Certification Provider: Microsoft
Exam: Microsoft Security Operations Analyst SC-200
Number of questions in the database: 178
Exam Version: April 7, 2023

Custom View Settings

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

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

Community vote distribution

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.
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 Most Voted

D. RegEx pattern matching Most Voted

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

Community vote distribution

D (59%) C (41%)

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: *BC*

Reference:

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

Next Questions →

Custom View Settings

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.

A. Resolve the alert automatically.

B. Hide the alert. Most Voted

C. Create a suppression rule scoped to any device.

D. Create a suppression rule scoped to a device group. Most Voted

E. Generate the alert. Most Voted

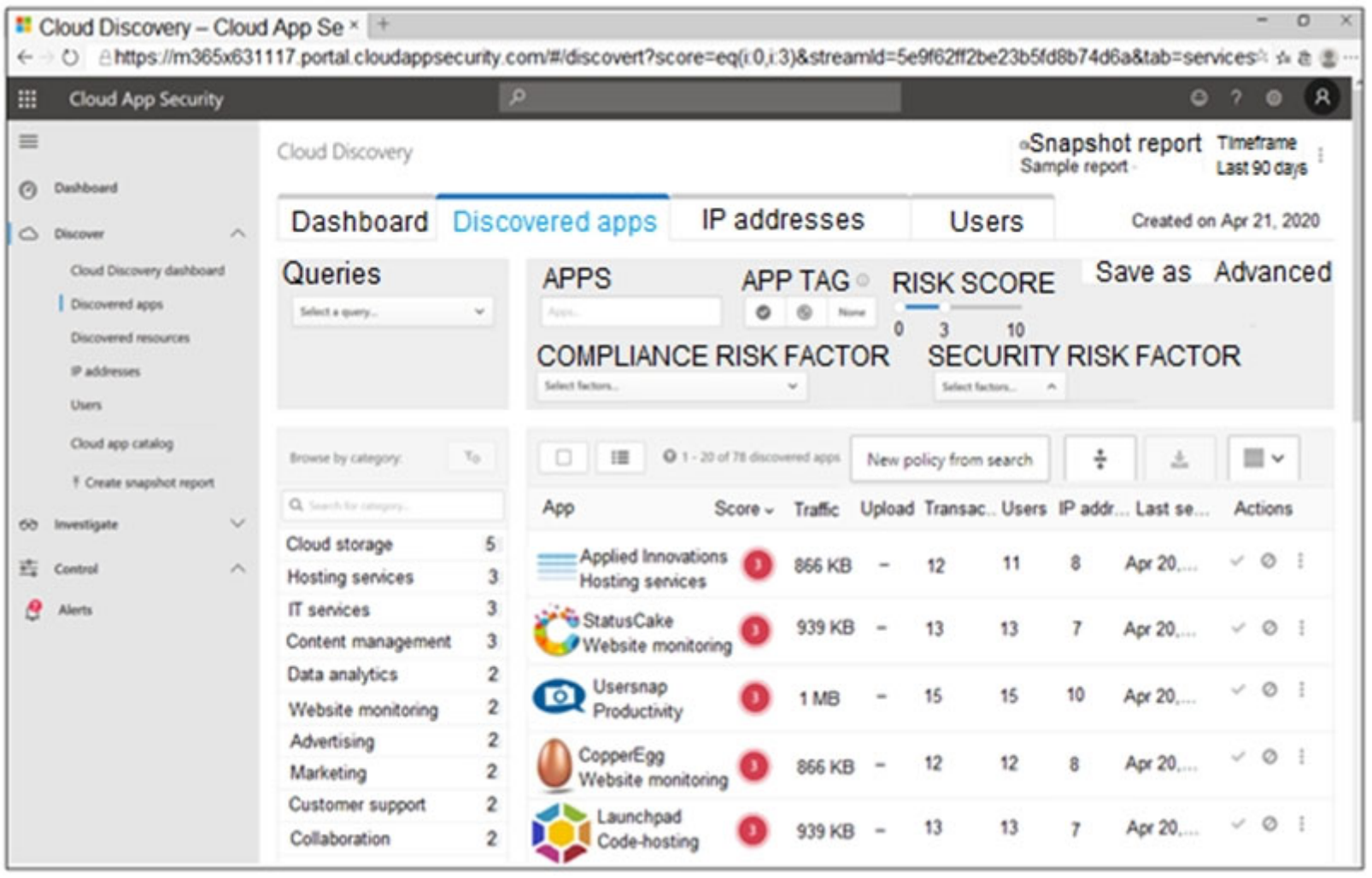
Correct Answer: *BCE*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

Community vote distribution
BDE (76%) BCE (15%) 9%

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.

Select and Place:

Actions	Answer Area
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.	

Correct Answer:

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

Reference:

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

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.

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:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [extend / join / project / union] (
    DeviceFileEvents
  | [extend / join / project / union] FileName, SHA256
  ) on SHA256
| [extend / join / project / union] 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

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. Most Voted

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. Most Voted

Correct Answer: *AE*

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

Community vote distribution

AE (94%) 6%

Custom View Settings

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. Assign a tag to the device group. Most Voted

B. Add the device users to the admin role.

C. Add a tag to the machines. Most Voted

D. Create a new device group that has a rank of 1. Most Voted

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

Community vote distribution
ACD (96%) 4%

Question #10 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Entity tags, you add the accounts as Honeytoken accounts.
Does this meet the goal?

A. Yes Most Voted

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution
A (100%)

Question #11 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Azure AD Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?

A. Yes

B. No Most Voted

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution

B (100%)

Question #12 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

A. Yes

B. No Most Voted

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution

B (100%)

Previous Questions Next Questions

Question #13 *Topic 1*

You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery Most Voted

B. Replace

C. Block and Enable redirect

D. Monitor and Enable redirect

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

Community vote distribution

A (100%)

Question #14 *Topic 1*

HOTSPOT -

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
let MaliciousEmails = [ ▼ ]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);
MaliciousEmails
| join ( [ ▼ ]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ ]
  select 20
  take 20
  top 20
```

Answer Area

```
let MaliciousEmails = [ ▼ ]
                      EmailAttachementInfo
                      EmailEvents
                      IdentityLogonEvents
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [ ▼ ]
         EmailAttachementInfo
         EmailEvents
         IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ ]
  select 20
  take 20
  top 20
```

Correct Answer:

Reference:

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

Question #15 *Topic 1*

You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only

B. a URL/domain indicator that has Action set to Alert and block

C. a file hash indicator that has Action set to Alert and block Most Voted

D. a certificate indicator that has Action set to Alert and block

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

Community vote distribution
C (100%)

Question #16 *Topic 1*

Your company deploys the following services:
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Office 365

You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.
Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

B. the Active remediation actions role in Microsoft Defender for Endpoint Most Voted

C. the Security Administrator role in Azure Active Directory (Azure AD)

D. the Security Reader role in Azure Active Directory (Azure AD) Most Voted

Correct Answer: *BD*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

Community vote distribution
BD (100%)

Previous Questions Next Questions

HOTSPOT -

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.

Hot Area:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

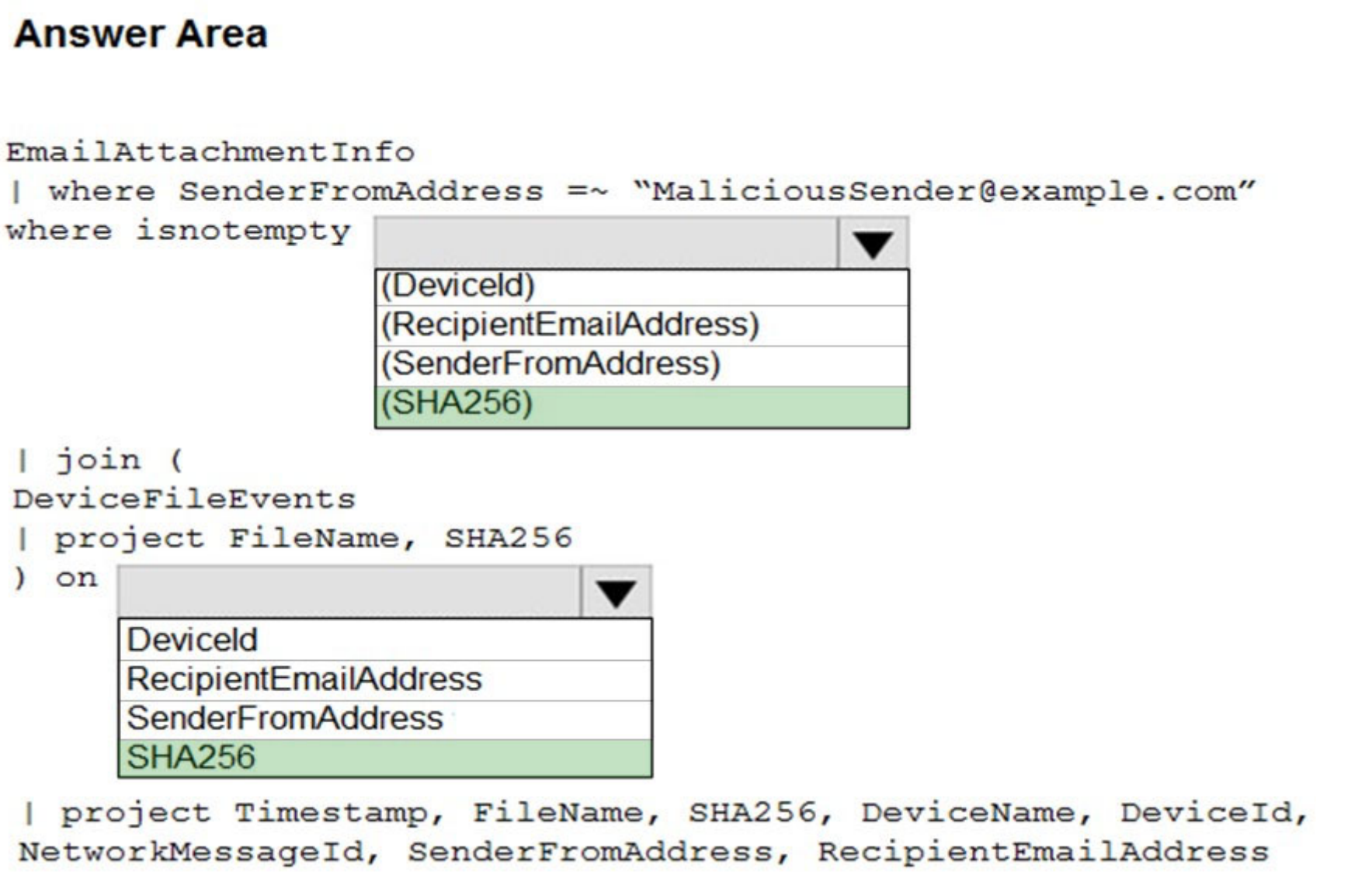
- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- DeviceId
- RecipientEmailAddress
- SenderFromAddress
- SHA256

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

Correct Answer:



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

Question #18 *Topic 1*

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.

B. Select Investigate files, and then filter App to Office 365.

C. Select Investigate files, and then select New policy from search.

D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings. Most Voted

E. From Settings, select Information Protection, select Files, and then enable file monitoring. Most Voted

F. Select Investigate files, and then filter File Type to Document.

Correct Answer: *DE*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Community vote distribution
DE (74%) CE (22%) 4%

HOTSPOT -

You purchase a Microsoft 365 subscription.

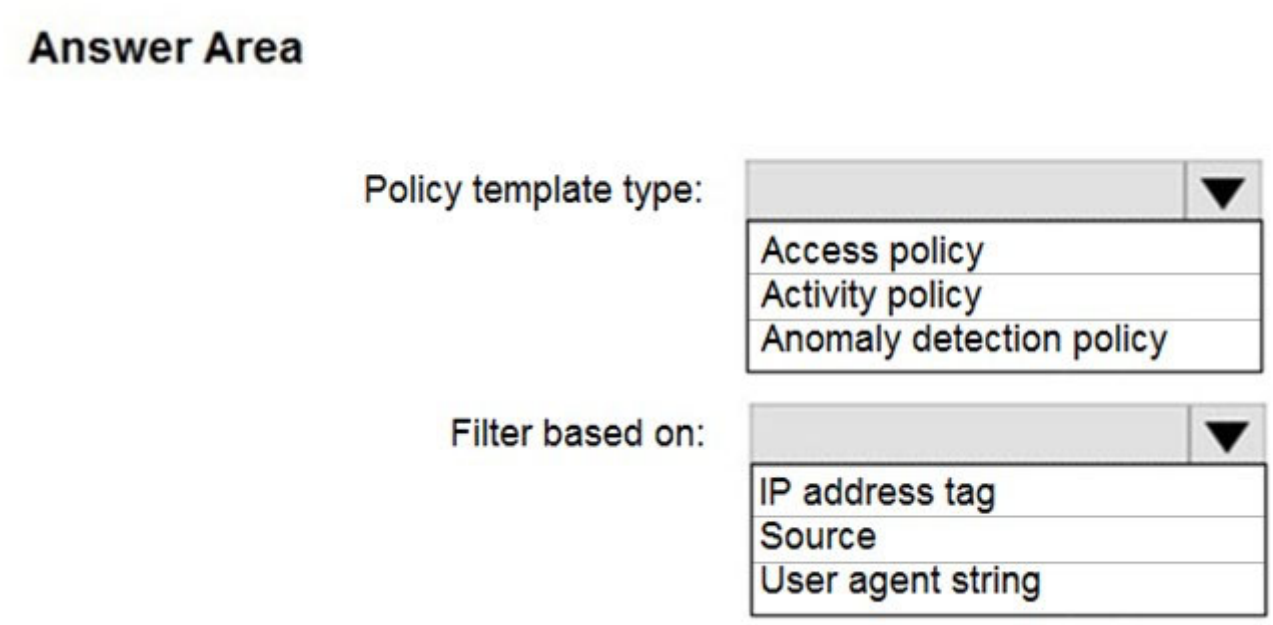
You plan to configure Microsoft Cloud App Security.

You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.

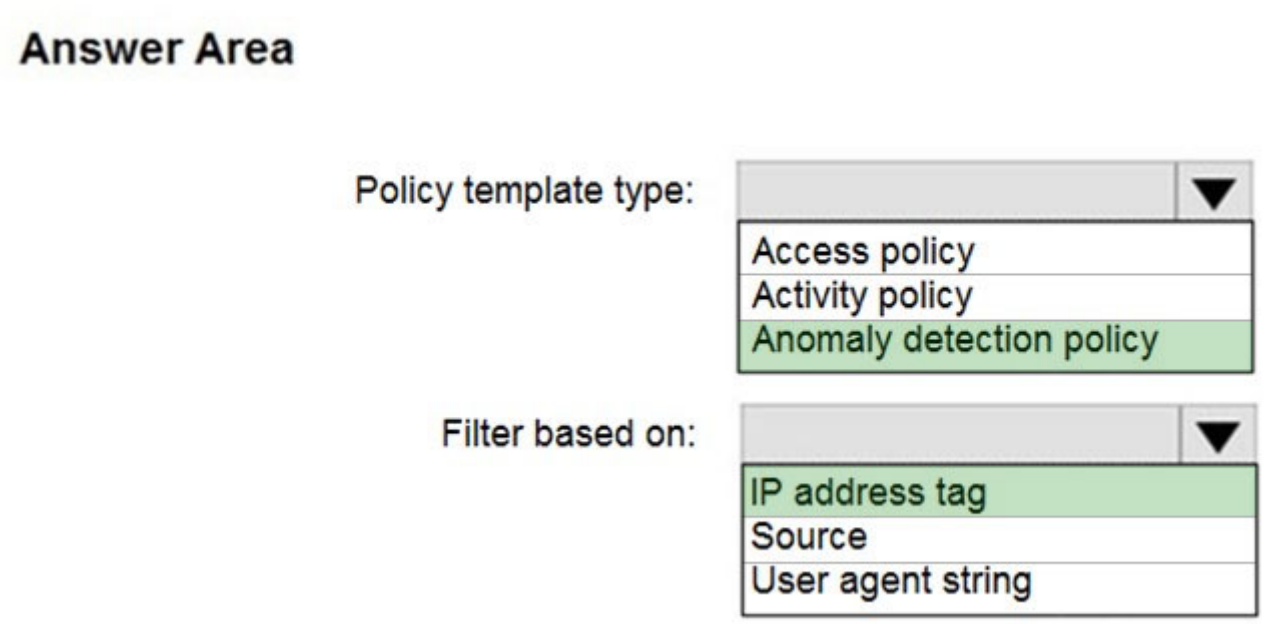
What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Question #20 *Topic 1*

Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely.
What should you include in the solution?

A. a fraud alert

B. a user risk policy

C. a named location Most Voted

D. a sign-in user policy

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution

C (100%)

Previous Questions

Next Questions

Custom View Settings

Question #21 *Topic 1*

You are configuring Microsoft Cloud App Security.
You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses.
You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.
You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure automatic data enrichment. Most Voted
B. Add the IP addresses to the corporate address range category. Most Voted
C. Increase the sensitivity level of the impossible travel anomaly detection policy.
D. Add the IP addresses to the other address range category and add a tag.
E. Create an activity policy that has an exclusion for the IP addresses.

Correct Answer: *AD*

Community vote distribution

AB (83%) Other

Question #22 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add each account as a Sensitive account.
Does this meet the goal?

A. Yes
B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution

B (100%)

Question #23 *Topic 1*

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.
What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365 Most Voted

B. the mailbox audit log in Exchange

C. the Safe Attachments file types report in Microsoft Defender for Office 365

D. the mail flow report in Exchange

Correct Answer: *A*
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Community vote distribution

A (100%)

Question #24 *Topic 1*

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
- Microsoft Excel macros that download scripts from untrusted websites
- Users that open executable attachments in Microsoft Outlook
- Outlook rules and forms exploits

What should you use?

A. Microsoft Defender Antivirus

B. attack surface reduction rules in Microsoft Defender for Endpoint Most Voted

C. Windows Defender Firewall

D. adaptive application control in Azure Defender

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

Community vote distribution

B (100%)

Previous Questions Next Questions

Question #25 *Topic 1*

You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Community vote distribution

B (100%)

DRAG DROP -

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

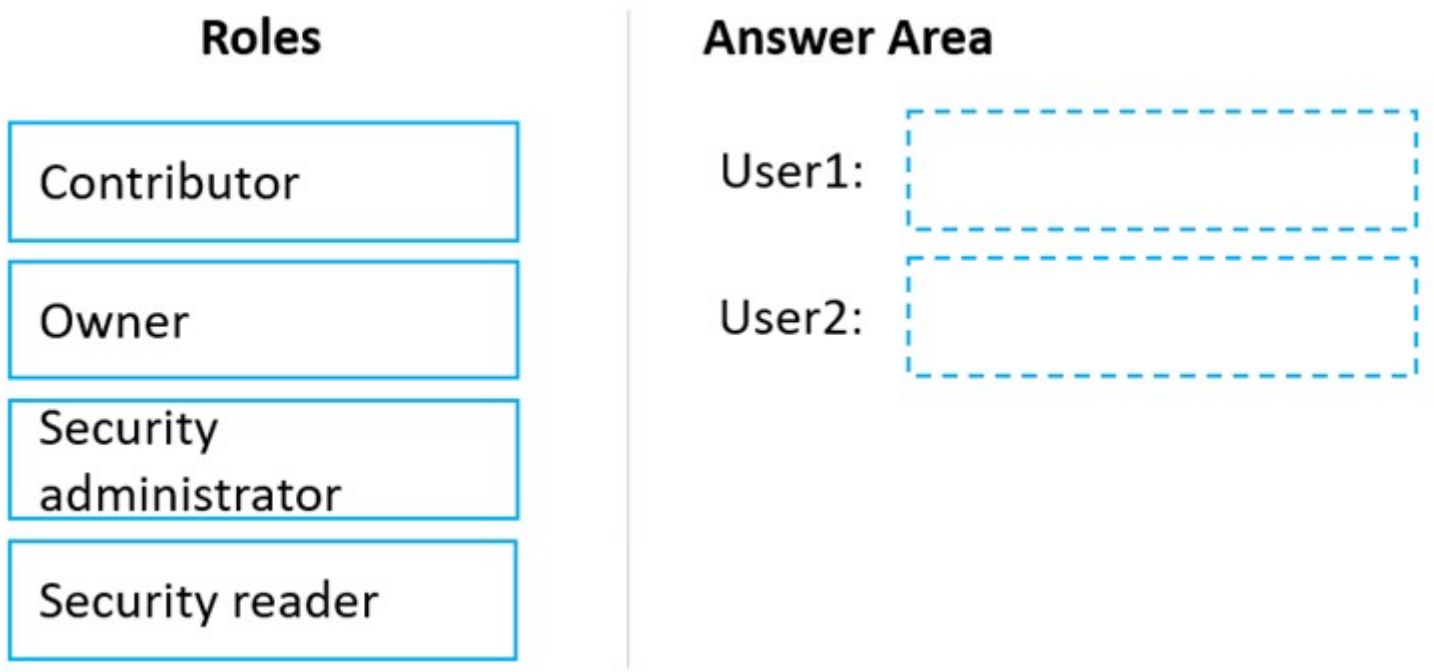
User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.

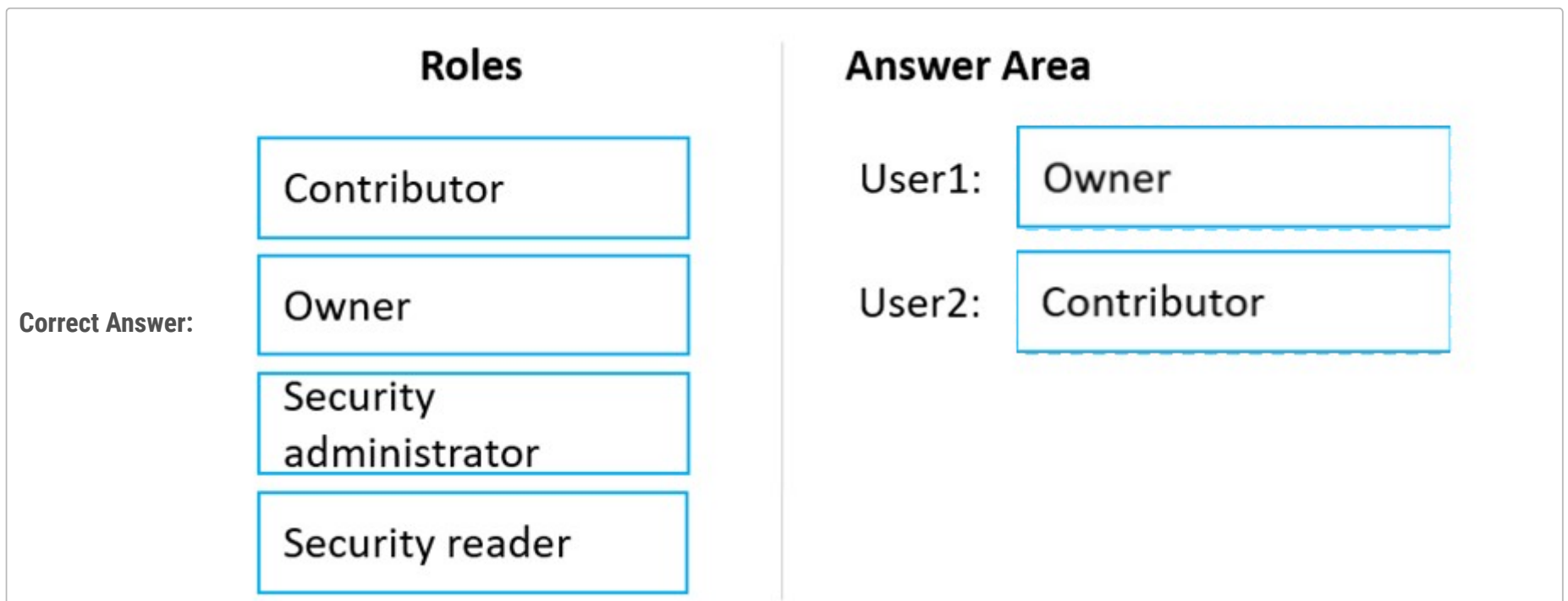
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

Select and Place:



Correct Answer:



Box 1: Owner -

Only the Owner can assign initiatives.

Box 2: Contributor -

Only the Contributor or the Owner can apply security recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

Question #27 *Topic 1*

HOTSPOT -
You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.
You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.
What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

To configure Microsoft Defender for Endpoint:
- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:
- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

Correct Answer:

Answer Area

To configure Microsoft Defender for Endpoint:
- Turn on endpoint detection and response (EDR) in block mode
- **Turn on Live Response**
- Turn off Tamper Protection

To configure the devices:
- **Add a network assessment job**
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

Box 1: Turn on Live Response -
Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 -
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldwide

HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  [ ]  kind=inner AlertEvidence on DeviceId
|  project AlertId
|  join AlertInfo on AlertId
|  [ ]  AlertId, Timestamp, Title, Severity, Category
```

- [ ]: extend / join / project
- [ ]: project / summarize / take

Correct Answer:

```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  [join]  kind=inner AlertEvidence on DeviceId
|  project AlertId
|  join AlertInfo on AlertId
|  [project]  AlertId, Timestamp, Title, Severity, Category
```

- [join]: extend / **join** / project
- [project]: **project** / summarize / take

Box 1: join -

An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

DeviceInfo -

//Query for devices that the potentially compromised account has logged onto

| where LoggedOnUsers contains '<account-name>'

| distinct DeviceId

//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables

| join kind=inner AlertEvidence on DeviceId

| project AlertId

//List all alerts on devices that user has logged on to

| join AlertInfo on AlertId

| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"

Box 2: project -
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

Previous Questions

Next Questions

Custom View Settings

Question #29 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.
You delete users from the subscription.
You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.
What should you use?

A. a file policy in Microsoft Defender for Cloud Apps

B. an access review policy

C. an alert policy in Microsoft Defender for Office 365

D. an insider risk policy Most Voted

Correct Answer: *C*
Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.
Default alert policies include:
Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Community vote distribution

D (100%)

Question #30 *Topic 1*

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days.
What should you use?

