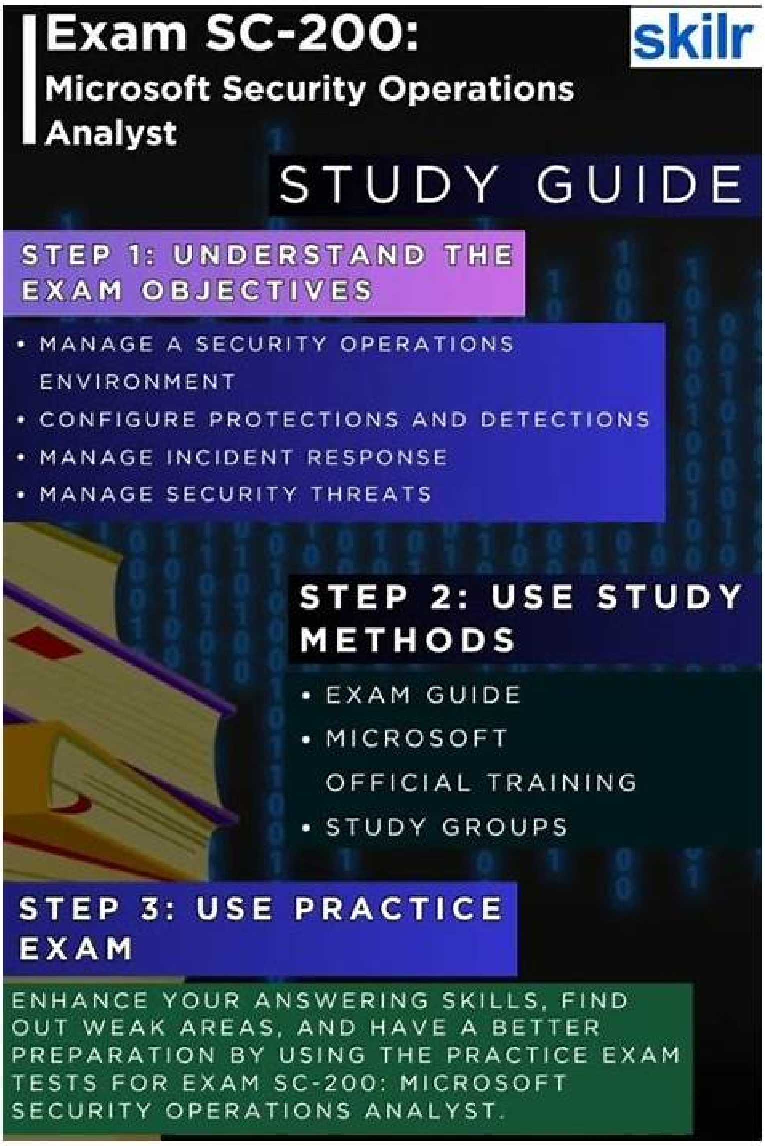
Quiz 2025 SC-200: Microsoft Security Operations Analyst Exam Fee



Exam SC-200:
Microsoft Security Operations Analyst

skilr

STUDY GUIDE

STEP 1: UNDERSTAND THE EXAM OBJECTIVES

- MANAGE A SECURITY OPERATIONS ENVIRONMENT
- CONFIGURE PROTECTIONS AND DETECTIONS
- MANAGE INCIDENT RESPONSE
- MANAGE SECURITY THREATS

STEP 2: USE STUDY METHODS

- EXAM GUIDE
- MICROSOFT OFFICIAL TRAINING
- STUDY GROUPS

STEP 3: USE PRACTICE EXAM

ENHANCE YOUR ANSWERING SKILLS, FIND OUT WEAK AREAS, AND HAVE A BETTER PREPARATION BY USING THE PRACTICE EXAM TESTS FOR EXAM SC-200: MICROSOFT SECURITY OPERATIONS ANALYST.

