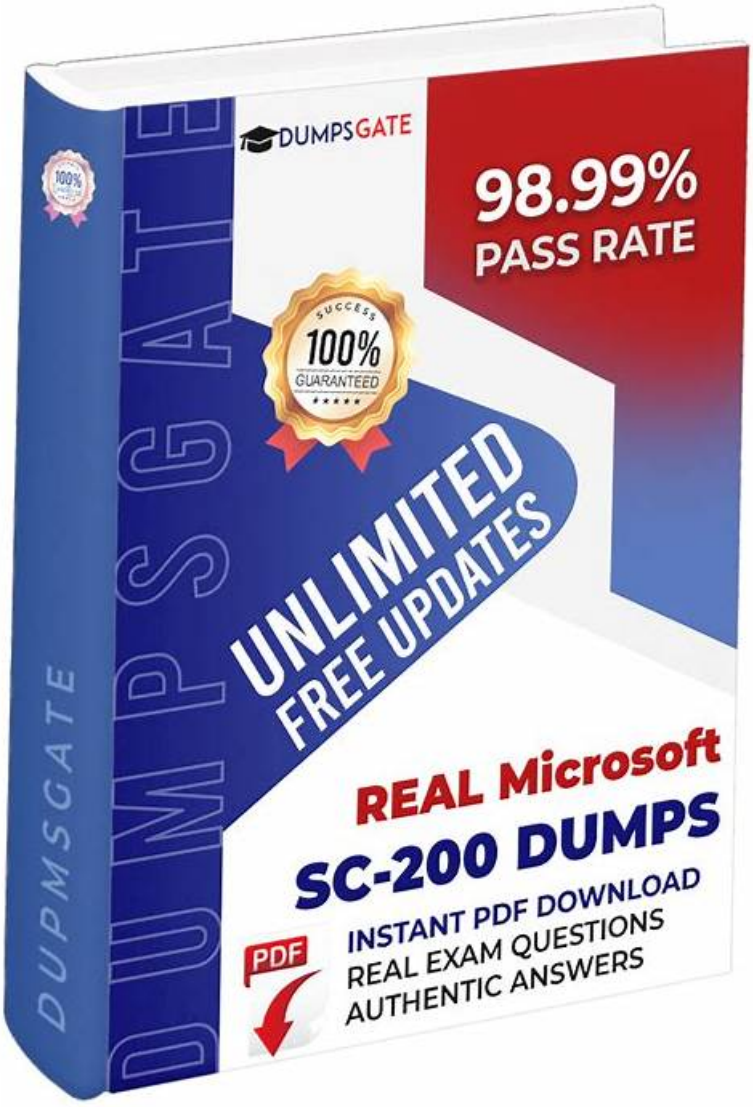
Get Unparalleled Dumps SC-200 Torrent and Fantastic Valid SC-200 Exam Pattern



BTW, DOWNLOAD part of PDFDumps SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=199I90BBfviDQvbOkiXTYCWngW3JplS-N

All exam materials in SC-200 learning materials contain PDF, APP, and PC formats. They have the same questions and answers but with different using methods. If you like to take notes randomly according to your own habits while studying, we recommend that you use the PDF format of our SC-200 Study Guide. And besides, you can take it with you wherever you go for it is portable and takes no place. So the PDF version of our SC-200 exam questions is convenient.

A brief introduction of Microsoft SC-200 Exam

Microsoft Security Operations Analyst Certification, often referred to as Microsoft SC-200 Exam is one of the most important courses among other courses provided by Microsoft. The course focuses on Security Analysis and Design, which is a very important factor in Network Administration. This helps us to create a secure environment for our organization. This certification provides you with the skills necessary to plan, deploy and monitor security solutions in an enterprise environment and also the skills required to administer and manage the computer security infrastructure. It gives you an edge over other candidates in terms of skill set and makes you more competitive in the job market of today's time. The course helps you understand how to plan, deploy and monitor security solutions in an enterprise environment and also how to administer and manage the computer security infrastructure. **SC-200 Dumps** is designed to make your Microsoft SC-200 Certification preparation easy and fast.

It gives you an edge over other candidates in terms of skill-set and makes you more competitive in the job market of today's time. SC-200 exam validates your ability to design, deploy, manage and monitor a security infrastructure for a private or public organization. The exam measures your knowledge of risk management; incident response; compliance with privacy laws; data protection; cryptography, access control; business continuity planning; auditing & monitoring; intrusion detection & prevention systems (IDS/IPS); web application firewall.

Dumps SC-200 Torrent High Hit Rate Questions Pool Only at PDFDumps

Every person in the IT industry has his own dream: to pass SC-200 certification exam, or a promotion, a raise and so on in the IT career. The dream of PDFDumps is to help you achieve SC-200 exam certification. After you purchase our SC-200 Exam Dumps training materials, we will provide one year free renewal service. If you fail SC-200 certification exam, we can guarantee you that we will give you a full refund.

