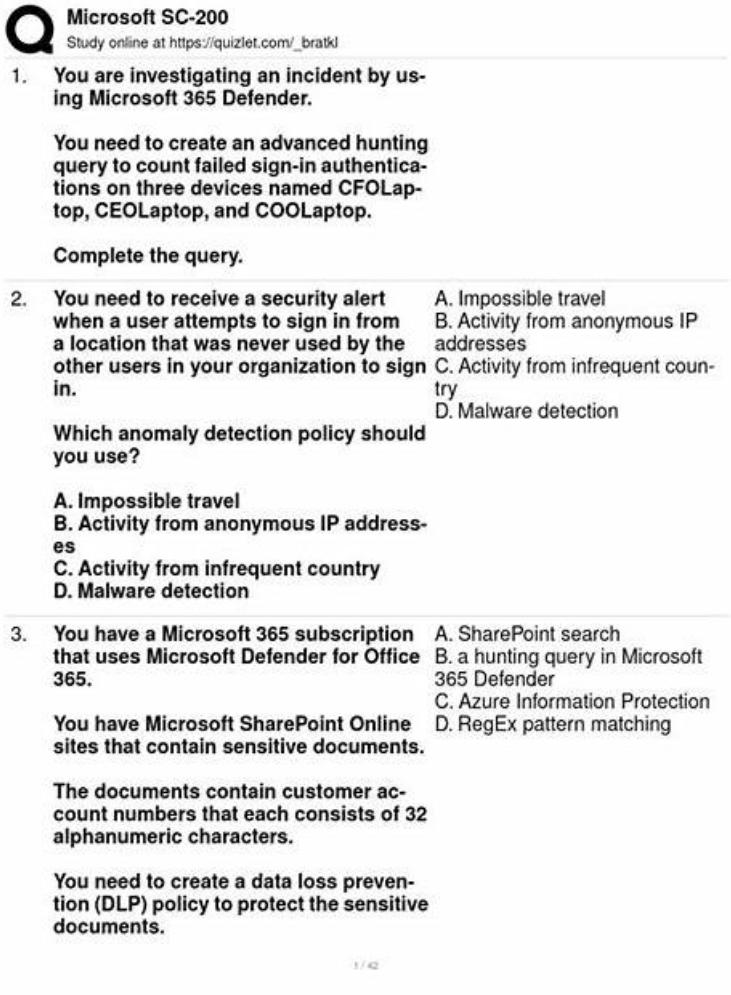
Valid Microsoft SC-200 Exam Question, Valid SC-200 Study Notes



Microsoft SC-200
Study online at https://quizlet.com/_bratkl

1. **You are investigating an incident by using Microsoft 365 Defender.**

   You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

   Complete the query.

2. **You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.**

   Which anomaly detection policy should you use?

   A. Impossible travel
   B. Activity from anonymous IP addresses
   C. Activity from infrequent country
   D. Malware detection

   A. Impossible travel
   B. Activity from anonymous IP addresses
   C. Activity from infrequent country
   D. Malware detection

3. **You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.**

   You have Microsoft SharePoint Online sites that contain sensitive documents.

   The documents contain customer account numbers that each consists of 32 alphanumeric characters.

   You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

   A. SharePoint search
   B. a hunting query in Microsoft 365 Defender
   C. Azure Information Protection
   D. RegEx pattern matching

What's more, part of that Pass4SureQuiz SC-200 dumps now are free: https://drive.google.com/open?id=1-cFHcuxs8BN6gvhHp2PX45gFZZRXlHv5

One of the biggest highlights of the Microsoft Security Operations Analyst prep torrent is the availability of three versions: PDF, app/online, and software/pc, each with its own advantages: The PDF version of SC-200 Exam Torrent has a free demo available for download. You can print exam materials out and read it just like you read a paper. The online version of SC-200 test guide is based on web browser usage design and can be used by any browser device. At the same time, the first time it is opened on the Internet, it can be used offline next time. You can practice anytime, anywhere. The Microsoft Security Operations Analyst software supports the MS operating system and can simulate the real test environment. The contents of the three versions are the same. Each of them neither limits the number of devices used or the number of users at the same time. You can choose according to your needs.

If you don't progress and surpass yourself, you will lose many opportunities to realize your life value. Our SC-200 study training materials goal is to help users to challenge the impossible, to break the bottleneck of their own. A lot of people can't do a thing because they don't have the ability, the fact is, they don't understand the meaning of persistence, and soon give up. Our SC-200 Latest Questions will help make you a persistent person. Change needs determination, so choose our SC-200 training braindump quickly! Our SC-200 exam questions can help you pass the SC-200 exam without difficulty.

