DumpExam Provides Microsoft SC-200 Exam Questions 2026

P.S. Free & New SC-200 dumps are available on Google Drive shared by DumpExam: https://drive.google.com/open?id=1KiK1Sr2sJg-PdhzdJQMMGY-zzyllWeiY

Career competitive is similar with playing tennis, if you want to defeat your opponents every time, you will improve yourself continuously. You can choose Microsoft SC-200 valid test dumps materials to help you clear exams. You will get an outstanding advantage over others while applying a same position. You will get better benefits and salary. Our SC-200 Valid Test Dumps materials will be the best preparation tool for every candidate.

How to Register For Exam SC-200: Microsoft Security Operations Analyst?

Exam Register Link: https://examregistration.microsoft.com/?locale=en-us&examcode=SC-200&examname=Exam%20SC-200:%20Microsoft%20Security%20Operations%20Analyst&returnToLearningUrl=https%3A%2F%2Fdocs.microsoft.com%2Flearn%2Fcertifications%2Fexams%2Fsc-200

Microsoft SC-200 Certification is a valuable credential for professionals who specialize in security operations. Microsoft Security Operations Analyst certification is aimed at individuals who are responsible for managing and protecting an organization's IT infrastructure. The SC-200 certification validates the skills and knowledge required to perform tasks such as threat management, incident response, and vulnerability management.

>> SC-200 Dumps Collection <<

Study Materials Microsoft SC-200 Review, Exam SC-200 Guide Materials

For candidates who will buy SC-200 training materials online, they may pay more attention to privacy protection. We respect your private information, and your personal identification information will be protected well if you choose us. Once the order finishes, your personal information will be concealed. In addition, SC-200 Exam Dumps contain not only quality but also certain quantity. It will be enough for you to pass the exam. In order to build up your confidence for SC-200 exam dumps, we are pass guarantee and money back guarantee, if you fail to pass the exam, we will give you full refund.

Achieving the Microsoft Security Operations Analyst certification can be a valuable asset for security professionals looking to advance their careers in the field of cybersecurity. Microsoft Security Operations Analyst certification demonstrates that the candidate has the skills and knowledge necessary to detect, investigate, and respond to security incidents in a Microsoft environment and can be a valuable addition to any security team.

Microsoft Security Operations Analyst Sample Questions (Q369-Q374):

NEW QUESTION # 369
You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

- A. Key Vault firewalls and virtual networks
- B. role-based access control (RBAC) for the key vault
- C. Azure Active Directory (Azure AD) permissions
- D. the access policy settings of the key vault

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security
Topic 2, Contoso Ltd
Existing Environment
End-User Environment
All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.
Cloud and Hybrid Infrastructure
All Contoso applications are deployed to Azure.
You enable Microsoft Cloud App Security.
Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.
Current Problems
The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.
The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced various attacks on their devices.
The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.
The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past 48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.
Requirements
Planned Changes
Contoso plans to integrate the security operations of both companies and manage all security operations centrally.
Technical Requirements
Contoso identifies the following technical requirements:
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.
BehaviorAnalytics
| where ActivityType == "FailedLogOn"
| where _____ == True

NEW QUESTION # 370
You have a Microsoft Sentine1 workspace that contains a custom workbook named Workbook1.
You need to create a visual in Workbook1 that will display the logon count for accounts that have logon event IDs of 4624 and 4634.
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:

Explanation:

Explanation:
First dropdown: join
Second dropdown: full
In Microsoft Sentinel and Kusto Query Language (KQL), when you need to combine two tables based on a common field, you use the join operator. In this scenario, both queries pull from the same SecurityEvent table but filter on different Event IDs - 4624 for logon and 4634 for logoff events. To correlate or compare the two results by Account, you need to join them.
The first query returns the number of logon events per account (LogOnCount), while the second returns the number of logoff events per account (LogOffCount). The join key is Account, which exists in both result sets.
To ensure that all accounts - those who may have only logon events or only logoff events - are included in the visualization, you use a full join. A full join combines matching records from both sides and keeps unmatched records from either side, filling missing values with nulls. This ensures that every account with either a logon or a logoff count appears in the results.
Therefore, the correct query completion is:

```
SecurityEvent
| where EventID == "4624"
| summarize LogOnCount = count() by EventID, Account
| project LogOnCount, Account
| join kind = full (
SecurityEvent
| where EventID == "4634"
| summarize LogOffCount = count() by EventID, Account
| project LogOffCount, Account
) on Account
```