BTW, DOWNLOAD part of ValidDumps SC-200 dumps from Cloud Storage: https://drive.google.com/open?id=1oxwd-xRNcH4GWpAIlK3xoSbu4gyDQ3xe

Similarly, the ValidDumps Microsoft SC-200 practice test creates an actual exam scenario on each and every step so that you may be well prepared before your actual Microsoft Security Operations Analyst examination time. Hence, it saves you time and money. ValidDumps provides three months of free updates if you purchase the Microsoft SC-200 Questions and the content of the examination changes after that.

Microsoft SC-200 Exam, also known as the Microsoft Security Operations Analyst exam, is a certification exam designed to test the candidate's knowledge and skills in implementing, managing, and monitoring security measures in Microsoft environments. SC-200 exam measures the candidate's ability to analyze security data, identify potential vulnerabilities and threats, and provide recommendations to improve security posture.

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 Exam Fee <<

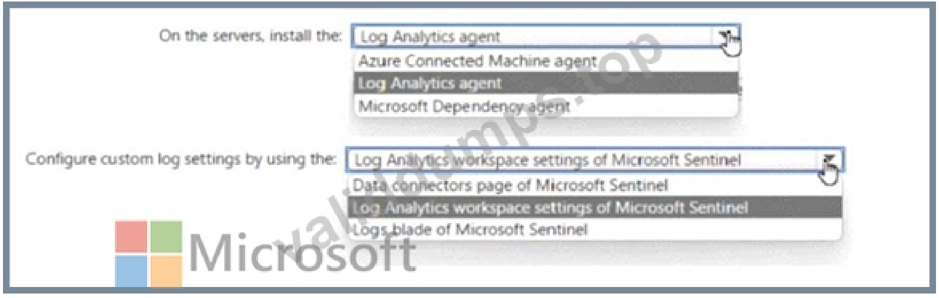
SC-200 Pass4sure Pass Guide - New SC-200 Test Syllabus

As is known to all, SC-200 practice test simulation plays an important part in the success of exams. By simulation, you can get the hang of the situation of the real exam with the help of our free demo. You can fight a hundred battles with no danger of defeat. Simulation of our SC-200 Training Materials make it possible to have a clear understanding of what your strong points and weak points are and at the same time, you can learn comprehensively about the exam. By combining the two aspects, you are more likely to achieve high grades in the real exam.

To prepare for the Microsoft SC-200 Exam, candidates should have experience working with Microsoft security solutions, such as Microsoft Defender for Endpoint, Azure Sentinel, and Azure Security Center. Additionally, candidates should have knowledge of security operations concepts, such as security incident response, threat hunting, and security automation. Microsoft offers training courses and resources to help candidates prepare for the exam.

Microsoft Security Operations Analyst Sample Questions (Q136-Q141):

NEW QUESTION # 136
Your on-premises network contains 100 servers that run Windows Server.
You have an Azure subscription that uses Microsoft Sentinel.
You need to upload custom logs from the on-premises servers to Microsoft Sentinel.
What should you do? To answer, select the appropriate options m the answer area.