A. the Incidents blade of the Microsoft 365 Defender portal

B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center

C. Activity explorer in the Microsoft 365 compliance center

D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Correct Answer: *C*
Labeling activities are available in Activity explorer.
For example:

Sensitivity label applied -
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.
It is captured at the time of save in Office native applications and web applications.
It is captured at the time of occurrence in Azure Information protection add-ins.
Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

Community vote distribution

C (100%)

Question #31 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations

B. Devices

C. Evidence and Response Most Voted

D. Alerts Most Voted

Correct Answer: *C*
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Incorrect:
* The Investigations tab lists all the automated investigations triggered by alerts in this incident. Automated investigations will perform remediation actions or wait for analyst approval of actions, depending on how you configured your automated investigations to run in Defender for Endpoint and Defender for Office 365.
* Devices
The Devices tab lists all the devices related to the incident.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

Community vote distribution

C (63%) D (38%)

Question #32 *Topic 1*

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A. the Modifications of sensitive groups report in Microsoft Defender for Identity

B. the identity security posture assessment in Microsoft Defender for Cloud Apps

C. the Azure Active Directory Provisioning Analysis workbook

D. the Overview settings of Insider risk management

Correct Answer: *A*

Community vote distribution

A (100%)

Previous Questions

Next Questions

Custom View Settings

Question #33 *Topic 1*

You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.

You need to identify the impacted entities in an aggregated alert.

What should you review in the DLP alert management dashboard of the Microsoft 365 compliance center?

A. the Events tab of the alert Most Voted

B. the Sensitive Info Types tab of the alert

C. Management log

D. the Details tab of the alert

Correct Answer: *C*

Community vote distribution

A (86%) 14%

Question #34 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Threat analytics

B. Advanced Hunting

C. Explorer

D. Policies & rules

Correct Answer: *B*

Community vote distribution

B (100%)

Question #35 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.34.32-171.23.34.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

A. Create an import file that contains the individual IP addresses in the range. Select Import and import the file. Most Voted

B. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.

C. Select Add indicator and set the IP address to 171.23.34.32-171.23.34.63.

D. Select Add indicator and set the IP address to 171.23.34.32/27.

Correct Answer: *A*

Community vote distribution

A (75%) B (25%)

Question #36 *Topic 1*

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addressed and URLs.

What should you enable first in the Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. custom network indicators

B. live response for servers

C. endpoint detection and response (EDR) in block mode

D. web content filtering

Correct Answer: *A*

Community vote distribution

A (100%)

Previous Questions Next Questions

Question #37 *Topic 1*

DRAG DROP
-

You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

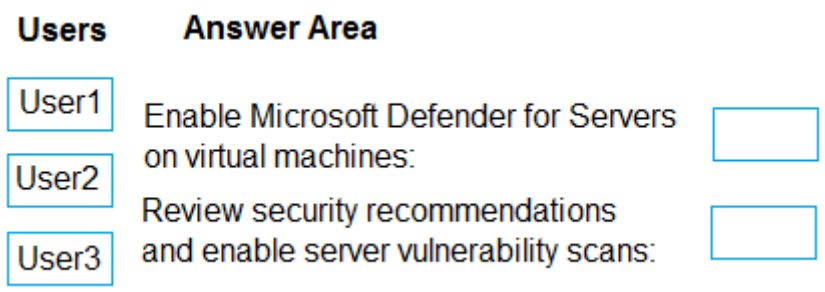
You need to delegate the following tasks:

• Enable Microsoft Defender for Servers on virtual machines.
• Review security recommendations and enable server vulnerability scans.

The solution must use the principle of least privilege.

Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Answer Area

Correct Answer:

Enable Microsoft Defender for Servers on virtual machines: User1

Review security recommendations and enable server vulnerability scans: User2

Question #38 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

• Only show emails sent during the last hour.
• Optimize query performance.

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
[ ▼ ]
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ ▼ ]
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

Correct Answer:

Answer Area

```
EmailAttachmentInfo
[ ▼ ]
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ ▼ ]
| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)
```

Question #39 *Topic 1*

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk.

What should you do?

A. Disable legacy protocols on the computers listed as exposed entities.

B. Enforce LDAP signing on the computers listed as exposed entities.

C. Modify the properties of the computer objects listed as exposed entities. Most Voted

D. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.

Correct Answer: *C*

Community vote distribution

C (100%)

Question #40 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

A remediation action for an automated investigation quarantines a file across multiple devices.

You need to mark the file as safe and remove the file from quarantine on the devices.

What should you use in the Microsoft 365 Defender portal?

A. From the History tab in the Action center, revert the actions.

B. From the investigation page, review the AIR processes.

C. From Quarantine from the Review page, modify the rules.

D. From Threat tracker, review the queries.

Correct Answer: *A*

Community vote distribution

A (100%)

Previous Questions

Next Questions

Custom View Settings

Question #41 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort.

Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting

B. Threat analytics

C. Incidents & alerts

D. Learning hub

Correct Answer: *B*

Community vote distribution

B (100%)

Topic 2 - Question Set 2

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.

Does this meet the goal?

A. Yes

B. No Most Voted

Correct Answer: *B*

You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution

B (88%) 13%

Question #2 *Topic 2*

You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall. Most Voted

C. Create an application security group.

D. Modify the access policy for the key vault.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

Community vote distribution

B (100%)

Question #3 *Topic 2*

HOTSPOT -

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Workflow automation
- Security alerts

Correct Answer:

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Workflow automation
- Security alerts

Reference:

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

Question #4 *Topic 2*

You have a Microsoft 365 subscription that uses Azure Defender.
You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1 Most Voted

D. the Owner role for RG1

Correct Answer: *C*

Community vote distribution

C (100%)

Question #5 *Topic 2*

You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.
Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n Most Voted

B. ./alerttest testing eicar pipe

C. cp /bin/echo ./alerttest

D. ./asc_alerttest_662jfi039n testing eicar pipe Most Voted

Correct Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-

Community vote distribution

AD (100%)

Question #6 *Topic 2*

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Azure Security Center and configure Security Center to use workspace1.

You need to collect security event logs from the Azure virtual machines that report to workspace1.

What should you do?

A. From Security Center, enable data collection Most Voted

B. In sub1, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace1, create a workbook.

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Community vote distribution

A (100%)

Custom View Settings

Question #7 *Topic 2*

DRAG DROP -

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines.

The solution must validate the configuration.

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

Select and Place:

Actions	Answer Area
Change the alert severity threshold for emails to **Medium**.	
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	
Enable Azure Defender for the subscription.	
Change the alert severity threshold for emails to **Low**.	
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

Correct Answer:

Actions	Answer Area
Change the alert severity threshold for emails to **Medium**.	Enable Azure Defender for the subscription.
Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.	Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
Enable Azure Defender for the subscription.	Run the executable file and specify the appropriate arguments.
Change the alert severity threshold for emails to **Low**.	
Run the executable file and specify the appropriate arguments.	
Rename the executable file as AlertTest.exe.	

Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

Question #8 *Topic 2*

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

A. Security solutions

B. Security policy

C. Pricing & settings Most Voted

D. Security alerts

E. Azure Defender

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

Community vote distribution

C (100%)

Question #9 *Topic 2*

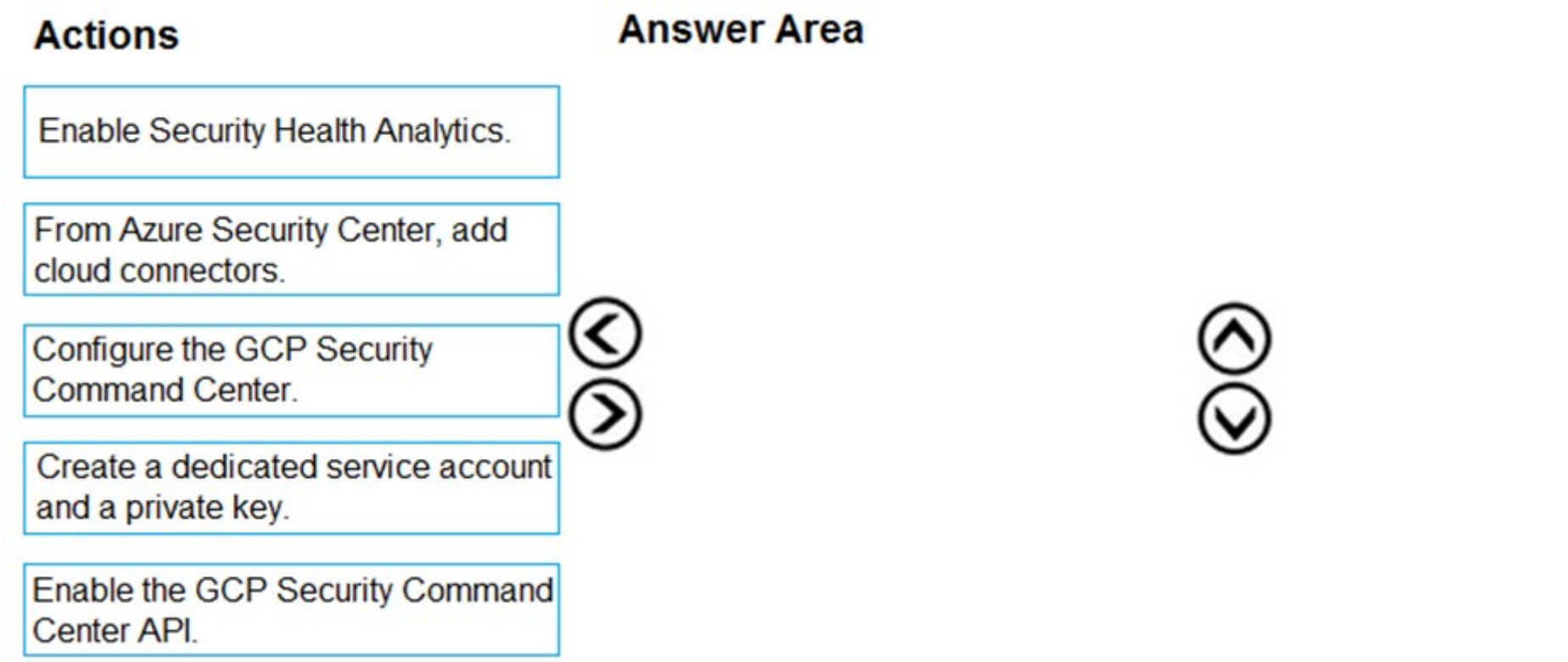
DRAG DROP -

You have resources in Azure and Google cloud.

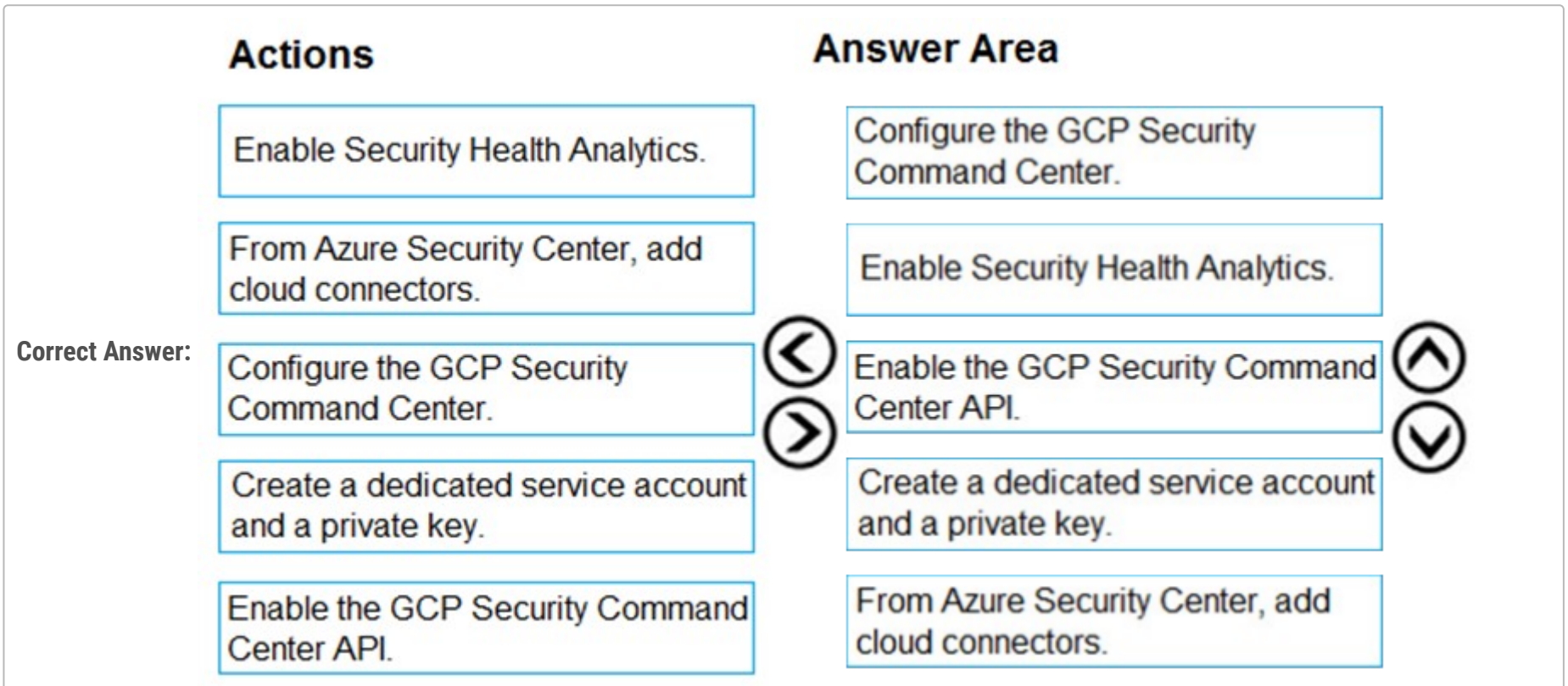
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

Question #10 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Regulatory compliance, you download the report.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution

B (100%)

Custom View Settings

Question #11 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.
Does this meet the goal?

A. Yes Most Voted

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution

A (100%)

Question #12 *Topic 2*

You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.
To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

D. Azure Data Lake

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal

Community vote distribution

C (100%)

Question #13 *Topic 2*

You are responsible for responding to Azure Defender for Key Vault alerts.

During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.

What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks

B. Azure Active Directory (Azure AD) permissions

C. role-based access control (RBAC) for the key vault

D. the access policy settings of the key vault

Correct Answer: *A*

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

Community vote distribution

A (100%)

