- **Vendor:** Microsoft
- **Exam Code:** SC-200
- **Exam Name:** Microsoft Security Operations Analyst
- **New Updated Questions from Braindump2go (Updated in July/2021)**

QUESTION 29
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel?Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a playbook.
B. Associate a playbook to an incident.
C. Enable Entity behavior analytics.
D. Create a workbook.
E. Enable the Fusion rule.

Answer: AB
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 30
You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC).
What should you use?

A. notebooks in Azure Sentinel
B. Microsoft Cloud App Security
C. Azure Monitor
D. hunting queries in Azure Sentinel

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION 31
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph.
What should you include in the query?

A. extend
B. bin

C. count
D. workspace

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

QUESTION 32
You use Azure Sentinel.
You need to receive an immediate alert 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 livestream
B. Add a data connector
C. Create an analytics rule
D. Create a hunting query.
E. Create a bookmark.

Answer: BD
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/livestream

QUESTION 33
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel.
What should you do first?

A. And a new scheduled query rule.
B. Add a data connector to Azure Sentinel.
C. Configure a custom Threat Intelligence connector in Azure Sentinel.
D. Modify the trigger in the logic app.

Answer: B

QUESTION 34
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

A. built-in queries
B. livestream
C. notebooks
D. bookmarks

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

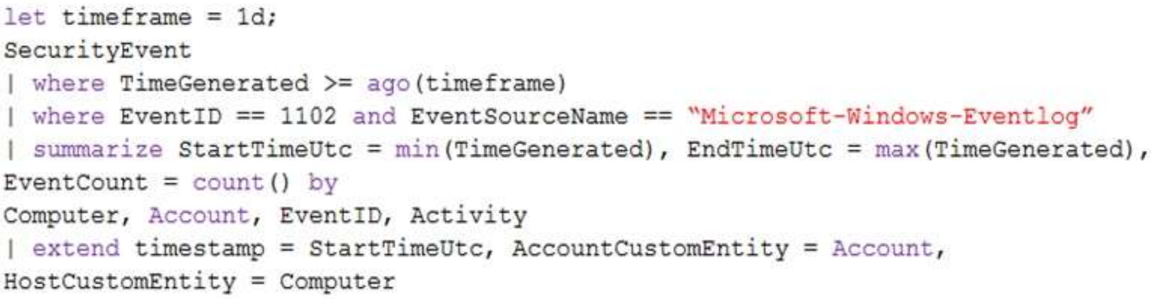
QUESTION 35
You have a playbook in Azure Sentinel.

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:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

