DBCLOUD
EXAMS

QUESTIONS & ANSWERS

verified

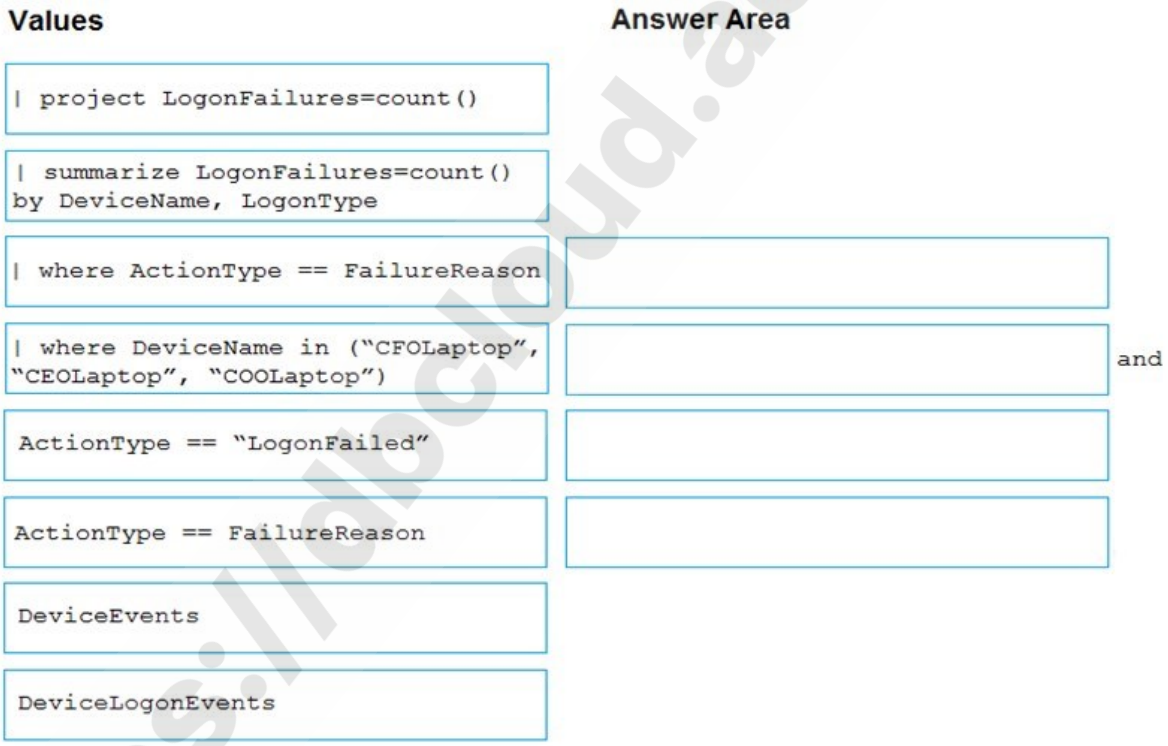


Technology Provider: Microsoft
Exam: Microsoft Security Operations Analyst
Number of questions in the database: 436
Exam Version: NOV.2026

