CertSharks

Microsoft Security Operations
SC-200: V23.01 - Demo

Topic 1 - Question Set 1

Question #1 Topic 1

DRAG DROP -

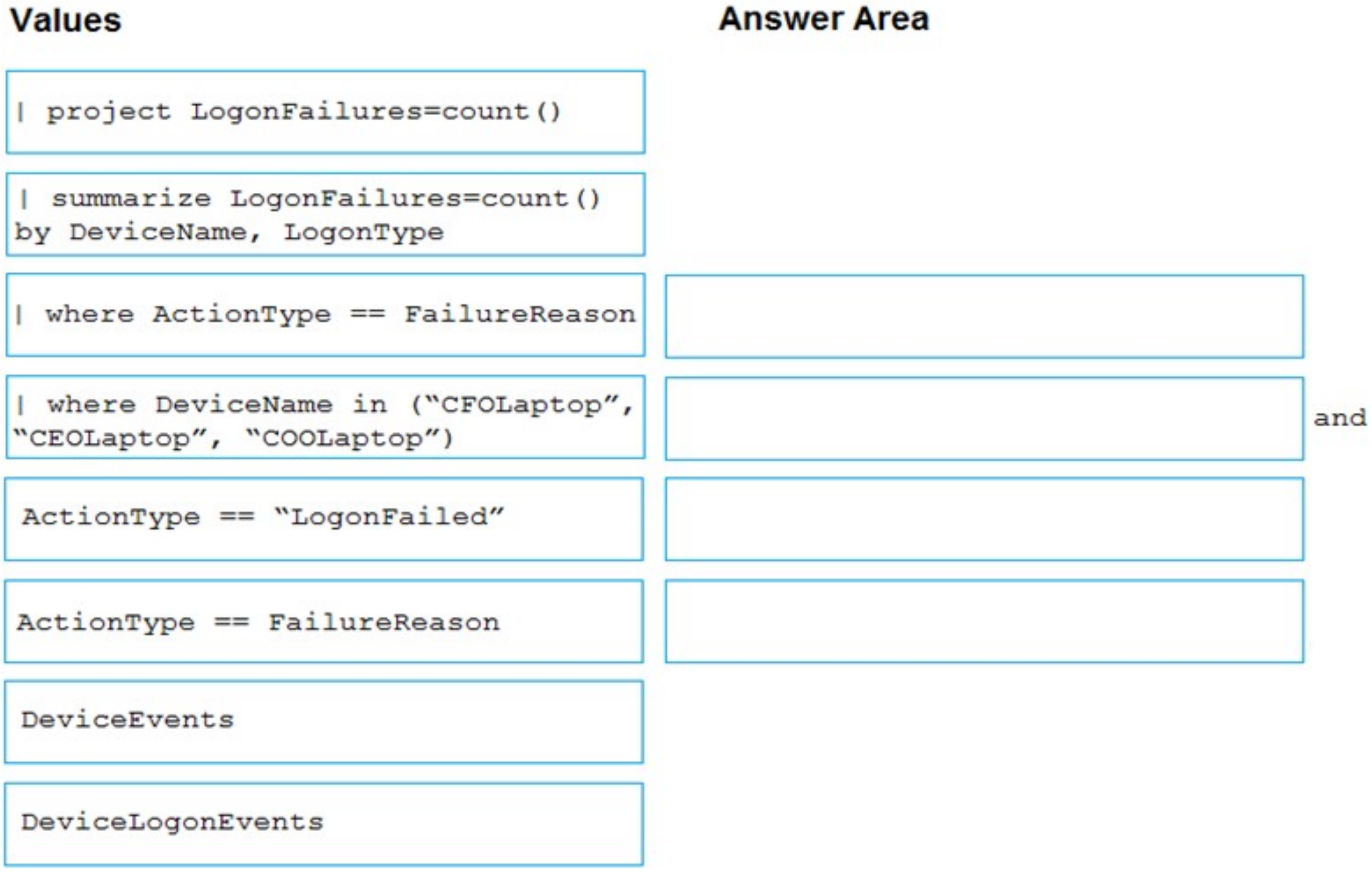
You are investigating an incident by using Microsoft 365 Defender.

