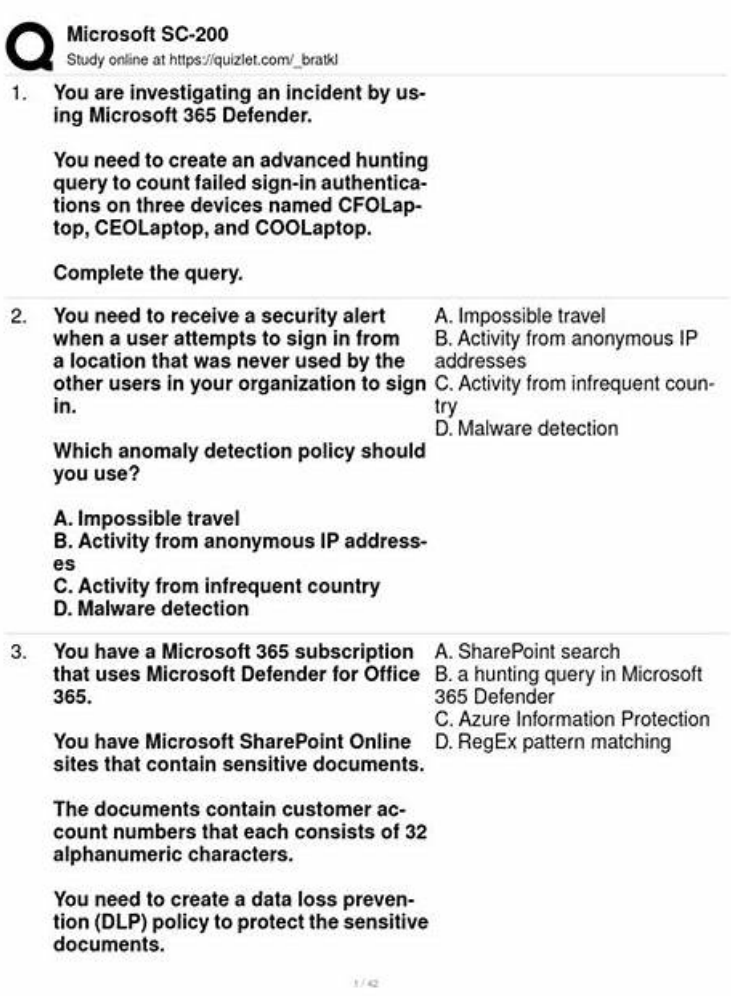
SC-200 New Guide Files - Exam SC-200 Study Guide



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 Pass4suresVCE SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=15zJdrMDTvuP0kJzikI4NxAQpX9TmHpzS

Now is not the time to be afraid to take any more difficult Microsoft Security Operations Analyst SC-200 certification exams. Our SC-200 learning quiz can relieve you of the issue within limited time. Our website provides excellent SC-200 learning guidance, practical questions and answers, and questions for your choice which are your real strength. You can take the Microsoft SC-200 Training Materials and pass it without any difficulty.

Microsoft SC-200 Certification Exam covers a wide range of topics related to security operations, including threat management, vulnerability management, incident response, and compliance. SC-200 exam is designed to test candidates' abilities to identify and mitigate security threats using Microsoft's security tools and technologies, such as Microsoft Defender for Endpoint, Azure Sentinel, and Microsoft Cloud App Security.

Schedule exam

Languages: English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Russian, Arabic (Saudi Arabia), Chinese (Traditional), Italian

Retirement date: none

This exam measures your ability to accomplish the following technical tasks: mitigate threats using Microsoft 365 Defender; mitigate threats using Azure Defender; and mitigate threats using Azure Sentinel.