>> Valid Microsoft SC-200 Exam Question <<

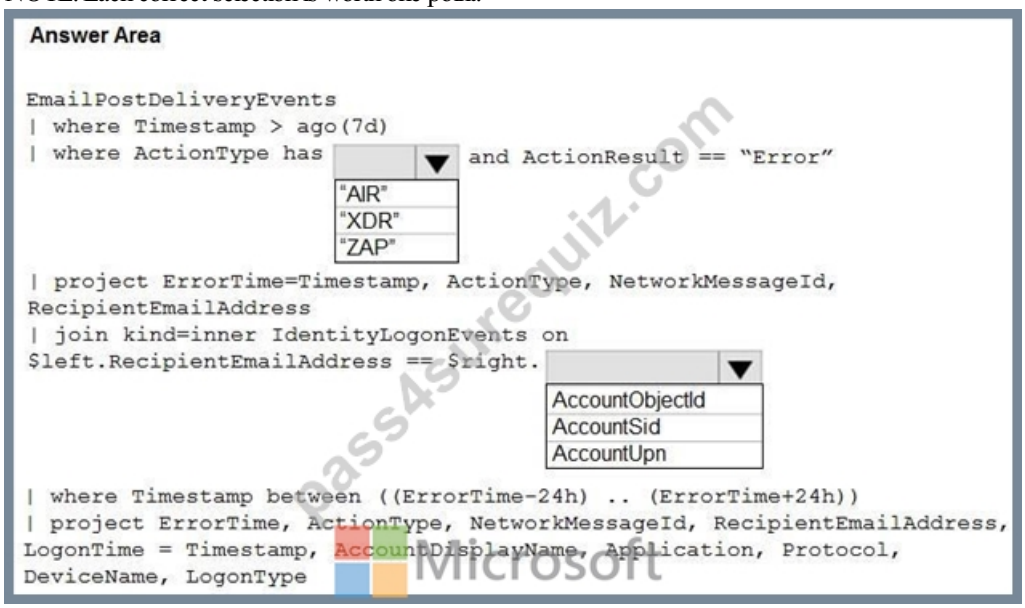
Free PDF Reliable Microsoft - SC-200 - Valid Microsoft Security Operations Analyst Exam Question

We have strong technical and research capabilities on this career for the reason that we have a professional and specialized expert team devoting themselves on the compiling the latest and most precise SC-200 exam materials. All questions and answers of SC-200 learning guide are tested by professionals who have passed the SC-200 Exam. All the experts we hired have been engaged in professional qualification exams for many years. The hit rate for SC-200 exam torrent is as high as 99%. You will pass the SC-200 exam for sure with our SC-200 exam questions.

Microsoft SC-200 Exam is a great way to demonstrate your expertise in security operations analysis and become a certified Microsoft Security Operations Analyst. By passing the exam, you will be able to demonstrate your knowledge of various security tools and technologies, as well as your ability to analyze and respond to threats. Microsoft Security Operations Analyst certification will help you stand out in the cybersecurity industry and advance your career.

Microsoft Security Operations Analyst Sample Questions (Q206-Q211):

NEW QUESTION # 206
Hotspot Question
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365.
You need to build a hunting query that will list events involving potentially malicious emails that were detected but NOT removed successfully from mailboxes after delivery. The solution must ensure that the events are correlated with the sign-in events of the email recipients.
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

```
EmailPostDeliveryEvents
| where Timestamp > ago(7d)
| where ActionType has [ ▼ ] and ActionResult == "Error"
```

"AIR"
"XDR"
"ZAP"

```
| project ErrorTime=Timestamp, ActionType, NetworkMessageId,
RecipientEmailAddress
| join kind=inner IdentityLogonEvents on
$left.RecipientEmailAddress == $right.[ ▼ ]
```

AccountObjectId
AccountSid
AccountUpn

```
| where Timestamp between ((ErrorTime-24h) .. (ErrorTime+24h))
| project ErrorTime, ActionType, NetworkMessageId, RecipientEmailAddress
LogonTime = Timestamp, AccountDisplayName, Application, Protocol,
DeviceName, LogonType
```

