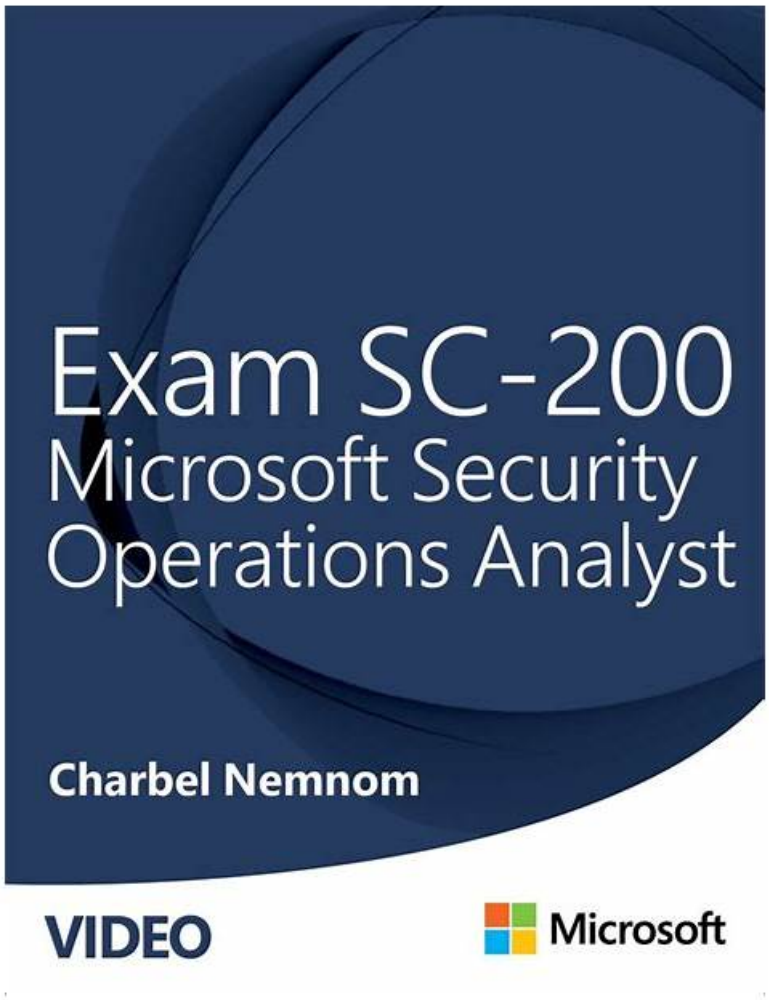
Pass Guaranteed Quiz Microsoft - Fantastic SC-200 - Test Microsoft Security Operations Analyst Book



P.S. Free & New SC-200 dumps are available on Google Drive shared by itPass4sure: https://drive.google.com/open?id=1lU9oREgWv2nPUq7bH4v3KBL5CHbMSTlr

We make sure that the Microsoft SC-200 exam questions prices are affordable for everyone. All three itPass4sure SC-200 exam practice test questions formats are being offered at the lowest price. Just get benefits from this cheap Microsoft Security Operations Analyst SC-200 Exam Questions price and download it right now.

You can acquire a sense of the SC-200 software by downloading a free trial version before deciding whether to buy it. This Microsoft SC-200 practice exam software lets you identify your strengths and shortcomings, allowing you to concentrate on those aspects of your Microsoft Security Operations Analyst (SC-200) test preparation that could use some work.

>> Test SC-200 Book <<

SC-200 – 100% Free Test Book | Trustable Microsoft Security Operations Analyst Exams Dumps

By Finishing the Microsoft Security Operations Analyst exam, you will save your work and even change to another better door way. By and by, it is not difficult to do Microsoft SC-200 dumps as you would confront two or three inconveniences during the trip. By utilizing Microsoft SC-200 Dumps, it is especially simple to appear at your goal. We can equip you with explicit tips that could show you the fundamental method for doing battling the difficulties and draw a definite guide toward your objective for the Microsoft Security Operations Analyst exam.

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.

The SC-200 Exam is intended for security analysts and security operations professionals who are responsible for monitoring, detecting, and responding to security threats. SC-200 exam is also suitable for IT professionals who wish to expand their knowledge of security operations and threat management.

Microsoft Security Operations Analyst Sample Questions (Q73-Q78):

NEW QUESTION # 73
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

- A. the Cloud Discovery settings in Cloud App Security
- B. the Onboarding settings from Device management in Microsoft Defender Security Center
- C. Cloud App Security anomaly detection policies
- D. Advanced features from Settings in Microsoft Defender Security Center

Answer: A,D

Explanation:
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern
Topic 3, Adatum Corporation
Overview
Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.
The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group! that syncs with adatum.com.
All the users at Adatum are assigned a Microsoft 365 E5 license and an Azure Active Directory Perineum 92 license.
The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant, and the resources shown in the following table.

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

The on-premises network contains the resources shown in the following table.

