations and enable server vulnerability scans:
User1
* Query successful
This is a role-based access control (RBAC) question using the principle of least privilege.
The table of users and roles is:
Name
Role
User1
Security administrator
User2
Security reader
User3
Contributor
Export to Sheets
* Action: This is a management/configuration task at the subscription level, often related to enabling Defender plans and installing extensions on VMs.
* Required Permissions: The ability to modify security policies and settings in Microsoft Defender for Cloud and the permission to install extensions on VMs.
* The Security Administrator role is explicitly designed for this, granting permissions to manage the security features, policies, and program enrollment (like enabling Defender plans).
* The Contributor role can also perform this by installing the necessary agents and extensions, but it grants broad access to manage all resources, violating the principle of least privilege for a purely security-focused task.
* Least Privilege User: User1 (Security administrator)
* Action: This task has two parts:
* Review security recommendations: This is a read-only action. The Security Reader role is sufficient.
* Enable server vulnerability scans: This means configuring a security feature (Vulnerability Assessment), which requires write access to the security configuration or the resource itself.
* The Security Reader role cannot perform the "enable" action.

* The Security Administrator role has the permissions required to modify security policy and configuration to enable scanning features.
* The Contributor role can also do this, but again, the Security Administrator role is the least privileged for a security-specific configuration change.
* Least Privilege User: Since the entire task includes an "enable" (write) action, we must use the role that can perform both read and write security actions. User1 (Security administrator) is the appropriate choice.
Task
User
Enable Microsoft Defender for Servers on virtual machines:
User1
Review security recommendations and enable server vulnerability scans:
User1

**170. Frage**
.....

Manchmal bedeutet ein kleinem Schritt ein großem Fortschritt des Lebens. Die Microsoft SC-200 Prüfung scheit nur ein kleinem Test zu sein, aber der Vorteil der Prüfungszertifizierung der Microsoft SC-200 für Ihr Arbeitsleben darf nicht übersehen werden. Diese internationale Zertifikat beweist Ihre ausgezeichnete IT-Fähigkeit. Neben Microsoft SC-200 sind auch andere Zertifizierungsprüfung sehr wichtig, deren neueste Unterlagen können Sie auch auf unserer Webseite finden.