SC-200 Certification Training | Detailed SC-200 Study Plan

What's more, part of that PrepPDF SC-200 dumps now are free: https://drive.google.com/open?id=1PXOmujLvPnMglkO0zhsdIt7joUbanYqT

It is known to us that passing the SC-200 exam is very difficult for a lot of people. Choosing the correct study materials is so important that all people have to pay more attention to the study materials. If you have any difficulty in choosing the correct SC-200 study braindumps, here comes a piece of good news for you. The SC-200 prep guide designed by a lot of experts and professors from company are very useful for all people to pass the practice exam and help them get the Microsoft certification in the shortest time. If you are preparing for the practice exam, we can make sure that the SC-200 Test Practice files from our company will be the best choice for you, and you cannot find the better study materials than our company'.

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is designed to test the knowledge and skills of security professionals in performing threat protection, incident response, and other security operations tasks using Microsoft security technologies. Microsoft Security Operations Analyst certification exam is intended for those who have expertise in security operations and experience working with Microsoft Azure Sentinel, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Cloud App Security.

Microsoft SC-200 Exam is designed to test your ability to analyze and respond to threats. You will be expected to demonstrate your knowledge of various security tools, including Microsoft 365 Defender, Azure Defender, and Azure Sentinel. You will also need to have a good understanding of threat intelligence and be able to apply this knowledge in real-world scenarios.

>> SC-200 Certification Training <<

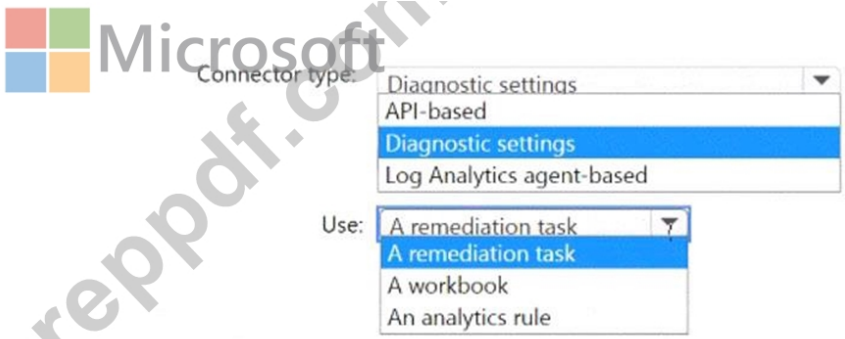
Detailed SC-200 Study Plan - SC-200 Test Testking

I am glad to introduce a secret weapon for all of the candidates to pass the exam as well as get the related certification without any more ado-- our SC-200 study materials. You can only get the most useful and efficient study materials with the most affordable price. With our SC-200 practice test, you only need to spend 20 to 30 hours in preparation since there are all essence contents in our SC-200 Study Materials. What's more, if you need any after service help on our SC-200 exam guide, our after service staffs will always offer the most thoughtful service for you.

Microsoft Security Operations Analyst Sample Questions (Q356-Q361):

NEW QUESTION # 356
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

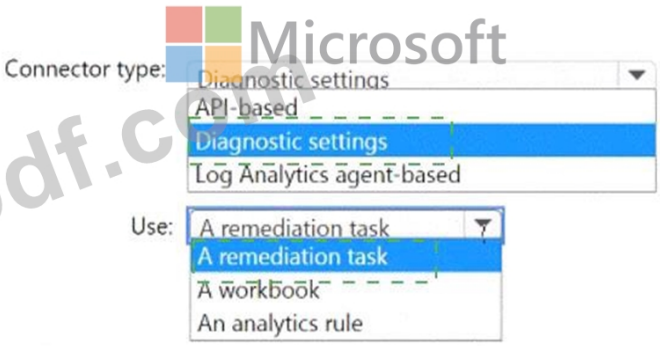
Answer Area



Answer:

Explanation:

Answer Area



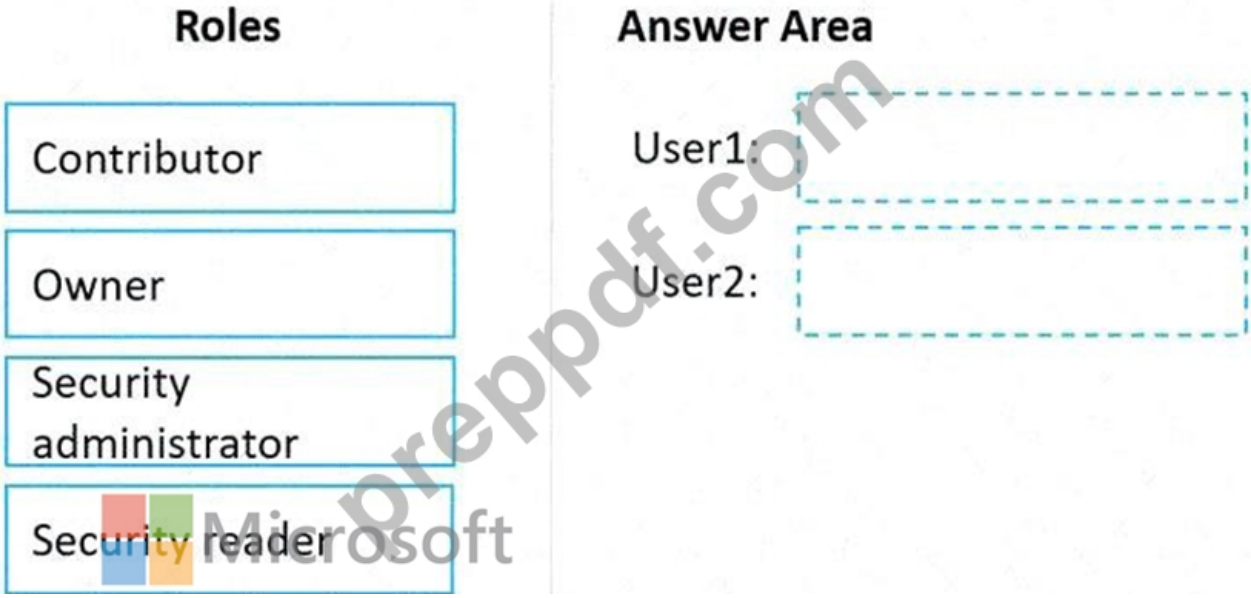
Explanation:

Answer Area

NEW QUESTION # 357
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.