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

Adatum plans to perform the following changes;
* Implement a query named rulequery1 that will include the following KQL query.

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

* Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.
Adatum identifies the following Microsoft Defender for Cloud requirements:
* The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
* Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
* Server2 must be excluded from agentless scanning.
Adatum identifies the following Microsoft Sentinel requirements:
* Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
* Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
* Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
* Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company's SecOps team.
* Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
* Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account
* Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
* Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
* Minimize the overhead associated with queries that use ASIM parsers.
* Ensure that the Group1 members can create and edit playbooks.
* Use built-in ASIM parsers whenever possible.
Adatum identifies the following business requirements:
* Follow the principle of least privilege whenever possible.
* Minimize administrative effort whenever possible.
Directory Perineum 92 license.

NEW QUESTION # 74
You need to complete the query for failed sign-ins to meet the technical requirements.
Where can you find the column name to complete the where clause?

- A. Activity log in Azure
- B. the query windows of the Log Analytics workspace

- C. Security alerts in Azure Security Center
- D. Azure Advisor

Answer: B

Explanation:
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.

NEW QUESTION # 75
You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

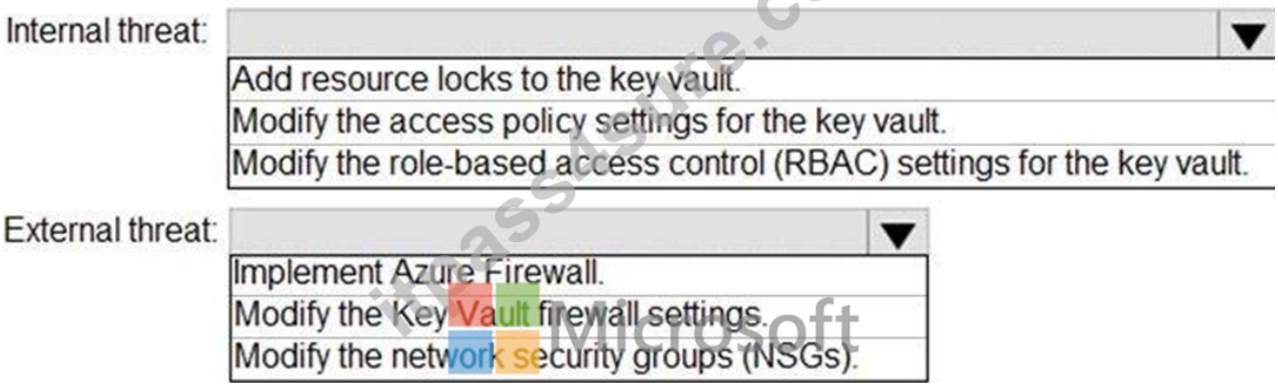
- A. at the subscription level
- B. at the resource level
- C. at the workspace level

Answer: A

Explanation:
Section: [none]
Explanation/Reference:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

NEW QUESTION # 76
HOTSPOT for the Azure virtual
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

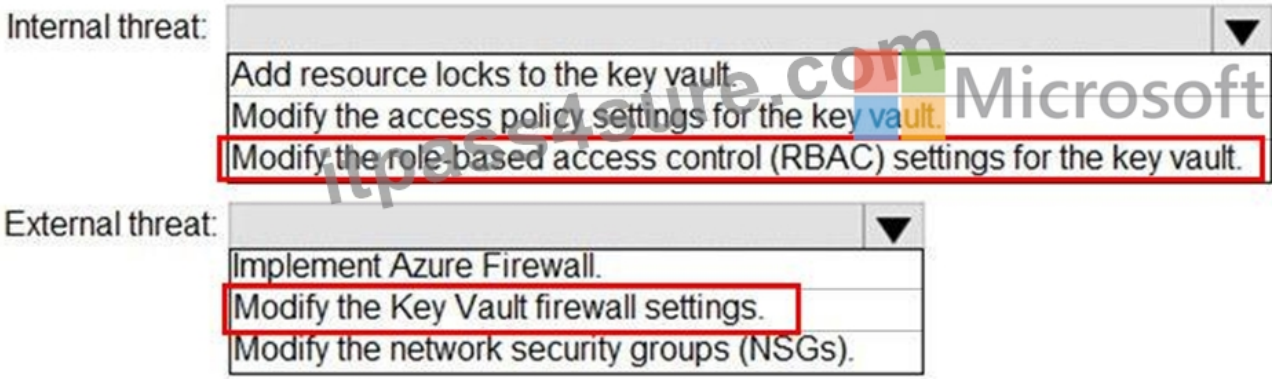
Answer Area



Answer:

Explanation:

Answer Area



Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

NEW QUESTION # 77
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

- A. sales
- B. marketing
- C. executive

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft- defender-atp-ios
Topic 1, Contoso Ltd
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
A company named Contoso Ltd. has a main office and five branch offices located throughout North America.
The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.
Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.
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 # 78
.....