SC-200 Valid Exam Test - New SC-200 Mock Exam

SKILLCERTPRO
Microsoft (SC-200) Microsoft Security Operations Analyst
Prepare and pass your certification in first attempt

P.S. Free 2025 Microsoft SC-200 dumps are available on Google Drive shared by TrainingDumps: https://drive.google.com/open?id=1UCVN-5obSTrnnxKCbkH3YdjvOruRLZpL

In order to allow our customers to better understand our SC-200 quiz prep, we will provide clues for customers to download in order to understand our SC-200 exam torrent in advance and see if our products are suitable for you. As long as you have questions, you can send us an email and we have staff responsible for ensuring 24-hour service to help you solve your problems. If you use our SC-200 Exam Torrent, we will provide you with a comprehensive service to overcome your difficulties and effectively improve your ability. If you can take the time to learn about our SC-200 quiz prep, I believe you will be interested in our products. Our learning materials are practically tested, choosing our SC-200 exam guide, you will get unexpected surprise.

We have authoritative production team made up by thousands of experts helping you get hang of our Microsoft Security Operations Analyst study question and enjoy the high quality study experience. We will update the content of SC-200 test guide from time to time according to recent changes of examination outline and current policies, so that every examiner can be well-focused and complete the exam focus in the shortest time. Besides, our SC-200 Exam Questions can help you optimize your learning method by simplifying obscure concepts so that you can master better. One more to mention, with our SC-200 test guide, there is no doubt that you can cut down your preparing time in 20-30 hours of practice before you take the exam.

>> SC-200 Valid Exam Test <<

Quiz High Hit-Rate Microsoft - SC-200 - Microsoft Security Operations Analyst Valid Exam Test

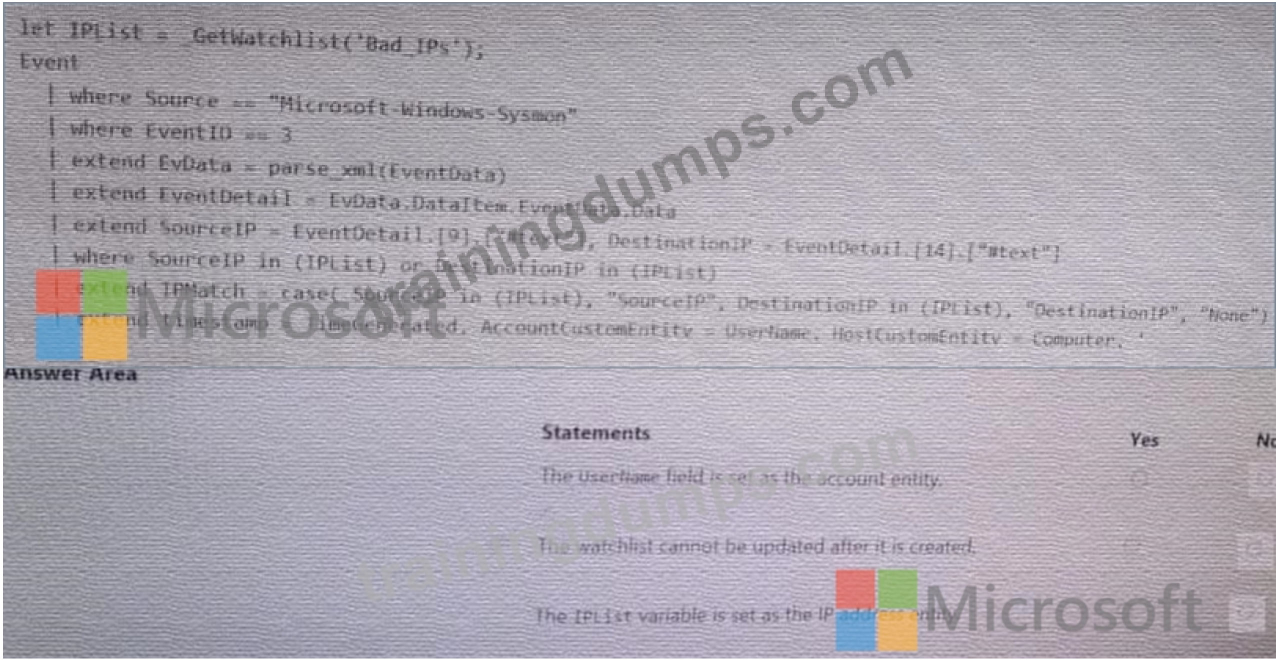
We strongly advise you to buy our online engine and windows software of the SC-200 study materials, which can simulate the real test environment. There is no doubt that you will never feel bored on learning our SC-200 practice materials because of the smooth operation. You will find that learning is becoming interesting and easy. And you will be more confident to pass the exam since that you have experience the Real SC-200 Exam.