QUESTION 36
You provision Azure Sentinel for a new Azure subscription.
You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event.
You create the following rule query.



```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents?Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address
D. computer

Answer: CD

QUESTION 37
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. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

Answer: BE

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

QUESTION 38
You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal.
From where can you run the test in Azure Sentinel?

A. Playbooks
B. Analytics
C. Threat intelligence
D. Incidents

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

QUESTION 39
You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.
B. The number of alerts exceeded 10,000 within two minutes.
C. The rule query takes too long to run and times out.
D. Permissions to one of the data sources of the rule query were modified.

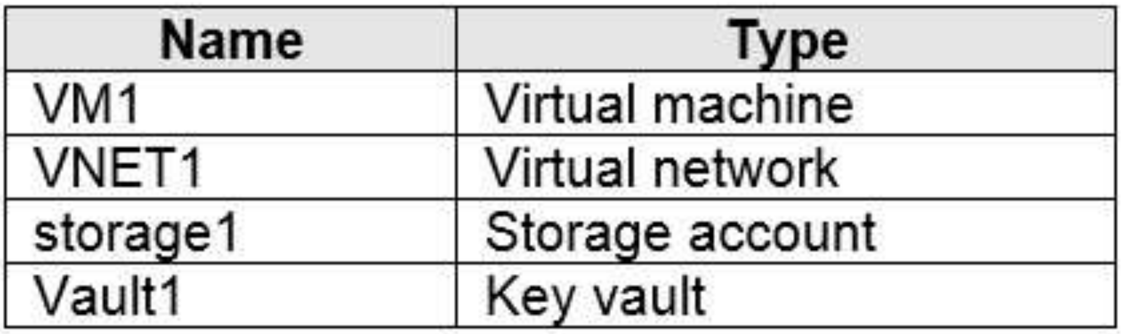
Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 40
Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel.
You need to resolve the issue for the analyst. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Responder
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION 41
You have an Azure subscription that contains the resources shown in the following table.



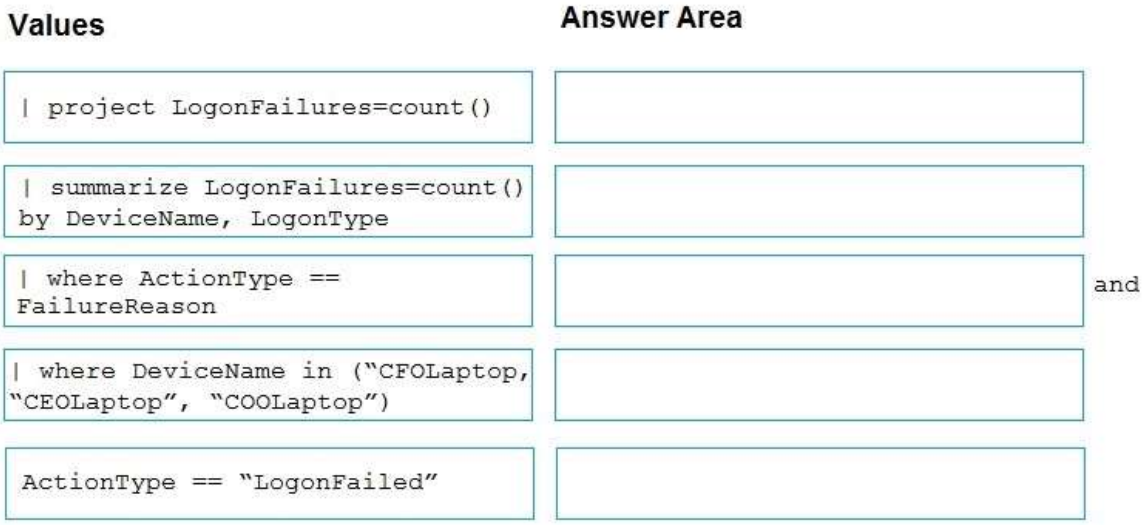
Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription.
Which resources can be protected by using Azure Defender?

A. VM1, VNET1, storage1, and Vault1
B. VM1, VNET1, and storage1 only
C. VM1, storage1, and Vault1 only
D. VM1 and VNET1 only
E. VM1 and storage1 only

Answer: C

QUESTION 42
Drag and Drop Question
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.
How should you complete the query?To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



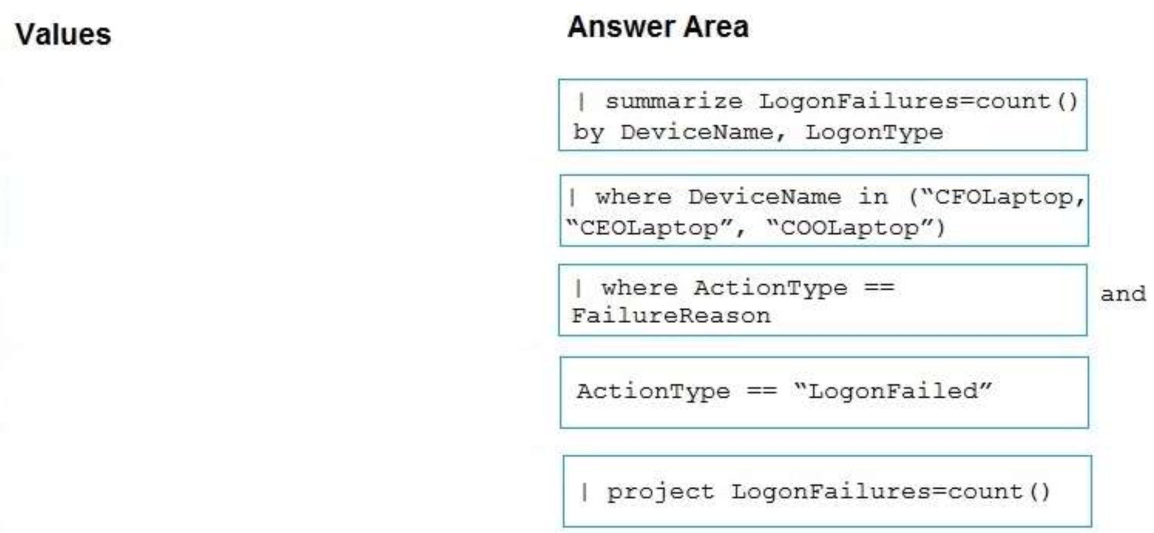
Values

