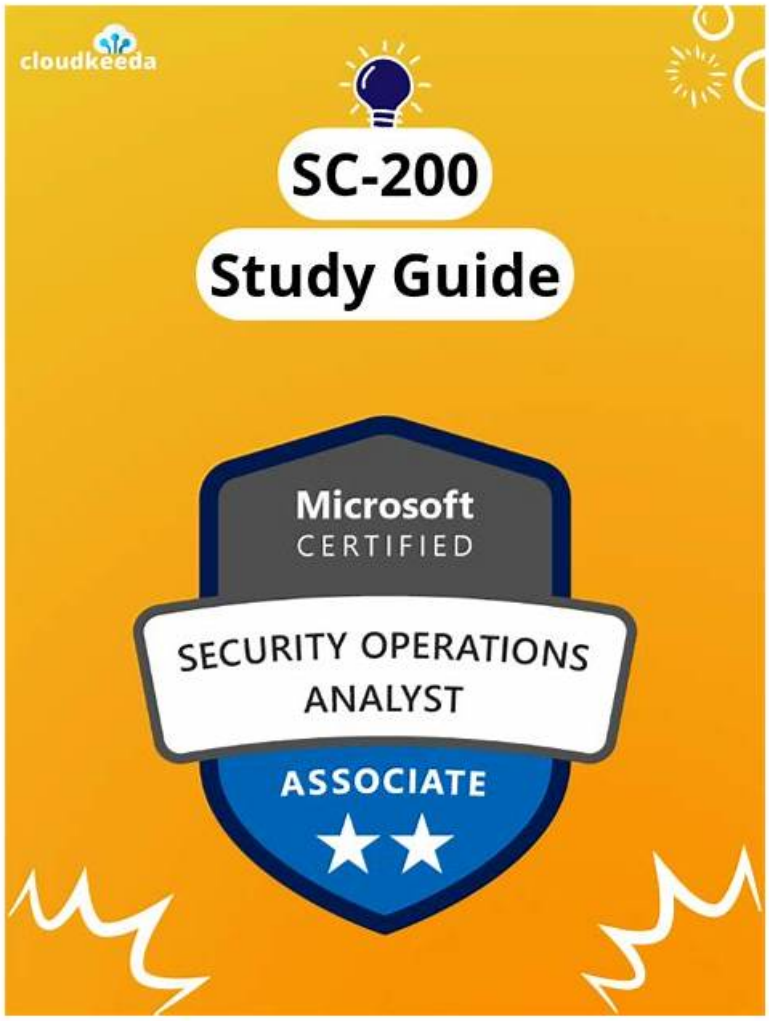
Well-Prepared New SC-200 Test Guide Spend Your Little Time and Energy to Pass SC-200 exam casually



DOWNLOAD the newest TestInsides SC-200 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1L9AGGEpfNRCm6sVfkdrmY3K8oaH2a2bq

Now they have become certified Microsoft Security Operations Analyst Certification Exam experts and pursue a rewarding career in the top world brands. You can also trust top-notch and easy-to-use Microsoft SC-200 practice test questions. The Microsoft Security Operations Analyst (SC-200) exam questions are checked and verified by experienced and qualified Microsoft Security Operations Analyst (SC-200) exam trainers. They have years of experience and knowledge to collect, design, and answer the real Microsoft Security Operations Analyst (SC-200) exam questions.

Microsoft Security Operations Analyst certification is recognized globally and is highly valued by employers. Microsoft Security Operations Analyst certification is proof of an individual's expertise in security operations and incident response. It is an excellent way for security professionals to demonstrate their skills and knowledge and to differentiate themselves from other candidates in the job market. Microsoft Security Operations Analyst certification is also an excellent way for organizations to ensure that their security professionals have the necessary skills and knowledge to protect their networks and systems from security threats.

>> New SC-200 Test Guide <<

Test SC-200 Pattern - Latest SC-200 Dumps Book

Maybe you have desired the SC-200 certification for a long time but don't have time or good methods to study. Maybe you always thought study was too boring for you. Our SC-200 study materials will change your mind. With our products, you will soon feel the

happiness of study. Thanks to our diligent experts, wonderful study tools are invented for you to pass the SC-200 Exam. You can try the demos first and find that you just can't stop studying. Using our SC-200 study materials, you will just want to challenge yourself and get to know more.