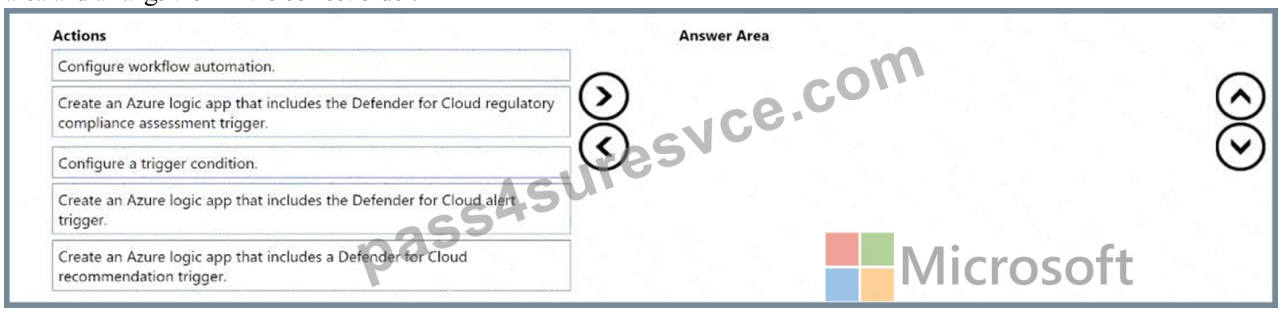
>> SC-200 New Guide Files <<

Exam SC-200 Study Guide | SC-200 Reliable Test Notes

Do you often envy the colleagues around you can successfully move to a larger company to achieve the value of life? Are you often wondering why your classmate, who has scores similar to yours, can receive a large company offer after graduation and you are rejected? In fact, what you lack is not hard work nor luck, but SC-200 Guide question. With SC-200 question torrent, you will suddenly find the joy of learning and you will pass the professional qualification exam very easily.

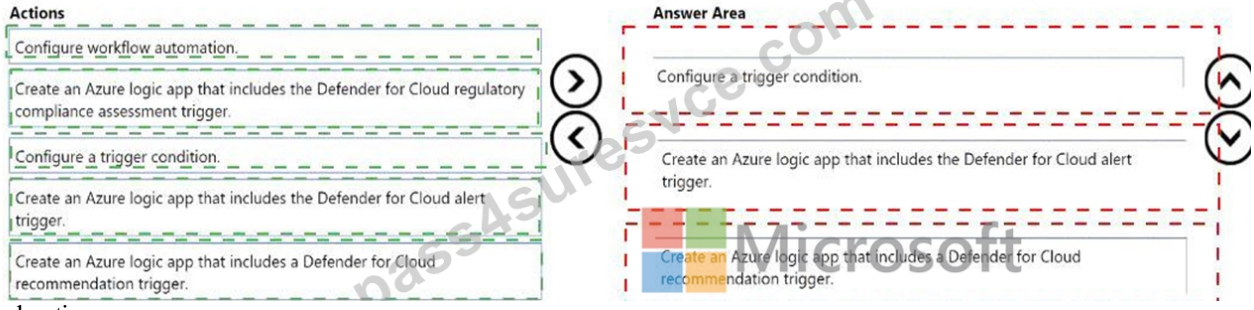
Microsoft Security Operations Analyst Sample Questions (Q152-Q157):

NEW QUESTION # 152
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

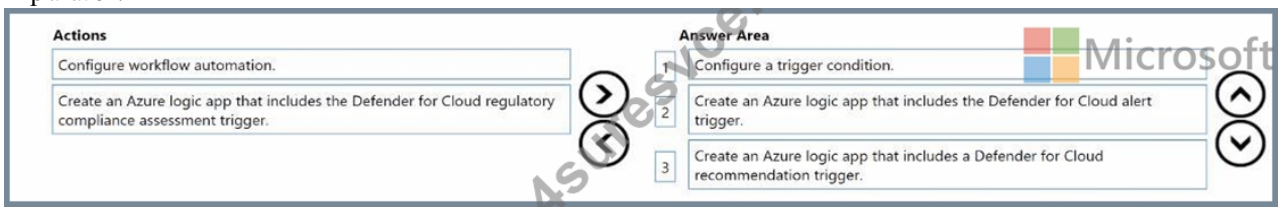


Answer:

Explanation:



Explanation:

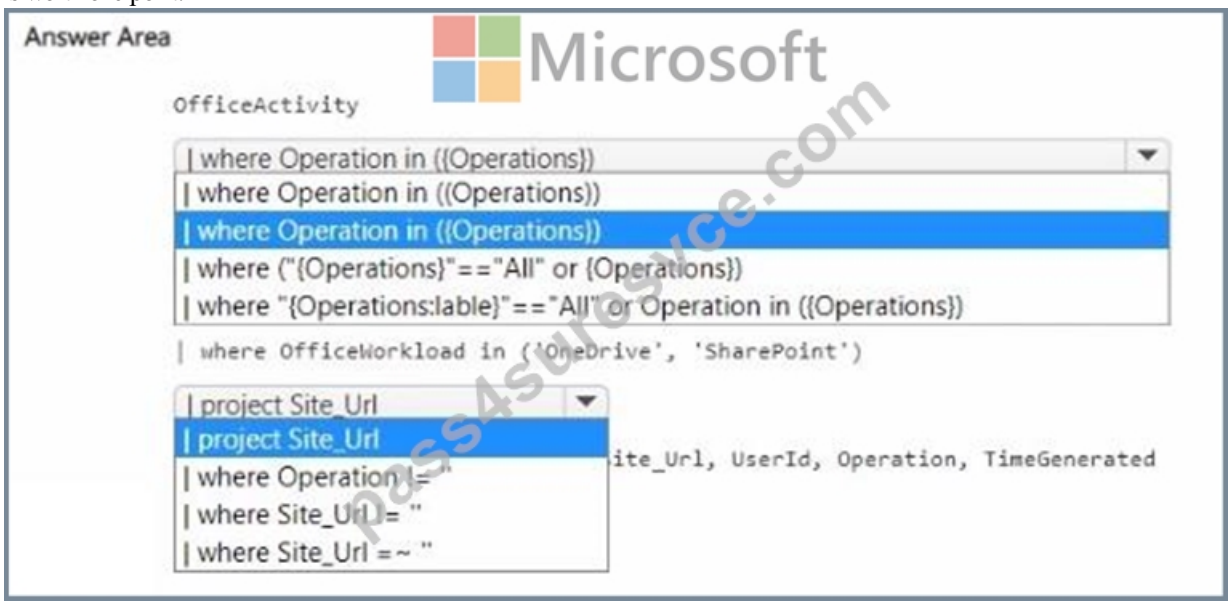


NEW QUESTION # 153
You have an Azure subscription that uses Microsoft Sentinel.
You need to create a custom workbook that will calculate the average time it takes to close security incidents.
The solution must minimize administrative effort.
Which built-in Microsoft Sentinel workbook template should you select?

- A. Security operations efficiency
- B. Investigation Insights
- C. Workspace Usage Report
- D. Incident Overview

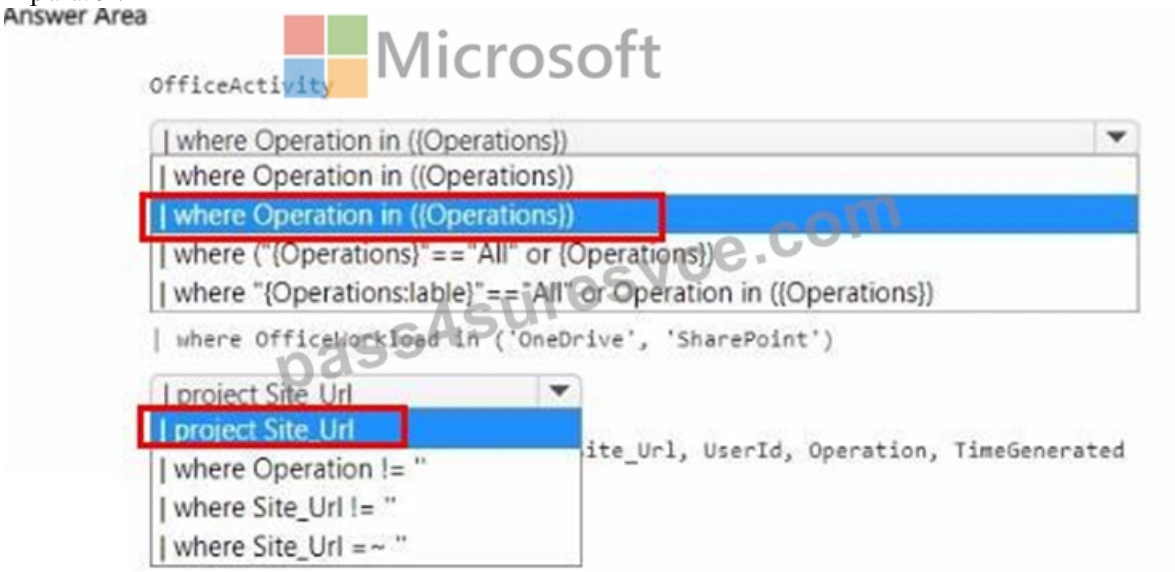
Answer: A

NEW QUESTION # 154
You have a Microsoft Sentinel workspace.
You plan to visualize data from Microsoft SharePoint Online and OneDrive sites.
You need to create a KQL query for the visual. The solution must meet the following requirements:
* Select all workloads as a single operation.
* Include two parameters named Operations and Users.
* In the results, exclude empty values for the site URLs.
How should you complete the query? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer:

Explanation:



NEW QUESTION # 155
You need to ensure that the Group1 members can meet the Microsoft Sentinel requirements.
Which role should you assign to Group1?