The SC-200 Certification Exam is ideal for security analysts, security operations center (SOC) analysts, incident response analysts, and threat intelligence analysts. SC-200 exam measures the candidate's ability to perform tasks such as configuring and using Microsoft Defender for Endpoint, analyzing security data using Azure Sentinel, investigating and responding to security incidents, and managing security operations. Microsoft Security Operations Analyst certification exam is intended to help professionals demonstrate their ability to use Microsoft technologies to protect their organization's assets from cyber threats.

Microsoft Security Operations Analyst Sample Questions (Q130-Q135):

NEW QUESTION # 130

You have the following SQL query.



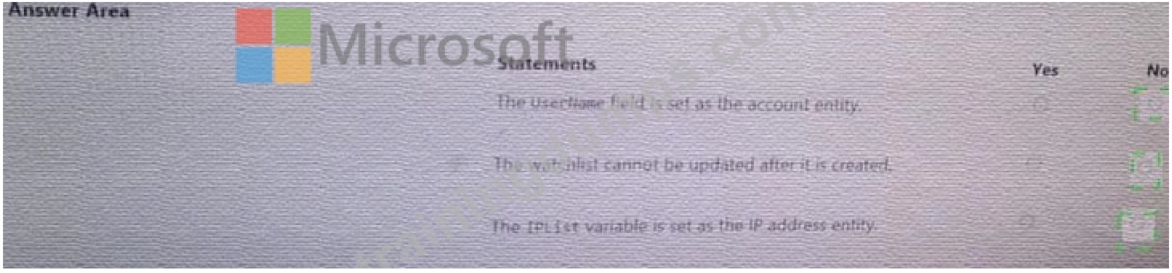
```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | 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, '
```

Answer Area

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:

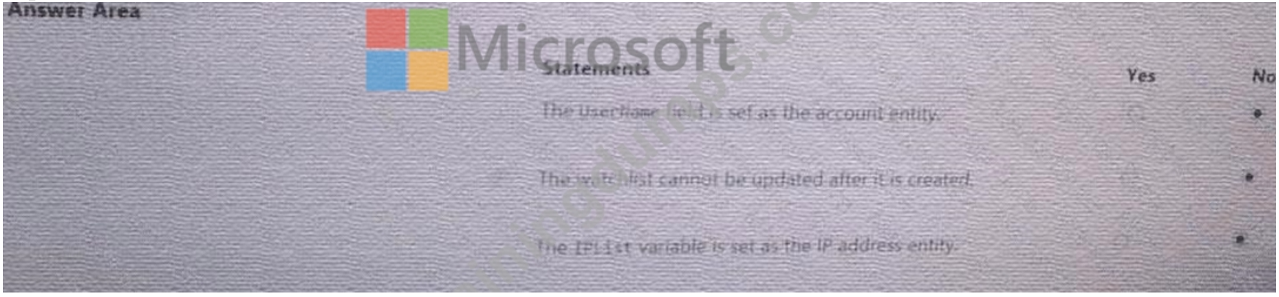
Explanation:



Answer Area

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.	○	●

Explanation:



Answer Area

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.	○	●

NEW QUESTION # 131

You use Microsoft Sentinel.

You need to receive an alert in near real-time whenever Azure Storage account keys are enumerated. 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 hunting query.
- B. Add a data connector.
- C. Create an analytics rule.
- D. Create a livestream.
- E. Create a bookmark.

Answer: C,D

Explanation:

In Microsoft Sentinel, to receive near real-time alerts when specific activities occur-such as Azure Storage account key enumeration-you combine two Sentinel capabilities: Livestream and Analytics rules

.

* Livestream provides real-time monitoring of events based on KQL queries. According to Microsoft Sentinel documentation, Livestream "lets you run queries continuously and get notified immediately when results match specific conditions." This allows SOC analysts to detect ongoing attacks (such as credential enumeration) as they happen.