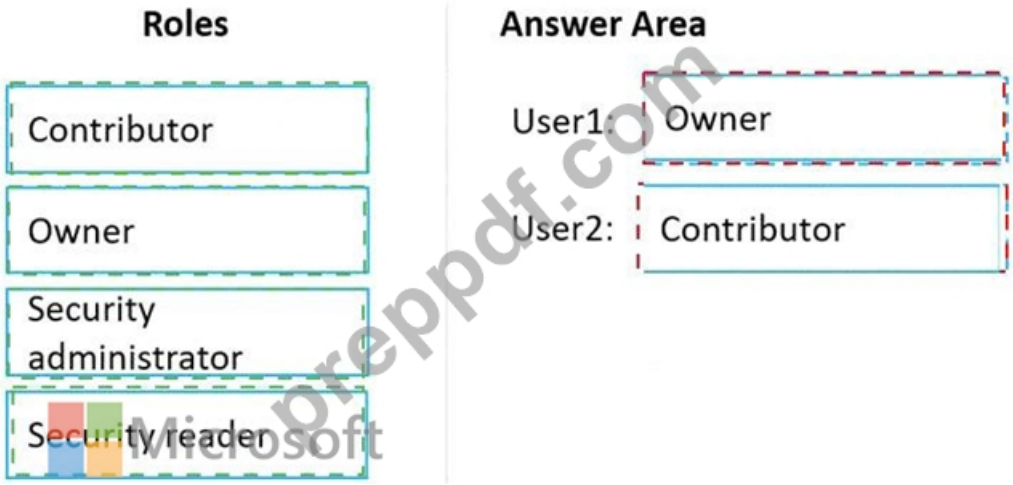
User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

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.



Answer:

Explanation:



Explanation:
Box 1: Owner
Only the Owner can assign initiatives.
Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

NEW QUESTION # 358
You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

- A. the status update time
- B. the certainty of the source computer
- C. the resolution method of the source computer
- D. the alert status

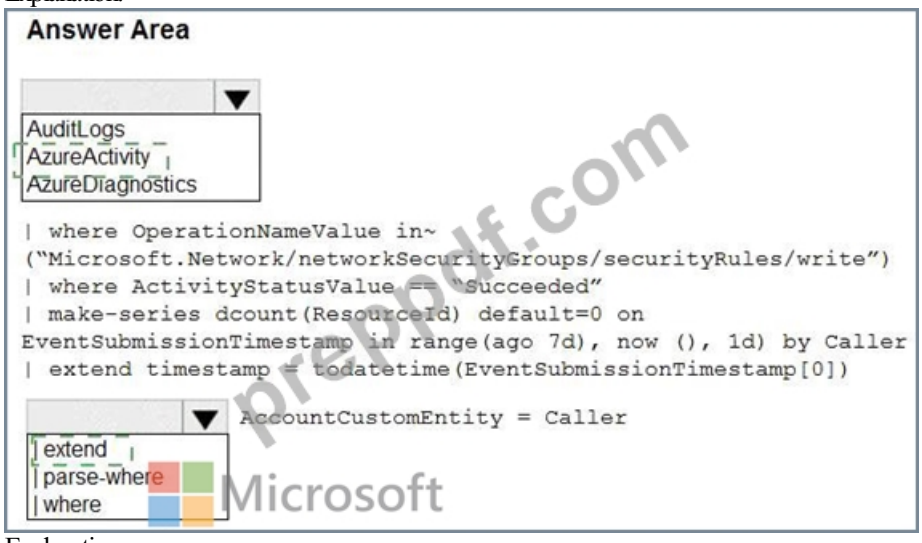
Answer: D

NEW QUESTION # 359
You have an Azure subscription that contains an Microsoft Sentinel workspace.
You need to create a hunting query using Kusto Query Language (KQL) that meets the following requirements:
* Identifies an anomalous number of changes to the rules of a network security group (NSG) made by the same security principal
* Automatically associates the security principal with an Microsoft Sentinel entity 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

Answer:

Explanation:



Explanation:
AzureActivity Extend

NEW QUESTION # 360

You have a Microsoft 365 subscription that uses Microsoft Defender XDR. You need to implement deception rules. The solution must ensure that you can limit the scope of the rules.
What should you create first?

- A. device tags
- B. honeytoken entity tags
- C. sensitive entity tags
- D. device groups

Answer: D

NEW QUESTION # 361
.....

The Microsoft SC-200 Certification Exam is one of the top-rated career advancement certifications in the market. With the Microsoft Security Operations Analyst SC-200 certification exam everyone can validate their skills and knowledge after passing the SC-200 text. The Microsoft Microsoft Security Operations Analyst certification exam will recognize your expertise and knowledge in the market. You will get solid proof of your proven skill set. There are other countless benefits that you can gain after passing the Microsoft Microsoft Security Operations Analyst certification exam.