

Professional Microsoft - SC-200 - Microsoft Security Operations Analyst Associate Level Exam

Microsoft Azure Certification Details

SC-200: Microsoft Security Operations Analyst

Prior Certification Not Required	Exam Validity 1 Years	Exam Fee \$165 USD
Exam Duration 110 minutes	No. of Questions 40-60 questions	Passing Marks 700
Recommended Experience Familiar with attack vectors, cyberthreats, incident management, Kusto Query Language (KQL), Microsoft 365 and Azure services (including Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender)		Exam Format Multiple Choice, Yes/No, Drag & Drop, Case Studies, and Multiple Response
Languages English, Japanese, Chinese (Simplified), Korean, French, German, Spanish, Portuguese (Brazil), Chinese (Traditional), Italian		

BONUS!!! Download part of Exams-boost SC-200 dumps for free: <https://drive.google.com/open?id=1L4WNcnOrfmhp7ocIwFj7KbfaiRUoMxE>

The rapid development of information will not infringe on the learning value of our SC-200 study materials, because our customers will have the privilege to enjoy the free update for one year. You will receive the renewal of SC-200 study materials through the email. And our SC-200 study materials have three different version can meet your demands. Firstly, PDF version is easy to read and print. Secondly software version does not limit to the number of installed computers, and it simulates the Real SC-200 Exam environment, but it can only run on Windows operating system.

Our SC-200 study braindumps for the overwhelming majority of users provide a powerful platform for the users to share. Here, the all users of the SC-200 exam questions can through own ID number to log on to the platform and other users to share and exchange, each other to solve their difficulties in study or life. The SC-200 Prep Guide provides user with not only a learning environment, but also create a learning atmosphere like home. And our SC-200 exam questions will help you obtain the certification for sure.

>> SC-200 Associate Level Exam <<

Valid Exam SC-200 Book, Latest SC-200 Exam Price

When you follow with our SC-200 exam questions to prepare for your coming exam, you will deeply touched by the high-quality and high-efficiency. Carefully devised by the professionals who have an extensive research of the SC-200 exam and its requirements, our SC-200 study braindumps are a real feast for all the candidates. And if you want to have an experience with our SC-200 learning guide, you can free download the demos on our website.

Microsoft SC-200 Exam is ideal for individuals who want to advance their careers in the cybersecurity industry. Microsoft Security Operations Analyst certification is intended for security analysts, security administrators, and other IT professionals who are responsible for monitoring, analyzing, and responding to security incidents. Additionally, the exam is suitable for individuals who want to demonstrate their expertise in Microsoft security technologies.

Microsoft Security Operations Analyst Sample Questions (Q218-Q223):

NEW QUESTION # 218

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Enable Azure Defender for the subscription.	
Change the alert severity threshold for emails to Low .	
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

Answer:

Explanation:

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	Enable Azure Defender for the subscription.
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Enable Azure Defender for the subscription.	Run the executable file and specify the appropriate arguments.
Change the alert severity threshold for emails to Low .	
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

Explanation

Actions	Answer Area
Change the alert severity threshold for emails to Medium .	Enable Azure Defender for the subscription.
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Enable Azure Defender for the subscription.	Run the executable file and specify the appropriate arguments.
Change the alert severity threshold for emails to Low .	
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation>

NEW QUESTION # 219

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?

- A. Monitor and Enable redirect
- B. Block and Enable redirect
- C. **Dynamic Delivery**
- D. Replace

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-world>

NEW QUESTION # 220

You need to implement Microsoft Sentinel queries for Contoso and Fabrikam to meet the technical requirements. What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

Answer:

Explanation:

Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

Explanation:

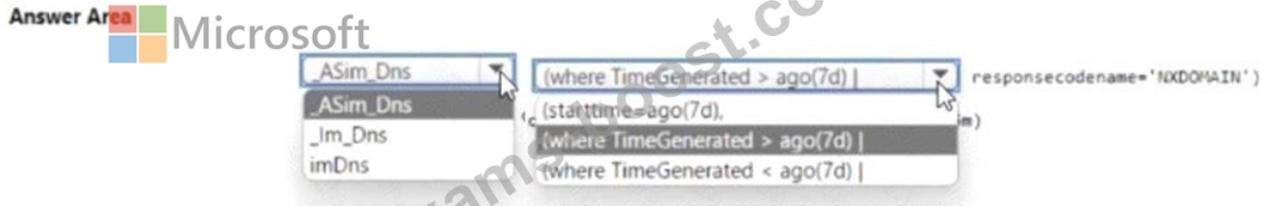
Answer Area

Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam: 1

Query element required to correlate data between tenants: workspace

NEW QUESTION # 221

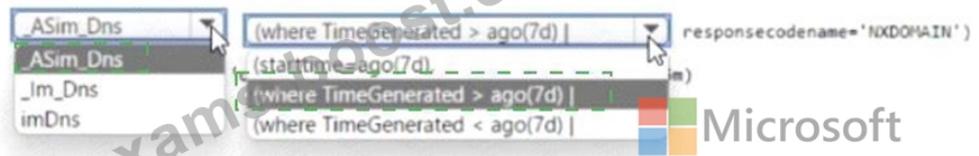
You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements. How should you complete the Query? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.



Answer:

Explanation:

Answer Area



Explanation

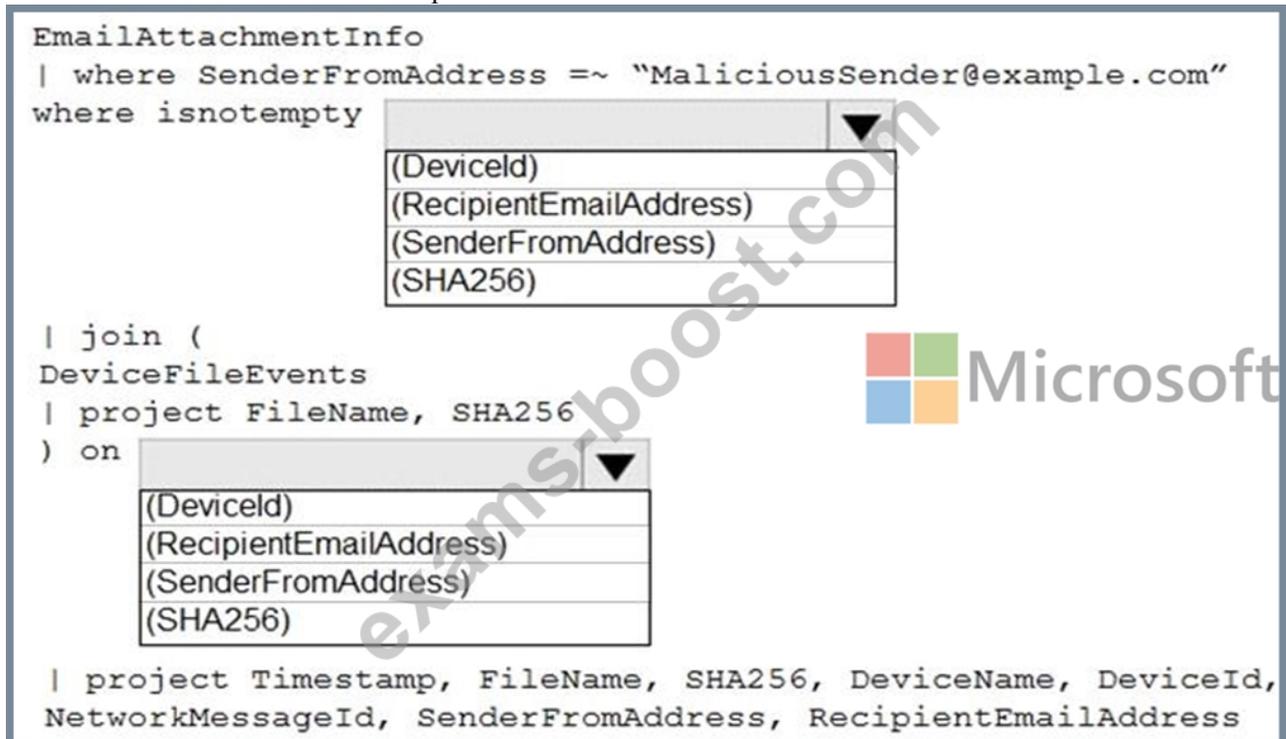


NEW QUESTION # 222

You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel. You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

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:

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```



Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide>

NEW QUESTION # 223

.....

Most of the candidates remain confused about the format of the actual SC-200 exam and the nature of questions therein. So our SC-200 exam questions can perfectly provide them with the newest information about the exam not only on the content but also on the format. And to help them adjust to the real exam, we also developed the Software version of the SC-200 learning prep which can simulate the real exam.

Valid Exam SC-200 Book: <https://www.exams-boost.com/SC-200-valid-materials.html>

- Latest SC-200 Exam Online Valid Test SC-200 Vce Free SC-200 Updated Testkings Open website www.prepawaypdf.com and search for 《 SC-200 》 for free download SC-200 Online Exam
- High-quality SC-200 Associate Level Exam - Leading Provider in Qualification Exams - Authorized Valid Exam SC-200 Book Search on www.pdfvce.com for 《 SC-200 》 to obtain exam materials for free download SC-200 Latest Test Sample
- SC-200 Exam Blueprint Valid SC-200 Test Preparation SC-200 Exam Blueprint Go to website www.troytecdumps.com open and search for ▶ SC-200 ◀ to download for free SC-200 Latest Test Sample
- Pass Guaranteed Microsoft - The Best SC-200 Associate Level Exam Enter www.pdfvce.com and search for [SC-200] to download for free SC-200 Current Exam Content
- Free Microsoft Security Operations Analyst Testking Torrent - SC-200 Valid Pdf - Microsoft Security Operations Analyst Prep Training Search for SC-200 and download exam materials for free through www.dumpsmaterials.com Valid SC-200 Test Preparation
- Trustworthy SC-200 Dumps Latest SC-200 Exam Online SC-200 Online Exam Simply search for “SC-200 ” for free download on www.pdfvce.com Valid Test SC-200 Tips
- SC-200 test dump, SC-200 pass exam Enter www.testkingpass.com and search for SC-200 to download for free SC-200 Updated Testkings
- High-quality SC-200 Associate Level Exam - Leading Provider in Qualification Exams - Authorized Valid Exam SC-200 Book Go to website { www.pdfvce.com } open and search for > SC-200 < to download for free Valid Test SC-200 Vce Free
- Microsoft SC-200 Questions - Reduce your Chances of Failure in Exam Search on www.verifiedumps.com for 《 SC-200 》 to obtain exam materials for free download SC-200 Latest Braindumps
- Well-Prepared SC-200 Associate Level Exam - Professional Valid Exam SC-200 Book - Excellent Latest SC-200 Exam

Price ☐ Go to website 《 www.pdfvce.com 》 open and search for ☐ SC-200 ☐ to download for free ☐SC-200 Reliable Exam Pass4sure

- Trustworthy SC-200 Dumps ☐ Valid Dumps SC-200 Free ☐ SC-200 Latest Test Camp ☐ Download { SC-200 } for free by simply entering 【 www.torrentvce.com 】 website ☐SC-200 Practice Exam Online
- www.stes.tyc.edu.tw, english.onlineeducoach.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, lviyo.com, kumu.io, 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, 40bbk.com, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that Exams-boost SC-200 dumps now are free: <https://drive.google.com/open?id=1L4WNCnOrfnhp7oclWfj7KbfaiRUoMxE>