Question #14 *Topic 2*

HOTSPOT -

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
"resources": [
   {
     "type": "                    /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                    /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Answer Area

```
"resources": [
   {
     "type": "                    /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                    /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Microsoft.Automation
Microsoft.Logic
Microsoft.Security

Correct Answer:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

Custom View Settings

Question #15 *Topic 2*

You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level

B. at the workspace level

C. at the resource level

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

Community vote distribution
A (100%)

Question #16 *Topic 2*

You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation. Most Voted

B. Create an Azure logic app that has a manual trigger.

C. Create an Azure logic app that has an Azure Security Center alert trigger. Most Voted

D. Create an Azure logic app that has an HTTP trigger.

E. From Azure Active Directory (Azure AD), add an app registration.

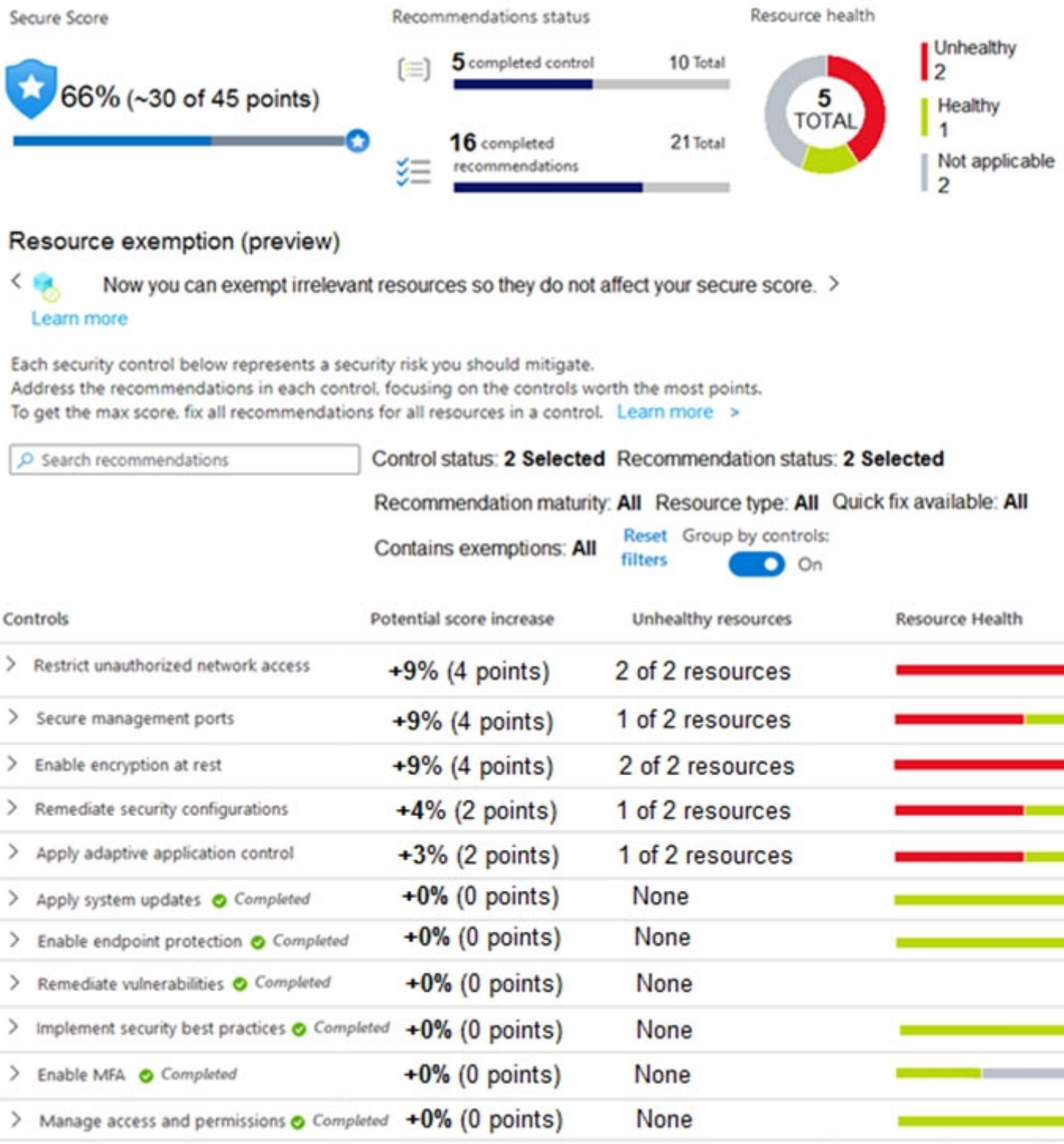
Correct Answer: *AC*
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Community vote distribution
AC (100%)

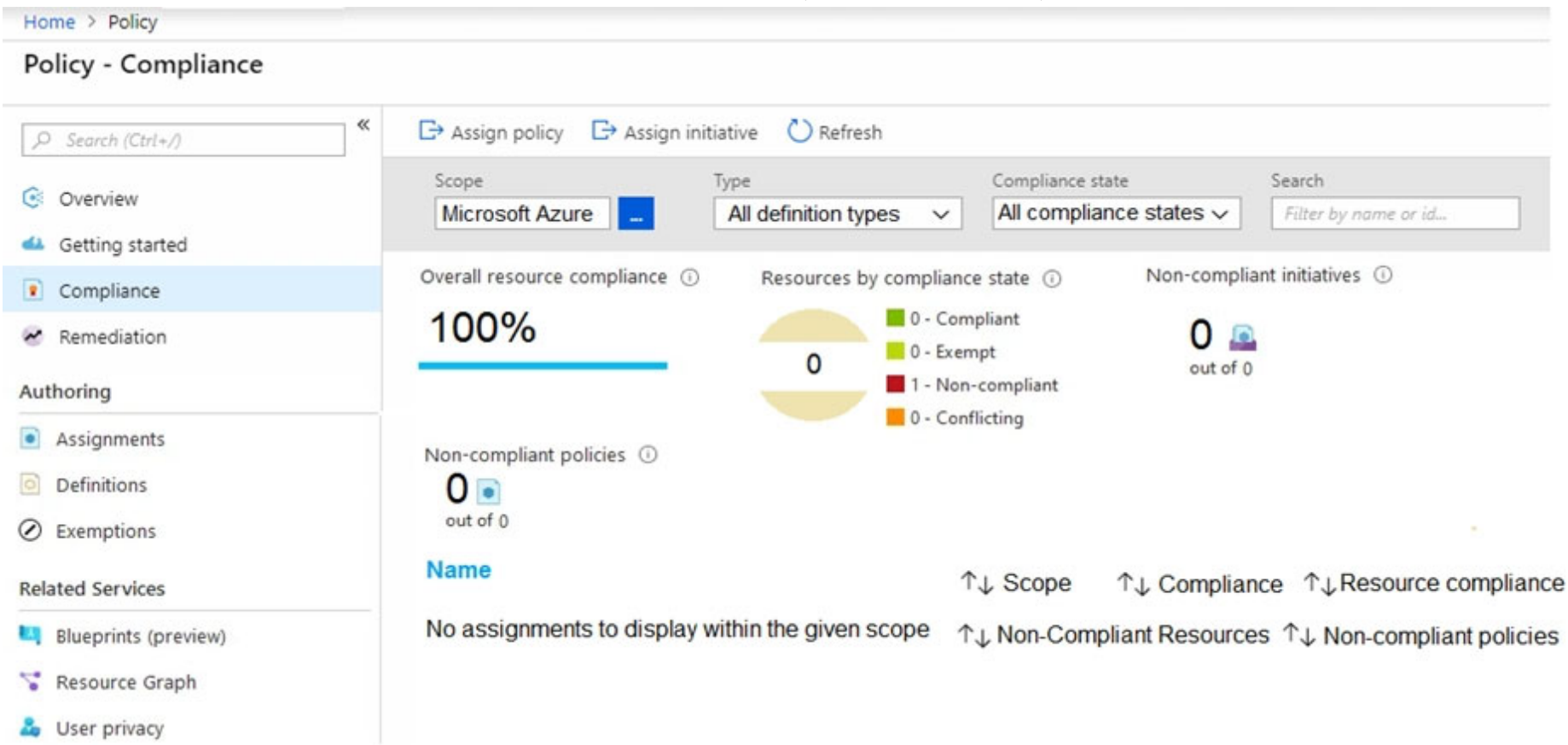
HOTSPOT -

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Answer Area

Statements	Yes	No
Correct Answer: Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

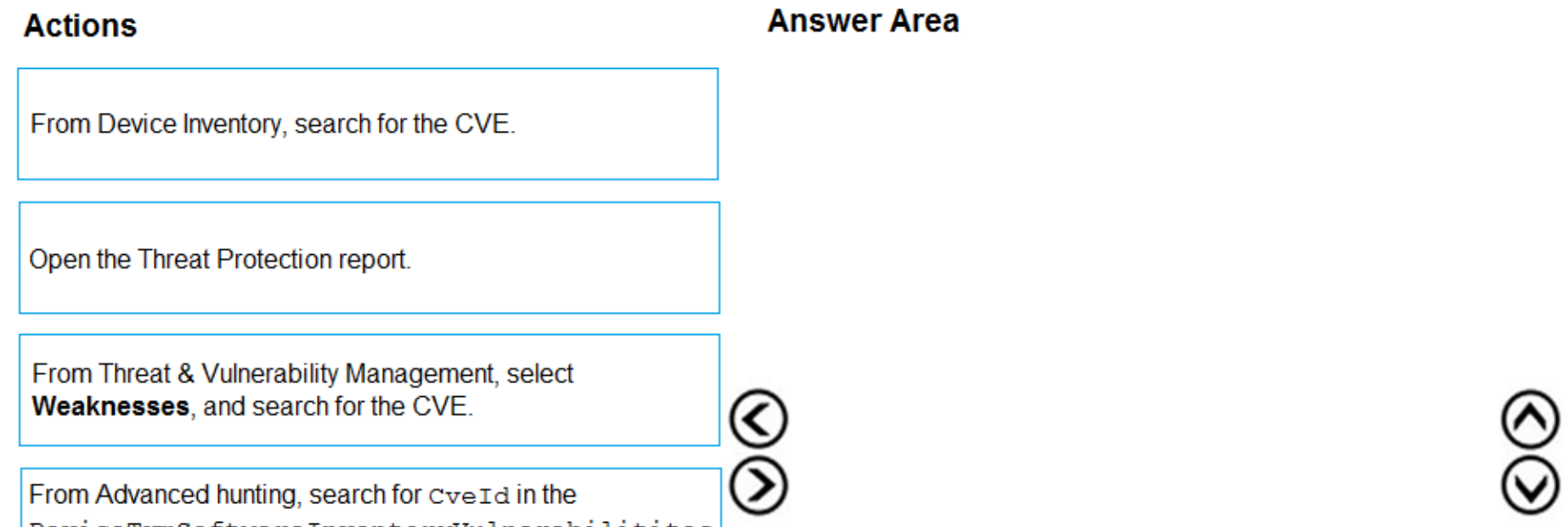
DRAG DROP -

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

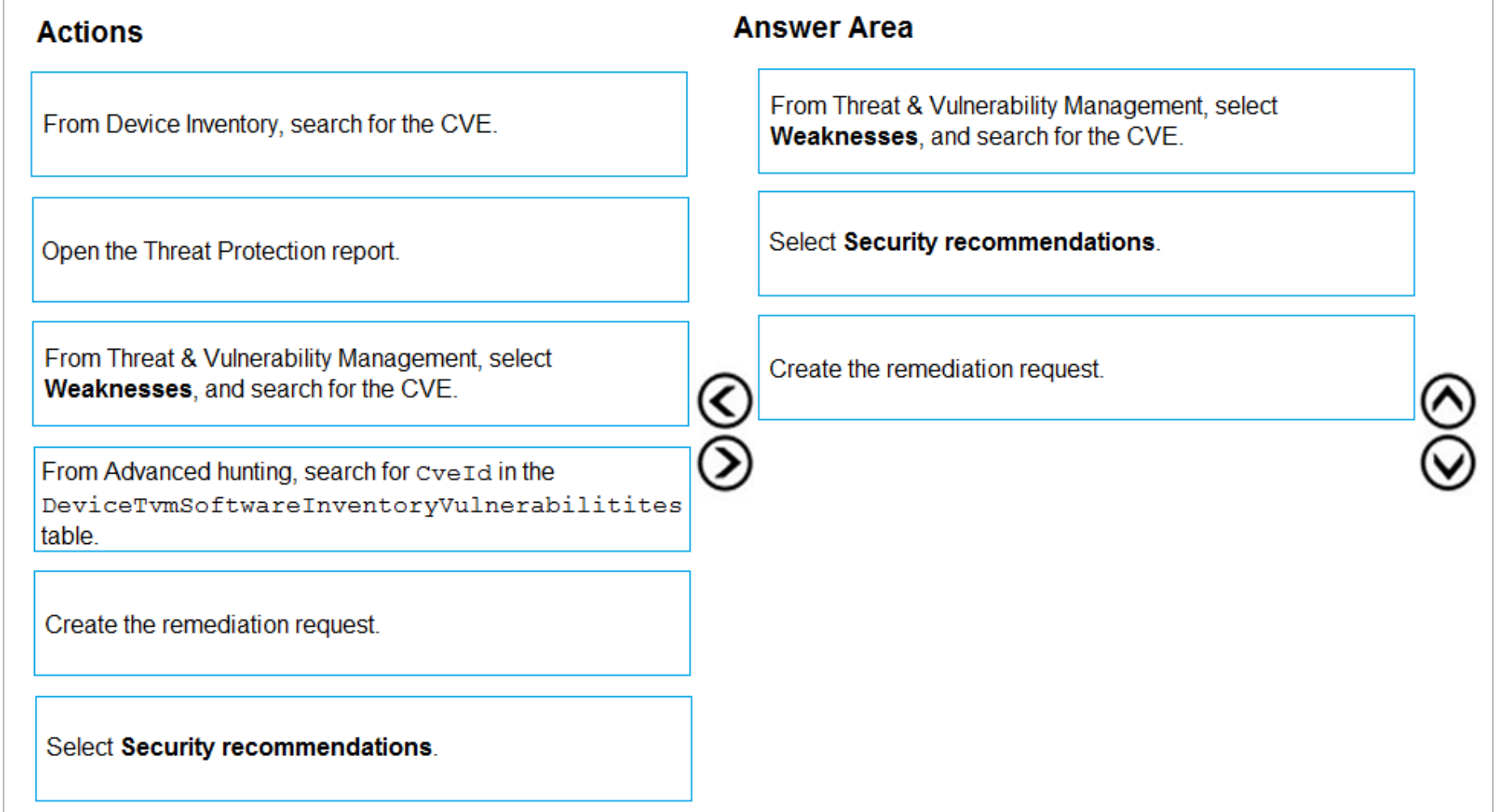
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three 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:



Correct Answer:



Reference:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

Custom View Settings

Question #19 *Topic 2*

You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.

B. From Security alerts, select Take Action, and then expand the Mitigate the threat section. Most Voted

C. From Regulatory compliance, download the report.

D. From Recommendations, download the CSV report.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution
B (85%) A (15%)

Question #20 *Topic 2*

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.

B. Change the state of the suppression rule to Disabled.

C. Modify the filter for the Security alerts page. Most Voted

D. View the Windows event logs on the virtual machines.

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

Community vote distribution
C (77%) B (23%)

Question #21 *Topic 2*

HOTSPOT -

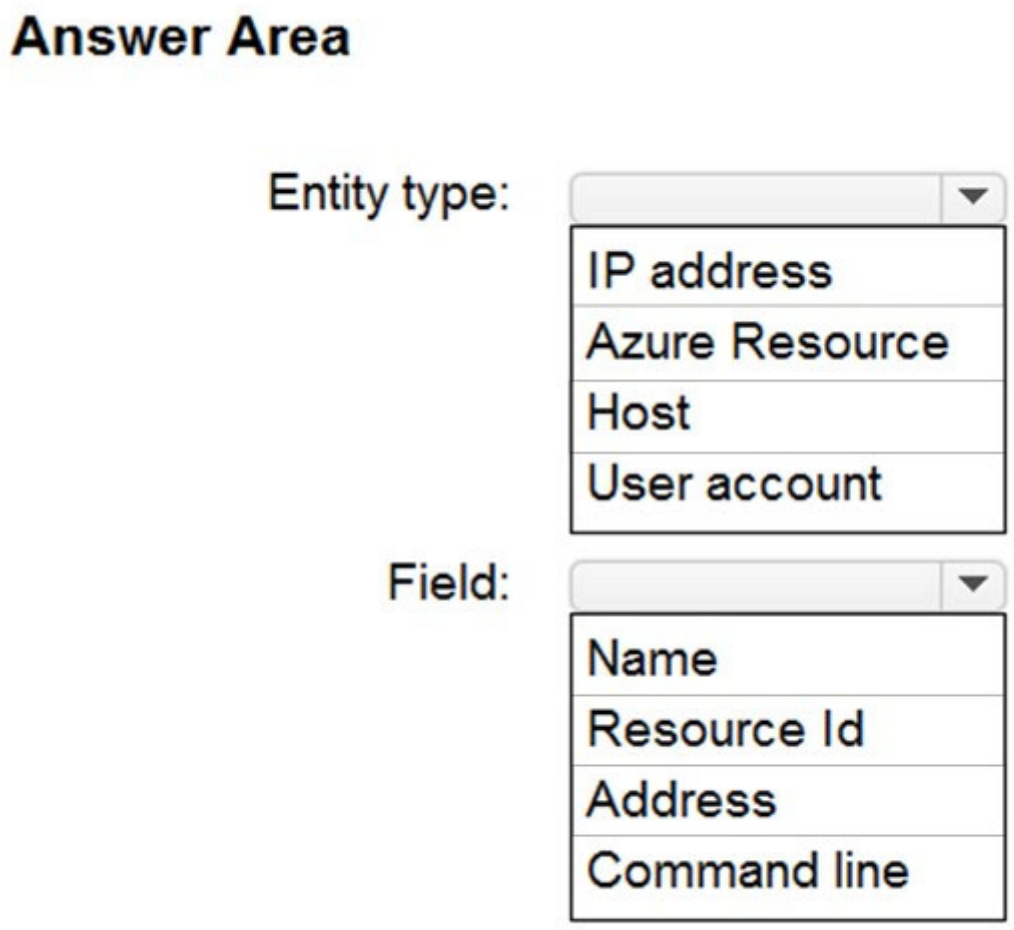
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.

You need to hide Azure Defender alerts for the storage account.

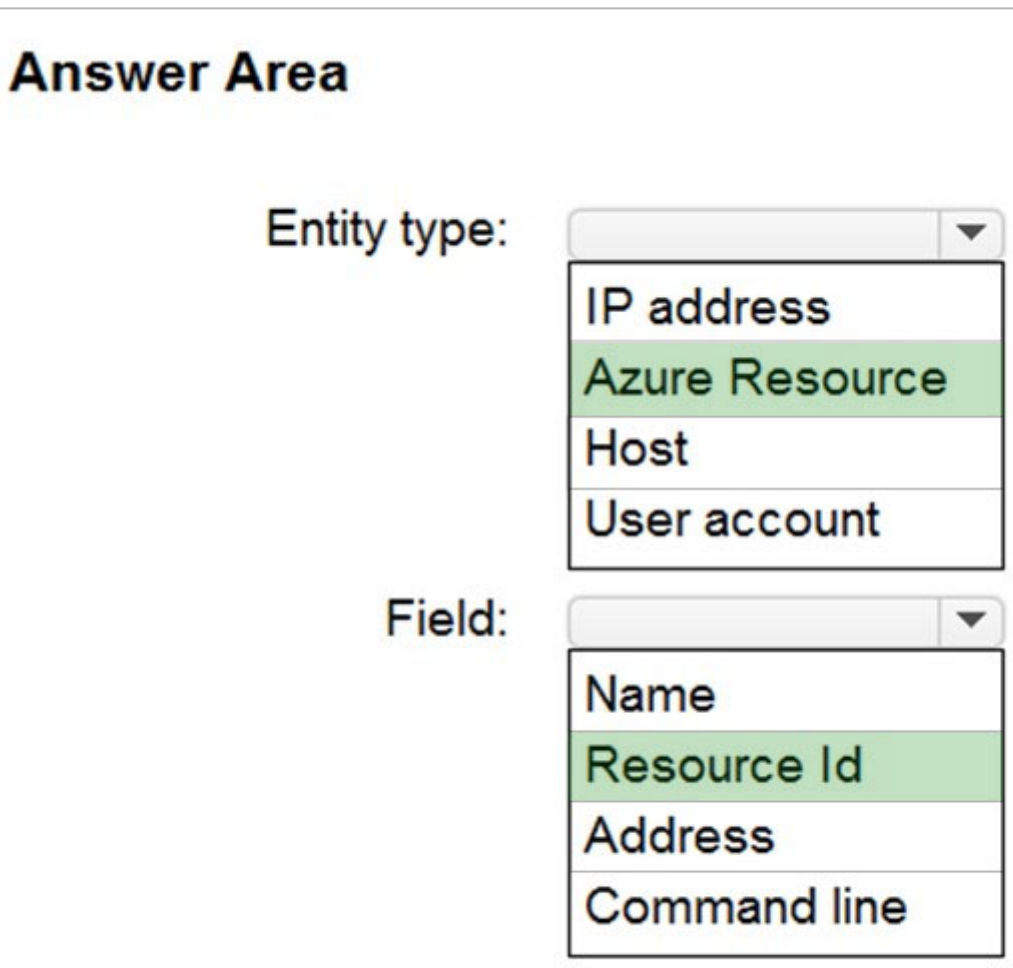
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

Question #22 *Topic 2*

You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers.
What should you do on the on-premises computers?

A. Install the Log Analytics agent. Most Voted

B. Install the Dependency agent.

C. Configure the Hybrid Runbook Worker role.

D. Install the Connected Machine agent.

Correct Answer: *A*
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
☞ The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
☞ Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Community vote distribution

A (100%)

Question #23 *Topic 2*

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in
Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

A. the severity level of email notifications

B. a cloud connector

C. the Azure Defender plans

D. the integration settings for Threat detection

Correct Answer: *A*
Reference:
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

Community vote distribution

A (100%)

DRAG DROP -

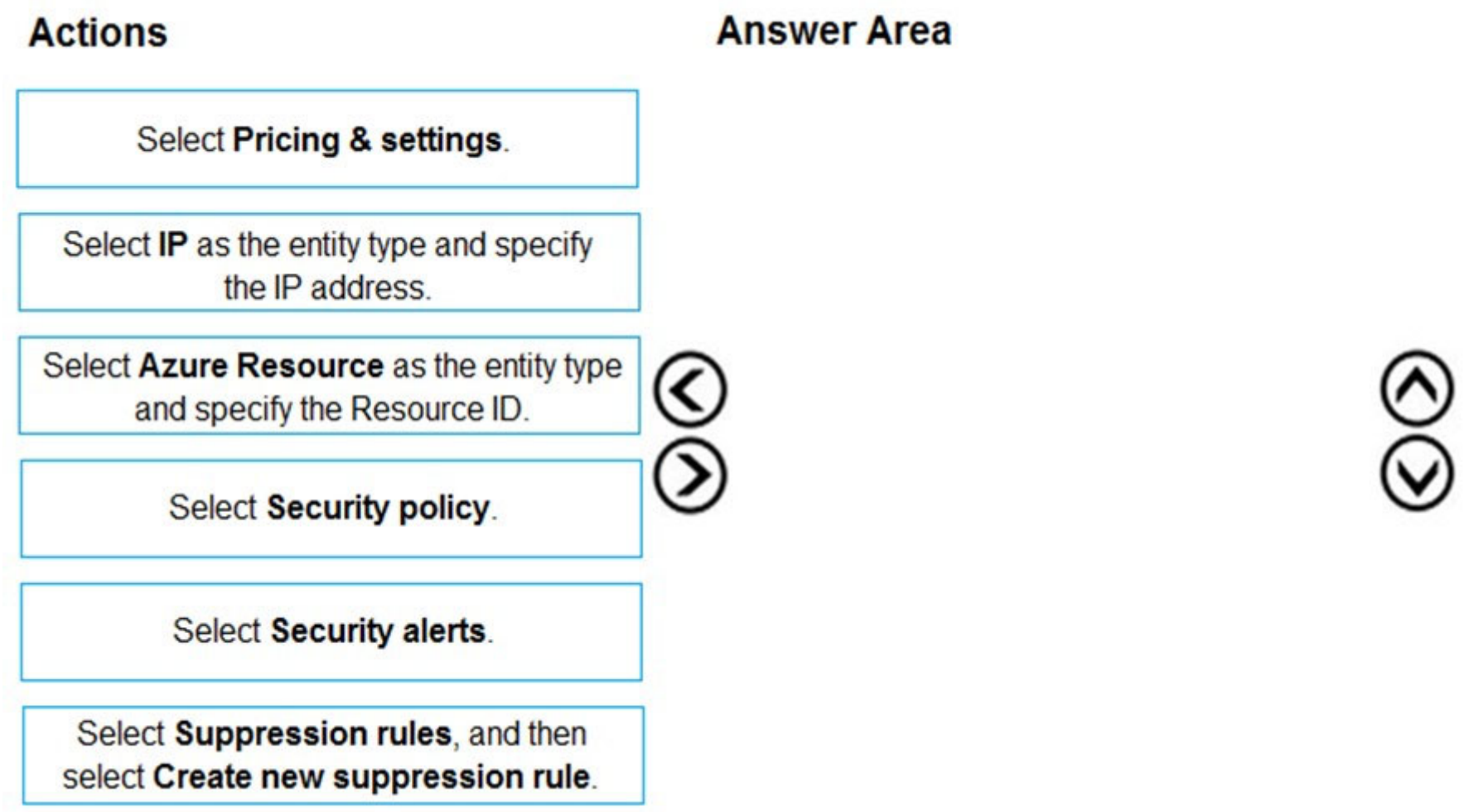
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

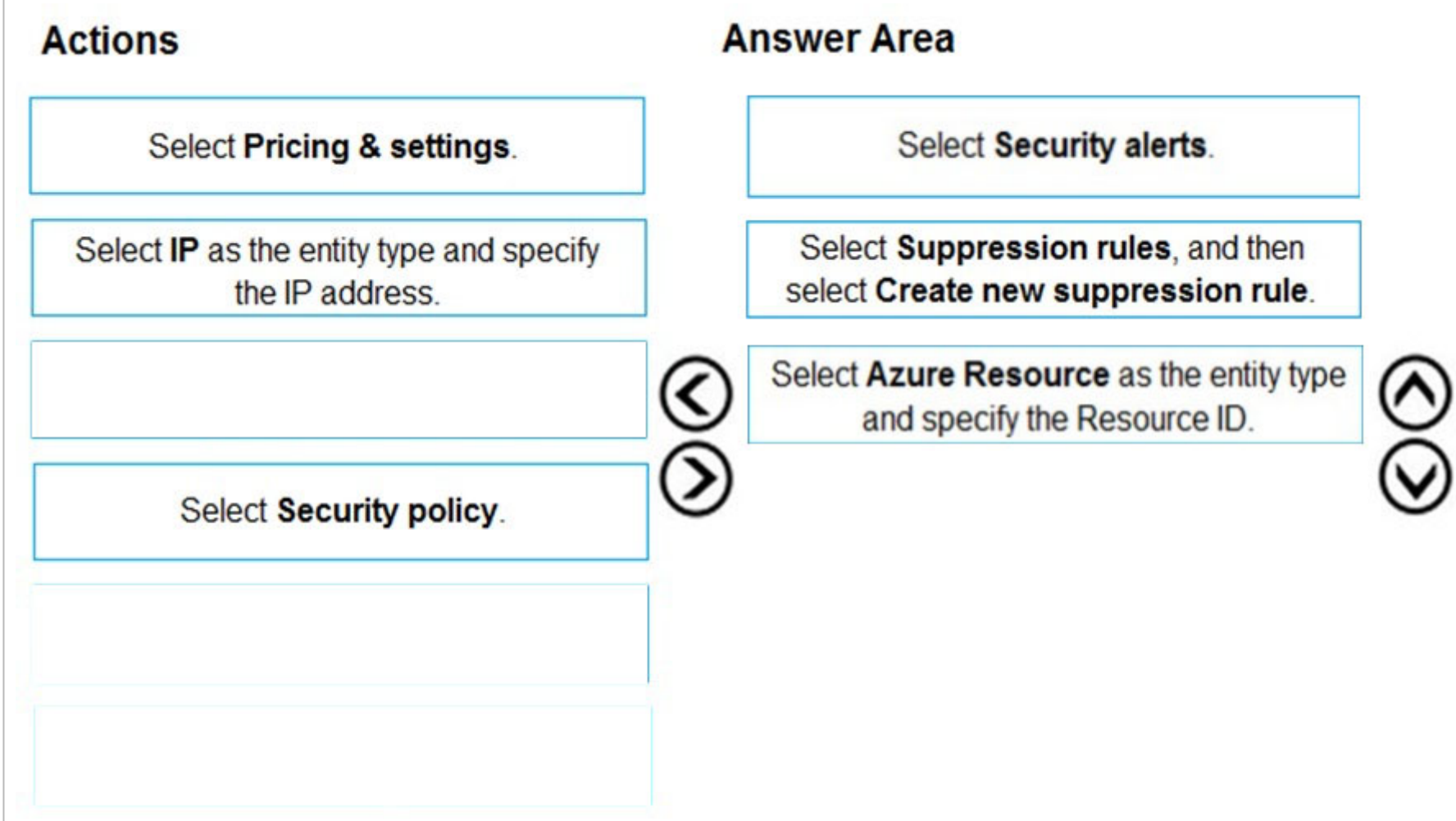
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

DRAG DROP -

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

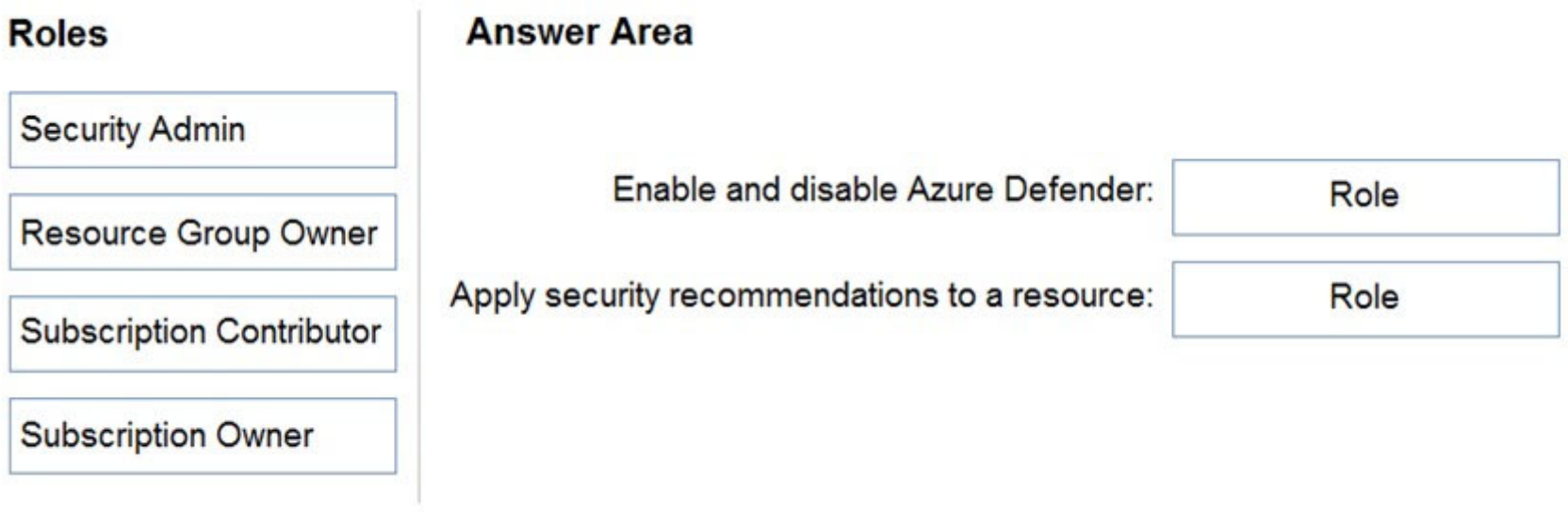
- Enable and disable Azure Defender.
- Apply security recommendations to resource.

The solution must use the principle of least privilege.

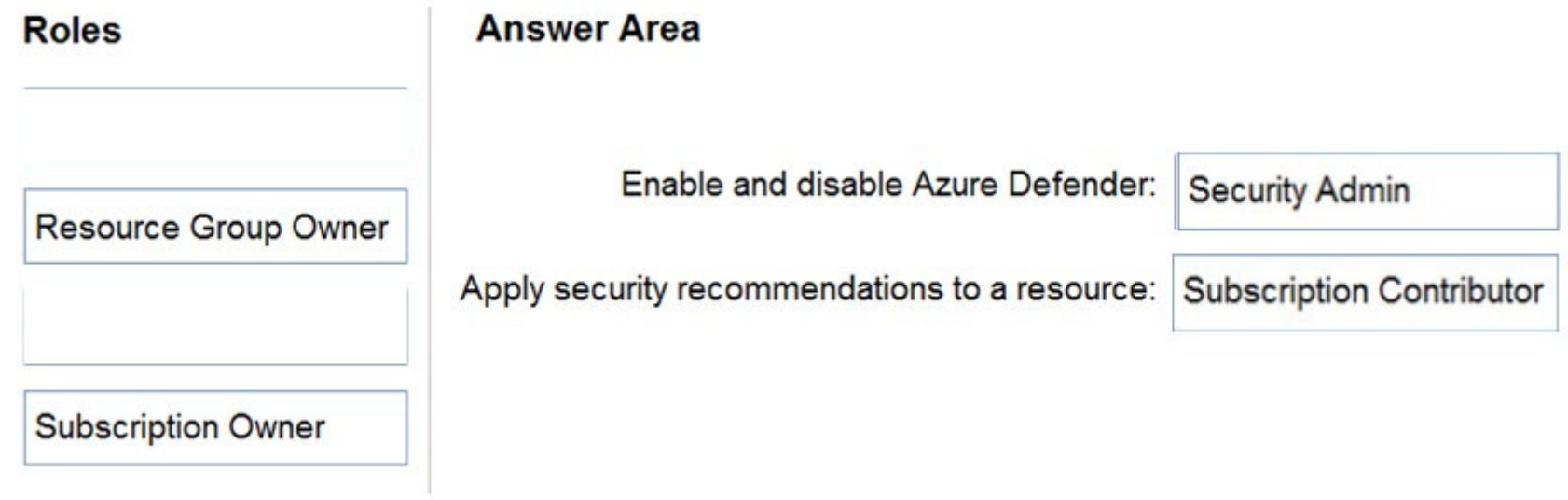
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

HOTSPOT -

You have an Azure subscription that uses Azure Defender.

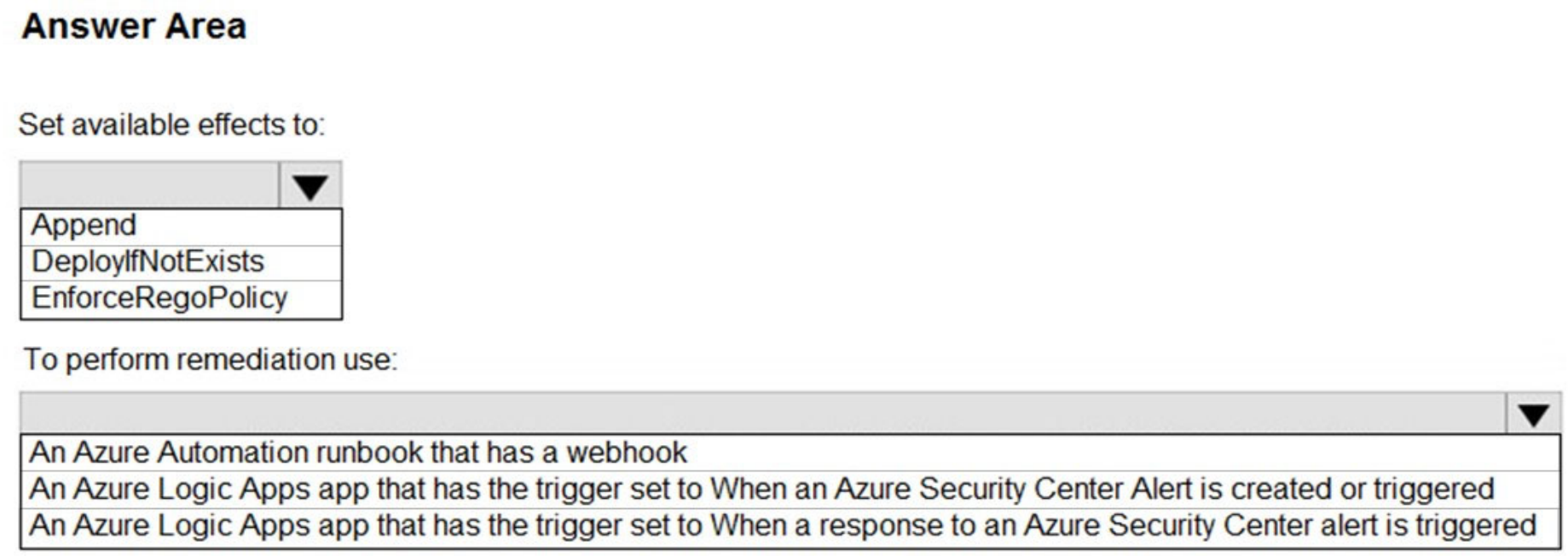
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

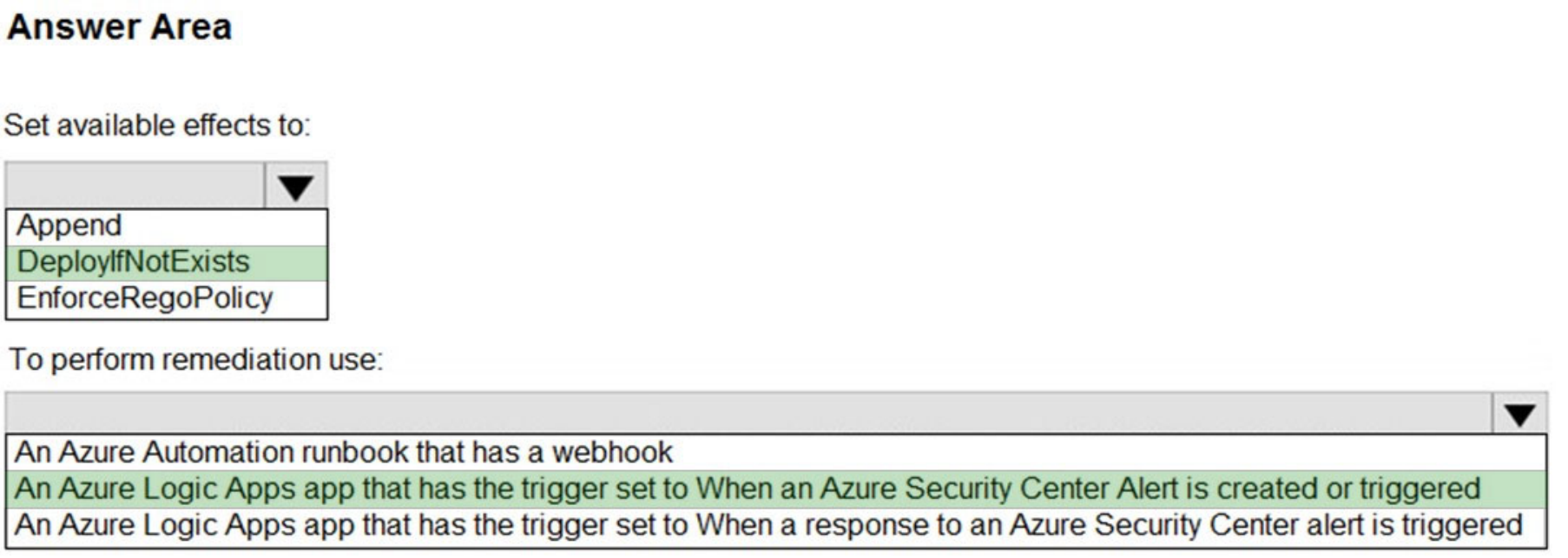
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Custom View Settings

Question #27 *Topic 2*

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.
You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.
What should you do first?

A. From Azure Security Center, add a workflow automation.

B. On VM1, run the Get-MPThreatCatalog cmdlet.

C. On VM1 trigger a PowerShell alert. Most Voted

D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

Community vote distribution
C (77%) A (23%)

Question #28 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.
Does this meet the goal?

A. Yes Most Voted

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Community vote distribution
A (71%) B (29%)

Question #29 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines.
Does this meet the goal?

A. Yes

B. No Most Voted

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Community vote distribution

B (100%)

Question #30 *Topic 2*

You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent

B. the Log Analytics agent Most Voted

C. the Azure Connected Machine agent

D. the Guest Configuration extension

Correct Answer: *B*
Defender for Cloud depends on the Log Analytics agent.
Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

Community vote distribution

B (58%) C (42%)

Question #31 *Topic 2*

DRAG DROP -

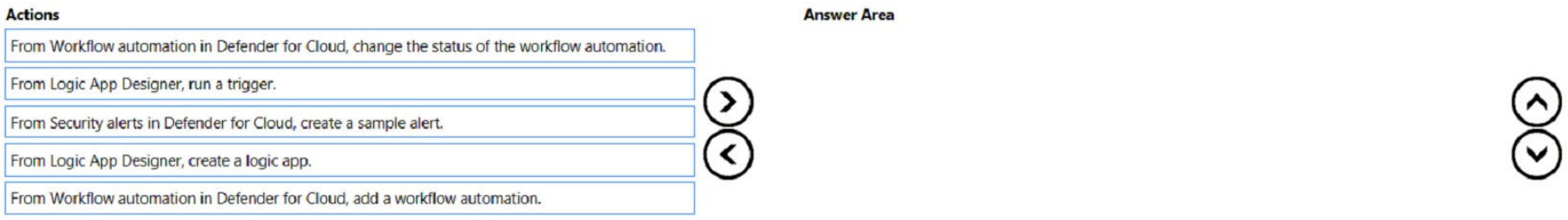
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.

You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification.

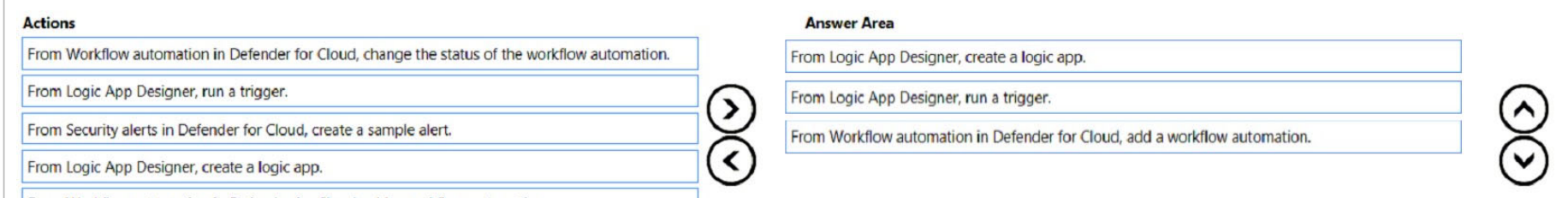
The solution must generate a test email.

Which three 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:



Correct Answer:

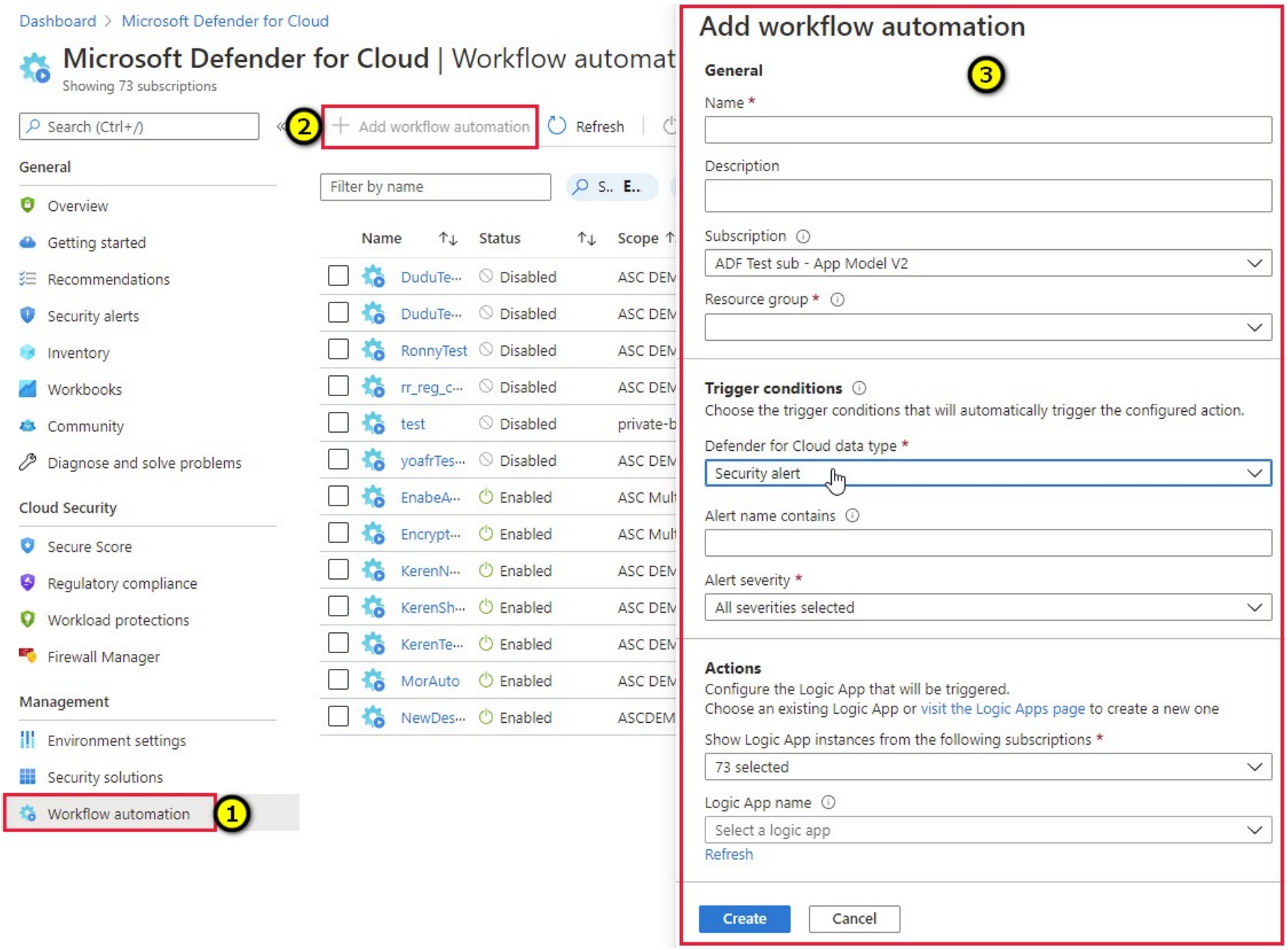


Step 1: From Logic App Designer, create a logic app.

Create a logic app and define when it should automatically run

1. From Defender for Cloud's sidebar, select Workflow automation.

2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

4. Etc.

Step 2: From Logic App Designer, run a trigger.

Manually trigger a Logic App -

You can also run Logic Apps manually when viewing any security alert or recommendation.

Step 3: From Workflow automation in Defender for cloud, add a workflow automation.

Configure workflow automation at scale using the supplied policies

Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Question #32 *Topic 2*

DRAG DROP
-

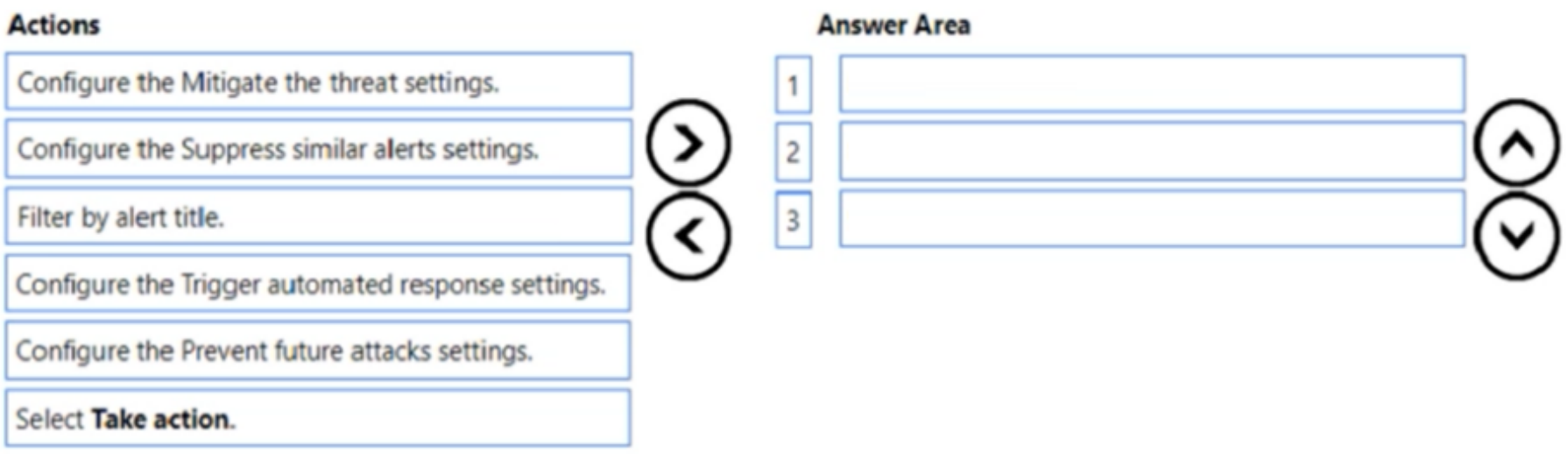
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled.

You configure the Azure logic apps shown in the following table.

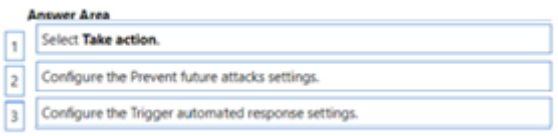
Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.

Which three 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.



Correct Answer:



Question #33 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

A. the Microsoft Monitoring Agent

B. the Azure Monitor agent

C. the Azure Arc agent Most Voted

D. the Azure Pipelines agent

Correct Answer: *B*

Community vote distribution

C (100%)

Question #34 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1.

You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

A. the activity logs of storage1

B. the Azure Storage Analytics logs

C. the alert details

D. the related entities of the alert

Correct Answer: *B*

Community vote distribution

B (57%) A (43%)

Custom View Settings

Question #35 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to filter the security alerts view to show the following alerts:

• Unusual user accessed a key vault
• Log on from an unusual location
• Impossible travel activity

Which severity should you use?

A. Informational
B. Low
C. Medium
D. High

Correct Answer: *C*

Community vote distribution

C (100%)

Question #36 *Topic 2*

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.

You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic.

Which JSON key should you search?

A. Description
B. Intent
C. ExtendedProperies
D. Entities

Correct Answer: *A*

Community vote distribution

B (100%)

DRAG DROP
-

You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

• Provide threat and vulnerability management.
• Support data collection rules.

Which three 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

- From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- From the Data controller settings in the Azure portal, create an Azure Arc data controller.
- On the on-premises servers, install the Log Analytics agent.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Azure Monitor agent.

Answer Area

Correct Answer:

Answer Area

- From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.
- On the on-premises servers, install the Azure Connected Machine agent.
- On the on-premises servers, install the Log Analytics agent.

HOTSPOT
-

You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.

You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.
How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"resources": [
    {
      "type": [                                          ▼
                Microsoft.Automation/automationAccounts",
                "Microsoft.Logic/workflows"',
                "Microsoft.Security/automations",
"apiVersion": "2019-01-01-preview",
"name": "[parameters('name')]",
"location": "[resourceGroup().location]",
"properties": {
  "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
  "isEnabled": true,
  "actions": [
    { "actionType": "LogicApp",
      "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
      "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
              'Microsoft.Logic/workflows/ [          ▼
                                          actions
                                          contents
                                          triggers
            parameters('app1'),'manual'), '2019-05-01').value]"
    }
  ],
```