- A. Logic App Contributor
- B. Automation Operator

- C. Microsoft Sentinel Playbook Operator
- D. Microsoft Sentinel Automation Contributor

Answer: C

NEW QUESTION # 156
You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.
You need to identify the impacted entities in an aggregated alert.
What should you review in the DIP alert management dashboard of the Microsoft Purview compliance portal?

- A. the Sensitive Info Types tab of the alert
- B. the Events tab of the alert
- C. the Details tab of the alert
- D. Management log

Answer: D

NEW QUESTION # 157
.....

Our evaluation system for SC-200 test material is smart and very powerful. First of all, our researchers have made great efforts to ensure that the data scoring system of our SC-200 test questions can stand the test of practicality. Once you have completed your study tasks and submitted your training results, the evaluation system will begin to quickly and accurately perform statistical assessments of your marks on the SC-200 Exam Torrent. If you encounter something you do not understand, in the process of learning our SC-200 exam torrent, you can ask our staff. We provide you with 24-hour online services to help you solve the problem. Therefore we can ensure that we will provide you with efficient services.

Exam SC-200 Study Guide: https://www.pass4suresvce.com/SC-200-pass4sure-vce-dumps.html

- Renowned SC-200 Guide Exam: Microsoft Security Operations Analyst Carry You High-efficient Practice Materials □ Search for ☀ SC-200 □☀□ and easily obtain a free download on ⇛ www.practicevce.com ⇚ □Exam SC-200 Cram Questions
- SC-200 Exam Score □ SC-200 Examcollection Vce □ SC-200 Authorized Pdf □ Download [SC-200] for free by simply searching on ➥ www.pdfvce.com □ □Valid SC-200 Exam Dumps
- Renowned SC-200 Guide Exam: Microsoft Security Operations Analyst Carry You High-efficient Practice Materials □ ▹ www.pass4test.com ◃ is best website to obtain ➡ SC-200 □□□ for free download □SC-200 Valid Exam Materials
- Pass Guaranteed 2026 High Hit-Rate Microsoft SC-200 New Guide Files □ Search for ➤ SC-200 □ and download it for free on 「 www.pdfvce.com 」 website □Latest SC-200 Training
- SC-200 Exam Score □ Standard SC-200 Answers □ Latest SC-200 Training □ Search for ➥ SC-200 □ on 「 www.practicevce.com 」 immediately to obtain a free download □Valid SC-200 Exam Topics
- Valid SC-200 Exam Voucher □ Valid SC-200 Exam Voucher □ SC-200 Exam Score □ Immediately open □ www.pdfvce.com □ and search for （ SC-200 ） to obtain a free download □Valid SC-200 Exam Dumps
- Vce SC-200 Torrent □ Exam SC-200 Cram Questions □ Exam SC-200 Cram Questions □ ➽ www.torrentvce.com □ is best website to obtain ➤ SC-200 □ for free download □Valid SC-200 Exam Topics
- 2026 SC-200 New Guide Files - Microsoft Microsoft Security Operations Analyst - Latest Exam SC-200 Study Guide □ Easily obtain □ SC-200 □ for free download through □ www.pdfvce.com □ □Reliable SC-200 Real Exam
- 2026 SC-200 New Guide Files - Microsoft Microsoft Security Operations Analyst - Latest Exam SC-200 Study Guide □ Go to website ⇛ www.prep4away.com ⇚ open and search for " SC-200 " to download for free □Reliable SC-200 Real Exam
- 100% Pass SC-200 Marvelous Microsoft Security Operations Analyst New Guide Files □ Download ➠ SC-200 □ for free by simply searching on ✔ www.pdfvce.com □✔□ □SC-200 Valid Exam Materials
- SC-200 Valid Exam Materials □ SC-200 Exam Score □ SC-200 Exam Score □ Search for 【 SC-200 】 and download it for free immediately on ▸ www.troytecdumps.com ◂ □SC-200 Valid Exam Questions
- socialfactories.com, bookmarkpath.com, delilahcicl658257.wikitron.com, minamycp974300.wikienlightenment.com, nanniesihj792956.blog2news.com, artybookmarks.com, flynnukbs044331.blog-eye.com, tedkqnn906943.nico-wiki.com, nelsonstfa508499.fare-blog.com, abelsitt867345.wikienlightenment.com, Disposable vapes

What's more, part of that Pass4suresVCE SC-200 dumps now are free: https://drive.google.com/open?

id=15zJdrMDTvuP0kJzikI4NxAQpX9TmHpzS