* Analytics rules provide ongoing automated monitoring and alerting. A scheduled analytics rule runs periodically (for example, every 5 minutes) and generates an alert when a defined condition is met. The

"Storage account keys enumerated" event comes from Microsoft Defender for Cloud (or Azure Activity) logs, so you can define a KQL-based rule to detect these activities.

Therefore:

* B (Analytics rule): to automatically generate alerts when the condition is met.

* C (Livestream): to receive those alerts or detections in near real-time as they occur.

Together, these meet the requirement for near real-time detection and alerting with minimal manual monitoring.

NEW QUESTION # 132

You have a Microsoft Sentinel workspace named Workspaces1.

The AzureActivity table in Workspace! has the following retention periods:

* Interactive: 180 days

* Total:180days

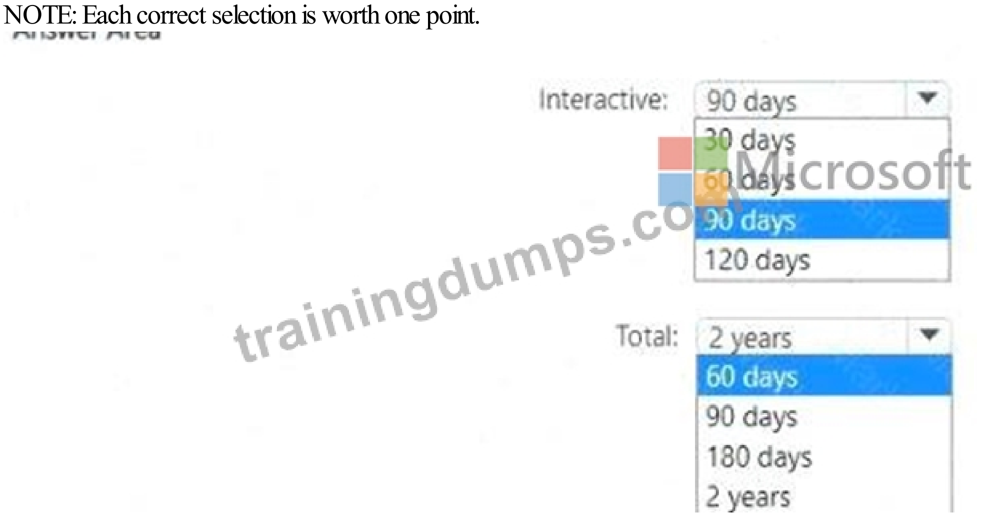
You need to modify the retention periods to meet the following requirements:

* Minimize the costs associated with storing data in the table.

* Maximize the period during which the table data remains available.

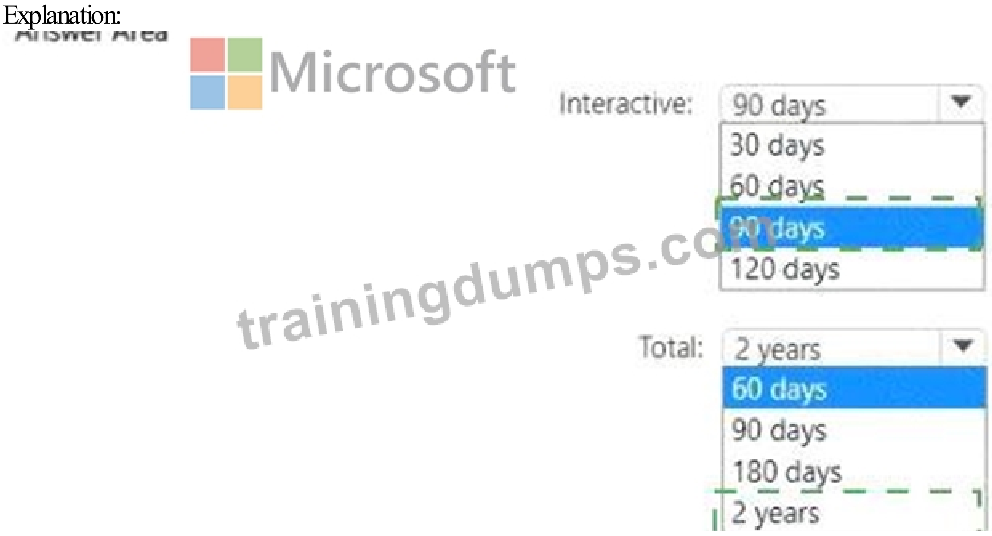
How should you configure each retention period? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