```
| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType ==
FailureReason

| where DeviceName in ("CFOLaptop,
"CEOLaptop", "COOLaptop")

ActionType == "LogonFailed"
```

Answer Area

and

Answer:



Values

Answer Area

```
| summarize LogonFailures=count()
by DeviceName, LogonType
```

```
| where DeviceName in ("CFOLaptop,
"CEOLaptop", "COOLaptop")
```

```
| where ActionType ==
FailureReason
```

and

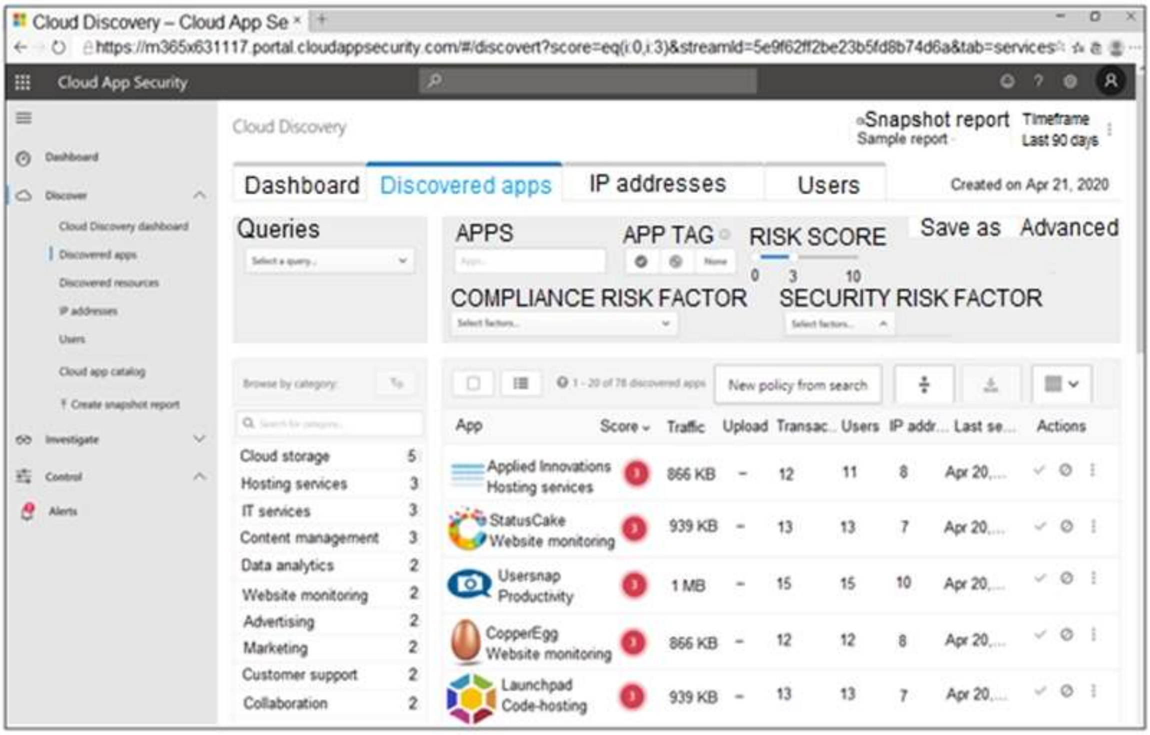
```
ActionType == "LogonFailed"
```