Topic 1 - Question Set 1

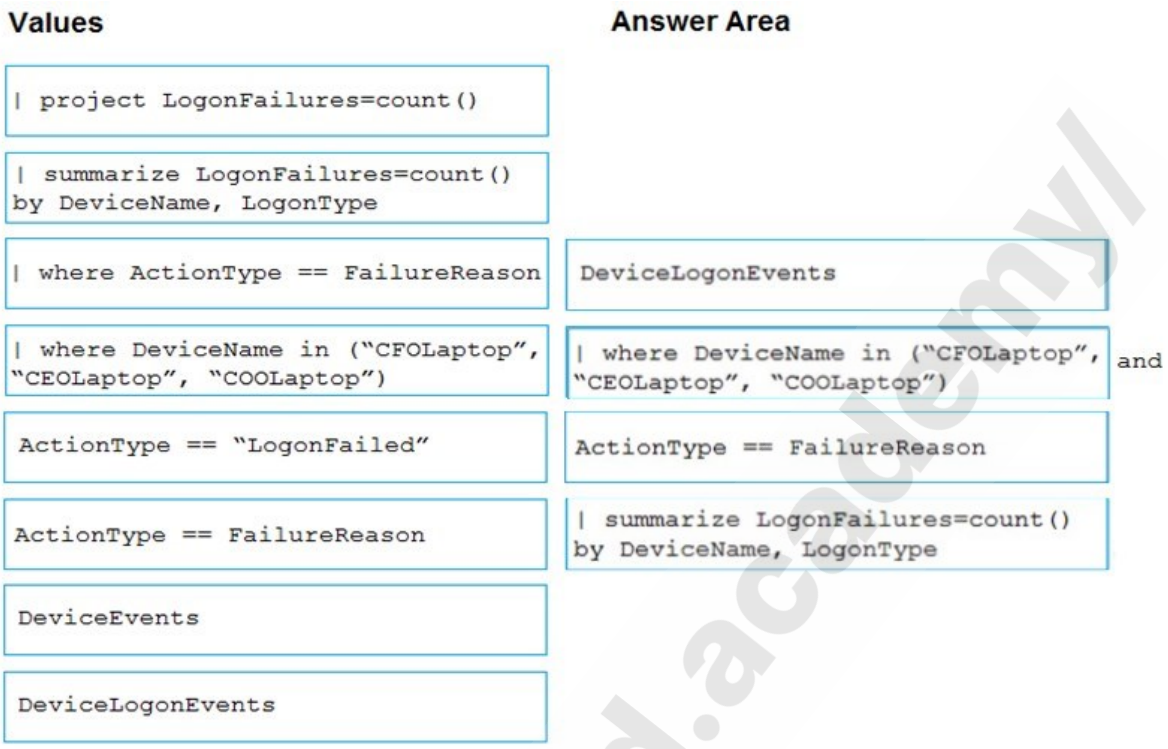
Question #1*Topic 1*

DRAG DROP -
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.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Select and Place:



Correct Answer:

https://dbcloud.academy/



Question #2*Topic 1*

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

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Respuesta por mayor votación de la comunidad

C (100%)

Question #3*Topic 1*

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.

https://dbcloud.academy/

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.
What should you use to detect which documents are sensitive?

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

Correct Answer: *D*

Respuesta por mayor votación de la comunidad

D (60%)

C (40%)

Question #4*Topic 1*

Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes.
Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

B.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

C.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC
-AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

D.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

Correct Answer: *AD*

Question #5*Topic 1*

Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

https://dbcloud.academy/

- A. Resolve the alert automatically.
- B. Hide the alert.
- C. Create a suppression rule scoped to any device.
- D. Create a suppression rule scoped to a device group.
- E. Generate the alert.

Correct Answer: *BDE*

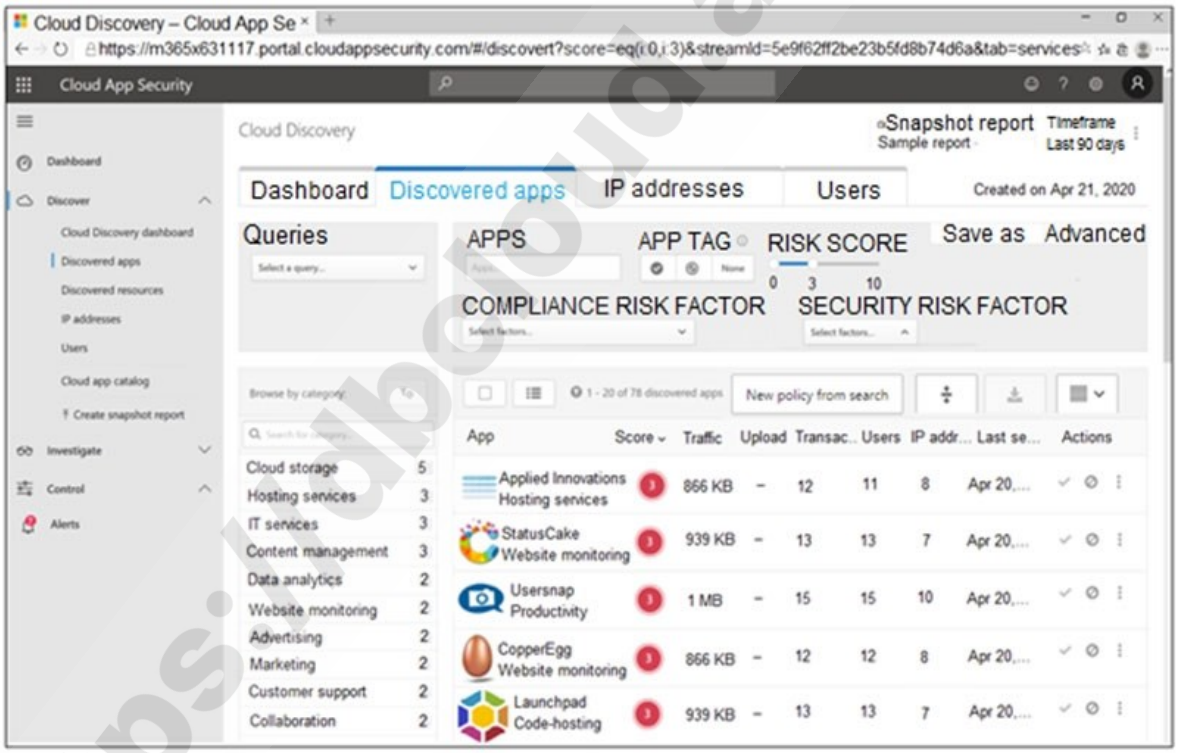
Respuesta por mayor votación de la comunidad

BDE (81%)

