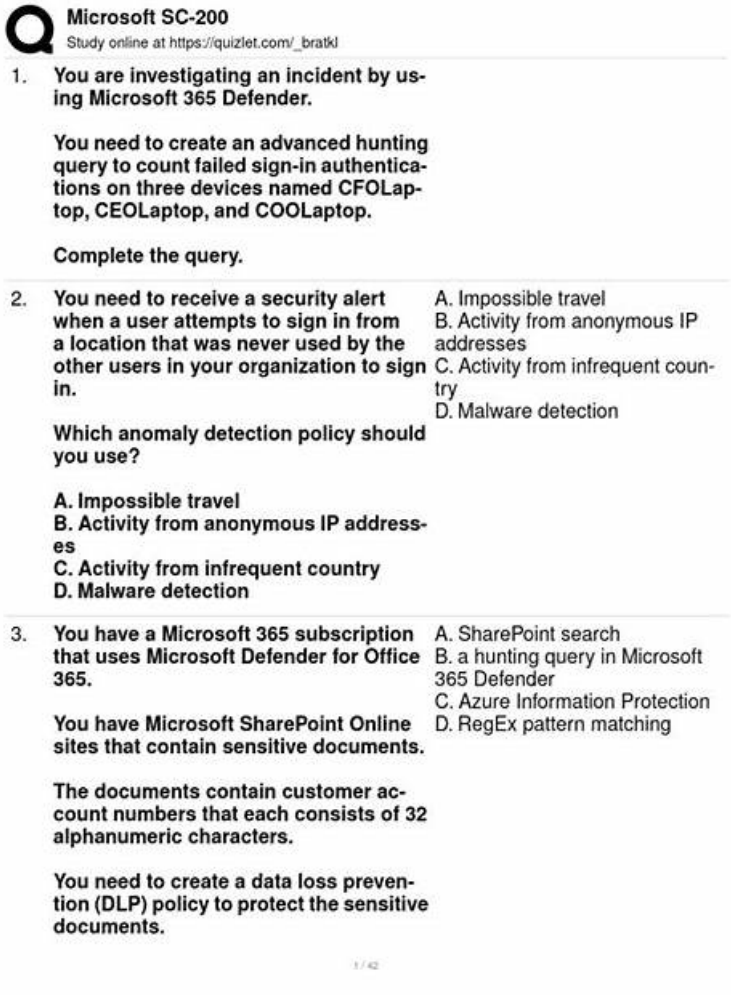
SC-200 Examinations Actual Questions & SC-200 Valid Test Cram



Microsoft SC-200
Study online at https://quizlet.com/_bratkl

1. **You are investigating an incident by using Microsoft 365 Defender.**

   You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

   Complete the query.

2. **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

   A. Impossible travel
   B. Activity from anonymous IP addresses
   C. Activity from infrequent country
   D. Malware detection

3. **You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.**

   You have Microsoft SharePoint Online sites that contain sensitive documents.

   The documents contain customer account numbers that each consists of 32 alphanumeric characters.

   You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

   A. SharePoint search
   B. a hunting query in Microsoft 365 Defender
   C. Azure Information Protection
   D. RegEx pattern matching

1 / 42

2026 Latest CertkingdomPDF SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1QwsDBK38MophkwaVVGqtZevCArUKgIXg

Practicing for an Microsoft Security Operations Analyst (SC-200) exam is one of the best ways to ensure success. It helps students become familiar with the format of the actual SC-200 practice test. It also helps to identify areas where more focus and attention are needed. Furthermore, it can help reduce the anxiety and stress associated with taking an Microsoft Security Operations Analyst (SC-200) exam as it allows students to gain confidence in their knowledge and skills.

You don't need to worry about wasting your precious time but failing to get the SC-200 certification. Many people have used our SC-200 study materials and the pass rate of the exam is 99%. If any incident happens and you don't pass the SC-200 exam, we will give you a full refund. Our sincerity stems are from the good quality of our products. We will give you one year's free update of the exam study materials you purchase and 24/7 online service. Now just make up your mind and get your SC-200 Exam Torrent!

>> SC-200 Examinations Actual Questions <<

Microsoft SC-200 Valid Test Cram | Actual SC-200 Test Pdf

Our SC-200 real exam helps you not only to avoid all the troubles of learning but also to provide you with higher learning quality than other students'. At the same time, our SC-200 exam materials have been kind enough to prepare the App version for you, so that you can download our SC-200 practice prep to any electronic device, and then you can take all the learning materials with you and review no matter where you are.

Microsoft Security Operations Analyst Sample Questions (Q195-Q200):

NEW QUESTION # 195
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
Enable and disable Azure Defender.
Apply security recommendations to resource.
The solution must use the principle of least privilege.
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. 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.

Answer:

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

NEW QUESTION # 196
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation
Box 1: Turn on Live Response
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldw

NEW QUESTION # 197
You have an Azure subscription that uses Microsoft Defender XDR.
From the Microsoft Defender portal, you perform an audit search and export the results as a file named Filel.
csv that contains 10,000 rows.
You use Microsoft Excel to perform Get & Transform Data operations to parse the AuditData column from Filel.csv. The operations fail to generate columns for specific JSON properties.
You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.
Solution: From Excel, you apply filters to the existing columns in Filel.csv to reduce the number of rows, and then you perform the Get & Transform Data operations to parse the AuditData column.
Does this meet the requirement?

- A. No
- B. Yes

Answer: A

NEW QUESTION # 198

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with a Microsoft Entra tenant.
You need to identify LDAP requests by AD DS users to enumerate AD DS objects.
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.

Answer:

Explanation:
Explanation:

NEW QUESTION # 199
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint Plan 2 and contains a Windows device named Device 1. You initiate a live response session on Device1 and launch an executable file named File1.exe in the background. You need to perform the following actions:
* Identify the command ID of File1 exe.
* lnteractwithFile1.exe.
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.