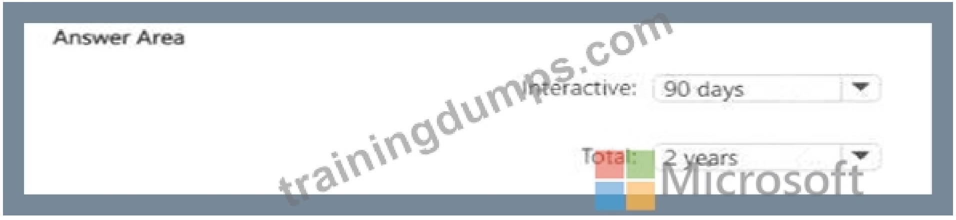


Answer:

Explanation:



Explanation:



Answer Area

Interactive: 90 days

Total: 2 years

NEW QUESTION # 133

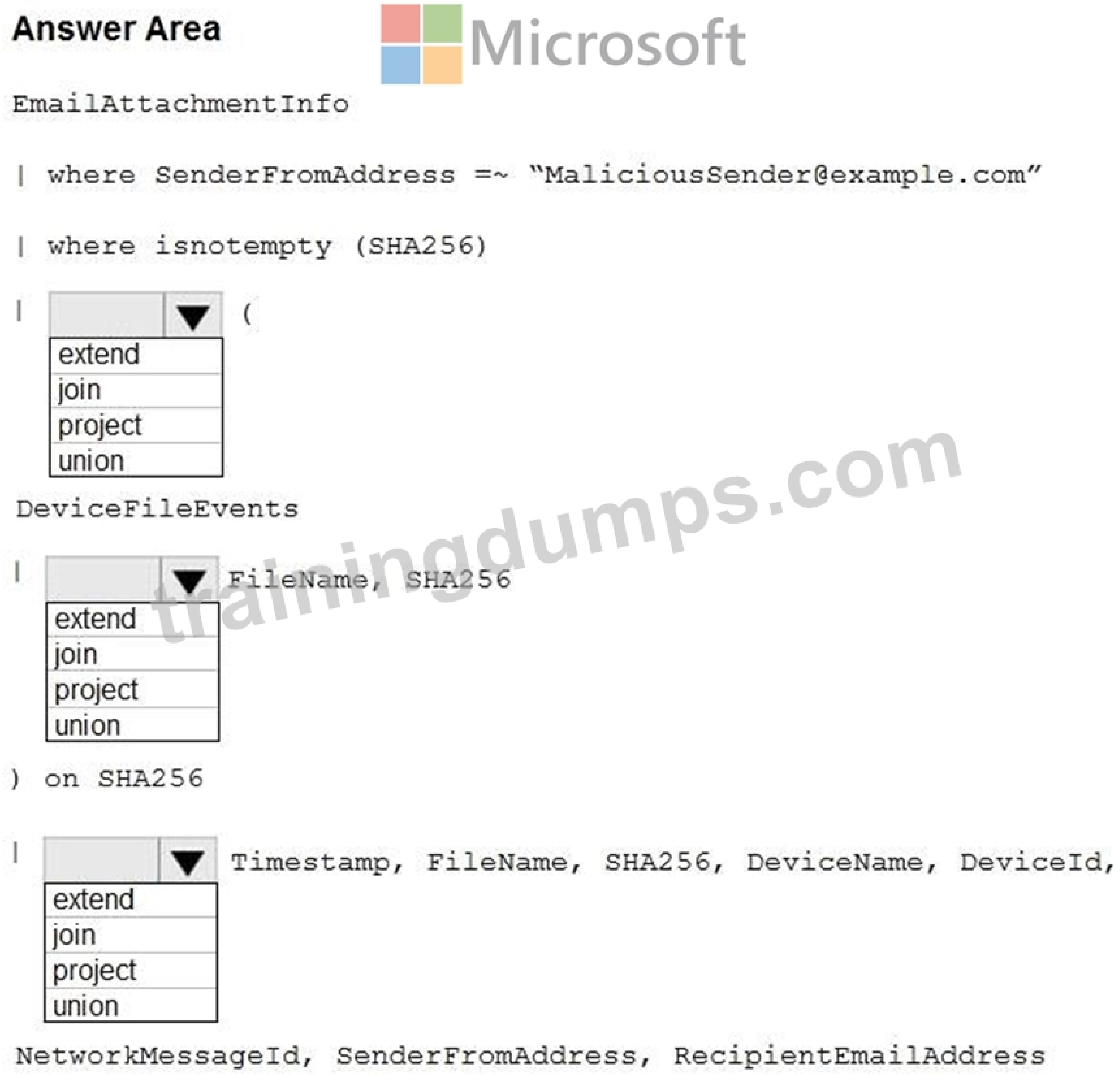
You have a Microsoft 365 E5 subscription.