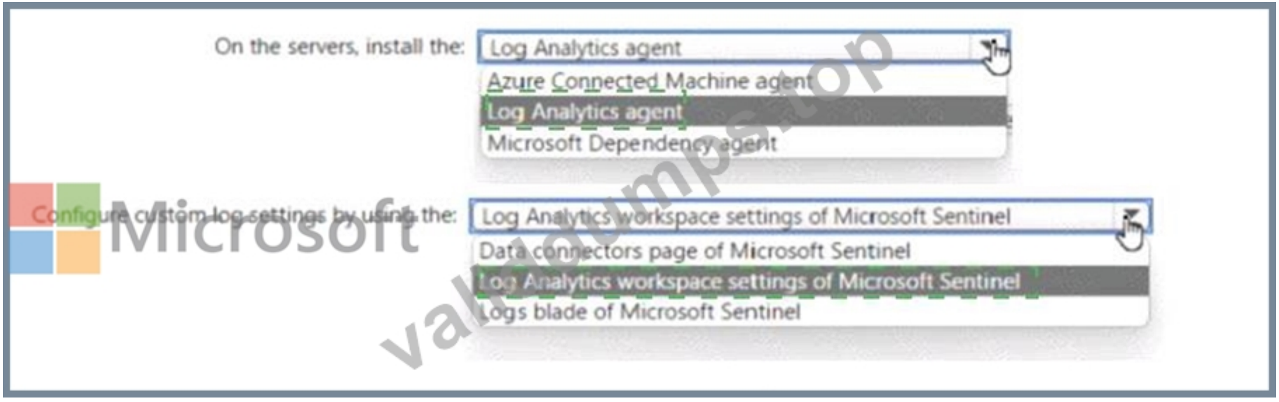


On the servers, install the: Log Analytics agent
- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel
- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

Answer:

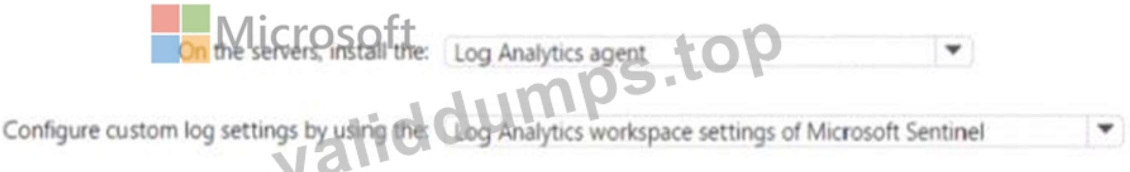
Explanation:



On the servers, install the: Log Analytics agent
- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel
- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

Explanation:



On the servers, install the: Log Analytics agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

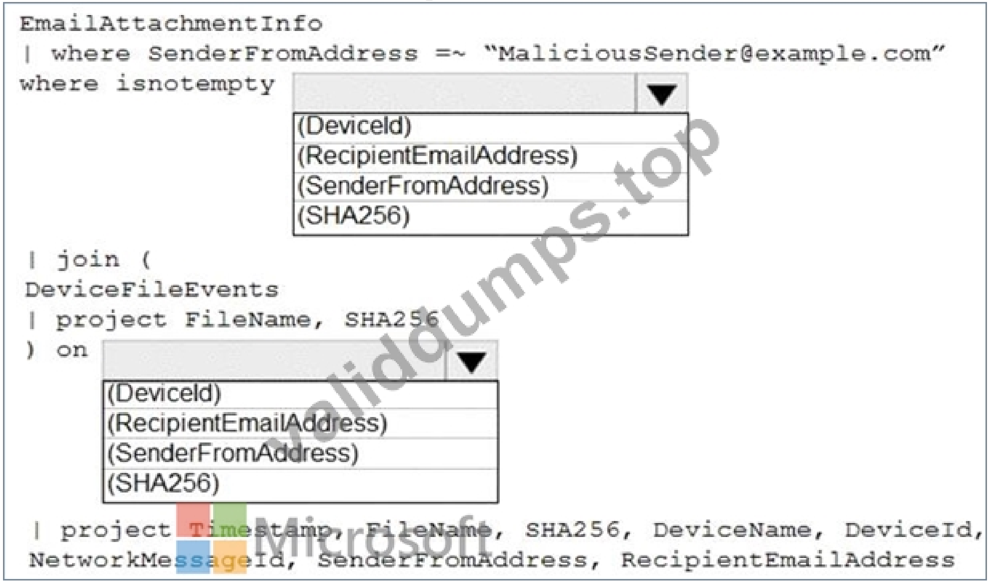
NEW QUESTION # 137

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.