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:



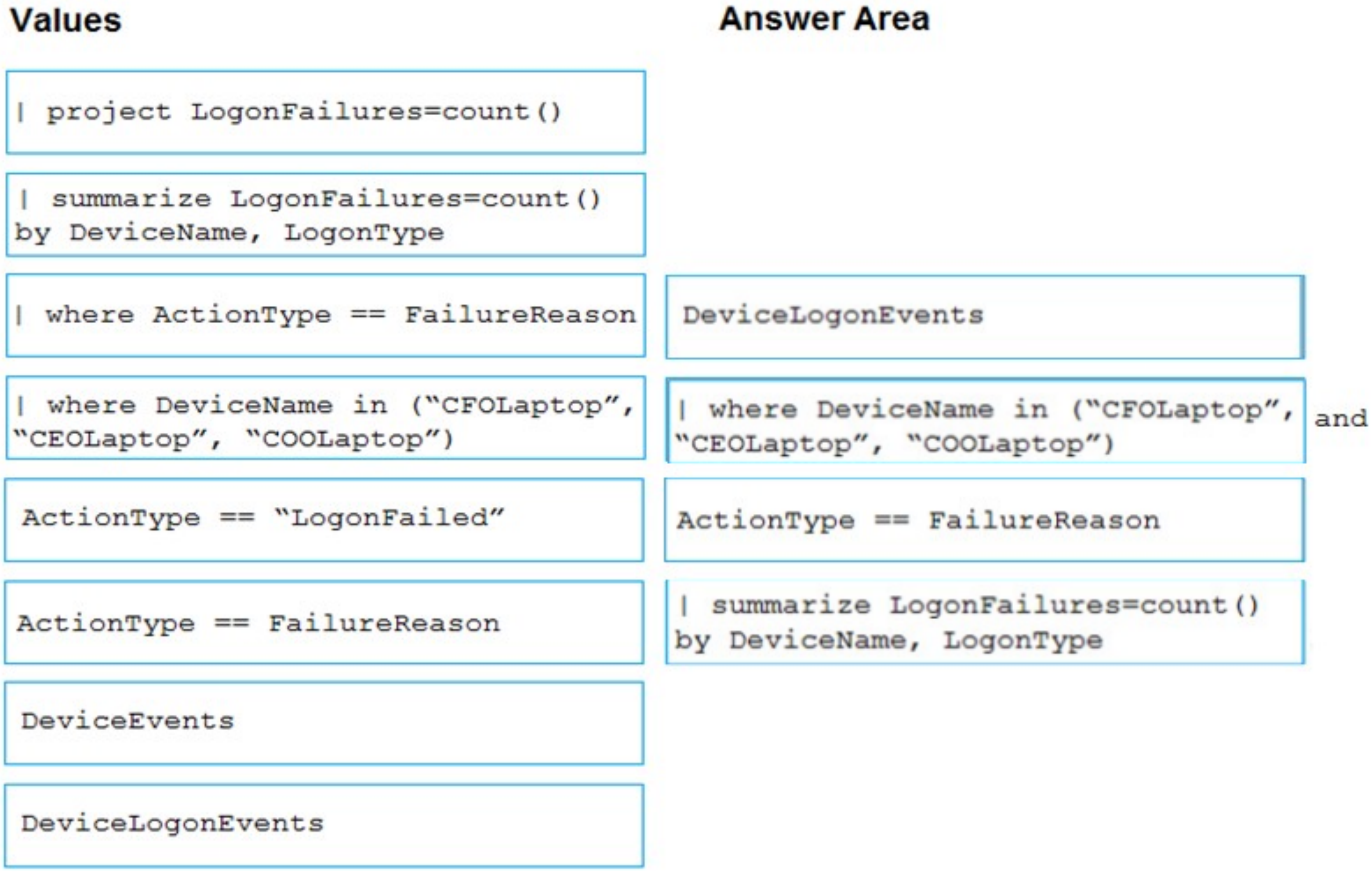
Values

```
| project LogonFailures=count()
| summarize LogonFailures=count()
by DeviceName, LogonType
| where ActionType == FailureReason
| where DeviceName in (“CFOLaptop”,
“CEOLaptop”, “COOLaptop”)
ActionType == “LogonFailed”
ActionType == FailureReason
DeviceEvents
DeviceLogonEvents
```

