

Valid Microsoft SC-200 Questions - Pass Exam And Advance Your Career



BONUS!!! Download part of Easy4Engine SC-200 dumps for free: <https://drive.google.com/open?id=1jFvbkg3m5wZNk-ZXaMEVq7mQ-QYZH2>

Why is Easy4Engine Microsoft SC-200 certification training so popular, especially among the same trade? Firstly, we really know what the candidates need. Secondly, Our Easy4Engine Microsoft SC-200 dumps are concerned on one thing only – how to help the candidates to pass Microsoft SC-200 test. Thirdly, Our Easy4Engine Microsoft SC-200 study guide is very technical and original. We provide you with the latest test questions and test answers. And the price is very cost-effective.

Microsoft SC-200 Certification Exam is an excellent credential for security professionals who are interested in validating their security operations skills. By passing the exam, you will demonstrate your ability to identify and mitigate security threats, analyze security data, and respond to security incidents. Microsoft Security Operations Analyst certification is a valuable credential that can help you advance your career and demonstrate your commitment to staying current with the latest security best practices and methodologies.

Microsoft SC-200, also known as the Microsoft Security Operations Analyst certification exam, is designed for security professionals who want to validate their skills and knowledge in implementing and managing security controls, threat and vulnerability management, incident response, and compliance frameworks in Microsoft technologies. Microsoft Security Operations Analyst certification exam is ideal for individuals who are responsible for monitoring, detecting, and responding to security incidents in Microsoft environments such as Azure, Microsoft 365, and Windows 10.

>> SC-200 Study Dumps <<

Quiz SC-200 - Microsoft Security Operations Analyst –The Best Study Dumps

SC-200 certification exam questions have very high quality services in addition to their high quality and efficiency. If you use SC-200 test prep, you will have a very enjoyable experience while improving your ability. We have always advocated customer first. If you use our SC-200 Learning Materials to achieve your goals, we will be honored. And our SC-200 pdf files give you more efficient learning efficiency and allows you to achieve the best results in a limited time. Our SC-200 pdf files are the best exam tool that you have to choose.

Microsoft Security Operations Analyst Sample Questions (Q79-Q84):

NEW QUESTION # 79


You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application. You need to hide Azure Defender alerts for the storage account. Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line



Answer:


Explanation:

Entity type:

IP address
Azure Resource
Host
User account

Field:

Name
Resource Id
Address
Command line



Reference:

<https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920>

NEW QUESTION # 80

Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.

Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.

You deploy Azure Sentinel to a new Azure subscription.

You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a query that uses the workspace expression and the union operator.

- B. Use the alias statement.
- C. Add the Azure Sentinel solution to each workspace.
- D. Add the Security Events connector to the Azure Sentinel workspace.
- E. Create a query that uses the resource expression and the alias operator.

Answer: A,C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>

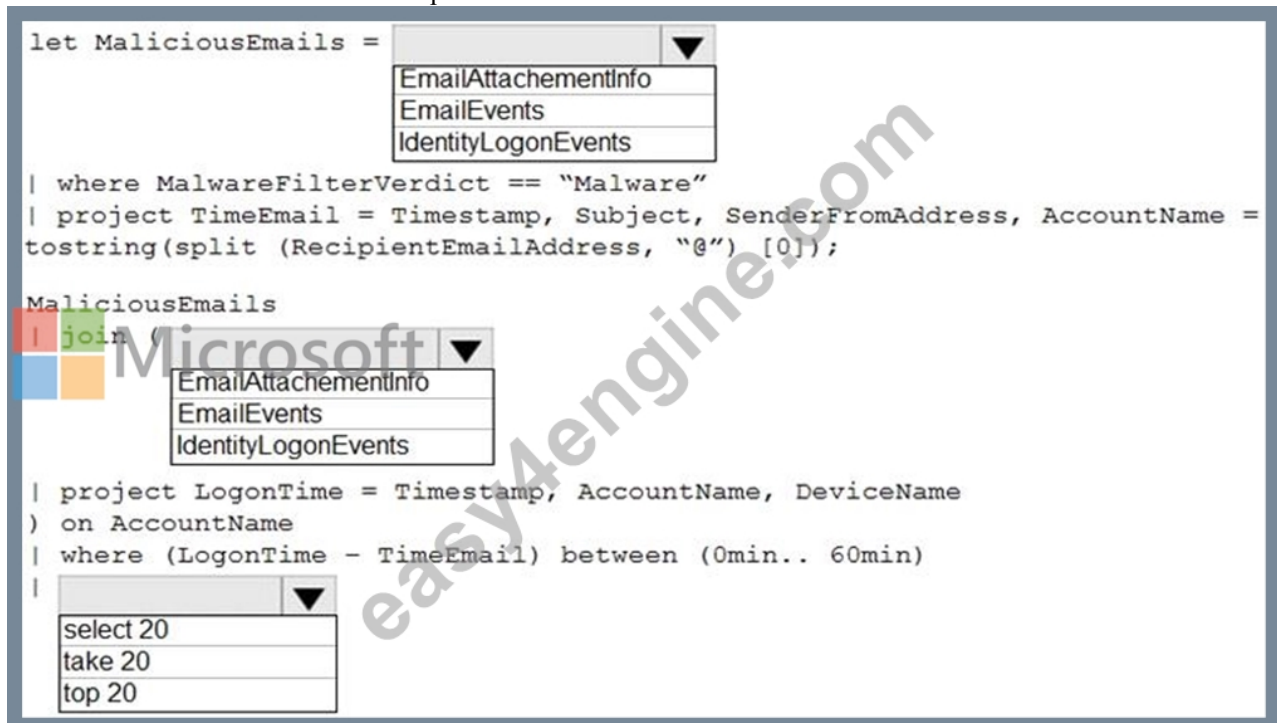
NEW QUESTION # 81

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



```

let MaliciousEmails =
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
select 20
take 20
top 20