Correct Answer:

```
"resources": [
    {
      "type": [Microsoft.Automation/automationAccounts" | "Microsoft.Logic/workflows" | "Microsoft.Security/automations"],
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('name')]",
      "location": "[resourceGroup().location]",
      "properties": {
        "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
          { "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
            "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
                    'Microsoft.Logic/workflows/' [actions | contents | triggers]
                    parameters('app1'),'manual'), '2019-05-01').value]"
          }
        ],
```

HOTSPOT
-

You have an Azure subscription that has Microsoft Defender for Cloud enabled for all supported resource types.

You create an Azure logic app named LA1.

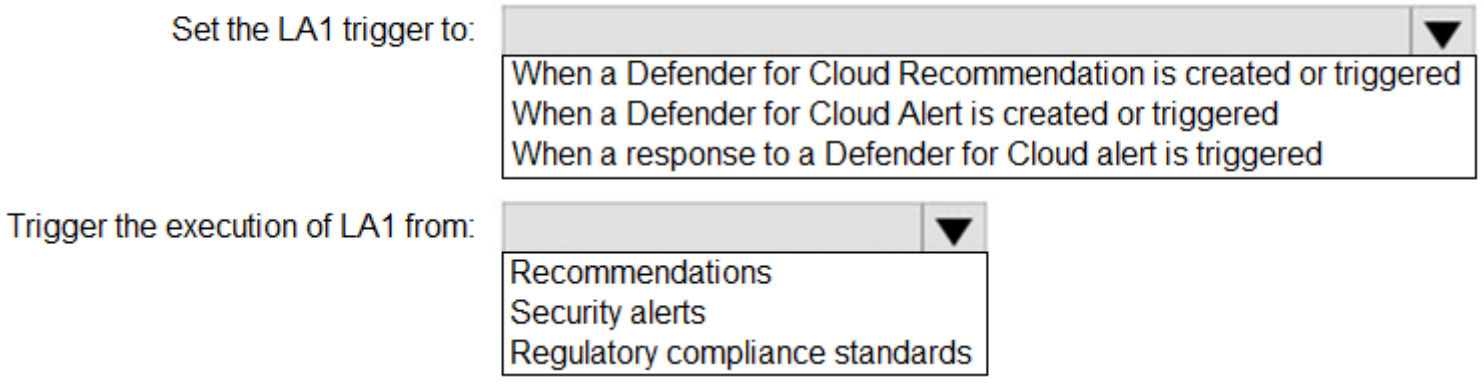
You plan to use LA1 to automatically remediate security risks detected in Defender for Cloud.

You need to test LA1 in Defender for Cloud.

What should you do? To answer, select the appropriate options in the answer area.

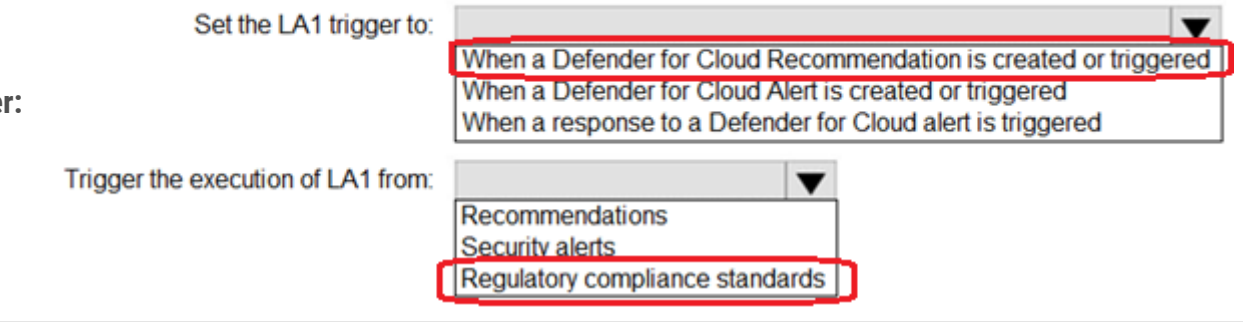
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



Previous Questions Next Questions

Custom View Settings

Question #40 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

A. Run the Log Analytics Troubleshooting Tool.

B. Copy and executable and rename the file as ASC_AlertTest_662jfi039N.exe. Most Voted

C. Modify the settings of the Microsoft Monitoring Agent.

D. Run the MMASetup executable and specify the –foo argument.

Correct Answer: *B*

Community vote distribution

B (80%) D (20%)

DRAG DROP
-

You create a new Azure subscription and start collecting logs for Azure Monitor.

You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

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

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

- Rename the executable file as AlertTest.exe.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Change the alert severity threshold for emails to **Medium**.
- Run the executable file and specify the appropriate arguments.
- Change the alert severity threshold for emails to **Low**.
- Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

Answer Area

Correct Answer:

Answer Area

- Change the alert severity threshold for emails to **Low**.
- Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
- Run the executable file and specify the appropriate arguments.

Question #42 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common.

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment. Most Voted

C. From the Azure portal, create an Azure Event Grid subscription.

D. From the workspace created by Defender for Cloud, set the data collection level to All Events.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines. Most Voted

Correct Answer: *AE*

Community vote distribution

BE (100%)

Question #43 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security operator

B. Security Admin Most Voted

C. Owner

D. Contributor

Correct Answer: *B*

Community vote distribution

B (100%)

Custom View Settings

Question #44 *Topic 2*

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license.

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

A. the risk detections report Most Voted

B. the risky users report

C. Identity Secure Score recommendations

D. the risky sign-ins report

Correct Answer: *B*

Community vote distribution

A (58%) D (25%) B (17%)

Question #45 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.

You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?

A. the Log Analytics agent

B. the Azure Connected Machine agent

C. the unified Microsoft Defender for Endpoint solution package

D. Microsoft Monitoring Agent

Correct Answer: *A*

Community vote distribution

B (75%) A (25%)

Question #46 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1 contains 20 virtual machines that run Windows Server 2019.

You need to configure just-in-time (JIT) access for the virtual machines in RG1. The solution must meet the following requirements:

• Limit the maximum request time to two hours.
• Limit protocols access to Remote Desktop Protocol (RDP) only.
• Minimize administrative effort.

What should you use?

A. Azure AD Privileged Identity Management (PIM)

B. Azure Policy

C. Azure Bastion

D. Azure Front Door

Correct Answer: *C*

Community vote distribution

C (67%) B (33%)

Custom View Settings

Topic 3 - Question Set 3

Question #1 *Topic 3*

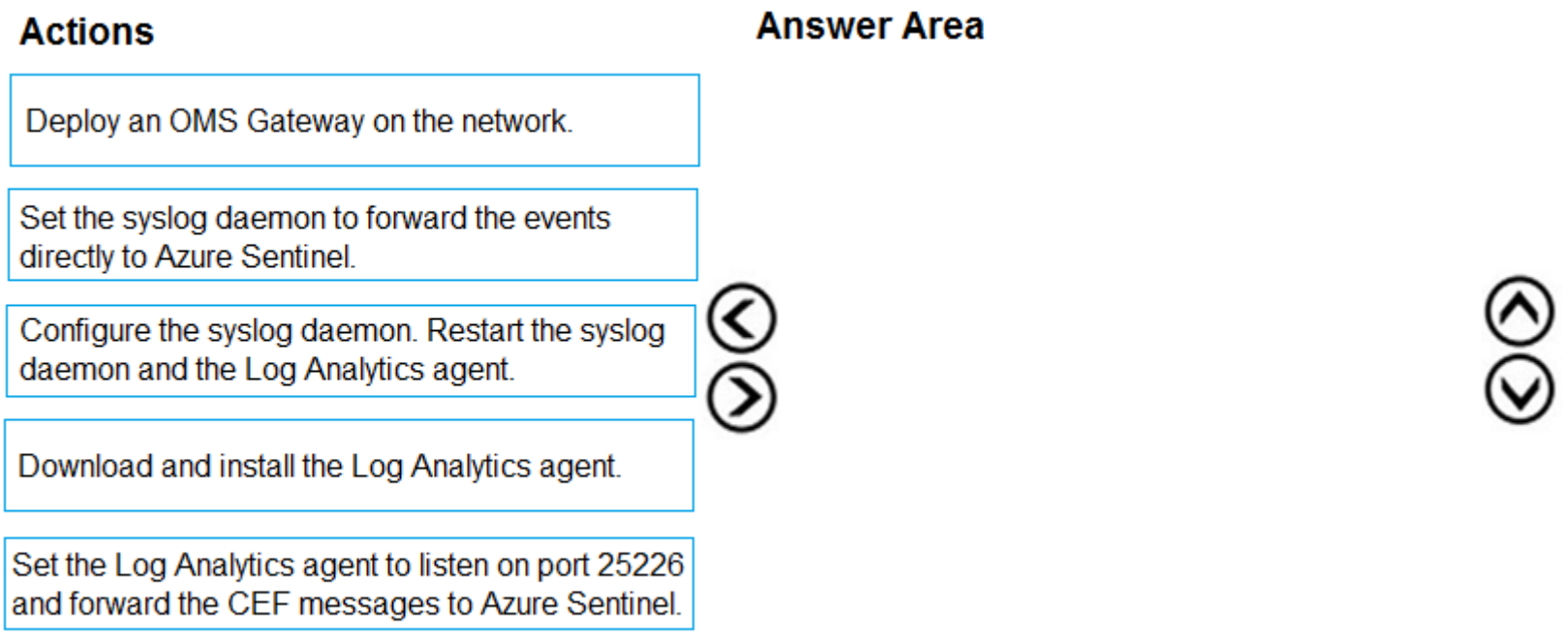
DRAG DROP -

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

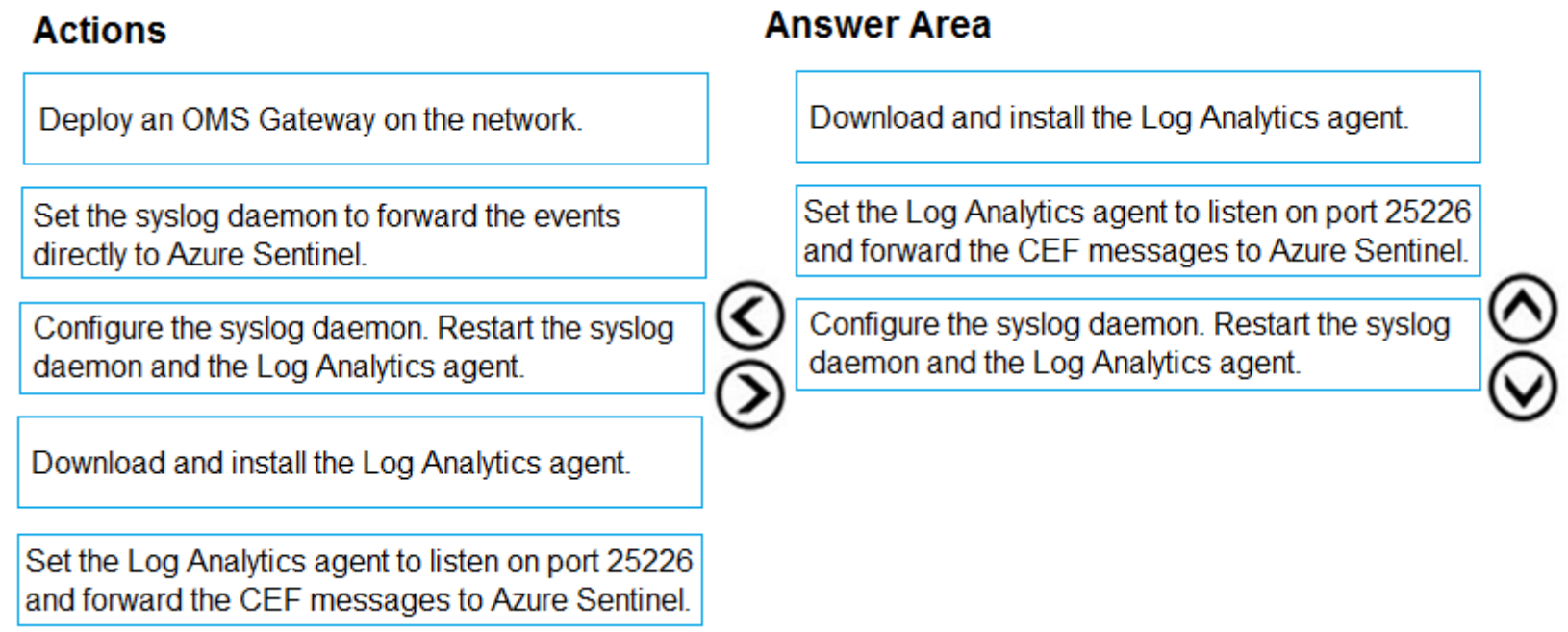
You need to deploy the log forwarder.