A Comprehensive Guide on How to Pass the Microsoft SC-200 Exam

Get Microsoft SC-200 certification successfully Using this Prep Material

Get Your Microsoft SC-200 Certified With Ease: a study guide around the top resources for studying and passing the Microsoft certification exam

Microsoft Platform and Infrastructure Security is a suite of products designed to enable IT to manage, secure, and protect the business information that drives top-line revenue growth and bottom-line profitability. Microsoft Platform and Infrastructure Security allow organizations to integrate security, reduce costs, improve productivity, and simplify IT management. If you are a job-seeker or an employee who is aiming to get Microsoft Platform and Infrastructure Security certification, then this article will help you a lot. It will provide you with basic information about the Microsoft Platform and Infrastructure Security certification exam (Microsoft SC-200). **SC-200 Dumps** is the most trusted and reliable source for getting Microsoft SC-200 Certified.

If you work in the IT field, chances are you are a Microsoft fan. If you are looking to move up your career ladder, earning a security compliance certification is an important step forward.

Microsoft SC-200 (Microsoft Security Operations Analyst) Certification Exam is designed to test the knowledge and skills of security professionals in performing threat protection, incident response, and other security operations tasks using Microsoft security technologies. Microsoft Security Operations Analyst certification exam is intended for those who have expertise in security operations and experience working with Microsoft Azure Sentinel, Microsoft Defender for Endpoint, Microsoft Defender for Identity, and Microsoft Cloud App Security.

Microsoft Security Operations Analyst Sample Questions (Q37-Q42):

NEW QUESTION # 37
You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.
You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.
How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Answer:

Explanation:
Explanation:

NEW QUESTION # 38
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)
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:
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-acc
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/15

NEW QUESTION # 39
You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment.
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:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

NEW QUESTION # 40
You have an Azure subscription that use Microsoft Defender for Cloud and contains a user named User1.
You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.
Which role should you assign to User1?

- A. Contributor
- B. Security Admin
- C. Owner
- D. Security operator

Answer: B

Explanation:
In Microsoft Defender for Cloud's role-based access model, specific Azure built-in roles define what users can view and configure:
* Security Reader: View-only access to Defender for Cloud recommendations and alerts.
* Security Operator: Can view and dismiss alerts but cannot modify security policies.
* Security Admin: Can view everything a reader can and additionally edit security policies, manage recommendations, and configure settings across Defender for Cloud.
* Owner/Contributor: Have broader Azure resource management rights, exceeding what's required to manage Defender for Cloud policies-violating the principle of least privilege.
The principle of least privilege dictates assigning the narrowest role that allows performing the required tasks.
In this case, the Security Admin role is explicitly documented by Microsoft as granting permission to modify security policies and settings in Defender for Cloud, without granting full subscription ownership rights.
Therefore, to allow User1 to modify Defender for Cloud security policies while maintaining least privilege:
Assign the Security Admin role.

NEW QUESTION # 41
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

- A. Add a data connector to Azure Sentinel.
- B. Modify the trigger in the logic app.
- C. And a new scheduled query rule.
- D. Configure a custom Threat Intelligence connector in Azure Sentinel.

Answer: B

Explanation:
In Microsoft Sentinel, playbooks are Azure Logic Apps that automate responses to alerts or incidents. To use an existing Logic App as a playbook in Sentinel, it must start with the "Microsoft Sentinel alert" trigger.
This trigger allows Sentinel to call and pass alert details to the Logic App automatically.
When an existing Logic App has a manual trigger, it cannot be invoked directly by Sentinel. Therefore, the first step is to modify the trigger to replace the manual trigger with the "When a response to an Azure Sentinel alert is triggered" trigger. After that, you can link it within Sentinel incidents or automation rules.
This process is detailed in Microsoft Defender XDR and Sentinel documentation under "Connect a Logic App to Sentinel as a

playbook." Hence, the correct answer is D. Modify the trigger in the logic app.

NEW QUESTION # 42

.....