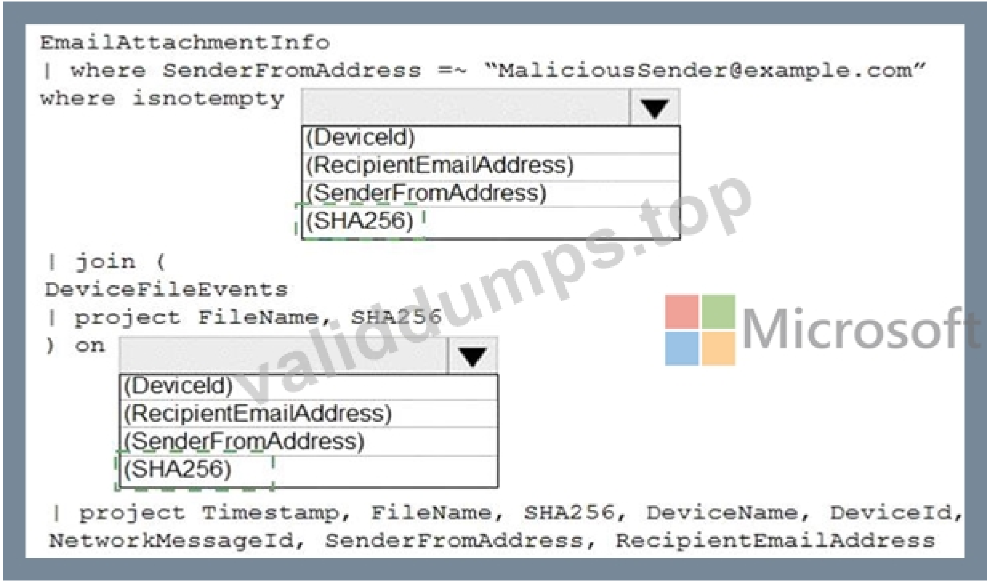
NOTE: Each correct selection is worth one point.



```
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
```

Answer:

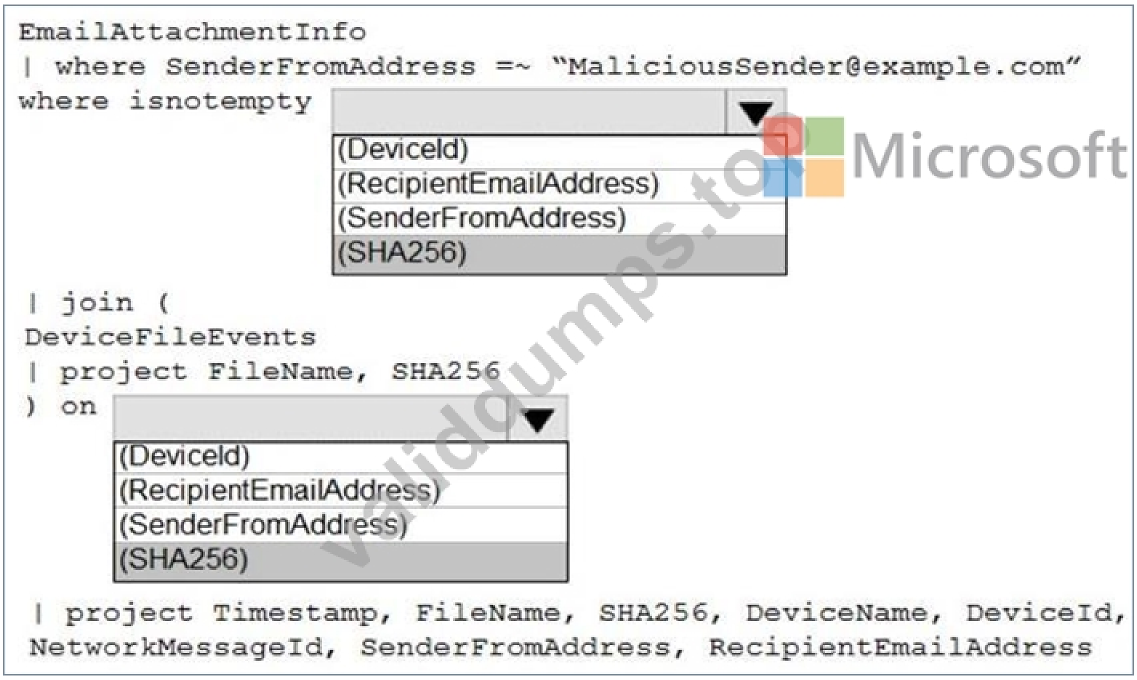
Explanation:



```
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
```