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.

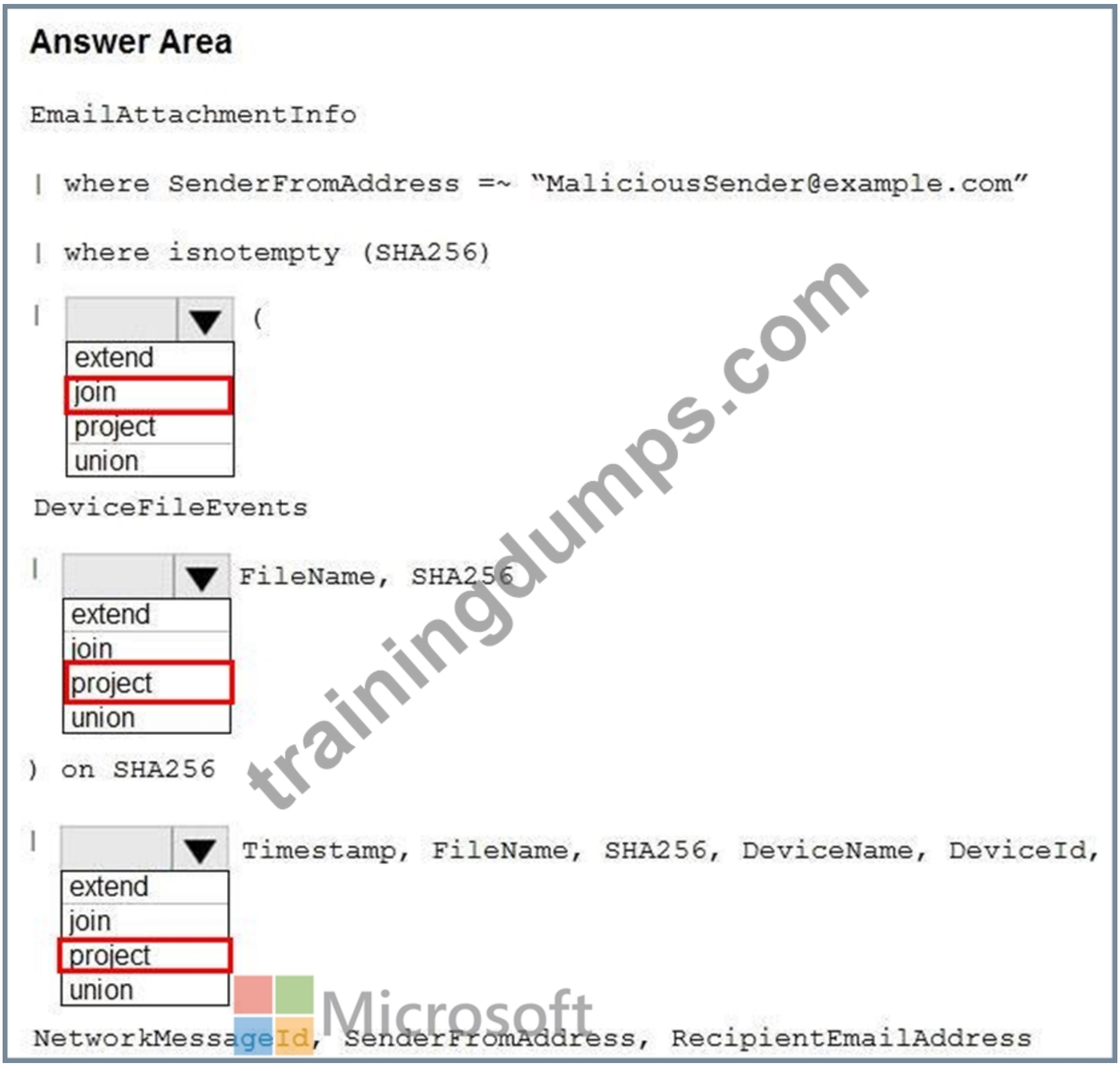


Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ “MaliciousSender@example.com”

| where isnotempty (SHA256)

|              (
   extend
   join
   project
   union
DeviceFileEvents

|              FileName, SHA256
   extend
   join
   project
   union
) on SHA256

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

Answer:

Explanation:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ “MaliciousSender@example.com”

| where isnotempty (SHA256)

|            (

DeviceFileEvents

|            FileName, SHA256

) on SHA256

|            Timestamp, FileName, SHA256, DeviceName, DeviceId,

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

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

NEW QUESTION # 134

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts. What should you review?

