Latest SC-200 Guide Files, SC-200 Testking Learning Materials

P.S. Free & New SC-200 dumps are available on Google Drive shared by Dumpexams: https://drive.google.com/open?id=14sEiOPTAqvJgogwYvlY9L2VqarJYzJJw

Web-based SC-200 practice test of Dumpexams is accessible from any place. You merely need an active internet connection to take this Microsoft SC-200 practice exam. Browsers including MS Edge, Internet Explorer, Safari, Opera, Chrome, and Firefox support this SC-200 Practice Exam. Additionally, this Microsoft Security Operations Analyst (SC-200) test is supported by operating systems including Android, Mac, iOS, Windows, and Linux.

What is the format of Microsoft SC-200 Exam

- Exam Duration: 130 minutes
- Language: English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Russian, Arabic (Saudi Arabia), Chinese (Traditional), Italian
- Exam Length: 40 questions
- Exam Format: Multiple choice questions
- Passing score: 70%

Microsoft SC-200 certification exam is designed for professionals who work with Microsoft security technologies and want to enhance their knowledge and skills in security operations analysis. SC-200 Exam covers a wide range of topics, including threat intelligence, incident response, data protection, and compliance. Microsoft Security Operations Analyst certification exam is an excellent way to demonstrate one's expertise in Microsoft security technologies and showcase their commitment to professional development.

>> Latest SC-200 Guide Files <<

Microsoft SC-200 Testking Learning Materials | Valid SC-200 Exam Topics

If you have a dream to get the Microsoft certification? Why don't you begin to act? The first step is to pass SC-200 exam. Time will wait for no one. Only if you pass the SC-200 exam, can you get a better promotion. And if you want to pass it more efficiently, we must be the best partner for you. Because we are professional SC-200 Questions torrent provider, and our SC-200 training materials are worth trusting; because we make great efforts on our SC-200 learning guide, we do better and better in this field for more than ten years. Our SC-200 study guide is your best choice.

Microsoft Security Operations Analyst Sample Questions (Q199-Q204):

NEW QUESTION # 199
HOTSPOT
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.
Hot Area:

Answer:

Explanation:
Section: [none]
Explanation/Reference:
Testlet 2
Case study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam.
You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.
Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.
On-premises Environment
The on-premises network contains the computers shown in the following table.
Current problems
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
* Create and configure Azure Sentinel in the Azure subscription.
* Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements
Litware identifies the following business requirements:
* The principle of least privilege must be used whenever possible.
* Costs must be minimized, as long as all other requirements are met.
* Logs collected by Log Analytics must provide a full audit trail of user activities.
* All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for

Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
* Integrate Azure Sentinel and Cloud App Security.
* Ensure that a user named admin1 can configure Azure Sentinel playbooks.
* Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
* Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
* Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION # 200
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Add a playbook.
- B. Create a workbook.
- C. Enable the Fusion rule.
- D. Enable Entity behavior analytics.
- E. Associate a playbook to the analytics rule that triggered the incident.

Answer: A,E

Explanation:
To automatically send a Microsoft Teams message when an incident (like a sign-in risk) is activated, you must use Logic Apps playbooks in Microsoft Sentinel.
Steps based on Microsoft documentation:
* Add (create) a playbook (Option D) - a Logic App workflow that defines the automation (e.g., post a message to a Teams channel).
* Associate the playbook to the analytics rule (Option B) that generates the incident - this ensures the playbook triggers automatically whenever that rule fires.
Other options do not accomplish the goal:
* Entity behavior analytics (A) provides user and entity context but does not automate actions.
* Fusion rule (C) correlates multi-stage attacks automatically but isn't used to trigger notifications.
* Workbooks (E) are for visualization, not automation.
# Final Answers:
* Question 80: D. Assign the incident
* Question 83: B and D

NEW QUESTION # 201
You have an Azure subscription that contains 50 virtual machines.
You plan to deploy Microsoft [Defender for Cloud.
You need to enable agentless scanning for 40 virtual machines. The solution must create disk snapshots of the virtual machines and perform out-of-band analysis of the snapshots.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 202
You need to assign role-based access control (RBAQ roles to Group1 and Group2 to meet The Microsoft Defender for Cloud requirements and the business requirements Which role should you assign to each group?
To answer, select the appropriate options in the answer area NOTE Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 203
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center- alerts-are-now/ba-p/1404920

NEW QUESTION # 204
.....

It is a virtual certainty that our SC-200 actual exam is high efficient with passing rate up to 98 percent and so on. We made it by persistence, patient and enthusiastic as well as responsibility. Moreover, about some tricky problems of SC-200 Exam Materials you do not to be anxious and choose to take a detour, our experts left notes for your reference. So our SC-200 practice materials are beyond the contrivance of all of you.

Learning Materials 󠁧 󠁧 www.prepawayete.com 󠁧 is best website to obtain ➤ SC-200 󠁧 for free download 󠁧SC-200 Valid Exam Dumps

- 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, 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.thingstogetme.com, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Dumpexams SC-200 dumps now are free: https://drive.google.com/open?id=14sEiOPTAqvJgogwYvlY9L2VqarJYzJJw