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

Select and Place:



Correct Answer:



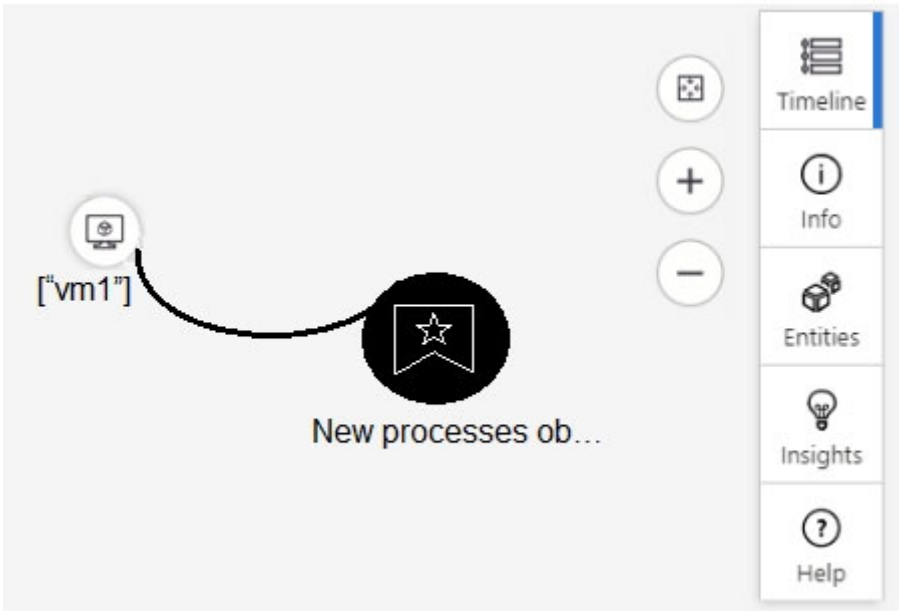
Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

Question #2 *Topic 3*

HOTSPOT -

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the items related to the incident.

- Entities
- Info
- Insights
- Timeline

Correct Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the items related to the incident.

- Entities
- Info
- Insights
- Timeline

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

Question #3 *Topic 3*

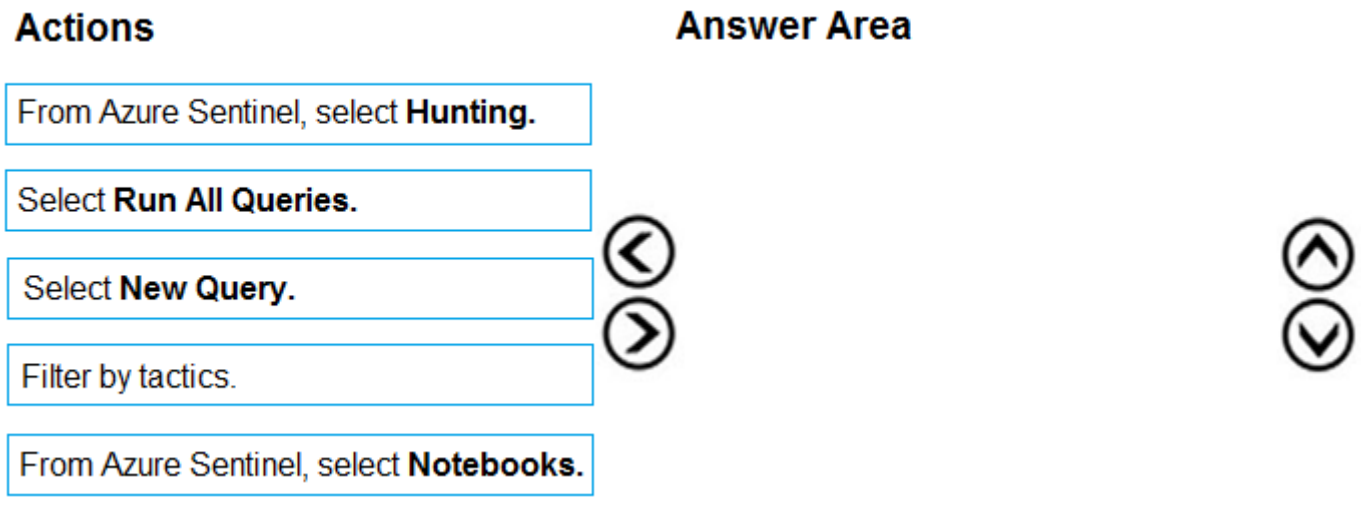
DRAG DROP -

You have an Azure Sentinel deployment.

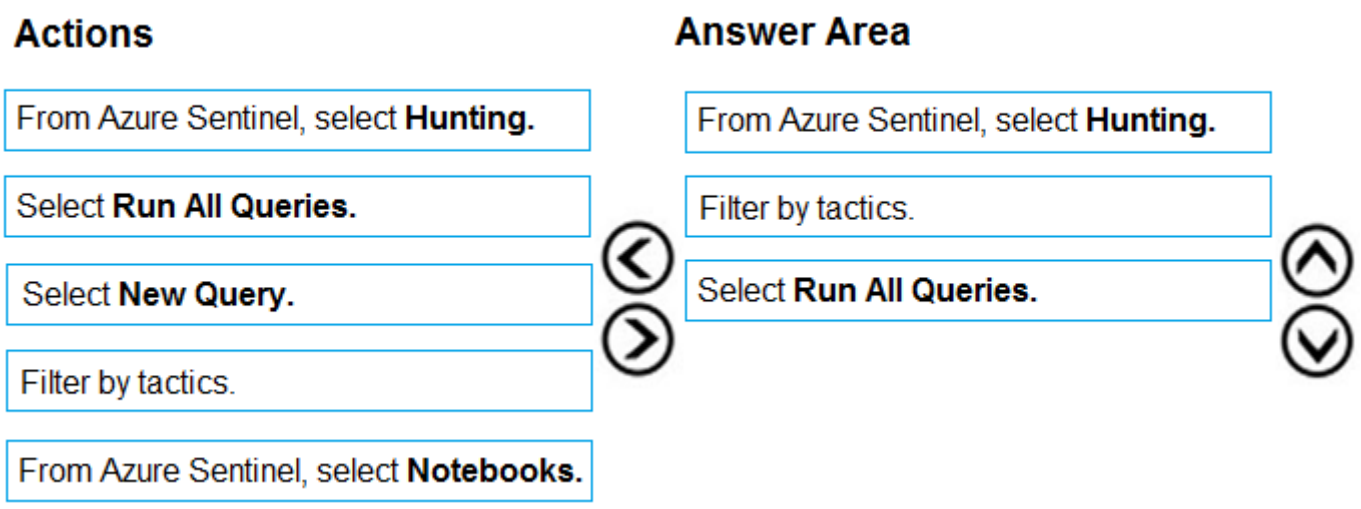
You need to query for all suspicious credential access activities.

Which three 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:



Correct Answer:



Reference:

https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/

Question #4 *Topic 3*

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. Most Voted

Correct Answer: *B*

Community vote distribution

D (73%) B (27%)

Custom View Settings

Question #5 *Topic 3*

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

Correct Answer: *C*

Reference:

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

Community vote distribution

C (100%)

Question #6 *Topic 3*

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 an alert and modify the action. Most Voted

Correct Answer: *D*

Reference:

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

Community vote distribution

D (70%) A (30%)

Question #7 *Topic 3*

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 Most Voted

B. resource group

C. IP address

D. computer Most Voted

Correct Answer: *CD*

Community vote distribution

AD (76%) CD (24%)

Question #8 *Topic 3*

Your company stores the data of 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. Most Voted

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. Most Voted

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

Community vote distribution

BE (100%)

Custom View Settings

Question #9 *Topic 3*

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

Correct Answer: *D*

Reference:

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

Community vote distribution

D (100%)

Question #10 *Topic 3*

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. Most Voted

Correct Answer: *D*

Reference:

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

Community vote distribution

D (100%)

Question #11 *Topic 3*

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and resolve incidents in Azure Sentinel.

You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.

Which role should you assign to the analyst?

A. Azure Sentinel Responder Most Voted

B. Logic App Contributor

C. Azure Sentinel Contributor

D. Azure Sentinel Reader

Correct Answer: *A*

Reference:

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

Community vote distribution

A (100%)

Question #12 *Topic 3*

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

Community vote distribution

B (100%)

Custom View Settings

Question #13 *Topic 3*

DRAG DROP -

Your company deploys Azure Sentinel.

You plan to delegate the administration of Azure Sentinel to various groups.

You need to delegate the following tasks:

- Create and run playbooks
- Create workbooks and analytic rules.

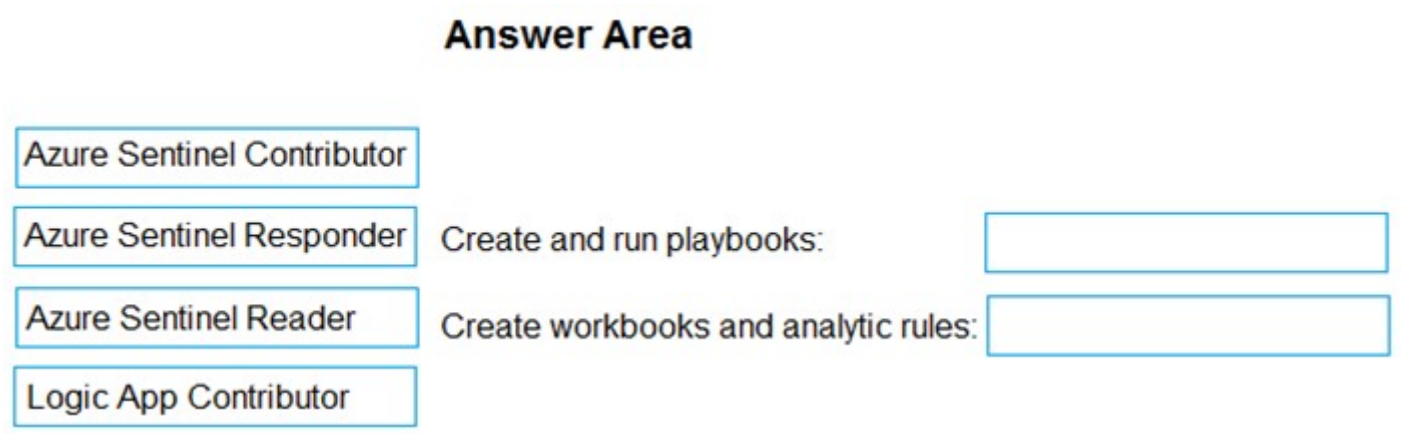
The solution must use the principle of least privilege.

Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.

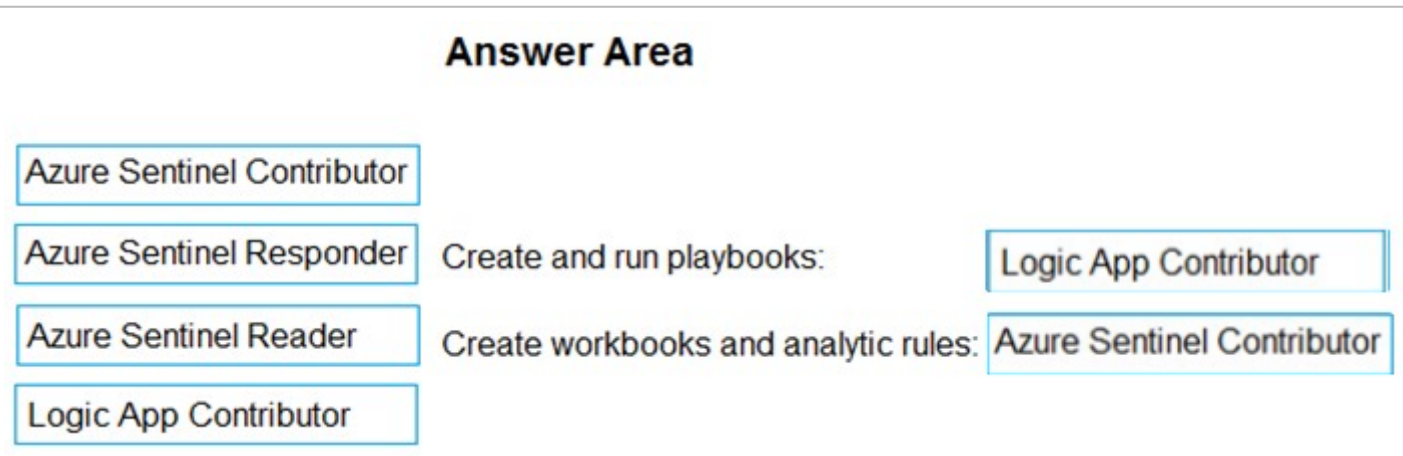
You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

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

Question #14 *Topic 3*

A company uses Azure Sentinel.

You need to create an automated threat response.

What should you use?

A. a data connector

B. a playbook

C. a workbook

D. a Microsoft incident creation rule

Correct Answer: *B*

Reference:

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

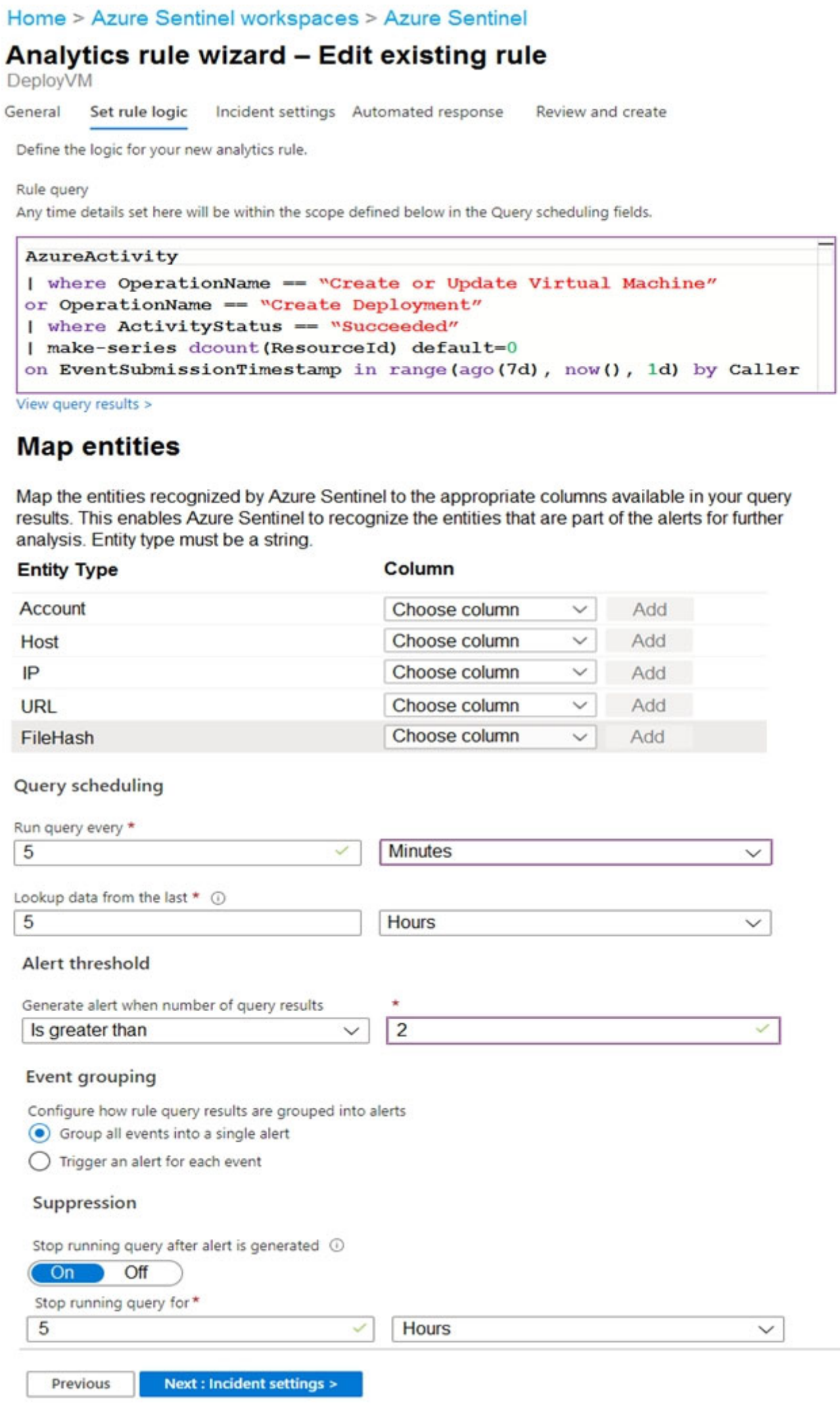
Community vote distribution

B (100%)

HOTSPOT -

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.



You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice].**

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

Correct Answer:

Answer Area

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice].**

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

Reference:

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

Question #16 *Topic 3*

You have an Azure Sentinel deployment in the East US Azure region.

You create a Log Analytics workspace named LogsWest in the West US Azure region.

You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.

What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment.

C. Add Azure Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Correct Answer: *C*

Reference:

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

Community vote distribution

C (100%)

Custom View Settings

Question #17 *Topic 3*

You create a custom analytics rule to detect threats in Azure Sentinel.
You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out. Most Voted

B. The target workspace was deleted.

C. Permissions to the data sources of the rule query were modified.

D. There are connectivity issues between the data sources and Log Analytics Most Voted

Correct Answer: *AD*
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

Community vote distribution

AD (100%)

Question #18 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a scheduled query rule for a data connector.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Question #19 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Community vote distribution

B (100%)

Question #20 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?

A. Yes

B. No

Correct Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Community vote distribution

A (100%)

Custom View Settings

Question #21 *Topic 3*

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.

You need to create a query that will be used to display the time chart.

What should you include in the query?

A. extend

B. bin

C. makeset

D. workspace

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

Community vote distribution

B (100%)

Question #22 *Topic 3*

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. Most Voted

B. Associate a playbook to an incident. Most Voted

C. Enable Entity behavior analytics.

D. Create a workbook.

E. Enable the Fusion rule.

Correct Answer: *AB*

Reference:

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

Community vote distribution

AB (100%)

Question #23 *Topic 3*

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

Correct Answer: *A*

Reference:

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

Community vote distribution

A (100%)

Question #24 *Topic 3*

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

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

Custom View Settings

Question #25 *Topic 3*

You use Azure 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 livestream Most Voted

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query. Most Voted

E. Create a bookmark.

Correct Answer: *BD*

Reference:

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

Community vote distribution

AD (55%) AB (45%)

HOTSPOT -

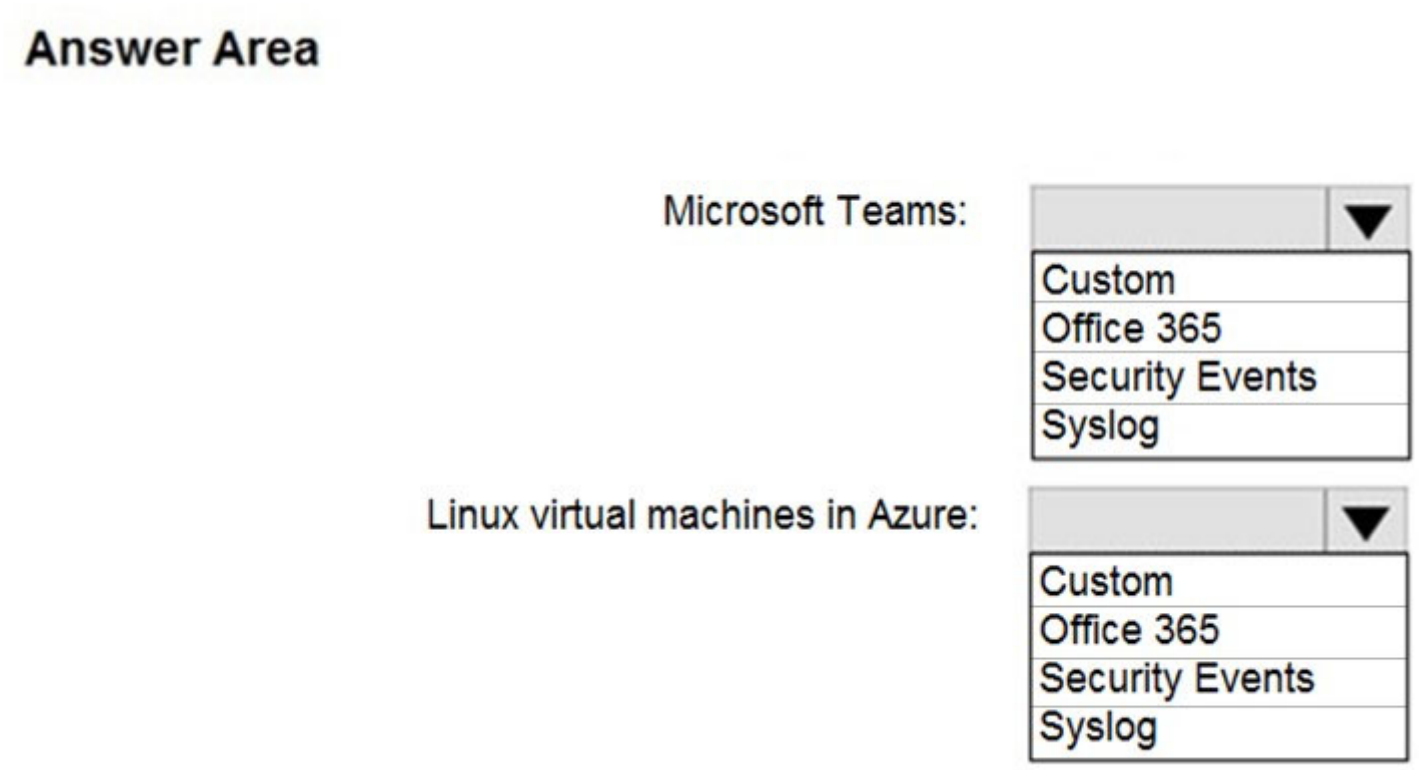
You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365 https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

Question #27 *Topic 3*

You are investigating an incident in Azure Sentinel that contains more than 127 alerts.
You discover eight alerts in the incident that require further investigation.
You need to escalate the alerts to another Azure Sentinel administrator.
What should you do to provide the alerts to the administrator?

A. Create a Microsoft incident creation rule

B. Share the incident URL

C. Create a scheduled query rule

D. Assign the incident

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

Community vote distribution

D (100%)

Question #28 *Topic 3*

You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
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. Enable Entity behavior analytics.

B. Associate a playbook to the analytics rule that triggered the incident. Most Voted

C. Enable the Fusion rule.

D. Add a playbook. Most Voted

E. Create a workbook.

Correct Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Community vote distribution

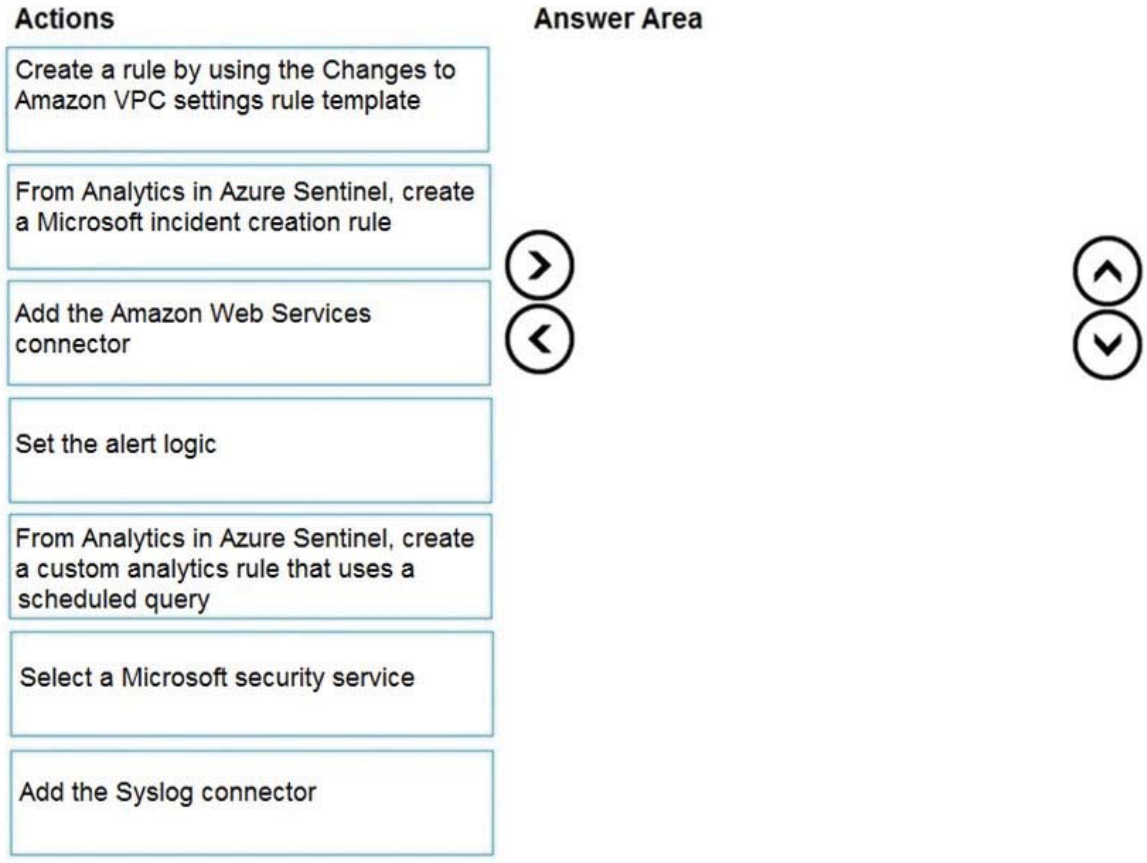
BD (75%) AB (20%) 5%

DRAG DROP -

You need to use an Azure Sentinel analytics rule to search for specific criteria in Amazon Web Services (AWS) logs and to generate incidents.

Which three 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:



Correct Answer:

Question #30 *Topic 3*

You have the following environment:

Azure Sentinel -

▪

⇨ A Microsoft 365 subscription

⇨ Microsoft Defender for Identity

⇨ An Azure Active Directory (Azure AD) tenant

You configure Azure Sentinel to collect security logs from all the Active Directory member servers and domain controllers.

You deploy Microsoft Defender for Identity by using standalone sensors.

You need to ensure that you can detect when sensitive groups are modified in Active Directory.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure the Advanced Audit Policy Configuration settings for the domain controllers.

B. Modify the permissions of the Domain Controllers organizational unit (OU).

C. Configure auditing in the Microsoft 365 compliance center.

D. Configure Windows Event Forwarding on the domain controllers.

Correct Answer: *AD*

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

Custom View Settings

Question #31 *Topic 3*

You use Azure Sentinel.
You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Contributor Most Voted

B. Security Administrator

C. Azure Sentinel Responder

D. Logic App Contributor

Correct Answer: *A*
Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Community vote distribution

A (100%)

Question #32 *Topic 3*

You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook

B. a notebook

C. a livestream Most Voted

D. a bookmark

Correct Answer: *C*
Use livestream to run a specific query constantly, presenting results as they come in.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/hunting

Community vote distribution

C (100%)

Custom View Settings

Question #33 *Topic 3*

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.

You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.

Which two actions should you perform? Each correct answer present part of the solution.

NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates. Most Voted

B. Create a Microsoft incident creation rule based on Azure Security Center.

C. Create a Microsoft Cloud App Security connector. Most Voted

D. Create an Azure AD Identity Protection connector. Most Voted Most Voted

Correct Answer: *AB*

Community vote distribution

CD (52%) AD (43%) 4%

Question #34 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a livestream from a query.

Does this meet the goal?

A. Yes

B. No

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

HOTSPOT -

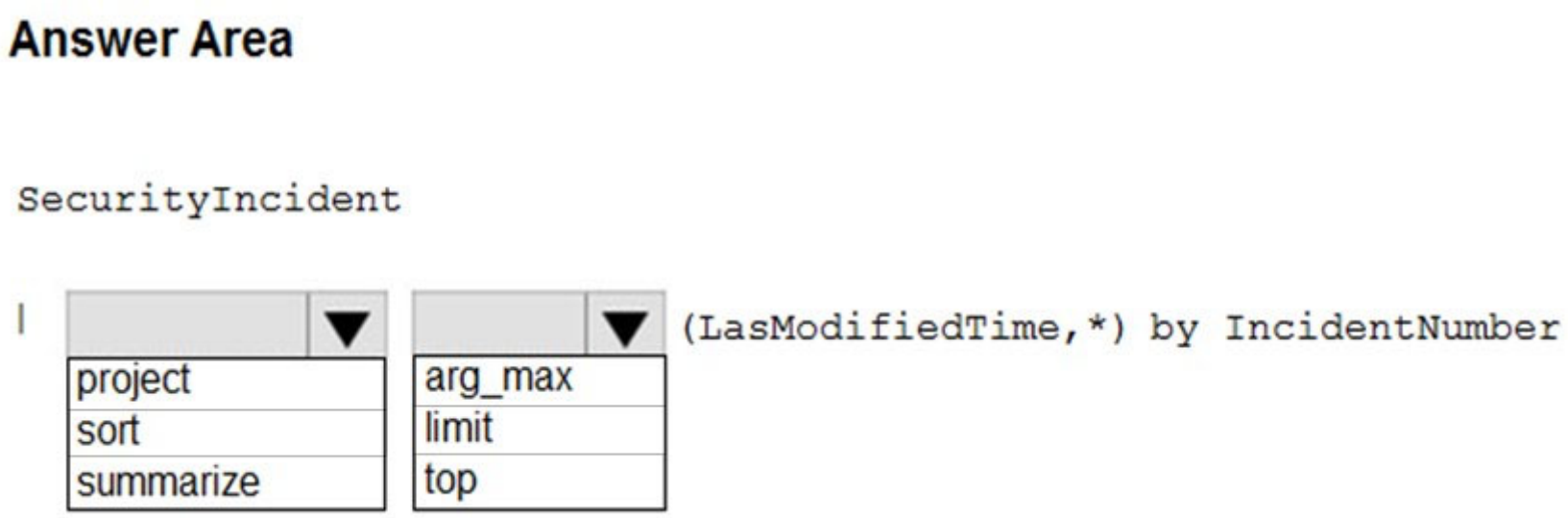
You need to create a query for a workbook. The query must meet the following requirements:

- ☞ List all incidents by incident number.
- ☞ Only include the most recent log for each incident.

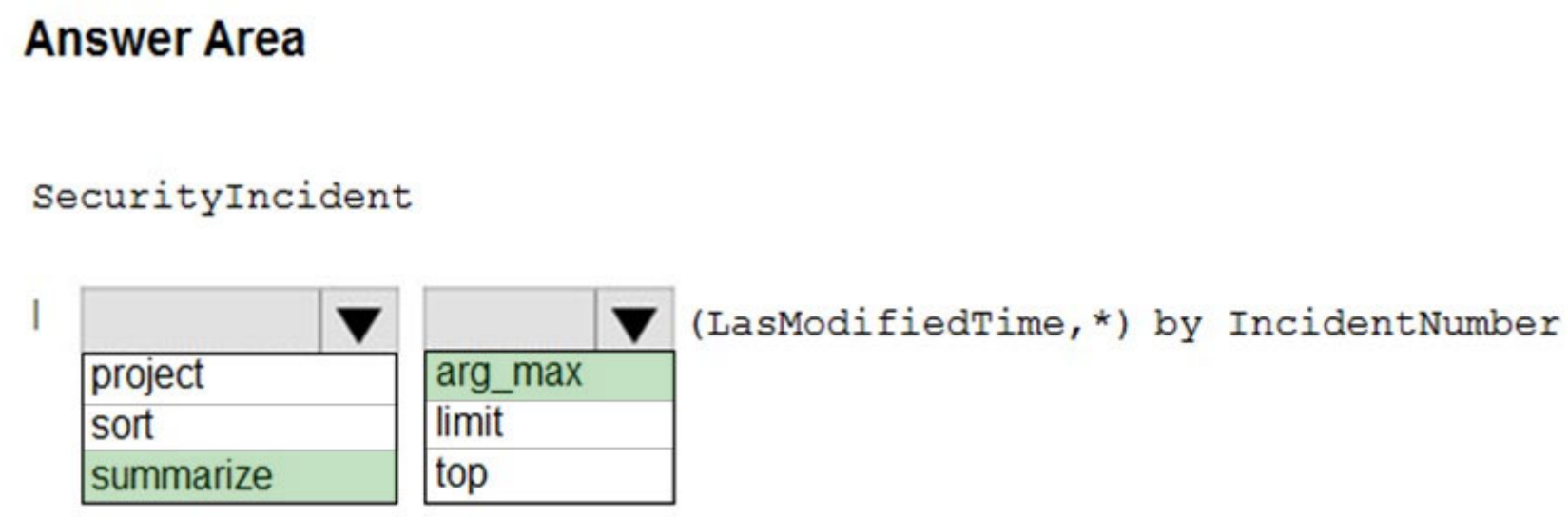
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference:

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

DRAG DROP -

You have the resources shown in the following table.

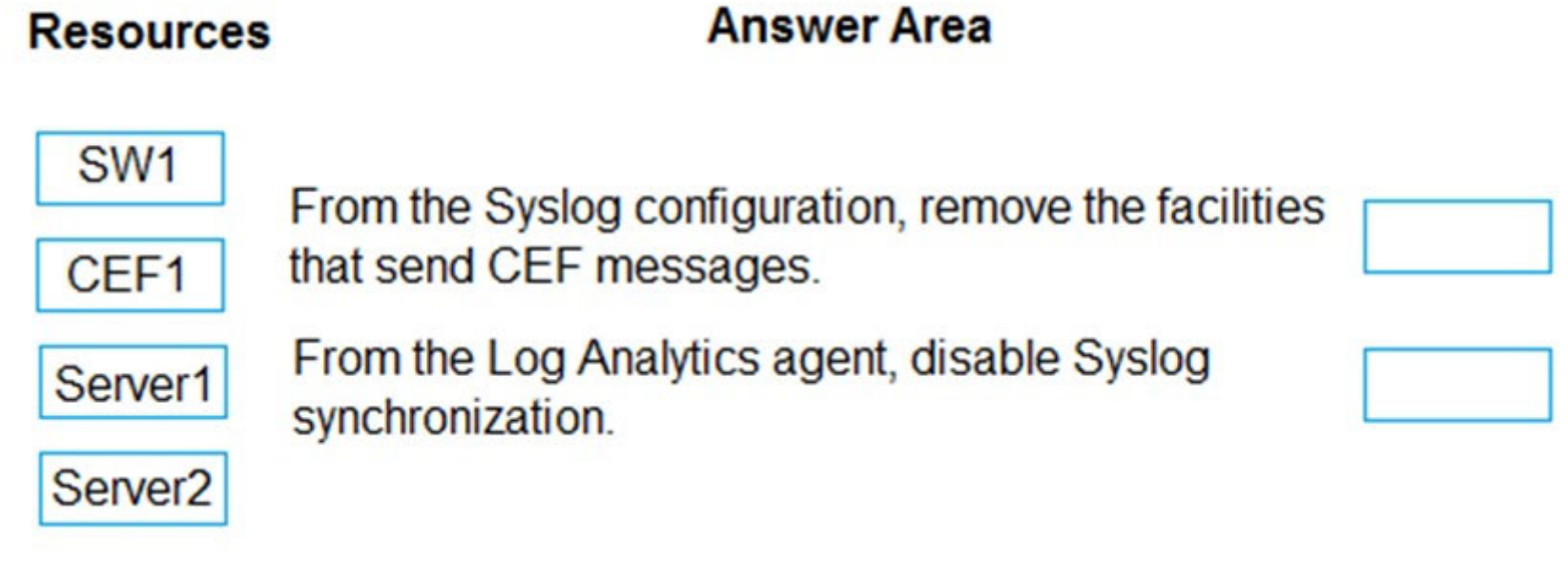
Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

You need to prevent duplicate events from occurring in SW1.

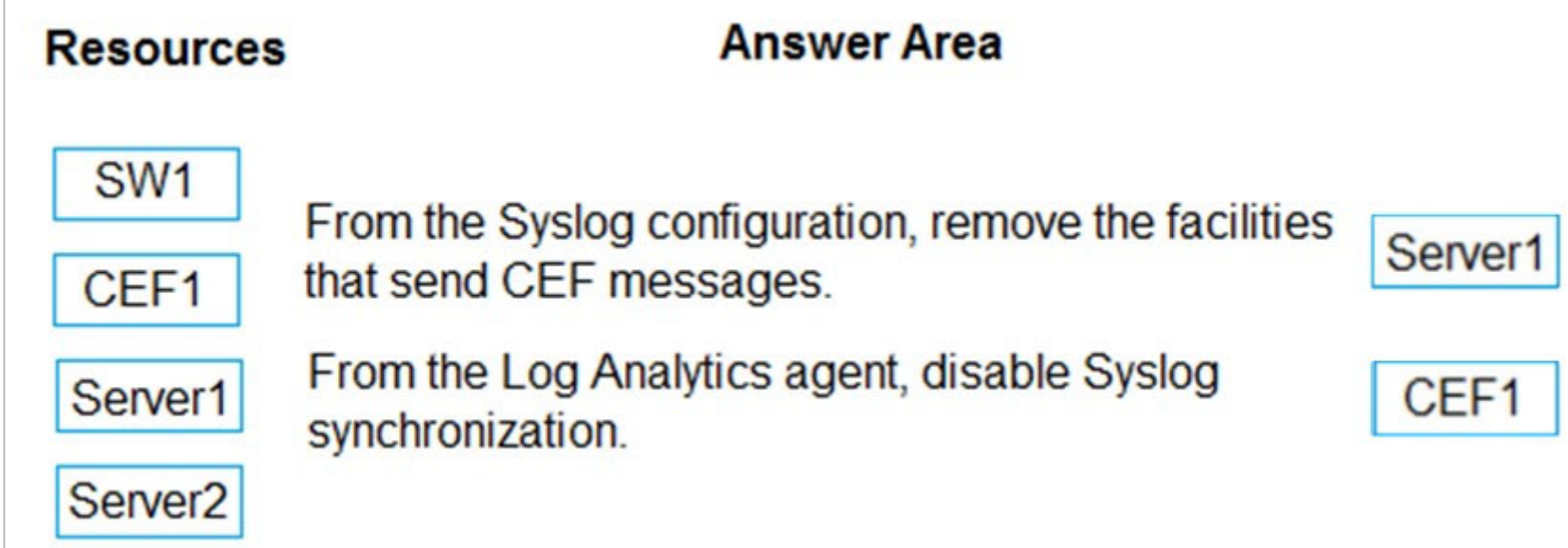
What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog

Question #37 *Topic 3*

You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks
B. Azure Automation runbooks
C. Microsoft Sentinel automation rules
D. Microsoft Sentinel playbooks
E. Azure Functions apps

Correct Answer: *CD*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

Question #38 *Topic 3*

You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.
What should you use to create the visuals?

A. plotly
B. TensorFlow
C. msticpy
D. matplotlib

Correct Answer: *C*
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:
Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.
Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
Visualization tools using event timelines, process trees, and geo mapping.
Advanced analyses, such as time series decomposition, anomaly detection, and clustering.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started https://msticpy.readthedocs.io/en/latest/

Question #39 *Topic 3*

HOTSPOT -

You have a Microsoft Sentinel workspace named sws1.

You need to create a hunting query to identify users that list storage keys of multiple Azure Storage accounts. The solution must exclude users that list storage keys for a single storage account.

How should you complete the query? To answer, select the appropriate options in the answer area.

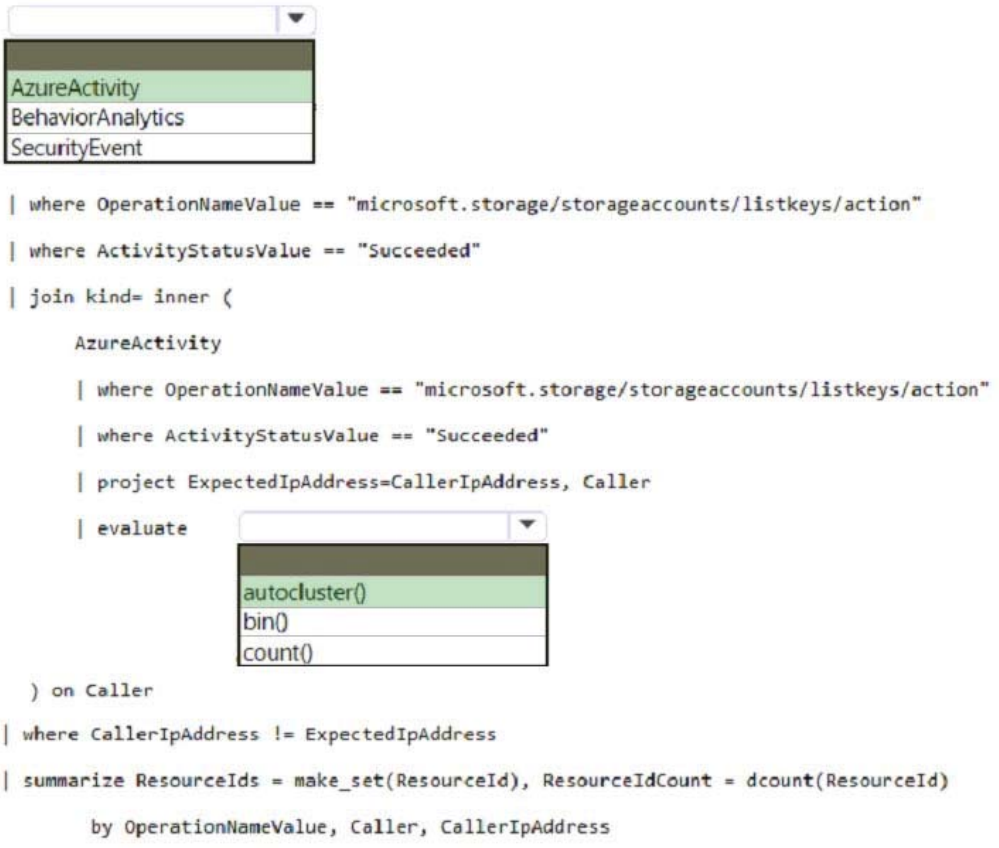
NOTE: Each correct selection is worth one point.

Hot Area:


```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
      AzureActivity
      | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
      | where ActivityStatusValue == "Succeeded"
      | project ExpectedIpAddress=CallerIpAddress, Caller
      | evaluate
```


```
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
        by OperationNameValue, Caller, CallerIpAddress
```

Correct Answer:



Box 1: AzureActivity -
The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:
Box 2: autocluster()
Example: description: |
'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.
The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.'

AzureActivity -
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (

AzureActivity -
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount
(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
Reference:
https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

DRAG DROP -

You have a Microsoft Sentinel workspace named workspace1 and an Azure virtual machine named VM1.

You receive an alert for suspicious use of PowerShell on VM1.

You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

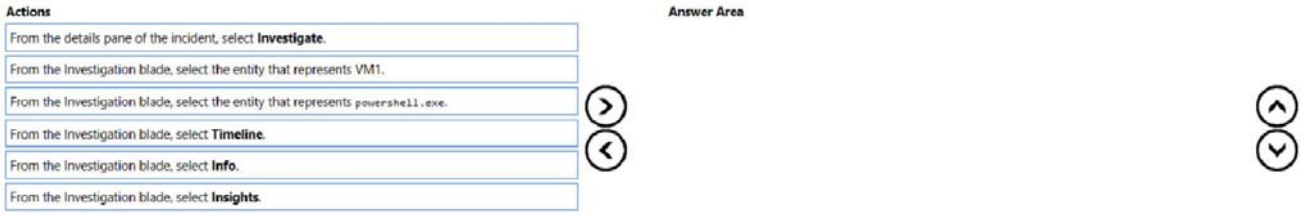
The modification of local group memberships

▪

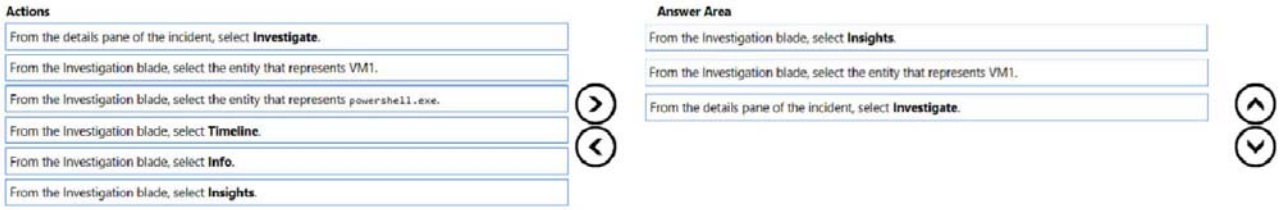
⇨ The purging of event logs

Which three actions should you perform in sequence in the Azure portal? 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:



Correct Answer:



Step 1: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights -

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights -

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address -

Account -

Host -

URL -

Step 3: From the details pane of the incident, select Investigate.

Choose a single incident and click View full details or Investigate.

Reference:

https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

Custom View Settings

Question #41 *Topic 3*

You have a Microsoft Sentinel workspace that contains the following incident.

Brute force attack against Azure Portal analytics rule has been triggered.

You need to identify the geolocation information that corresponds to the incident.

What should you do?

A. From Overview, review the Potential malicious events map.

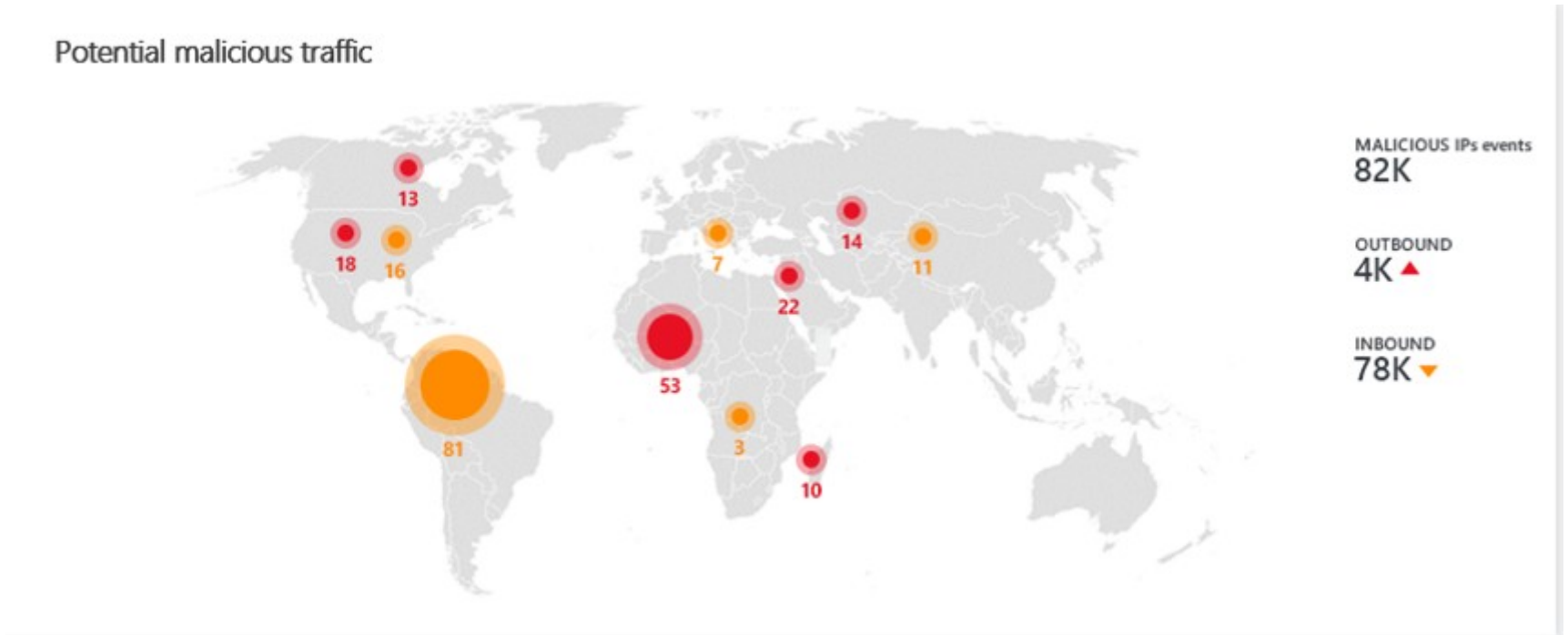
B. From Incidents, review the details of the IPCustomEntity entity associated with the incident.

C. From Incidents, review the details of the AccountCustomEntity entity associated with the incident.

D. From Investigation, review insights on the incident entity.

Correct Answer: *A*

Potential malicious events: When traffic is detected from sources that are known to be malicious, Microsoft Sentinel alerts you on the map. If you see orange, it is inbound traffic: someone is trying to access your organization from a known malicious IP address. If you see Outbound (red) activity, it means that data from your network is being streamed out of your organization to a known malicious IP address.



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/get-visibility#get-visualization

Community vote distribution

B (60%) A (40%)

Question #42 *Topic 3*

You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

A. Create an Azure Policy assignment. Most Voted

B. Modify the Workload protections settings in Defender for Cloud.

C. Create an alert rule in Azure Monitor.

D. Modify the alert settings in Defender for Cloud.

Correct Answer: *D*
You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud.
Note: To create a rule directly in the Azure portal:
1. From Defender for Cloud's security alerts page:
Select the specific alert you don't want to see anymore, and from the details pane, select Take action.
Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:
2. In the new suppression rule pane, enter the details of your new rule.
Your rule can dismiss the alert on all resources so you don't get any alerts like this one in the future.
Your rule can dismiss the alert on specific criteria - when it relates to a specific IP address, process name, user account, Azure resource, or location.
3. Enter details of the rule.
4. Save the rule.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules

Community vote distribution
A (86%) 14%

Question #43 *Topic 3*

You have an Azure subscription that has the enhanced security features in Microsoft Defender for Cloud enabled and contains a user named User1.
You need to ensure that User1 can export alert data from Defender for Cloud. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. User Access Administrator

B. Owner

C. Contributor

D. Reader

Correct Answer: *B*

Community vote distribution
B (100%)

Question #44 *Topic 3*

You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector.
You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD-generated alert.
What should you create first?

A. a repository connection

B. a watchlist

C. an analytics rule

D. an automation rule Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Previous Questions

Next Questions

Custom View Settings

Question #45 *Topic 3*

You have a Microsoft Sentinel workspace.

You need to identify which rules are used to detect advanced multistage attacks that comprise two or more alerts or activities. The solution must minimize administrative effort.

Which rule type should you query?

A. Fusion Most Voted

B. Microsoft Security

C. ML Behavior Analytics

D. Scheduled

Correct Answer: *A*

Community vote distribution

A (100%)

Question #46 *Topic 3*

You have an Azure subscription that uses Microsoft Sentinel and contains 100 Linux virtual machines.

You need to monitor the virtual machines by using Microsoft Sentinel. The solution must meet the following requirements:

☞ Minimize administrative effort.

☞ Minimize the parsing required to read fog data.

What should you configure?

A. a Log Analytics Data Collector API

B. REST API integration

C. a Common Evert Format (CEF) connector Most Voted

D. a Syslog connector

Correct Answer: *D*

Community vote distribution

C (56%) D (44%)

HOTSPOT -

You have 100 Azure subscriptions that have enhanced security features in Microsoft Defender for Cloud enabled. All the subscriptions are inked to a single Azure

Active Directory (Azure AD) tenant.