Explanation

Graphical user interface, text, application Description automatically generated



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

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

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

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

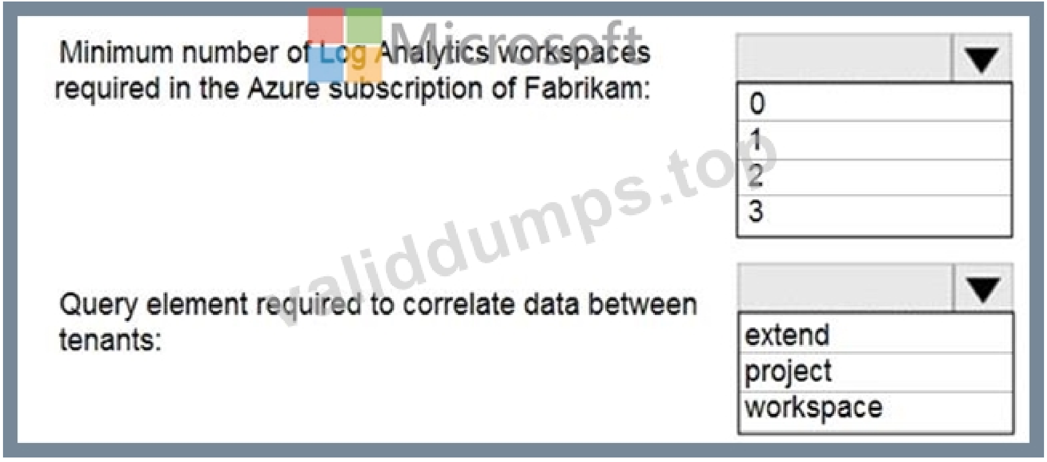
```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

validdumps.top Microsoft

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

NEW QUESTION # 138

You need to implement Azure 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.



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

0
1
2
3

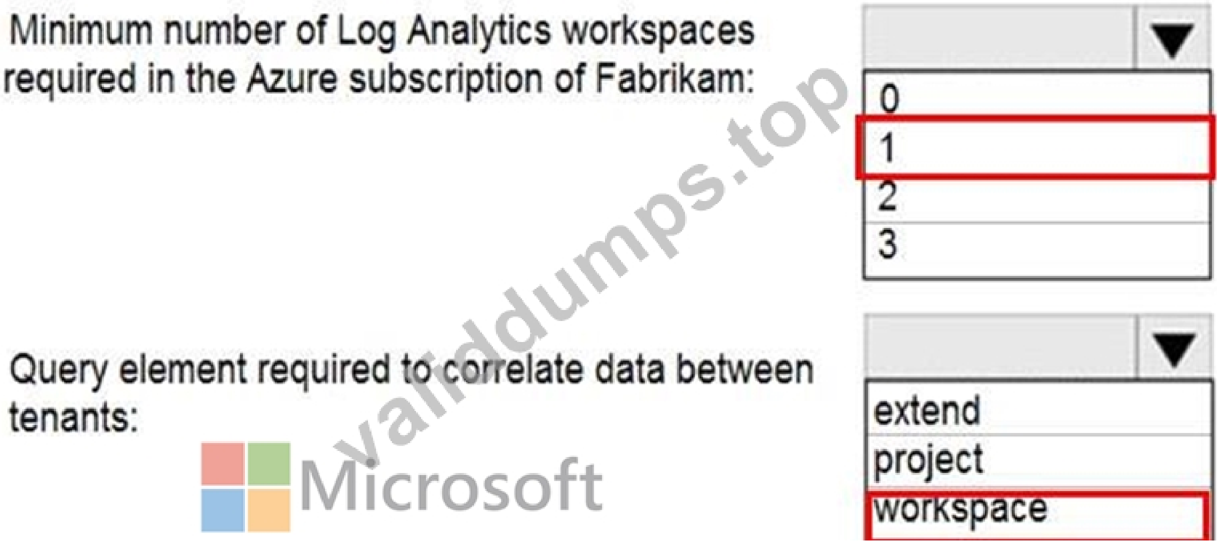
Query element required to correlate data between tenants:

extend
project
workspace

validdumps.top Microsoft

Answer:

Explanation:



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

- 0
- [✓ 1]
