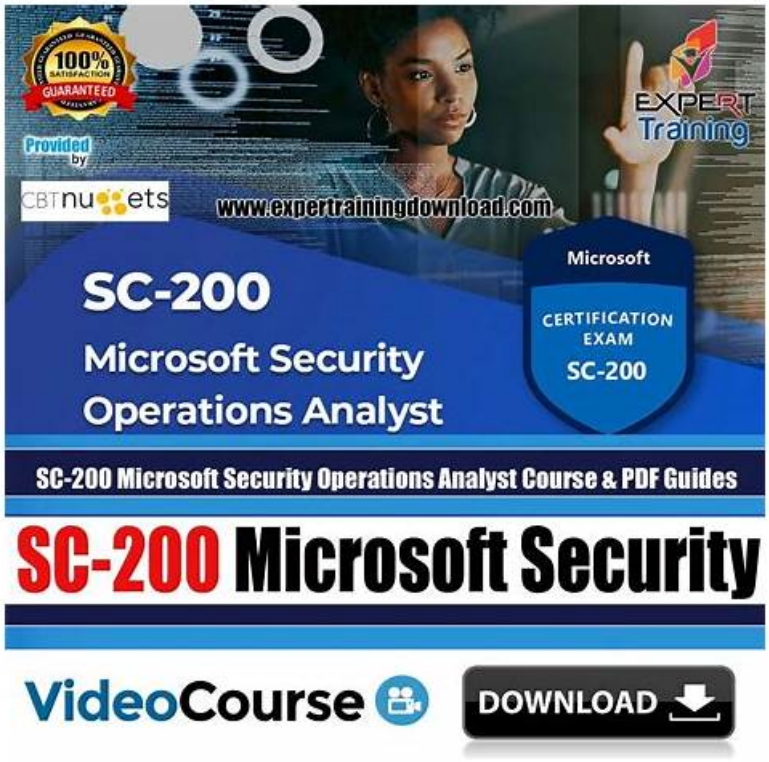
Free PDF Quiz Microsoft SC-200 Microsoft Security Operations Analyst First-grade Detailed Answers



BONUS!!! Download part of Pass4cram SC-200 dumps for free: https://drive.google.com/open?id=1gZG_mUtaQDxjyjSJciQmhBBPl5U91an-

Pass4cram releases a new high pass-rate SC-200 valid exam preparation recently. If you are still puzzled by your test you can set your heart at rest to purchase our valid exam materials which will assist you to clear exam easily. We can guarantee purchasing Microsoft SC-200 Valid Exam Preparation will be the best passing methods and it always help you pass exam at first attempt. Now it is really an opportunity. Stop waiting and hesitate again!

Microsoft SC-200 (Microsoft Security Operations Analyst) Exam is a valuable certification for professionals looking to advance their career in security operations. It provides a comprehensive coverage of the skills and knowledge required to perform security operations tasks and demonstrates the candidate's proficiency in Microsoft security technologies. By achieving this certification, professionals can enhance their credentials and demonstrate their commitment to the field of security operations.

The Microsoft SC-200 exam comprises of 40-60 questions and has a time limit of 180 minutes. The questions are presented in multiple-choice format and may include simulations, case studies, and other types of questions. SC-200 Exam is available in English and Japanese, and the cost of the exam is $165.

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.

>> Detailed SC-200 Answers <<

Only The Validest Detailed SC-200 Answers Can Provide The Promise of Passing Microsoft Security Operations Analyst

According to the survey, the average pass rate of our candidates has reached 99%. High passing rate must be the key factor for choosing, which is also one of the advantages of our SC-200 real study dumps. Once our customers pay successfully, we will check about your email address and other information to avoid any error, and send you the SC-200 prep guide in 5-10 minutes, so you

can get our SC-200 Exam Questions at first time. And then you can start your study after downloading the SC-200 exam questions in the email attachments. High efficiency service has won reputation for us among multitude of customers, so choosing our SC-200 real study dumps we guarantee that you won't be regret of your decision.

Microsoft Security Operations Analyst Sample Questions (Q456-Q461):

NEW QUESTION # 456
You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
View the window
You need to test LA1 in Security Center.
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
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-whe

NEW QUESTION # 457
You have a Microsoft 365 subscription that uses Microsoft Defender XDR. The subscription contains 500 devices that are joined to Microsoft Entra, are in the Microsoft Defender for Endpoint default device group, and are managed by using Microsoft Intune.
You need to implement Microsoft Defender Vulnerability Management. The solution must minimize the administrative effort.
What should you do first in the Microsoft Defender portal?

- A. Configure auto remediation for the default device group.
- B. Set Microsoft Intune connection to On.
- C. Set Live Response to On.
- D. From Configuration management, configure the Enforcement scope settings.

Answer: B

Explanation:
To get Defender Vulnerability Management (TVM) working with Intune-managed devices, first enable the Intune connection in the Defender portal (Settings > Endpoints > Advanced features) and then use Endpoint Security Policies (Configuration profiles) in Intune or the Defender portal to deploy security settings and onboard devices, creating device groups in Entra ID to target these policies effectively for vulnerabilities and remediation.
Here are the key configuration steps:
In the Microsoft Defender Portal (security.microsoft.com):
*-> 1. Connect to Intune: Go to Settings > Endpoints > Advanced features, find the "Microsoft Intune connection," and turn the toggle On, then Save.
2. Check Device Onboarding: Verify devices appear in the Assets > Devices inventory, showing their risk, exposure, and management status.
3. Use Device Groups: Navigate to Endpoints > Device groups, create/manage groups (e.g., for Windows 11) to filter vulnerability data and apply specific settings.
In Microsoft Intune (Microsoft Endpoint Manager admin center):
1. Onboard Devices
2. Deploy Security Settings
3. Create Remediation Tasks
Reference:
https://learn.microsoft.com/en-us/intune/intune-service/protect/microsoft-defender-integrate

NEW QUESTION # 458
Which rule setting should you configure to meet the Microsoft Sentinel requirements?