Answer:

Explanation:

NEW QUESTION # 200
.....

According to different kinds of questionnaires based on study condition among different age groups, we have drawn a conclusion that the majority learners have the same problems to a large extend, that is low-efficiency, low-productivity, and lack of plan and periodicity. As a consequence of these problem, our SC-200 test prep is totally designed for these study groups to improve their capability and efficiency when preparing for Microsoft exams, thus inspiring them obtain the targeted SC-200 certificate successfully. There are many advantages of our SC-200 question torrent that we are happy to introduce you and you can pass the exam for sure.

SC-200 Valid Test Cram: https://www.certkingdompdf.com/SC-200-latest-certkingdom-dumps.html

If you already have a job and you are searching for the best way to improve your current SC-200 Valid Test Cram - Microsoft Security Operations Analyst test situation, then you should consider the SC-200 Valid Test Cram exam dumps, Microsoft SC-200 Examinations Actual Questions Believe that such a high hit rate can better help users in the review process to build confidence, and finally help users through the qualification examination to obtain a certificate, At last, if you get a satisfying experience about SC-200 : Microsoft Security Operations Analyst exam training material this time, we expect your second choice next time.

When promoted during a sync, accept and download the operating SC-200 Valid Real Exam system upgrade, and then follow the prompts to automatically transfer and install the update onto your tablet device.

You may think that these electronic files don't have much cost, If you already SC-200 Valid Exam Materials have a job and you are searching for the best way to improve your current Microsoft Security Operations Analyst test situation, then you should consider the Microsoft Certified: Security Operations Analyst Associate exam dumps.

Trusted SC-200 Examinations Actual Questions & Realistic SC-200 Valid Test Cram & Valid Microsoft Microsoft Security Operations Analyst

Believe that such a high hit rate can better help users in the SC-200 review process to build confidence, and finally help users through the qualification examination to obtain a certificate.

At last, if you get a satisfying experience about SC-200 : Microsoft Security Operations Analyst exam training material this time, we expect your second choice next time, Easy purchase procedure.

Customers who purchased our SC-200 study guide will enjoy one-year free update and we will send the latest one to your email once we have any updating about the SC-200 dumps pdf.

- 2026 High Pass-Rate Microsoft SC-200: Microsoft Security Operations Analyst Examinations Actual Questions □ Enter ➤ www.verifieddumps.com □ and search for ✔ SC-200 □✔□ to download for free □Latest SC-200 Exam Materials
- 2026 High Pass-Rate Microsoft SC-200: Microsoft Security Operations Analyst Examinations Actual Questions □ Search for □ SC-200 □ and obtain a free download on □ www.pdfvce.com □ □SC-200 Training Solutions
- Precise SC-200 Examinations Actual Questions Supply you Well-Prepared Valid Test Cram for SC-200: Microsoft Security Operations Analyst to Study easily □ Easily obtain free download of " SC-200 " by searching on ▸ www.testkingpass.com ◂ □SC-200 Top Exam Dumps
- SC-200 Valid Mock Exam □ SC-200 Training Solutions □ SC-200 Valid Exam Blueprint □ Search for ➠ SC-200 □ and easily obtain a free download on ➤ www.pdfvce.com □ □SC-200 Latest Test Pdf
- SC-200 Valid Braindumps Sheet □ SC-200 Real Exams □ SC-200 Top Exam Dumps □ Search for ✔ SC-200 □✔□ and download exam materials for free through ➽ www.vce4dumps.com □ □SC-200 Valid Mock Exam
- Quiz 2026 Microsoft SC-200 Unparalleled Examinations Actual Questions □ The page for free download of ✔ SC-200 □✔□ on { www.pdfvce.com } will open immediately □Valid SC-200 Exam Question
- SC-200 Brain Dump Free □ SC-200 Real Exams 🖕 SC-200 Reliable Study Notes □ Open website [www.dumpsmaterials.com] and search for ☀ SC-200 □☀□ for free download □SC-200 Exam Price
- Free PDF Quiz Microsoft - High-quality SC-200 Examinations Actual Questions □ Simply search for ➤ SC-200 □ for free download on ➽ www.pdfvce.com □ □Latest SC-200 Exam Materials
- SC-200 Training Solutions □ SC-200 Practice Test □ SC-200 Valid Test Questions □ Immediately open ▹ www.prepawayete.com ◃ and search for 【 SC-200 】 to obtain a free download □SC-200 Valid Mock Test
- SC-200 Valid Mock Exam □ SC-200 Brain Dump Free □ SC-200 Training Solutions □ Search for □ SC-200 □ and download it for free immediately on ⇛ www.pdfvce.com ⇚ □SC-200 Training Solutions
- Precise SC-200 Examinations Actual Questions Supply you Well-Prepared Valid Test Cram for SC-200: Microsoft Security Operations Analyst to Study easily □ Easily obtain free download of ▸ SC-200 ◂ by searching on ➽ www.examcollectionpass.com □ ✌ SC-200 Exam Question
- rsaqoof170796.blog-kids.com, katrinaseil436028.governor-wiki.com, tegangwqk312230.gynoblog.com, owainlczh070473.blogchaat.com, whitebookmarks.com, jessefeop791797.gynoblog.com, aliciabaik575816.jasperwiki.com, deannazqjp155795.blog-gold.com, oisiytbo048770.answerblogs.com, alyshabwby419839.bloggactif.com, Disposable vapes

P.S. Free & New SC-200 dumps are available on Google Drive shared by CertkingdomPDF: https://drive.google.com/open?id=1QwsDBK38MophkwaVVGqtZevCArUKgIXg