```

Answer:

Explanation:

```

let MaliciousEmails =
    EmailAttachmentsInfo
    EmailEvents
    IdentityLogonEvents


where MalwareFilterVerdict == "Malware"
project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
    ostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
join (
    EmailAttachmentsInfo
    EmailEvents
    IdentityLogonEvents

project LogonTime = Timestamp, AccountName, DeviceName
on AccountName
where (LogonTime - TimeEmail) between (0min.. 60min)

select 20
take 20
top 20

```



Reference:

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

NEW QUESTION # 82


You have a Microsoft Sentinel workspace that contains a custom workbook.

You need to query the number of daily security alerts. The solution must meet the following requirements:

- * Identify alerts that occurred during the last 30 days.
- * Display the results in a timechart.

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 Area



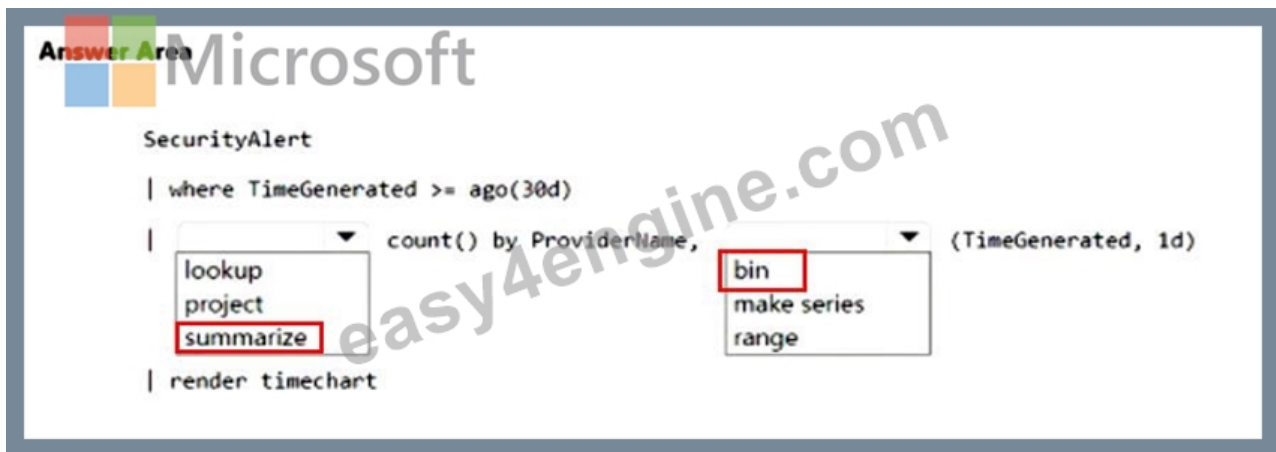
```

SecurityAlert
| where TimeGenerated >= ago(30d)
| count() by ProviderName,
lookup
project
summarize
| render timechart
bin
make series
range
(TimeGenerated, 1d)

```

Answer:

Explanation:



NEW QUESTION # 83

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

In the Cloud App Security portal:	<input type="text"/> Add a security extension Configure app connectors Configure log collectors
From Azure Sentinel in the Azure portal:	<input type="text"/> Add a data connector Add a workbook Configure the Logs settings

Answer:

Explanation:

In the Cloud App Security portal:



From Azure Sentinel in the Azure portal:

<input type="text"/> Add a security extension Configure app connectors Configure log collectors
<input type="text"/> Add a data connector Add a workbook Configure the Logs settings

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel>

NEW QUESTION # 84

.....

It is our consistent aim to serve our customers wholeheartedly. Our SC-200 real exam try to ensure that every customer is satisfied, which can be embodied in the convenient and quick refund process. Although the passing rate of our SC-200 training quiz is close to 100%, if you are still worried, we can give you another guarantee: if you don't pass the exam, you can get a full refund. So there is nothing to worry about, just buy our SC-200 exam questions.

Exam SC-200 Torrent: <https://www.easy4engine.com/SC-200-test-engine.html>

- Reliable SC-200 Exam Prep ☐ Valid Test SC-200 Experience ☐ Valid SC-200 Exam Simulator ☐ Search for ☀ SC-200 ☐ ☀ on "www.dumps4pdf.com" immediately to obtain a free download ☐ Free SC-200 Download
- Microsoft SC-200 Study Dumps - Pass SC-200 in One Time - Microsoft Exam SC-200 Torrent ☐ Copy URL ☐

[illegible]

2025 Latest Easy4Engine SC-200 PDF Dumps and SC-200 Exam Engine Free Share: <https://drive.google.com/open?id=1jFvbkg3m5wZNk-ZXaMEhVq7mQ-QYZH2>