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- [✓ workspace]

validdumps.top

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

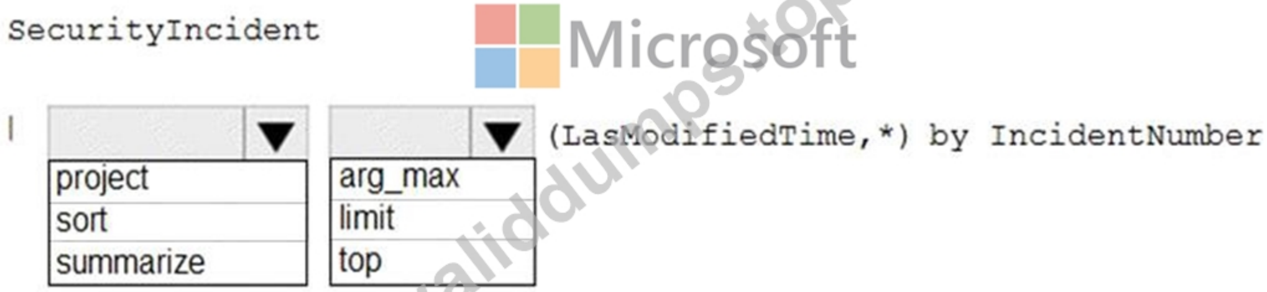
NEW QUESTION # 139
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

- A. Add a parameter and modify the trigger.
- B. Add a custom data connector and modify the trigger.
- C. Add a condition and modify the action.
- D. Add a parameter and modify the action.

Answer: D

Explanation:
Section: [none]
Explanation/Reference:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

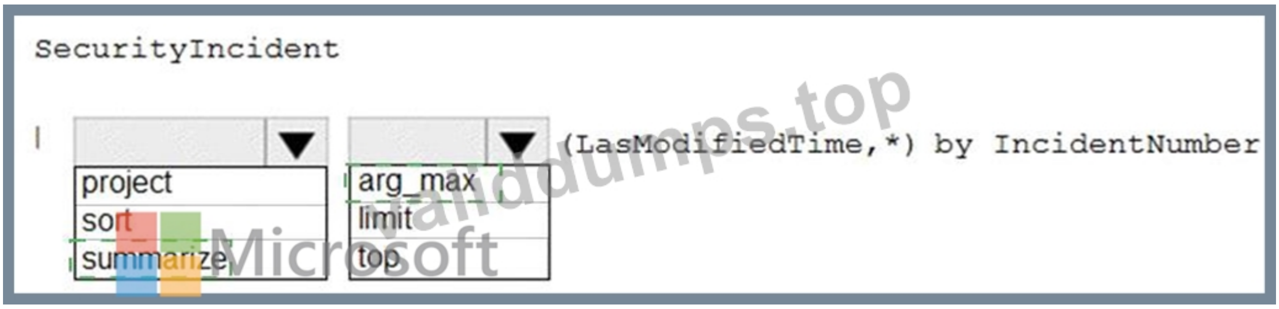
NEW QUESTION # 140
You need to create a query for a workbook. The query must meet the following requirements:
* List all incidents by incident number.
* Only include the most recent log for each incident.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

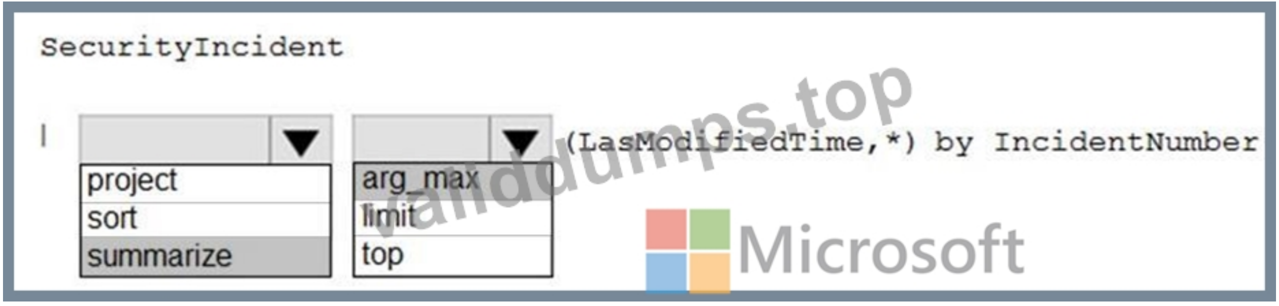
Answer:

Explanation:



```
SecurityIncident
|                           (LasModifiedTime,*) by IncidentNumber
```

Explanation:



```
SecurityIncident
|                           (LasModifiedTime,*) by IncidentNumber
```

Reference:
https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

NEW QUESTION # 141

......

SC-200 Pass4sure Pass Guide: https://www.validdumps.top/SC-200-exam-torrent.html

- Excel in the Certification Exam With Real Microsoft SC-200 Questions □ Copy URL □ www.passtestking.com □ open and search for ➡ SC-200 □□□ to download for free □Actual SC-200 Tests
- Free SC-200 Practice Exams □ SC-200 Online Exam □ SC-200 Certification Exam Infor □ Open ⇛ www.pdfvce.com ⇚ enter 【 SC-200 】 and obtain a free download □SC-200 Study Group
- Reliable SC-200 Test Practice □ SC-200 Latest Test Simulations □ Actual SC-200 Tests □ Search for [SC-200] and download exam materials for free through ➥ www.prep4away.com □ □SC-200 Study Group
- Free PDF Microsoft - Useful SC-200 Exam Fee □ Easily obtain □ SC-200 □ for free download through [www.pdfvce.com] □SC-200 Study Group
- Helpful Features of SC-200 PDF Questions □ Search for ✔ SC-200 □✔□ on □ www.free4dump.com □ immediately to obtain a free download □Accurate SC-200 Test
- Free PDF Microsoft - Useful SC-200 Exam Fee □ Download □ SC-200 □ for free by simply entering ➽ www.pdfvce.com □ website □SC-200 Pass Guaranteed
- SC-200 Certification Exam Infor □ Reliable SC-200 Test Practice □ Detailed SC-200 Study Plan □ Go to website ➥ www.pdfdumps.com □ open and search for □ SC-200 □ to download for free 🖑 SC-200 Pass Guaranteed
- SC-200 Pdf Dumps □ New SC-200 Exam Simulator □ SC-200 Official Practice Test □ Search for □ SC-200 □ and easily obtain a free download on ✔ www.pdfvce.com □✔□ □New SC-200 Test Tutorial
- SC-200 Study Group □ Reliable SC-200 Test Practice □ New SC-200 Test Tutorial □ Simply search for □ SC-200 □ for free download on ➤ www.prep4away.com □ □Reliable SC-200 Real Exam
- 2025 Microsoft Pass-Sure SC-200: Microsoft Security Operations Analyst Exam Fee □ Easily obtain 《 SC-200 》 for free download through { www.pdfvce.com } □SC-200 Study Group
- Actual SC-200 Tests □ Valid SC-200 Exam Format ↪ Free SC-200 Practice Exams □ Search for ✔ SC-200 □✔□ and download it for free immediately on ➤ www.passcollection.com □ □Detailed SC-200 Study Plan
- www.stes.tyc.edu.tw, study.stcs.edu.np, shortcourses.russellcollege.edu.au, lms.ait.edu.za, qudurataleabqariu.online, myportal.utt.edu.tt, www.51ffff.xyz, 40bbk.com, lifeshine.themespirit.com, Disposable vapes

P.S. Free & New SC-200 dumps are available on Google Drive shared by ValidDumps: https://drive.google.com/open?id=1oxwd-xRNcH4GWpAIlK3xoSbu4gyDQ3xe