Other

Question #6*Topic 1*

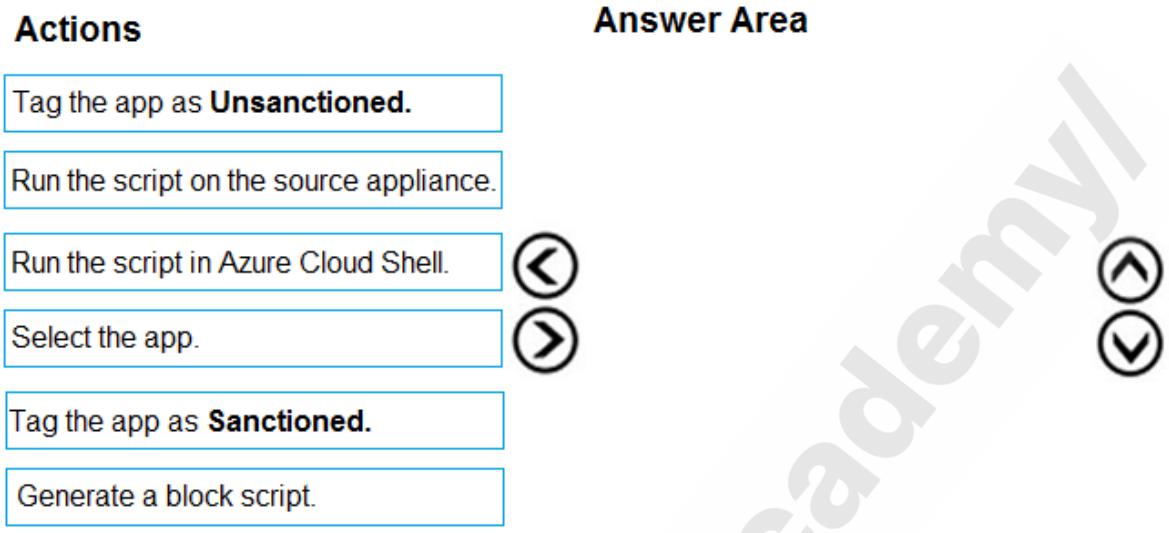
DRAG DROP -
You open the Cloud App Security portal as shown in the following exhibit.



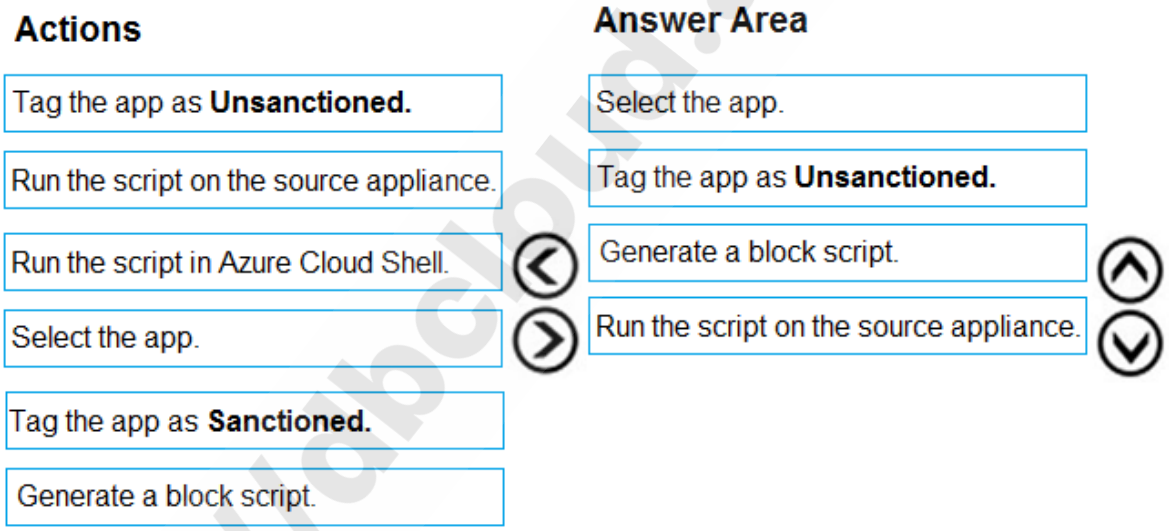
Your environment does NOT have Microsoft Defender for Endpoint enabled.
You need to remediate the risk for the Launchpad app.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

https://dbcloud.academy/

Select and Place:



Correct Answer:



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

Question #7*Topic 1*

HOTSPOT -
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.

https://dbcloud.academy/

Hot Area:

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
```

Correct Answer:

https://dbcloud.academy/

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
```

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

Question #8*Topic 1*

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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 detection rule.
- B. Create a suppression rule.
- C. Add | order by Timestamp to the query.
- D. Replace DeviceProcessEvents with DeviceNetworkEvents.
- E. Add DeviceId and ReportId to the output of the query.

Correct Answer: *AE*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

Respuesta por mayor votación de la comunidad

AE (88%)

12%

Question #9*Topic 1*

You are investigating a potential attack that deploys a new ransomware strain.
You have three custom device groups. The groups contain devices that store highly sensitive information.
You plan to perform automated actions on all devices.
You need to be able to temporarily group the machines to perform actions on the devices.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group.
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role.
- F. Create a new device group that has a rank of 4.

Correct Answer: *ACD*
Reference:
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

Respuesta por mayor votación de la comunidad

ACD (98%)

https://dbcloud.academy/