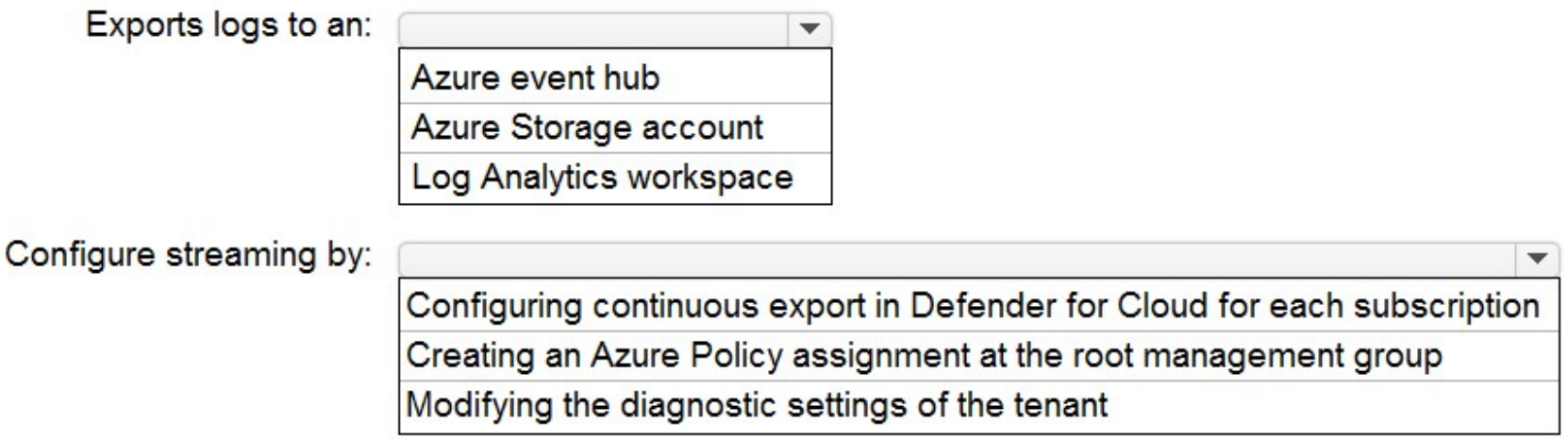
You need to stream the Defender for Cloud logs to a syslog server. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

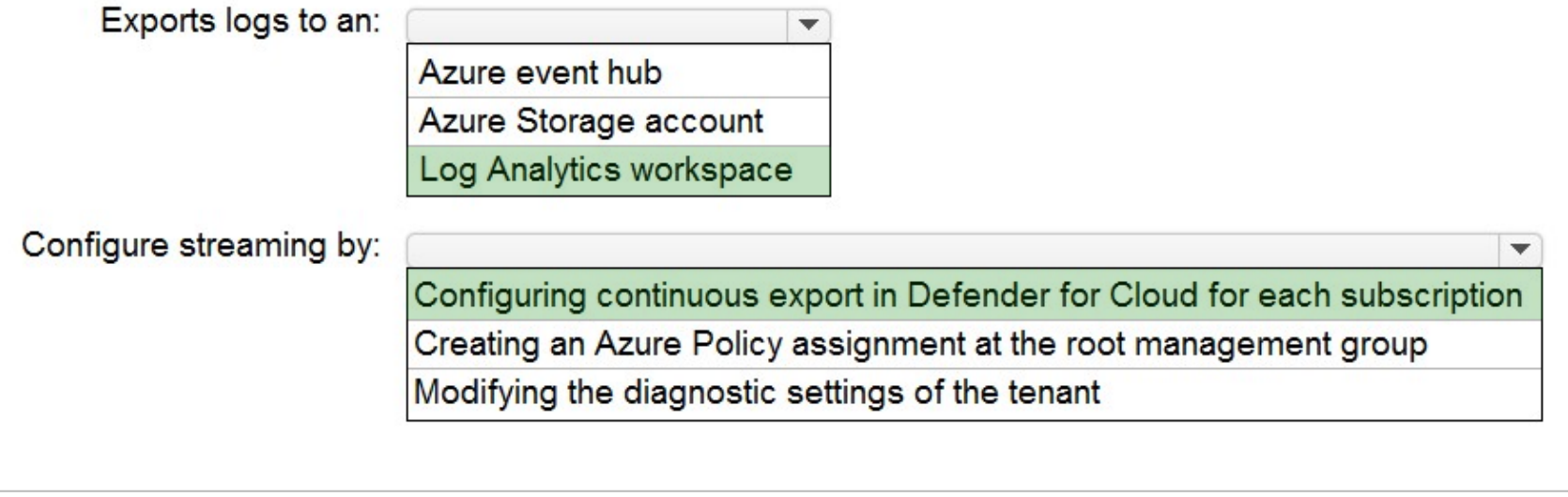
Hot Area:

Answer Area



Correct Answer:

Answer Area



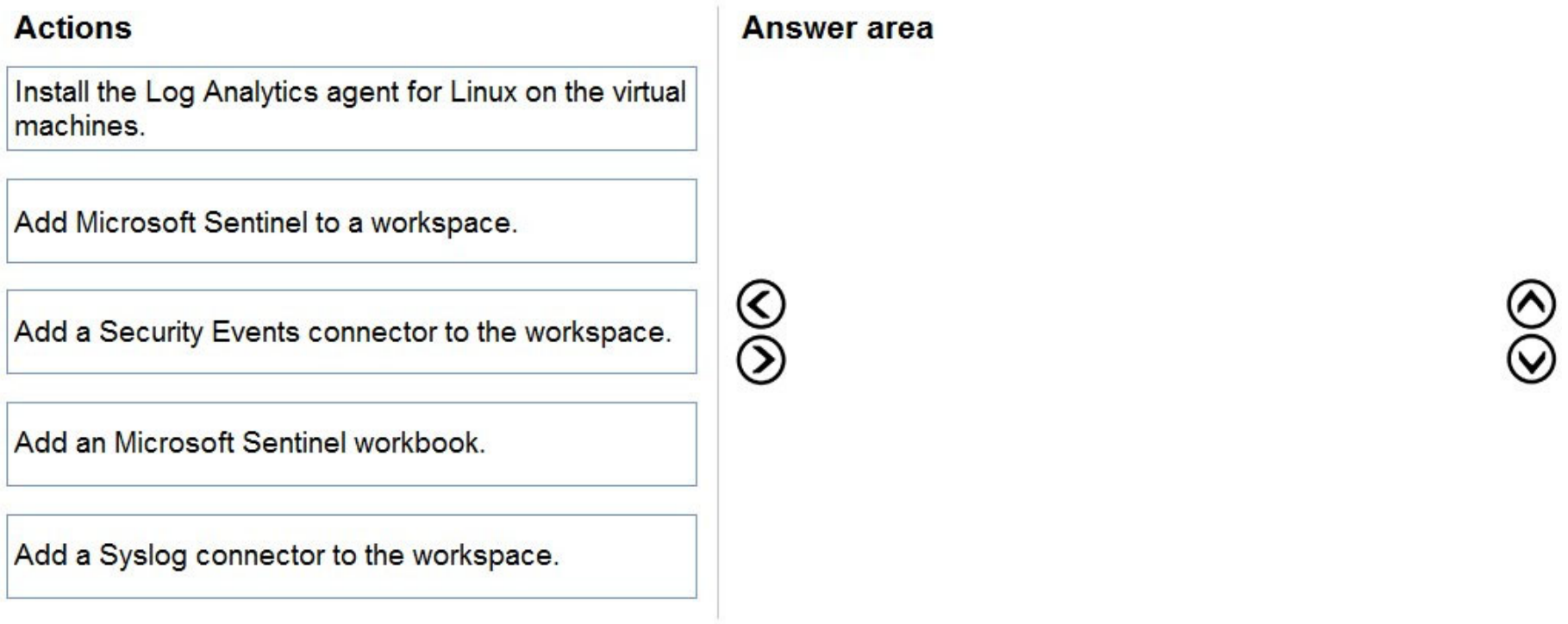
DRAG DROP -

You have an Azure subscription that contains 100 Linux virtual machines.

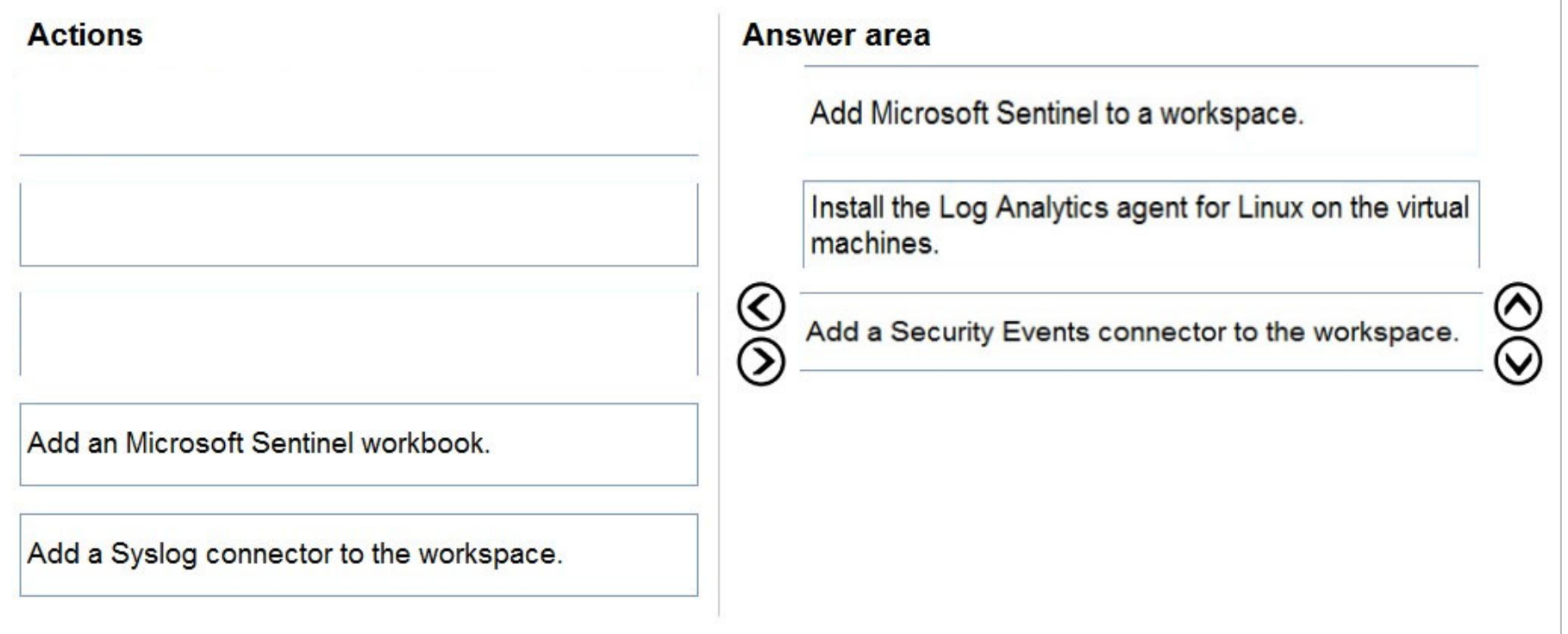
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.

Which three 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:



Correct Answer:



Question #49 *Topic 3*

You have an Azure subscription that uses Microsoft Sentinel.

You detect a new threat by using a hunting query.

You need to ensure that Microsoft Sentinel automatically detects the threat. The solution must minimize administrative effort.

What should you do?

A. Create an analytics rule. Most Voted

B. Add the query to a workbook.

C. Create a watchlist.

D. Create a playbook.

Correct Answer: *D*

Community vote distribution

A (100%)

Previous Questions

Next Questions

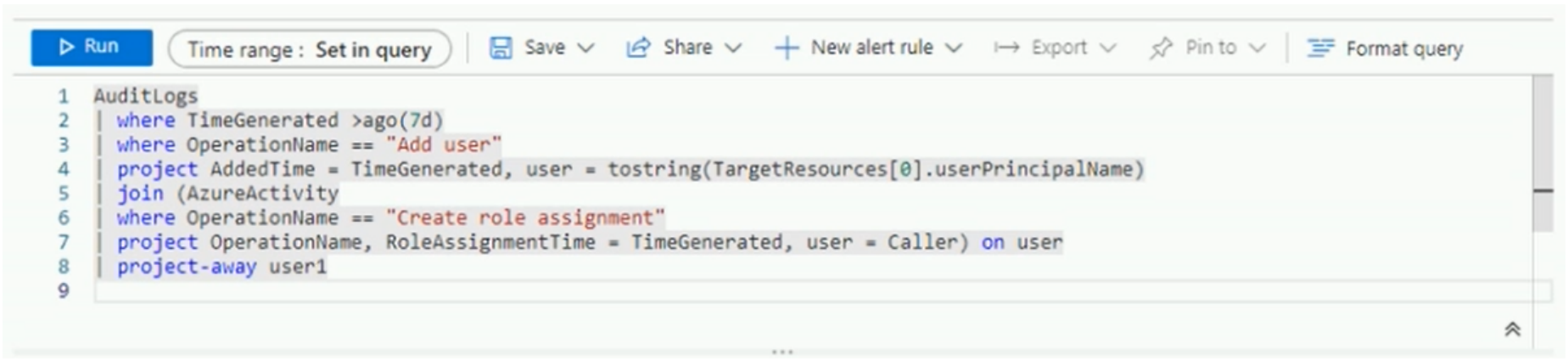
Question #53 *Topic 3*

HOTSPOT

-

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

You have the hunting query shown in the following exhibit.



The users perform the following actions:

- User1 assigns User2 the Global administrator role.
- User1 creates a new user named User3 and assigns the user a Microsoft Teams license.
- User2 creates a new user named User4 and assigns the user the Security reader role.
- User2 creates a new user named User5 and assigns the user the Security operator role.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