- A. the status update time
- B. the certainty of the source computer
- C. the alert status
- D. the resolution method of the source computer

Answer: C

NEW QUESTION # 135

......

More and more people look forward to getting the SC-200 certification by taking an exam. However, the exam is very difficult for a lot of people. Especially if you do not choose the correct study materials and find a suitable way, it will be more difficult for you to pass the exam and get the SC-200 related certification. If you want to get the related certification in an efficient method, please choose the SC-200 study materials from our company.

New SC-200 Mock Exam: https://www.trainingdumps.com/SC-200_exam-valid-dumps.html

- Quiz 2025 Microsoft First-grade SC-200: Microsoft Security Operations Analyst Valid Exam Test □ Enter ▹ www.torrentvce.com ◃ and search for 【 SC-200 】 to download for free □SC-200 Training Kit
- SC-200 Valid Test Materials □ Practice SC-200 Online □ SC-200 Valid Test Materials □ Search for 《 SC-200 》 on □ www.pdfvce.com □ immediately to obtain a free download □SC-200 Latest Mock Exam
- 2025 Realistic Microsoft SC-200 Valid Exam Test ❣ Open ✔ www.pass4leader.com □✔□ and search for 「 SC-200 」 to download exam materials for free □SC-200 Valid Dumps Ebook
- Professional Microsoft SC-200 Valid Exam Test and Reliable New SC-200 Mock Exam □ Download （ SC-200 ） for free by simply entering [www.pdfvce.com] website □New SC-200 Test Vce Free
- Pass Guaranteed Quiz Microsoft - SC-200 - Microsoft Security Operations Analyst –Professional Valid Exam Test □ Search for ▹ SC-200 ◃ and obtain a free download on ✔ www.torrentvalid.com □✔□ □Reliable SC-200 Test Question
- SC-200 Training Kit □ SC-200 Valuable Feedback □ New SC-200 Dumps Ppt □ Immediately open “ www.pdfvce.com ” and search for □ SC-200 □ to obtain a free download □SC-200 Practice Exams Free
- SC-200 Valid Dumps Ebook □ SC-200 Latest Mock Exam □ SC-200 Valid Examcollection □ ▸ www.passcollection.com ◂ is best website to obtain ➠ SC-200 □ for free download □New SC-200 Test Vce Free
- SC-200 Valid Test Materials □ Exam SC-200 Sample □ New SC-200 Dumps Ppt □ Search for ▸ SC-200 ◂ and download it for free on ✔ www.pdfvce.com □✔□ website □New SC-200 Test Vce Free
- 2025 Reliable SC-200 – 100% Free Valid Exam Test | New SC-200 Mock Exam □ Download □ SC-200 □ for free by simply entering ➤ www.exams4collection.com □ website □SC-200 Valid Test Materials
- 2025 Realistic Microsoft SC-200 Valid Exam Test □ Search for ▸ SC-200 ◂ and download it for free immediately on ➥ www.pdfvce.com □ □Valid SC-200 Study Guide
- Pass Guaranteed 2025 SC-200: Fantastic Microsoft Security Operations Analyst Valid Exam Test □ Search for ✔ SC-200 □✔□ and obtain a free download on □ www.itcerttest.com □ □New SC-200 Test Vce Free
- mentorteach.com, global.edu.bd, record.srinivasaacademy.com, netflowbangladesh.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.wcs.edu.eu, rabonystudywork.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, myportal.utt.edu.tt, myportal.utt.edu.tt, ncon.edu.sa, Disposable vapes

P.S. Free 2025 Microsoft SC-200 dumps are available on Google Drive shared by TrainingDumps: https://drive.google.com/open?id=1UCVN-5obSTmnxKCbkH3YdjvOruRLZpL