```
| project LogonFailures=count()
```

QUESTION 43

Drag and Drop Question

You open the Cloud App Security portal as shown in the following exhibit.



Cloud Discovery – Cloud App Se ×

https://m365x631117.portal.cloudappsecurity.com/#/discovert?score=eq(i:0,i:3)&streamId=5e9f62ff2be23b5fd8b74d6a&tab=services

Cloud App Security

Cloud Discovery

Snapshot report
Sample report

Timeframe
Last 90 days

Created on Apr 21, 2020

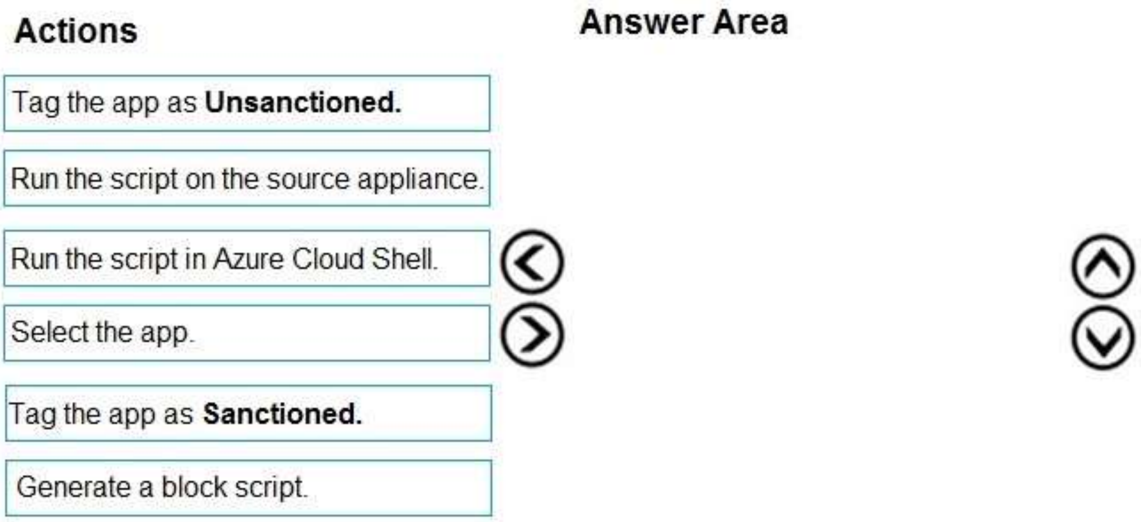
1 - 20 of 78 discovered apps

Cloud storage	5
Hosting services	3
IT services	3
Content management	3
Data analytics	2
Website monitoring	2
Advertising	2
Marketing	2
Customer support	2
Collaboration	2

App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	-	12	11	8	Apr 20,...	✓ ⊘ ⋮