- A. From Set rule logic, turn off suppression.
- B. From Analytic rule details, configure the severity.
- C. From Set rule logic, map the entities.
- D. From Analytic rule details, configure the tactics.

Answer: C

Explanation:
In Microsoft Sentinel, entity mapping is a critical configuration that ensures detected events and alerts are correctly represented in the investigation graph, incidents, and hunting experiences. The Sentinel requirements in the case study specify:
"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." To meet this requirement, the analytic rule must be configured to map entities such as IP address, user, hostname, or URL in the Set rule logic section. This mapping allows the incident and its related alerts to visually associate with those entities, enabling analysts to pivot and investigate in the Sentinel investigation graph.
According to Microsoft Sentinel documentation:
"Entity mapping in analytic rules helps correlate alerts and incidents to specific entities such as accounts, IPs, or hosts, enabling richer investigation experiences and faster triage." Therefore, configuring entity mapping directly under Set rule logic ensures that incidents are enriched with contextual information (for example, the specific IP address), meeting both the functional and investigative requirements.
Final Answer for Question 2: C. From Set rule logic, map the entities.
Topic 1, Litware inc.
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 # 459
You have a Microsoft Sentinel workspace.
You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.
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:

NEW QUESTION # 460
You have a Microsoft 365 E5 subscription that contains two users named User! and User2. You have the hunting query shown in the following exhibit.
The users perform the following anions:
* User1 assigns User2 the Global administrator role.
* User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
* User2 creates a new user named User4 and assigns the user the Security reader role.
* User2 creates a new user named User5 and assigns the user the Security operator role.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 461
.....

With our SC-200 learning quiz, the exam will be a piece of cake. And SC-200 training materials serve as a breakthrough of your

entire career. Meanwhile, SC-200 study guide provides you considerable solution through the exam and efficient acquaintance. By imparting the knowledge of the exam to those ardent exam candidates who are eager to succeed like you, our experts treat it as responsibility to offer help. So please prepare to get striking progress if you can get our SC-200 Study Guide with following traits for your information.

Updated SC-200 Dumps: https://www.pass4cram.com/SC-200_free-download.html

- Valid SC-200 Exam Prep □ SC-200 Latest Dumps Sheet □ Exam SC-200 Topic □ The page for free download of ➡ SC-200 □□□ on ➡ www.testkingpass.com □□□ will open immediately □Valid SC-200 Cram Materials
- High Pass-Rate Microsoft Detailed SC-200 Answers - Trustable Pdfvce - Leading Provider in Qualification Exams □ Search for { SC-200 } and download it for free on { www.pdfvce.com } website □Exam SC-200 Revision Plan
- SC-200 Latest Dumps Sheet □ Exam SC-200 Answers □ SC-200 Customized Lab Simulation □ The page for free download of ➽ SC-200 □ on ▹ www.easy4engine.com ◃ will open immediately □Reliable SC-200 Exam Topics
- Best SC-200 Practice □ Valid Braindumps SC-200 Ppt □ Valid SC-200 Cram Materials □ Immediately open ▸ www.pdfvce.com ◂ and search for ➤ SC-200 □ to obtain a free download ♣SC-200 Practice Test Engine
- SC-200 Valid Test Questions □ Exam SC-200 Revision Plan □ SC-200 Valid Exam Practice □ Go to website （ www.prepawayexam.com ） open and search for ▸ SC-200 ◂ to download for free □Valid Braindumps SC-200 Ppt
- Valid SC-200 Cram Materials □ Valid Braindumps SC-200 Ppt □ Valid SC-200 Test Labs □ ➡ www.pdfvce.com □□□ is best website to obtain ▸ SC-200 ◂ for free download ♣Related SC-200 Certifications
- Detailed SC-200 Answers - Successfully Pass The Microsoft Security Operations Analyst □ Search for { SC-200 } and easily obtain a free download on ➽ www.exam4labs.com □ □SC-200 Valid Exam Practice
- Latest SC-200 Exam Torrent - SC-200 Quiz Prep -amp; SC-200 Quiz Torrent □ Open □ www.pdfvce.com □ and search for 【 SC-200 】 to download exam materials for free □Valid SC-200 Cram Materials
- Proven and Quick Way to Pass the Microsoft SC-200 Exam □ Easily obtain □ SC-200 □ for free download through ➤ www.testkingpass.com □ □Valid SC-200 Exam Duration
- Free PDF Quiz 2026 SC-200: Microsoft Security Operations Analyst Authoritative Detailed Answers □ Immediately open 「 www.pdfvce.com 」 and search for { SC-200 } to obtain a free download □Valid SC-200 Cram Materials
- New SC-200 Exam Pass4sure □ Free SC-200 Pdf Guide ✏ Free SC-200 Pdf Guide □ Search for 【 SC-200 】 and download it for free immediately on □ www.vce4dumps.com □ ↕SC-200 Valid Test Questions
- www.stes.tyc.edu.tw, listfav.com, imogenapse993535.wikigop.com, woodyayjo399384.blog4youth.com, madesocials.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, poppycvvg069960.vigilwiki.com, socialmarkz.com, marvinjlce592660.activablog.com, Disposable vapes

P.S. Free 2026 Microsoft SC-200 dumps are available on Google Drive shared by Pass4cram: https://drive.google.com/open?id=1gZG_mUtaQDxjyjSJciQmhBBPl5U91an-