This query gives a complete view of all accounts and their corresponding logon/logoff counts.
Correct selections:
* First box # join
* Second box # full

NEW QUESTION # 371
You deploy Azure Sentinel.
You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

NEW QUESTION # 372
You need to meet the Microsoft Sentinel requirements for collecting Windows Security event logs. What should you do? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.

Answer:

Explanation:

NEW QUESTION # 373
You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.
You have a team named Team1 that has a project named Project 1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.
Which KQL query should you run?

- A. □
- B. □
- C. □
- D. □

Answer: B

NEW QUESTION # 374
.....

Study Materials SC-200 Review: https://www.dumpexam.com/SC-200-valid-torrent.html

- 100% Pass SC-200 - Microsoft Security Operations Analyst Latest Dumps Collection □ Enter □ www.exam4labs.com □ and search for □ SC-200 □ to download for free □SC-200 Reliable Exam Simulator
- Quiz 2026 Microsoft Latest SC-200 Dumps Collection □ Download [SC-200] for free by simply searching on ✔ www.pdfvce.com □✔□ □SC-200 Sample Test Online
- Latest SC-200 Study Guide □ SC-200 Latest Learning Materials □ SC-200 Guide Torrent □ Search for ➥ SC-200 □ □ on 【 www.torrentvce.com 】 immediately to obtain a free download □SC-200 Sample Test Online
- SC-200 Exam Simulator Fee □ SC-200 Reliable Exam Simulator □ SC-200 Advanced Testing Engine □ Search for □ SC-200 □ and download it for free immediately on ➥ www.pdfvce.com □ □VCE SC-200 Dumps
- Try Microsoft SC-200 Exam Questions For Sure Success □ The page for free download of □ SC-200 □ on ⇛ www.testkingpass.com ⇚ will open immediately □SC-200 Latest Test Testking
- 2026 SC-200 – 100% Free Dumps Collection | Useful Study Materials SC-200 Review □ Search for ▹ SC-200 ◃ and download exam materials for free through □ www.pdfvce.com □ □SC-200 Latest Test Testking
- 2026 SC-200 – 100% Free Dumps Collection | Useful Study Materials SC-200 Review □ Go to website ➥ www.practicevce.com □ open and search for ➥ SC-200 □ to download for free ↗ Latest SC-200 Study Guide
- VCE SC-200 Dumps □ SC-200 Latest Test Testking □ Latest SC-200 Study Guide □ Search for ➥ SC-200 □ and download exam materials for free through ➽ www.pdfvce.com □ □SC-200 Latest Learning Materials
- New Release Microsoft SC-200 Dumps For Brilliant Exam Study 2026 □ Go to website " www.testkingpass.com " open and search for □ SC-200 □ to download for free □SC-200 Exam Simulator Fee
- SC-200 Exam Simulator Fee □ Exam SC-200 Braindumps □ SC-200 Sample Test Online □ The page for free download of ➡ SC-200 □□□ on □ www.pdfvce.com □ will open immediately □SC-200 Exam Simulator Fee
- Examcollection SC-200 Vce □ SC-200 Guide Torrent □ SC-200 Latest Exam Camp □ Simply search for ➥ SC-200 □ for free download on 「 www.exam4labs.com 」 □SC-200 Reliable Exam Simulator
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, telegra.ph, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that DumpExam SC-200 dumps now are free: https://drive.google.com/open?id=1KiK1Sr2sJg-PdhzdJQMMGY-zzylIWeiY