Answer Area

and

Correct Answer:



Values

```
| project LogonFailures=count()
| summarize LogonFailures=count()
by DeviceName, LogonType
| where ActionType == FailureReason
| where DeviceName in (“CFOLaptop”,
“CEOLaptop”, “COOLaptop”)
ActionType == “LogonFailed”
ActionType == FailureReason
DeviceEvents
DeviceLogonEvents
```

Answer Area

```
DeviceLogonEvents
| where DeviceName in (“CFOLaptop”,
“CEOLaptop”, “COOLaptop”)                and
ActionType == FailureReason
| summarize LogonFailures=count()
by DeviceName, LogonType
```

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

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.
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:
C

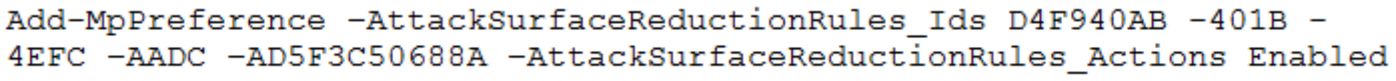
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

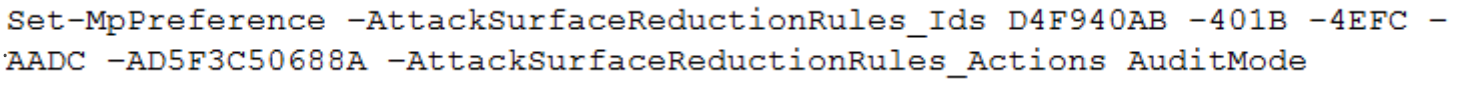
You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

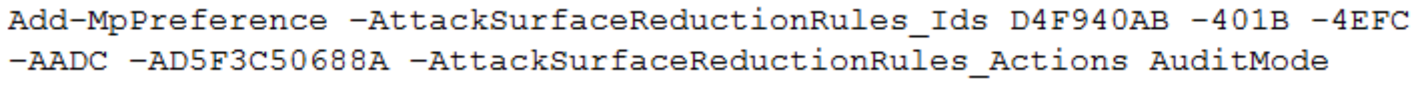
NOTE: Each correct selection is worth one point.

A.