Microsoft SC-200 certification exam is designed for security operations analysts who want to validate their skills in protecting an organization's assets, detecting and responding to security incidents, and implementing security controls. SC-200 exam is part of the Microsoft Certified: Security Operations Analyst Associate certification, which also includes the SC-900 Fundamentals exam. The SC-200 exam measures your ability to use Microsoft security technologies to identify and respond to security threats.

The SC-200 Exam consists of about 40-60 multiple-choice questions that must be completed within 150 minutes. SC-200 exam is available in English, Japanese, Korean, and Simplified Chinese. Candidates who pass the exam earn the Microsoft Security Operations Analyst certification, which is valid for two years. To maintain their certification, candidates must pass a renewal exam or complete certain continuing education requirements.

Microsoft Security Operations Analyst Sample Questions (Q177-Q182):

NEW QUESTION # 177
You have an Azure subscription that contains a guest user named User1 and a Microsoft Sentinel workspace named workspace1.
You need to ensure that User1 can triage Microsoft Sentinel incidents in workspace1. The solution must use the principle of least privilege.
Which roles should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:
In Microsoft Sentinel, incident management and investigation permissions are controlled through Sentinel- specific Azure roles . To allow a user (including a guest user) to triage incidents - meaning they can view, assign, and update incident statuses , but not modify analytics rules or automation logic - the correct Azure role is Microsoft Sentinel Res ponder .
Here's the breakdown:
1# # Azure role # Microsoft Sentinel Responder
* The Sentinel Responder role grants permissions to view incidents, update incident status, assign incidents, and run playbooks on incidents.
* It follows the principle of least privilege by limiting access to only incident response and not allowing rule creation, workbook management, or data connector configuration.
* The Sentinel Contributor role, on the other hand, provides broader permissions (including modifying analytic rules) , which exceeds the requirement of "triaging incidents."
* Therefore, Microsoft Sentinel Responder is the correct and least-privilege Azure role.
2# # Azure AD role # Directory readers
* To investigate and triage incidents effectively, Sentinel users must be ab le to resolve user identities (such as usernames, group membership, and object IDs) within Microsoft Entra ID (Azure AD).
* The Directory Readers role provides read-only access to directory data, allowing the user to view identities but not modify them.
* This minimal permission satisfies Sentinel's identity lookup needs without elevating the user to a global administrative or global reader role.
# Final Answers:
* Azure role: Microsoft Sentinel Responder
* Azure AD role: Directory readers

NEW QUESTION # 178
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep- dive

NEW QUESTION # 179
You have a Microsoft 365 subscription. The subscription contains 500 Windows 11 devices that are onboarded to Microsoft Defender for Endpoint.
You need to perform the following actions in Microsoft Defender XDR:
* For your company's finance department, populate random endpoints with fake cached credentials.
* Ensure That an incident is created in Microsoft Defender XDR if an attacker attempts to use the fake cached credentials.
The solution must ensure that the fake cached credentials are planted only on endpoints of the finance department.
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.
NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Answer:

Explanation:
Explanation:

NEW QUESTION # 180
You need to deploy the native cloud connector to Account! to meet the Microsoft Defender for Cloud requirements. What should you do in Account! first?

- A. Deploy the AWS Systems Manager (SSM) agent
- B. Create an AWS user for Defender for Cloud.
- C. Create an Access control (1AM) role for Defender for Cloud.
- D. Configure AWS Security Hub.

Answer: B

NEW QUESTION # 181
Hotspot Question
You have the resources shown in the following table.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect VM1 and Server1. The solution must meet the following requirements:
- Support Advanced Threat Protection and vulnerability assessment.
- Register each SQL Server 2022 instance as a SQL virtual machine.
- Minimize implementation and administrative effort.
What should you deploy to each server? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Explanation:

Explanation:
Box 1: The Azure Connected Machine agent and an Azure virtual machine extension.
Microsoft Defender for Cloud, Enable Microsoft Defender for SQL servers on machines Set up Microsoft Defender for SQL servers on machines The Defender for SQL server on machines plan requires Azure Monitoring Agent (AMA) to prevent attacks and detect misconfigurations.
Note: The Azure Connected Machine agent (Azure Arc agent) connects your non-Azure machine to Azure for management and governance, while the Azure Monitor agent (AMA) collects performance data, logs, and metrics from the machine. The Connected Machine agent is a prerequisite, acting as a bridge to Azure, and it enables you to install the AMA as an extension to send monitoring data to Azure Monitor.
Box 2: The Azure Connected Machine agent and an Azure virtual machine extension.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-usage
https://learn.microsoft.com/en-us/sql/sql-server/azure-arc/overview

NEW QUESTION # 182
.....