NEW QUESTION # 207
You have the following KQL query.

```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

Answer:

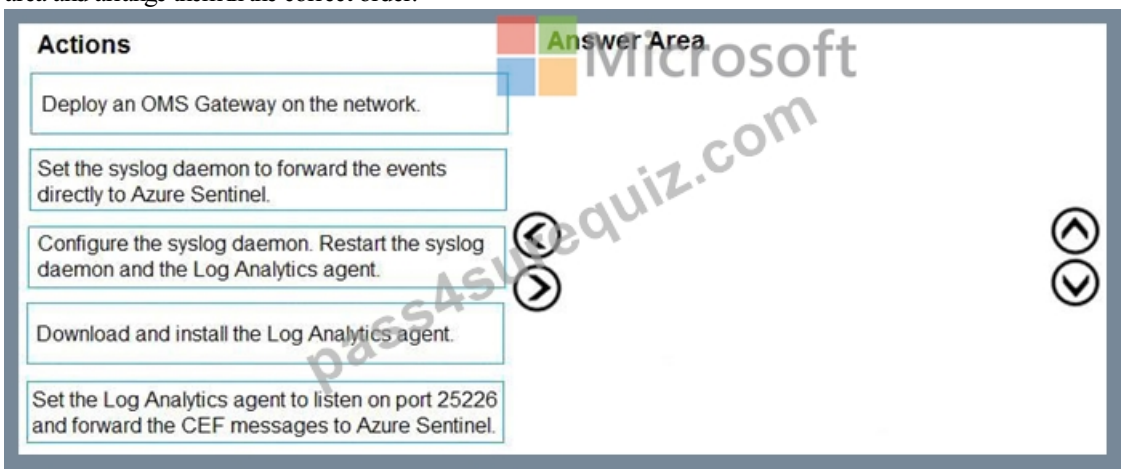
Explanation:
Explanation:

NEW QUESTION # 208
You need to configure event monitoring for Server1. The solution must meet the Microsoft Sentinel requirements.
What should you create first?

- A. a Microsoft Sentinel automation rule
- B. a Data Collection Rule (DCR)
- C. an Azure Event Grid topic
- D. a Microsoft Sentinel scheduled query rule

Answer: B

NEW QUESTION # 209
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.



Answer:

Explanation:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

NEW QUESTION # 210
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 2, Litware inc.
Overview
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
Litware Inc. is a renewable company.
Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.
Existing Environment
Identity Environment
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.
Microsoft 365 Environment
Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.
Azure Environment
Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.
Network Environment
Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.
On-premises Environment
The on-premises network contains the computers shown in the following table.
Current problems
Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.
Planned Changes
Litware plans to implement the following changes:
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.
Business Requirements
Litware identifies the following business requirements:
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection - Data discovery dashboard.
Microsoft Defender for Endpoint Requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security Requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.
Azure Defender Requirements
All servers must send logs to the same Log Analytics workspace.
Azure Sentinel Requirements
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

NEW QUESTION # 211
.....

Valid SC-200 Study Notes: https://www.pass4surequiz.com/SC-200-exam-quiz.html

- Reliable SC-200 Test Objectives SC-200 Free Updates Latest SC-200 Exam Notes Search for { SC-200 } on ➡ www.exam4labs.com immediately to obtain a free download Valid SC-200 Test Review
- Latest SC-200 Material Premium SC-200 Exam Latest SC-200 Material Easily obtain free download of " SC-200 " by searching on ▹ www.pdfvce.com ◃ SC-200 Free Sample
- Latest SC-200 Exam Online ☀ Frequent SC-200 Updates SC-200 Learning Engine Simply search for ⇛ SC-200 ⇚ for free download on 《 www.testkingpass.com 》 Valid SC-200 Exam Forum
- SC-200 Dumps Torrent Latest SC-200 Material Latest SC-200 Exam Online Go to website www.pdfvce.com open and search for SC-200 to download for free Latest SC-200 Braindumps Questions
- SC-200 Free Sample SC-200 Learning Engine SC-200 Dumps Torrent Search for ▸ SC-200 ◂ and easily obtain a free download on www.prepawaypdf.com SC-200 Test Free
- Quiz 2026 The Best SC-200: Valid Microsoft Security Operations Analyst Exam Question Open website （ www.pdfvce.com ） and search for ▸ SC-200 ◂ for free download SC-200 Learning Engine
- SC-200 actual exam dumps, Microsoft SC-200 practice test Search for （ SC-200 ） and easily obtain a free download on ⇛ www.testkingpass.com ⇚ Latest SC-200 Material
- Reliable SC-200 Test Objectives Valid SC-200 Test Review Latest SC-200 Exam Notes { www.pdfvce.com } is best website to obtain （ SC-200 ） for free download SC-200 Reliable Exam Question
- SC-200 Free Sample Latest SC-200 Exam Notes SC-200 Valid Torrent Open ➠ www.examdiscuss.com enter ➠ SC-200 and obtain a free download SC-200 Dumps Torrent
- High Pass-Rate Valid SC-200 Exam Question - Win Your Microsoft Certificate with Top Score Download " SC-200 " for free by simply entering （ www.pdfvce.com ） website SC-200 Latest Test Fee
- SC-200 Latest Test Fee Latest SC-200 Exam Notes Latest SC-200 Exam Online Search for { SC-200 } and download it for free immediately on www.troytecdumps.com SC-200 Pass4sure Study Materials
- www.flirtic.com, www.taowang.com, www.300300.net, sg588.tw, myportal.utt.edu.tt, www.maoyestudio.com, myportal.utt.edu.tt, Disposable vapes

2026 Latest Pass4SureQuiz SC-200 PDF Dumps and SC-200 Exam Engine Free Share: https://drive.google.com/open?id=1-cFHcuxs8BN6gvhHp2PX45gFZZRXlHv5