StatusCake Website monitoring	3	939 KB	-	13	13	7	Apr 20,...	✓ ⊘ ⋮
Usersnap Productivity	3	1 MB	-	15	15	10	Apr 20,...	✓ ⊘ ⋮
CopperEgg Website monitoring	3	866 KB	-	12	12	8	Apr 20,...	✓ ⊘ ⋮
Launchpad Code-hosting	3	939 KB	-	13	13	7	Apr 20,...	✓ ⊘ ⋮

You need to remediate the risk for the Launchpad app.

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



Actions

Tag the app as **Unsanctioned.**

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

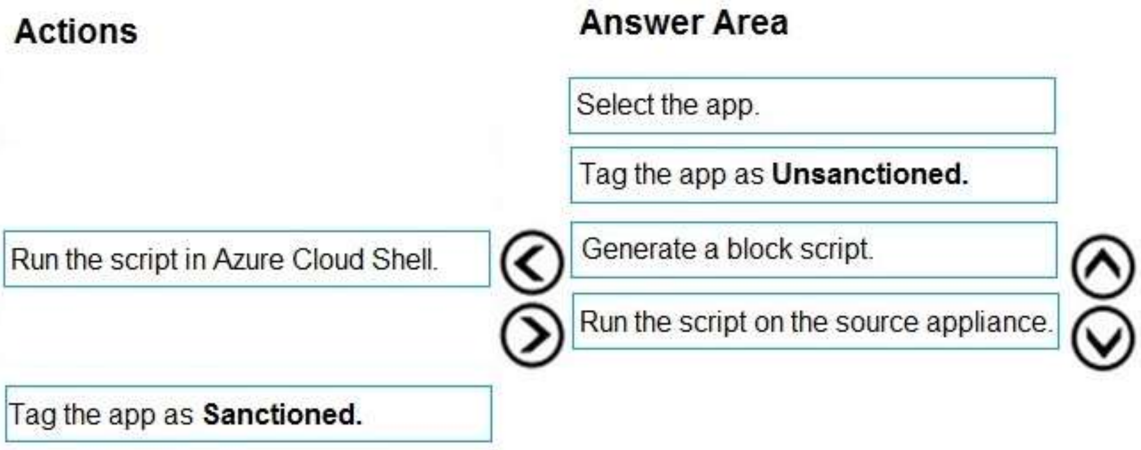
Select the app.

Tag the app as **Sanctioned.**

Generate a block script.

Answer Area

Answer:



Actions

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned.**

Answer Area

Select the app.