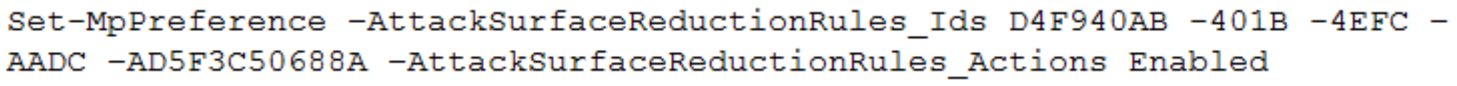
```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

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:

BC

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

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.

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:

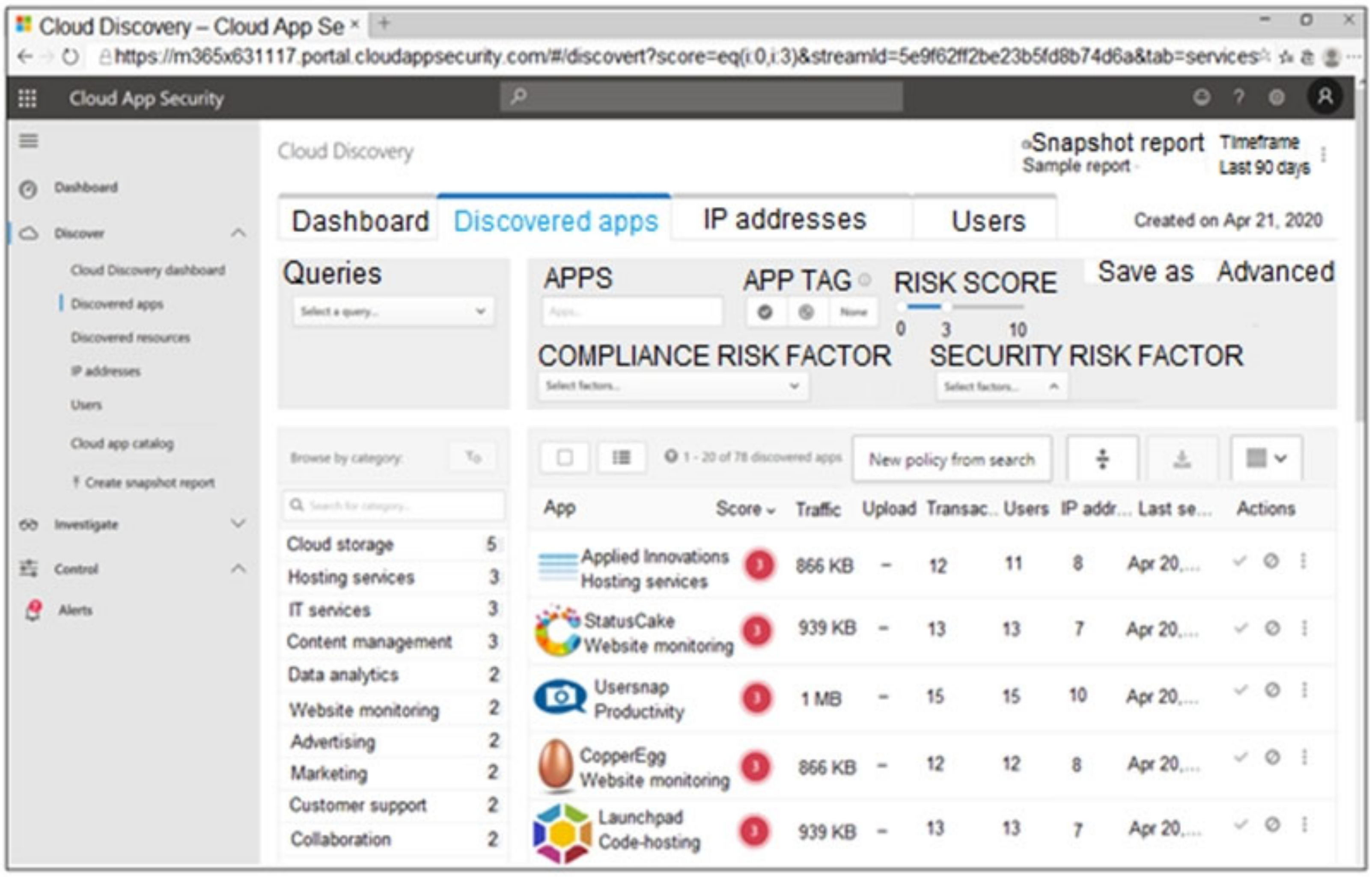
BCE

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

DRAG DROP -

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



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

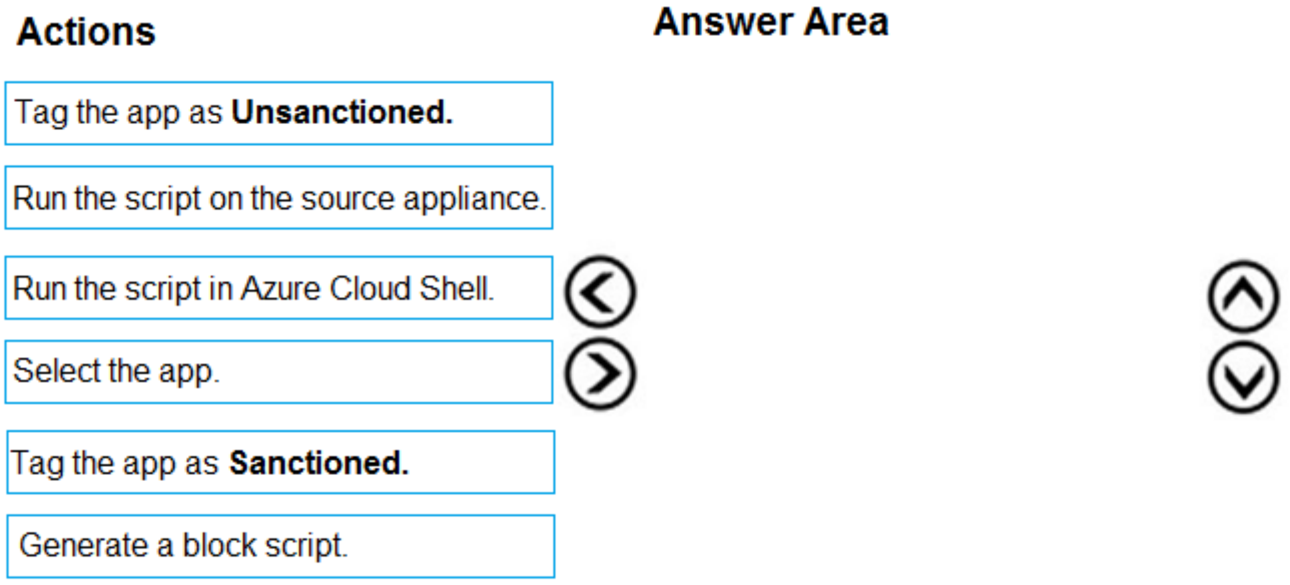
App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	–	12	11	8	Apr 20,...	✓ ⊘ ⋮
StatusCake Website monitoring	3	939 KB	–	13	13	7	Apr 20,...	✓ ⊘ ⋮
Usersnap Productivity	3	1 MB	–	15	15	10	Apr 20,...	✓ ⊘ ⋮
CopperEgg Website monitoring	3	866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

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.

Select and Place:

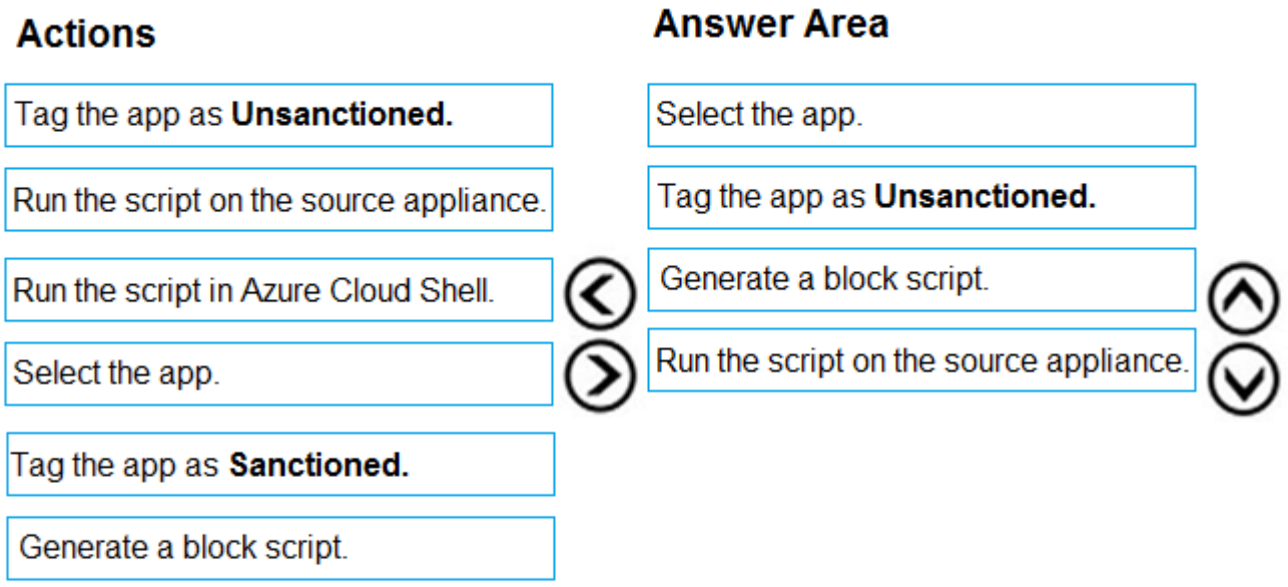


Actions

- 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

Correct Answer:



Actions

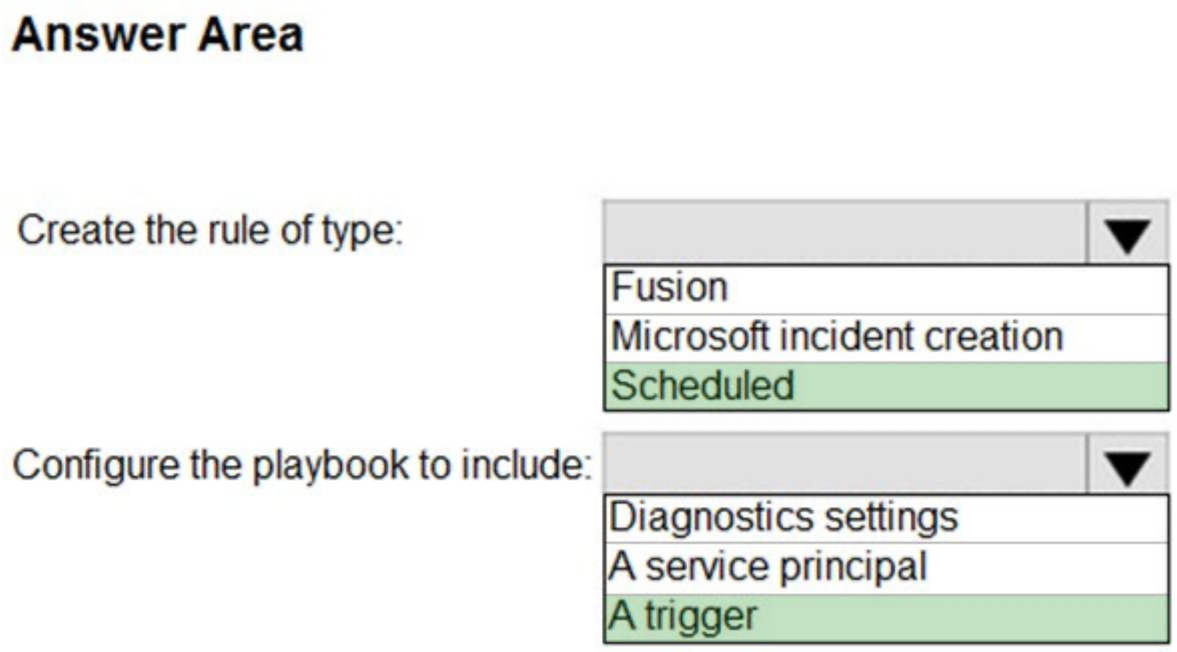
- Tag the app as **Unsanctioned.**
- Run the script on the source appliance.
- Run the script in Azure Cloud Shell.
- Select the app.
- Tag the app as **Sanctioned.**
- Generate a block script.

Answer Area

- Select the app.
- Tag the app as **Unsanctioned.**
- Generate a block script.
- Run the script on the source appliance.

Reference:

Correct Answer:



Answer Area

Create the rule of type:

- Fusion
- Microsoft incident creation
- [✓ Scheduled]

Configure the playbook to include:

- Diagnostics settings
- A service principal
- [✓ A trigger]

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule

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