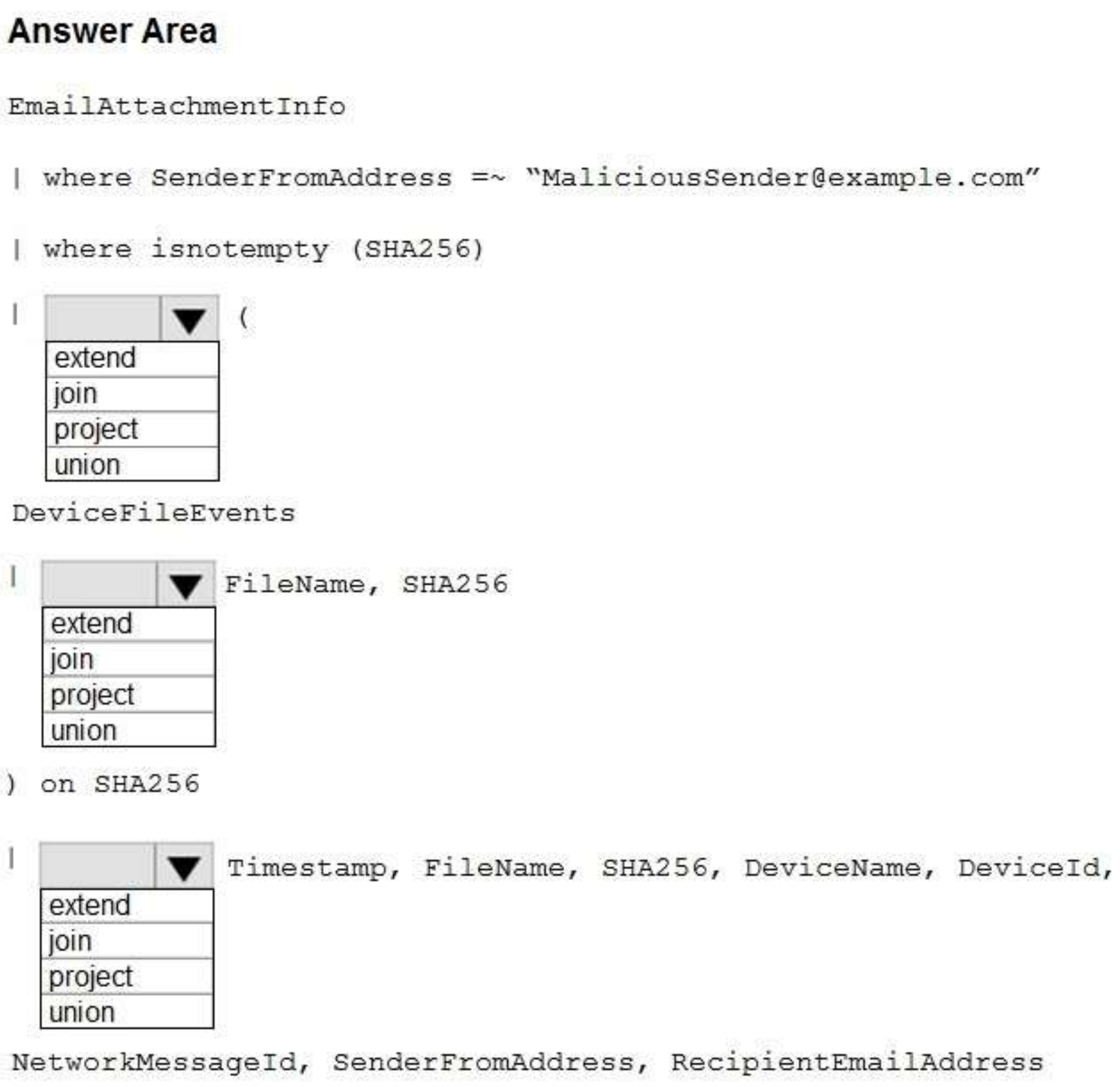
Tag the app as **Unsanctioned.**

Generate a block script.

Run the script on the source appliance.

Explanation:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

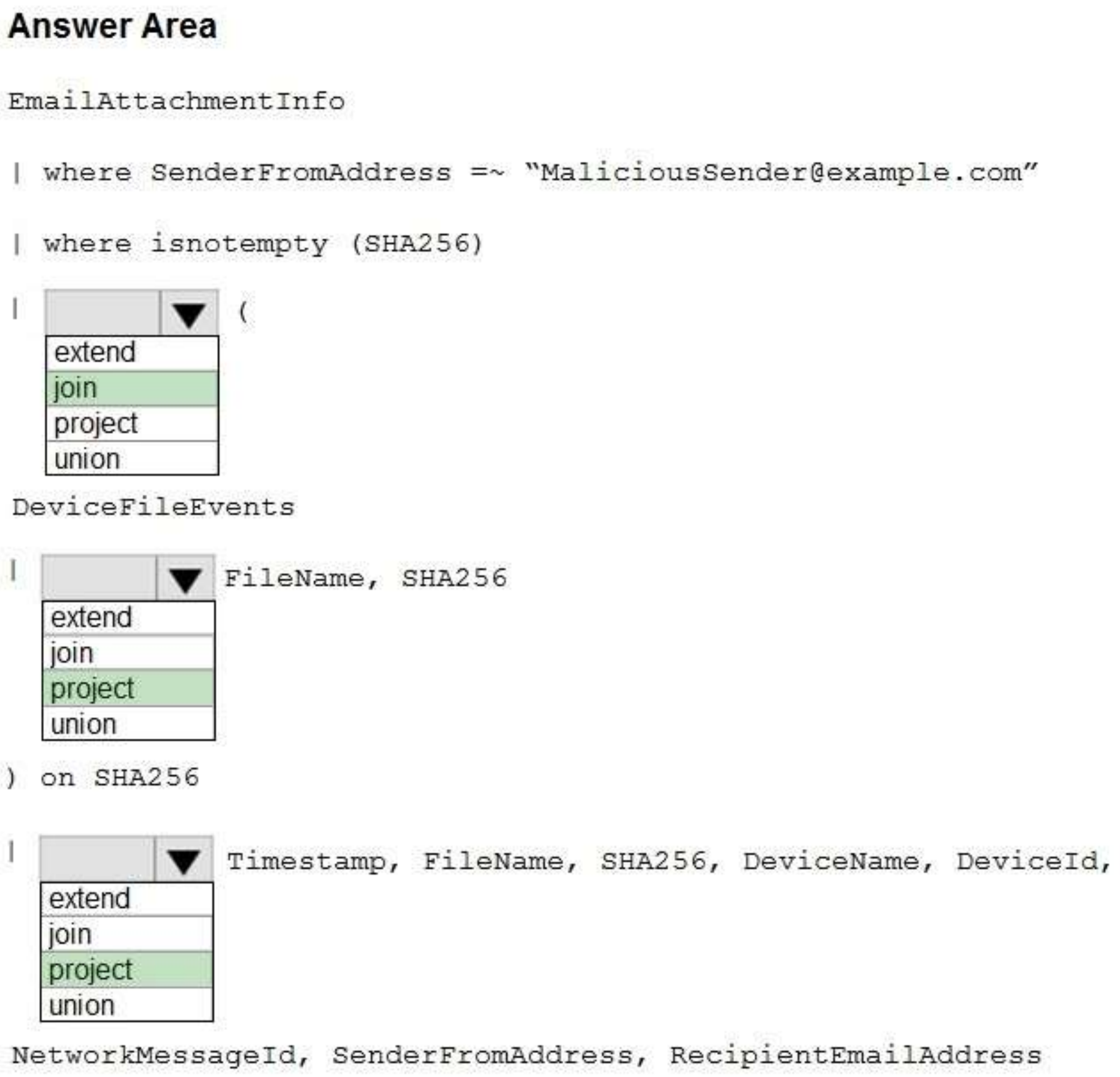
QUESTION 44
Hotspot Question
You have a Microsoft 365 E5 subscription.
You plan to perform cross-domain investigations by using Microsoft 365 Defender.
You need to create an advanced hunting query to identify devices affected by a malicious email attachment.
How should you complete the query?To answer, 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:



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
```

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