HOTSPOT

-

You have the following KQL 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, '
   IPCustomEntity = case(IPMatch == "SourceIP", SourceIP, IPMatch == "DestinationIP", DestinationIP, "None")
```

For each of the following statements, select Yes if the statement is true. Otherwise. select No.

NOTE: Each correct selection is worth one point.

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.	○	○

Correct Answer:

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.	○	○

HOTSPOT
-

You have a Microsoft Sentinel workspace.

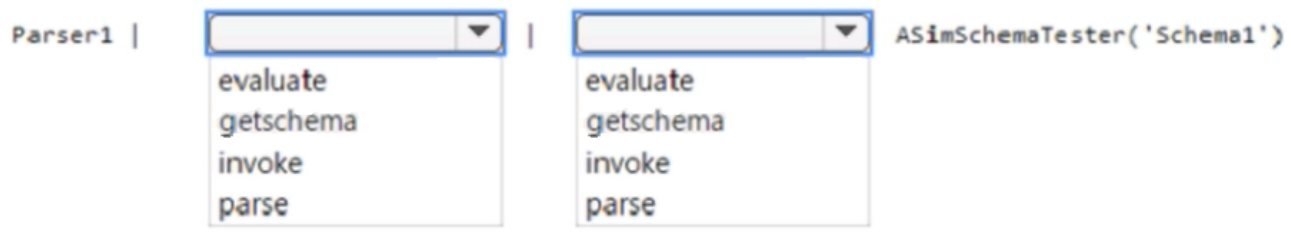
You develop a custom Advanced Security Information Model (ASIM) parser named Parser1 that produces a schema named Schema1.

You need to validate Schema1.

How should you complete the command? To answer, select the appropriate options in the answer area.

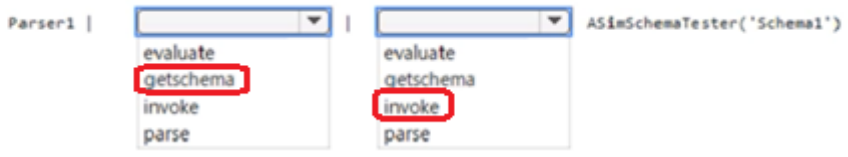
NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:

Answer Area



HOTSPOT
-

You have a Microsoft Sentinel workspace that has User and Entity Behavior Analytics (UEBA) enabled.

You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:

• Only include security-sensitive actions by users that are NOT members of the IT department.
• Minimize the number of false positives.

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

Correct Answer:

Answer Area

Previous Questions Next Questions

Question #57 *Topic 3*

HOTSPOT
-

You have a Microsoft Sentinel workspace.

You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.

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

Correct Answer:

Answer Area

HOTSPOT
-

You have an Azure subscription.

You plan to implement a Microsoft Sentinel workspace. You anticipate that you will ingest 20 GB of security log data per day.

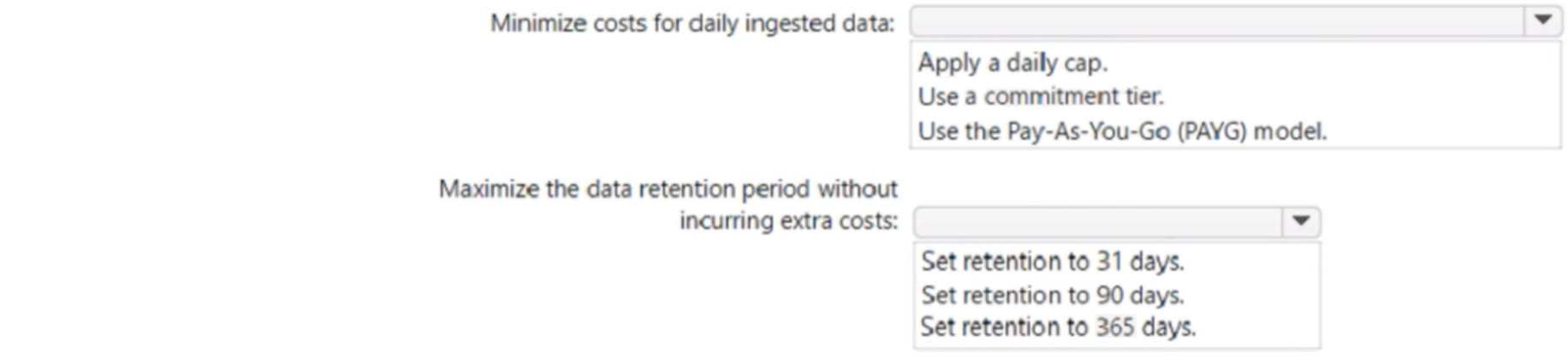
You need to configure storage for the workspace. The solution must meet the following requirements:

• Minimize costs for daily ingested data.
• Maximize the data retention period without incurring extra costs.

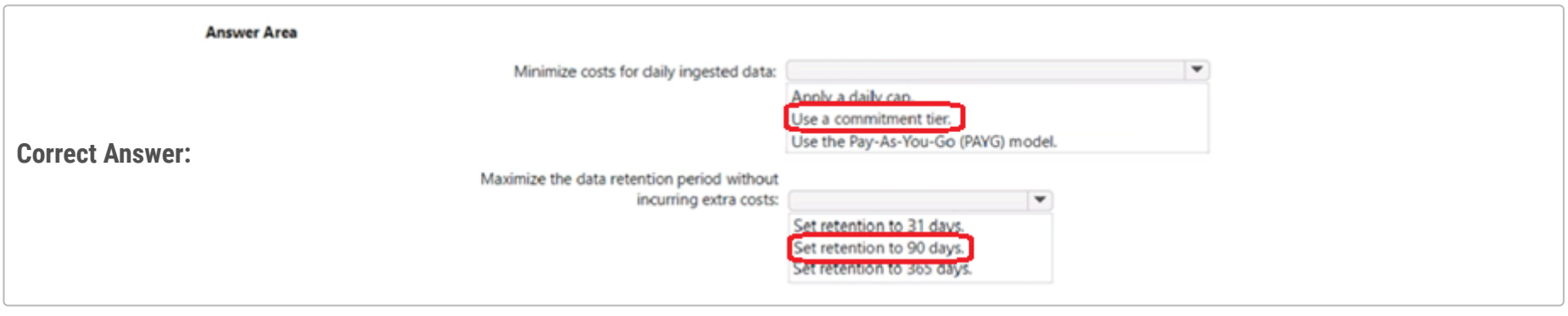
What should you do for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:



Question #59 *Topic 3*

HOTSPOT
-

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

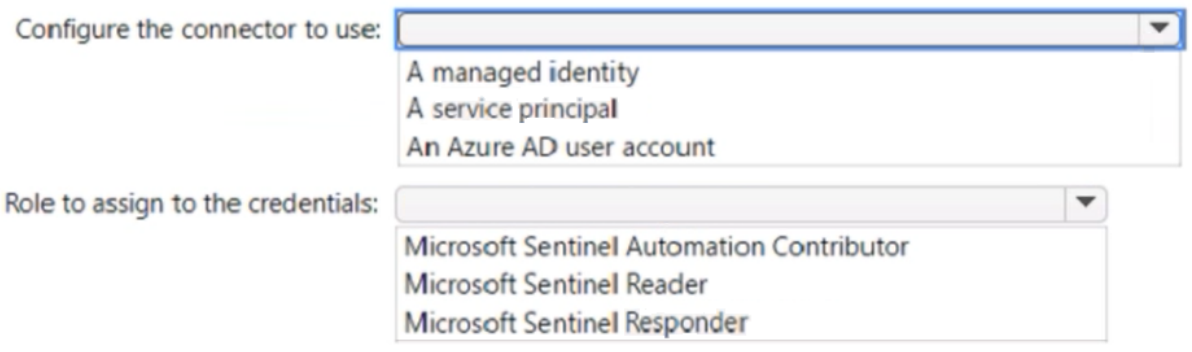
You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

• Minimize administrative effort.
• Use the principle of least privilege.

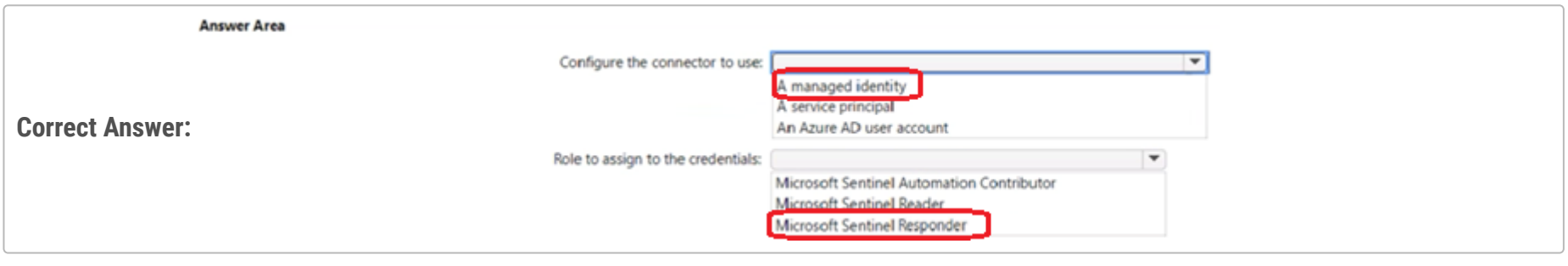
How should you configure the credentials? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Correct Answer:



Question #60 *Topic 3*

You have a Microsoft Sentinel workspace.

You need to prevent a built-in Advanced Security Information Model (ASIM) parser from being updated automatically.

What are two ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Create a hunting query that references the built-in parser.

B. Build a custom unifying parser and include the built-in parser version.

C. Redeploy the built-in parser and specify a CallerContext parameter of Any and a SourceSpecificParser parameter of Any.

D. Redeploy the built-in parser and specify a CallerContext parameter of Built-in.

E. Create an analytics rule that includes the built-in parser.

Correct Answer: *BC*

Community vote distribution

BC (100%)

Previous Questions

Next Questions

Custom View Settings

Question #61 *Topic 3*

You have a custom Microsoft Sentinel workbook named Workbook1.

You need to add a grid to Workbook1. The solution must ensure that the grid contains a maximum of 100 rows.

What should you do?

A. In the grid query, include the take operator. Most Voted

B. In the grid query, include the project operator.

C. In the query editor interface, configure Settings.

D. In the query editor interface, select Advanced Editor.

Correct Answer: *D*

Community vote distribution

A (86%) 14%

Question #62 *Topic 3*

HOTSPOT
-

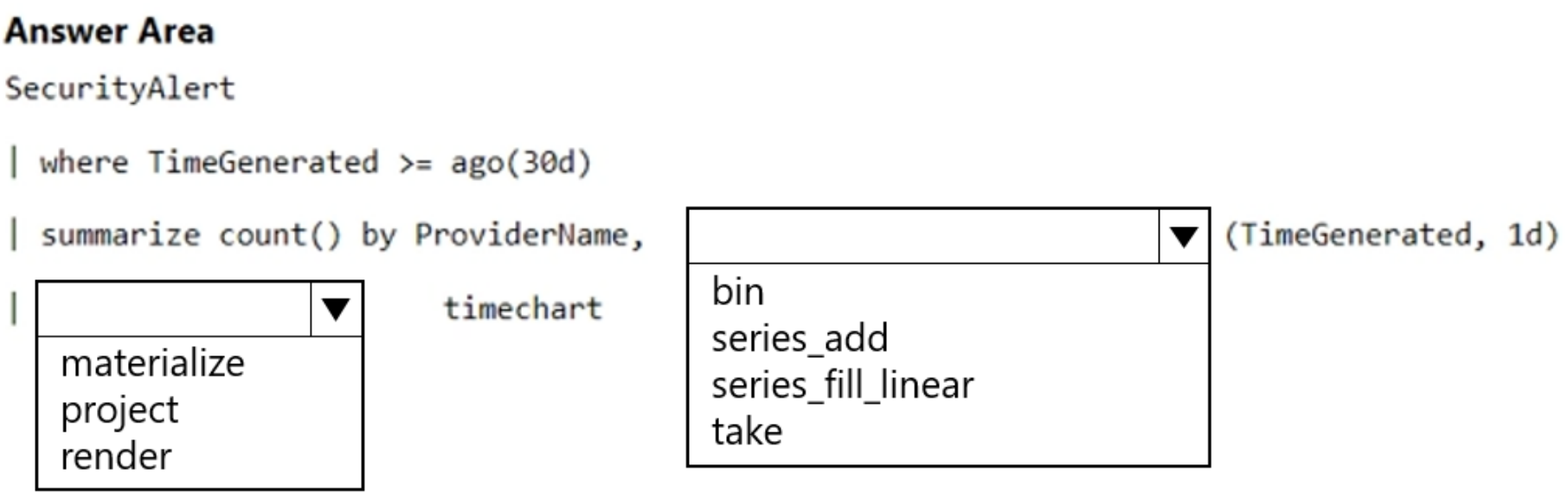
You have a Microsoft Sentinel workspace named SW1.

You plan to create a custom workbook that will include a time chart.

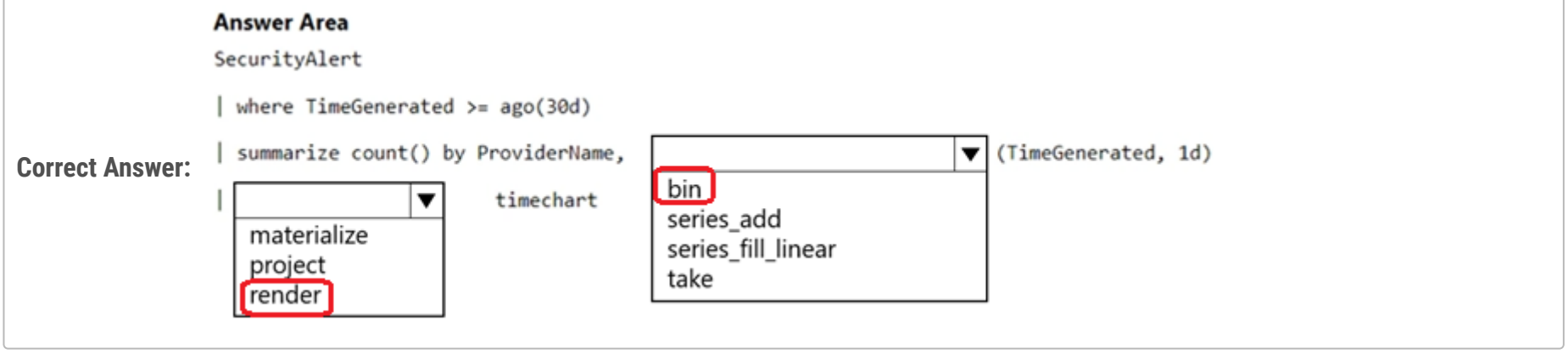
You need to create a query that will identify the number of security alerts per day for each provider.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



Question #63 *Topic 3*

You have a Microsoft Sentinel workspace named Workspace1.

You need to exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.

What should you create in Workspace1?

A. an analytic rule

B. a watchlist Most Voted

C. a workbook

D. a hunting query

Correct Answer: *B*

Community vote distribution

B (82%) A (18%)

Question #64 *Topic 3*

You have an Azure subscription that contains a Microsoft Sentinel workspace.

You need to create a playbook that will run automatically in response to a Microsoft Sentinel alert.

What should you create first?

A. a hunting query in Microsoft Sentinel

B. an Azure logic app Most Voted

C. an automation rule in Microsoft Sentinel

D. a trigger in Azure Functions

Correct Answer: *C*

Community vote distribution

B (100%)

HOTSPOT
-

You have a Microsoft Sentinel workspace named Workspace1.

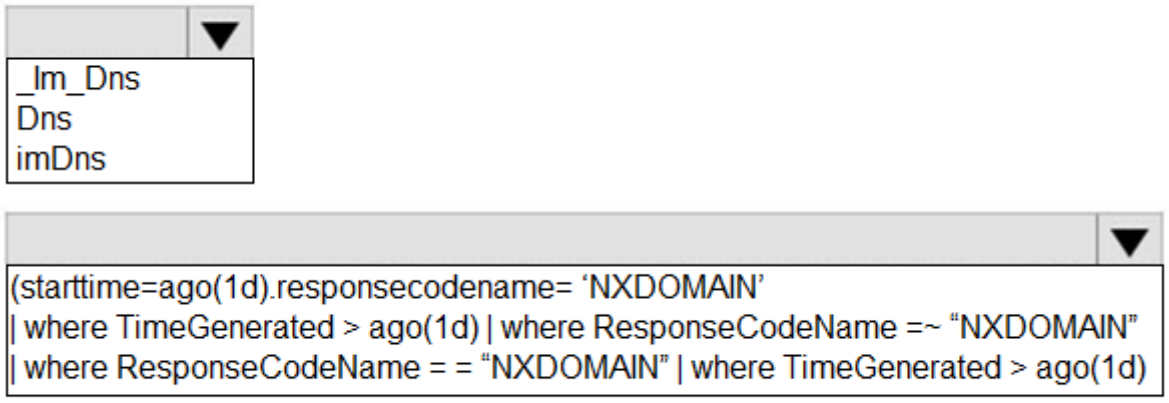
You configure Workspace1 to collect DNS events and deploy the Advanced Security Information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.

How should you complete the query? To answer, select the appropriate options in the answer area.

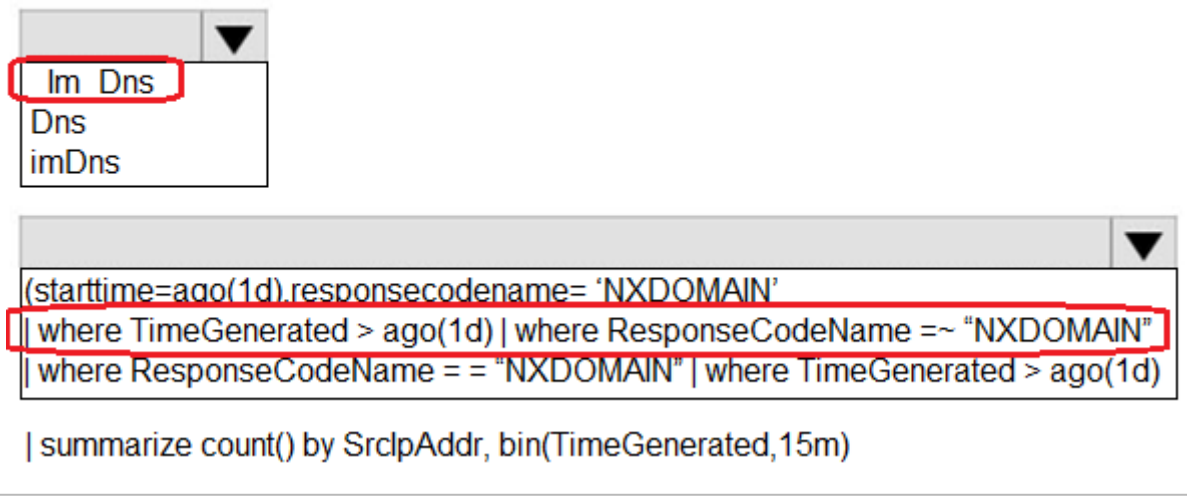
NOTE: Each correct selection is worth one point.

Answer Area



Answer Area

Correct Answer:



Previous Questions Next Questions

Custom View Settings

Question #66 *Topic 3*

HOTSPOT
-

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 in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

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

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

Correct Answer:

Answer Area

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

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

Question #67 *Topic 3*

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector.

You need to customize which details will be included when an alert is created for a specific event.

What should you do?

A. Enable User and Entity Behavior Analytics (UEBA).

B. Create a Data Collection Rule (DCR).

C. Modify the properties of the connector.

D. Create a scheduled query rule. Most Voted

Correct Answer: *A*

Community vote distribution

D (78%) C (22%)

Question #68 *Topic 3*

You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema.

You need to make the 200 parses available in Workspace1. The solution must minimize administrative effort.

What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.

B. Create a JSON file based on the DNS template.

C. Create an XML file based on the DNS template.

D. Create a YAML file based on the DNS template.

Correct Answer: *D*

Community vote distribution

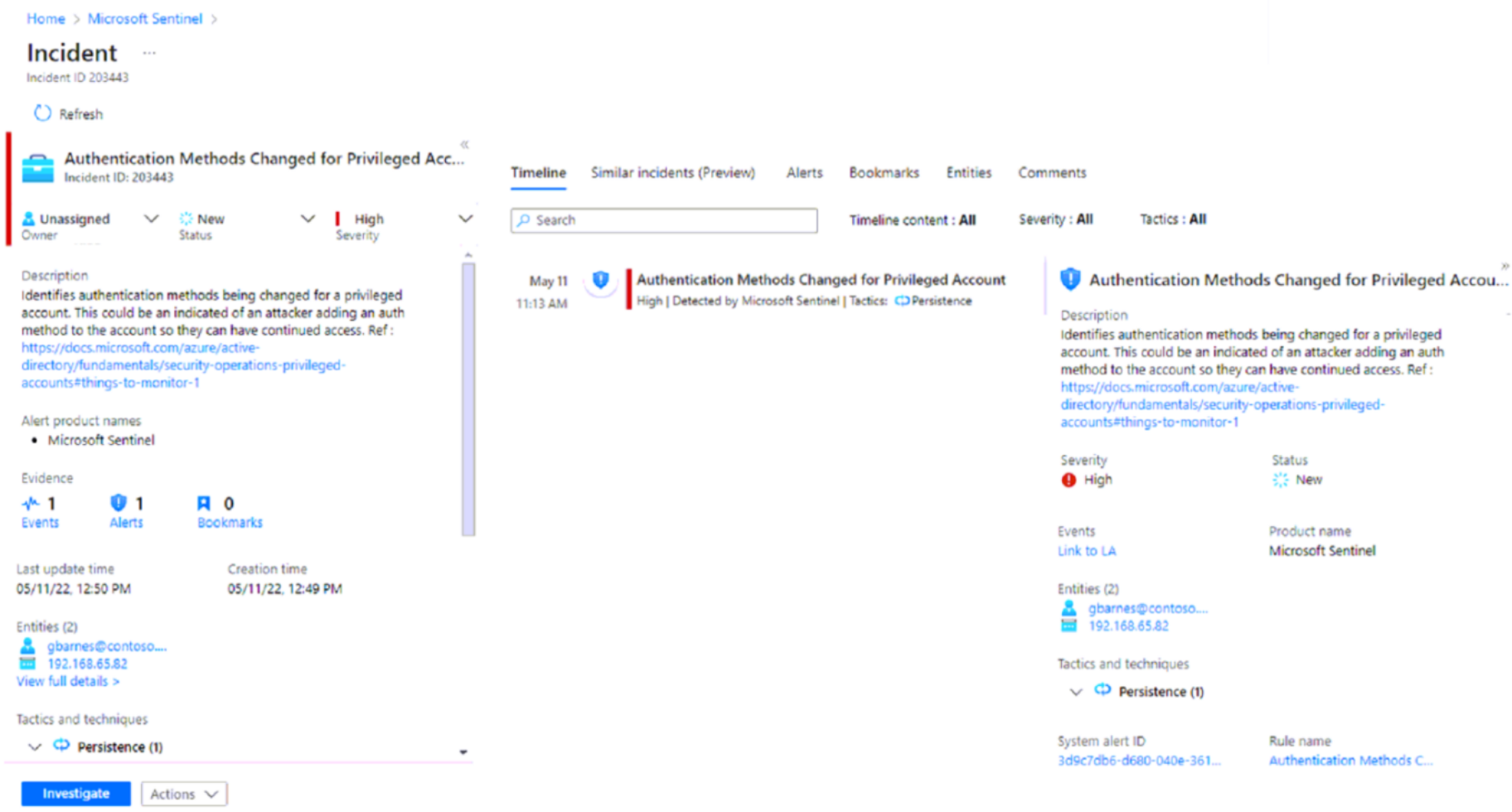
D (67%) A (17%) B (17%)

HOTSPOT

-

You have a Microsoft Sentinel workspace.

A Microsoft Sentinel incident is generated as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

A map of the entities connected to the alert can be viewed by selecting [▼]
- Alerts
- Entities
- Investigate

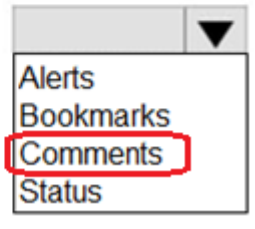
A list of the activities performed during the investigation can be viewed by selecting [▼]
- Alerts
- Bookmarks
- Comments
- Status

Correct Answer:

Answer Area

A map of the entities connected to the alert can be viewed by selecting

A list of the activities performed during the investigation can be viewed by selecting



Previous Questions

Next Questions

Topic 4 - Testlet 1

Question #1 *Topic 4*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive

B. sales Most Voted

C. marketing

Correct Answer: *B*

Reference:

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

Community vote distribution

B (100%)

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question

The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive

B. marketing Most Voted

C. security

D. sales

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

Community vote distribution

B (100%)

Topic 5 - Testlet 2

Question #1 *Topic 5*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -
Litware plans to implement the following changes:
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
▪
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
You need to implement the Azure Information Protection requirements.
What should you configure first?

A. Device health and compliance reports settings in Microsoft Defender Security Center
B. scanner clusters in Azure Information Protection from the Azure portal
C. content scan jobs in Azure Information Protection from the Azure portal
D. Advanced features from Settings in Microsoft Defender Security Center Most Voted

Correct Answer: *D*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview

Community vote distribution
D (91%) 9%

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
▪
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements and resolve the reported problem.
Which policy should you modify?

A. Activity from suspicious IP addresses
B. Activity from anonymous IP addresses
C. Impossible travel
D. Risky sign-in

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

Community vote distribution
C (67%) B (33%)

Previous Questions Next Questions

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

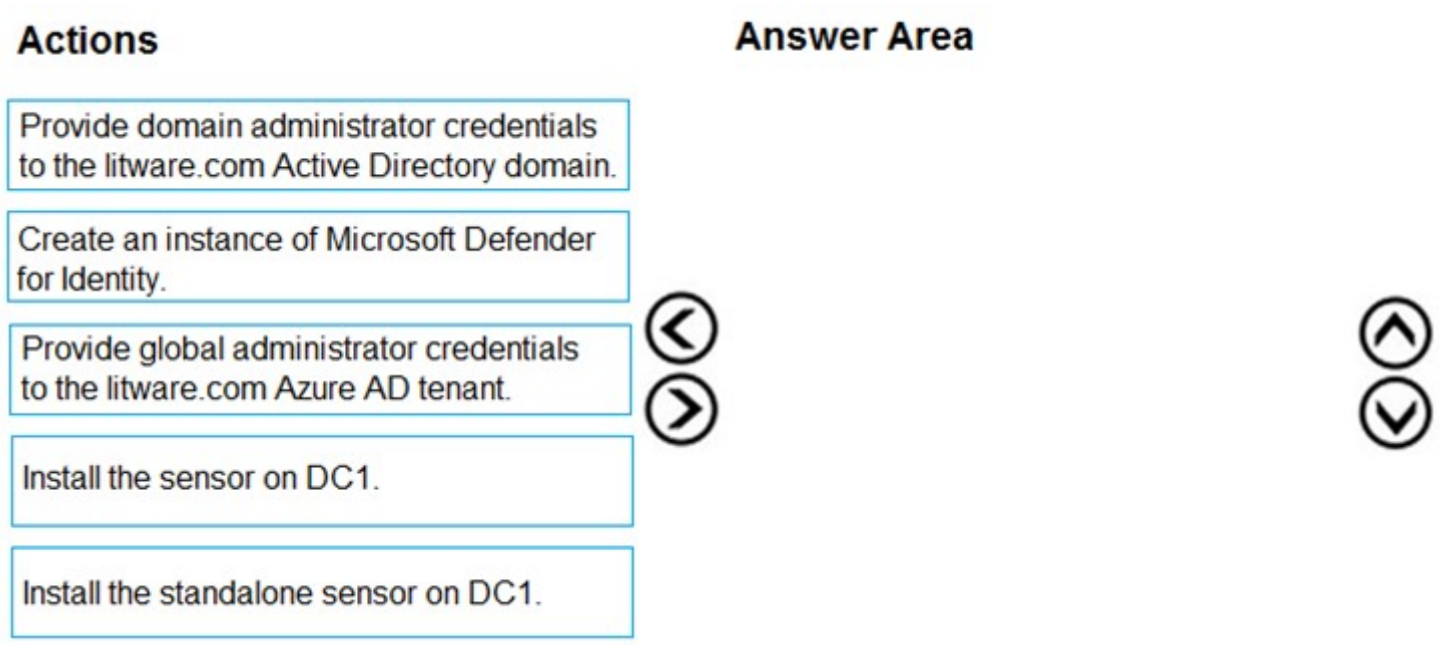
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
▪
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

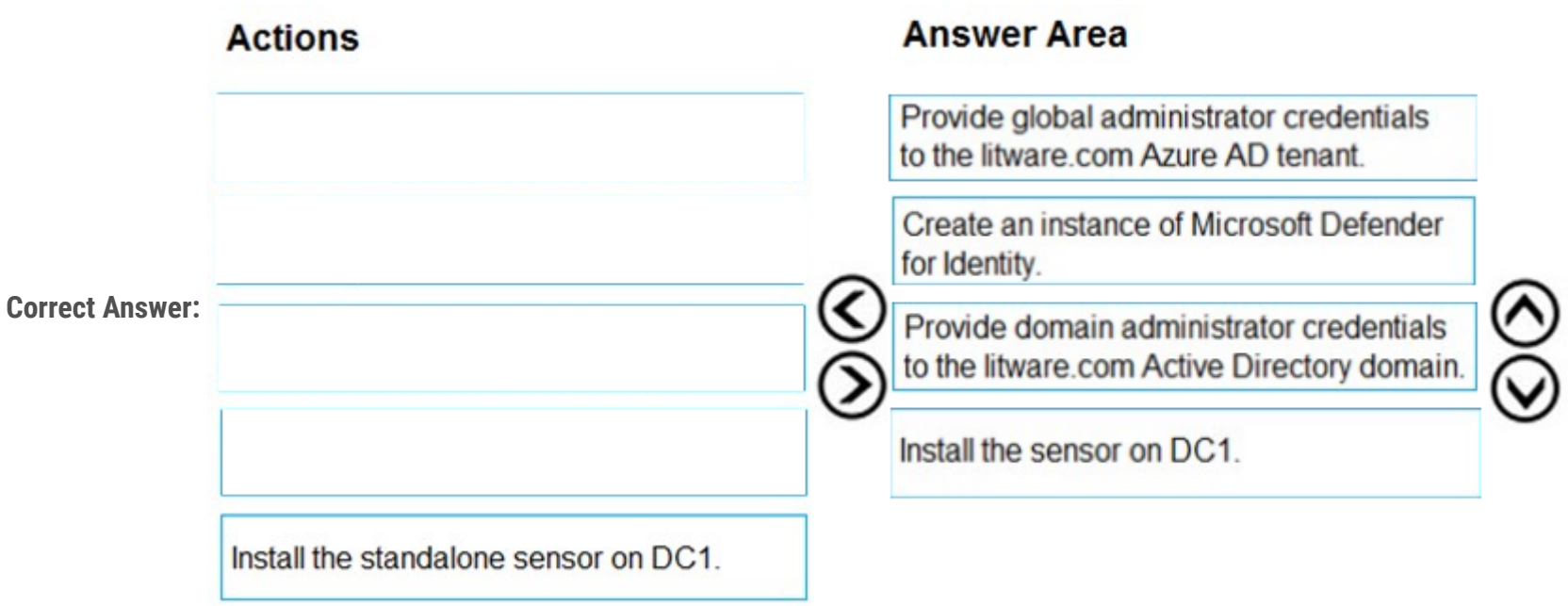
Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
DRAG DROP -
You need to configure DC1 to meet the business requirements.
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:



Correct Answer:



Step 1: log in to https://portal.atp.azure.com as a global admin

Step 2: Create the instance -

Step 3. Connect the instance to Active Directory

Step 4. Download and install the sensor.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/install-step1 https://docs.microsoft.com/en-us/defender-for-identity/install-step4

Topic 6 - Testlet 3

Question #1 *Topic 6*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -
Litware plans to implement the following changes:
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
▪
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
HOTSPOT -
You need to implement Azure Defender to meet the Azure Defender requirements and the business 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.
Hot Area:

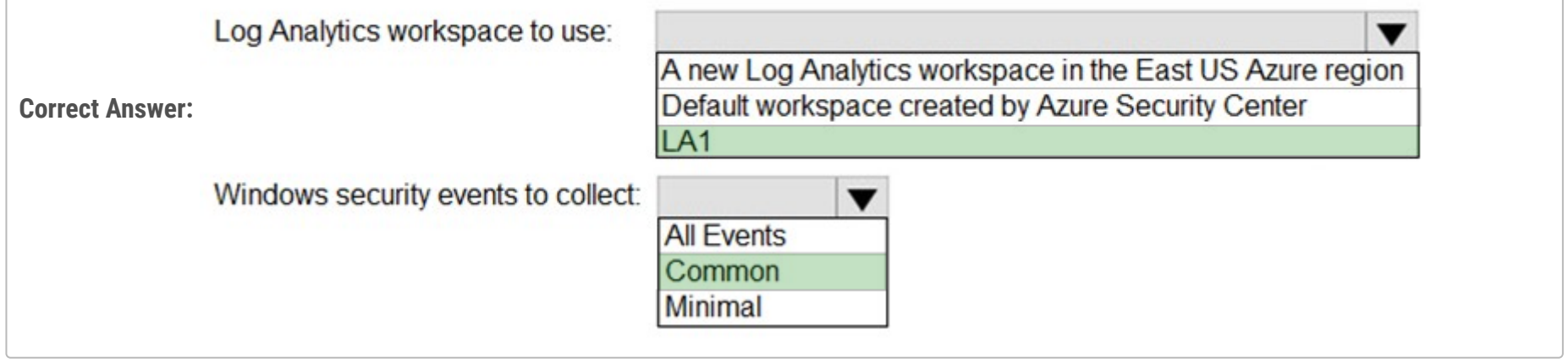
Answer Area

Log Analytics workspace to use:
- A new Log Analytics workspace in the East US Azure region
- Default workspace created by Azure Security Center
- LA1

Windows security events to collect:
- All Events
- Common
- Minimal

Answer Area

Correct Answer:



Topic 7 - Testlet 4

Question #1 *Topic 7*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

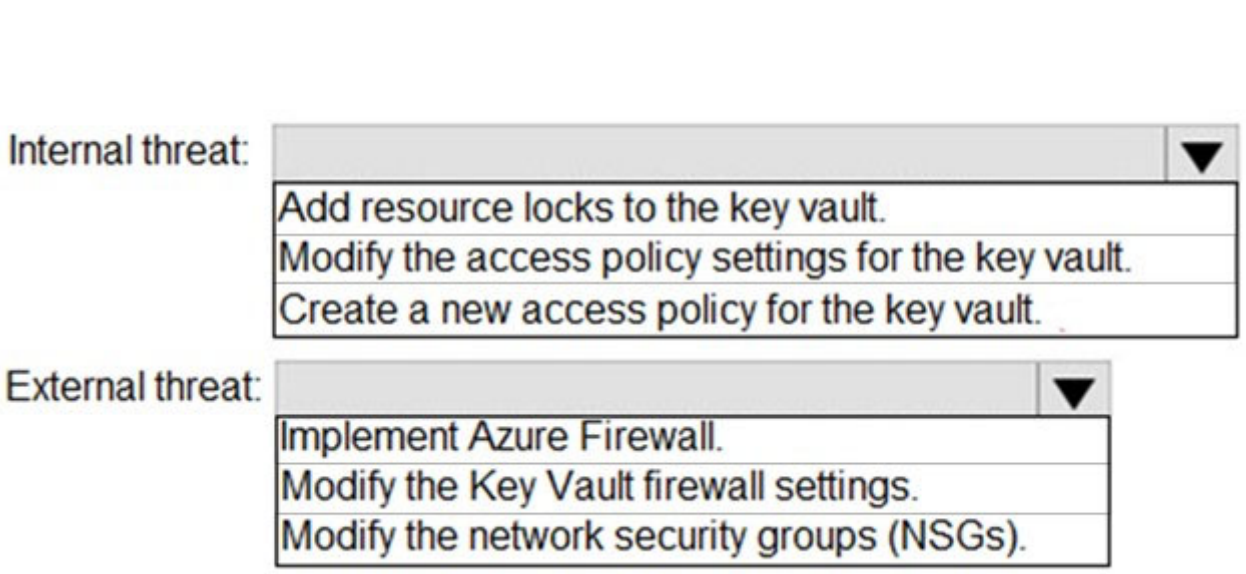
Technical Requirements -

Contoso identifies the following technical requirements:

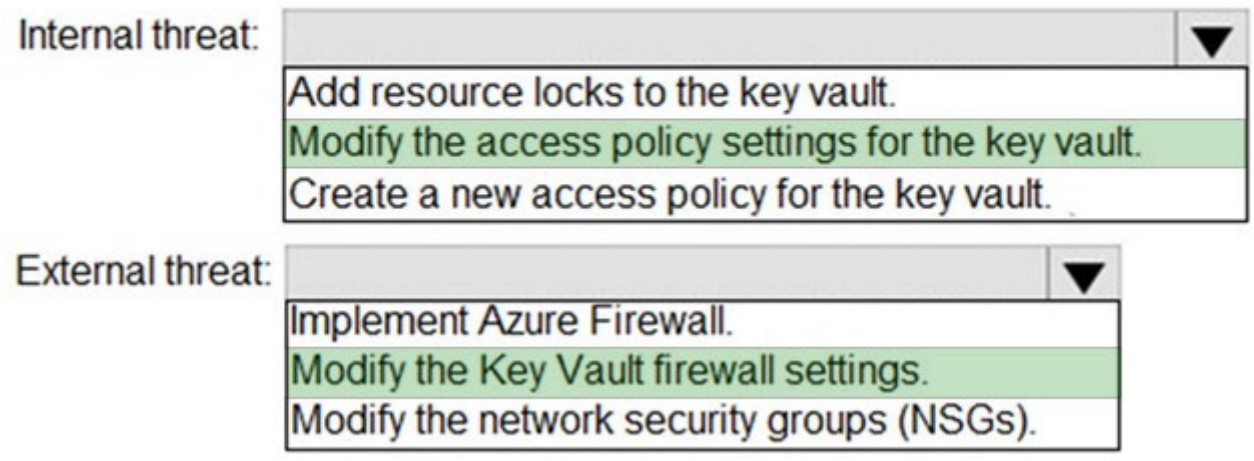
Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Contoso in case of external and internal threats. The solution must minimize the impact on legitimate attempts to access the key vault content.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question
HOTSPOT -
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Correct Answer:



Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/security-features https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Contoso in case of external and internal threats. The solution must minimize the impact on legitimate attempts to access the key vault content.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.
What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender Most Voted

C. Azure Firewall

D. Azure Application Gateway

Correct Answer: *B*

Reference:

https://docs.microsoft.com/en-us/azure/security-center/azure-defender

Community vote distribution

B (100%)

Previous Questions

Next Questions

Topic 8 - Testlet 5

Question #1 *Topic 8*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.
Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question
You need to complete the query for failed sign-ins to meet the technical requirements.
Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center

B. Activity log in Azure

C. Azure Advisor

D. the query windows of the Log Analytics workspace Most Voted

Correct Answer: *D*

Community vote distribution

D (100%)

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question

You need to remediate active attacks to meet the technical requirements.
What should you include in the solution?

A. Azure Automation runbooks

B. Azure Logic Apps

C. Azure Functions

D. Azure Sentinel livestreams

Correct Answer: *B*

Reference:
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Community vote distribution

B (100%)

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question

HOTSPOT -
You need to create an advanced hunting query to investigate the executive team issue.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

[▼]
- CloudAppEvents
- DeviceFileEvents
- DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount = [ ▼ ] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

- avg()
- count()
- sum()

Correct Answer:

Answer Area

[▼]
- CloudAppEvents
- DeviceFileEvents
- DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount = [ ▼ ] by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

- avg()
- count()
- sum()

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

A company named Contoso Ltd. has a main office and five branch offices located throughout North America. The main office is in Seattle. The branch offices are in Toronto, Miami, Houston, Los Angeles, and Vancouver.

Contoso has a subsidiary named Fabrikam, Ltd. that has offices in New York and San Francisco.

Existing Environment -

End-User Environment -

All users at Contoso use Windows 10 devices. Each user is licensed for Microsoft 365. In addition, iOS devices are distributed to the members of the sales team at Contoso.

Cloud and Hybrid Infrastructure -

All Contoso applications are deployed to Azure.

You enable Microsoft Cloud App Security.

Contoso and Fabrikam have different Azure Active Directory (Azure AD) tenants. Fabrikam recently purchased an Azure subscription and enabled Azure Defender for all supported resource types.

Current Problems -

The security team at Contoso receives a large number of cybersecurity alerts. The security team spends too much time identifying which cybersecurity alerts are legitimate threats, and which are not.

The Contoso sales team uses only iOS devices. The sales team members exchange files with customers by using a variety of third-party tools. In the past, the sales team experienced phishing attacks on their devices.

The marketing team at Contoso has several Microsoft SharePoint Online sites for collaborating with external vendors. The marketing team has had several incidents in which vendors uploaded files that contain malware.

The executive team at Contoso suspects a security breach. The executive team requests that you identify which files had more than five activities during the past

48 hours, including data access, download, or deletion for Microsoft Cloud App Security-protected applications.

Requirements -

Planned Changes -

Contoso plans to integrate the security operations of both companies and manage all security operations centrally.

Technical Requirements -

Contoso identifies the following technical requirements:

Receive alerts if an Azure virtual machine is under brute force attack.

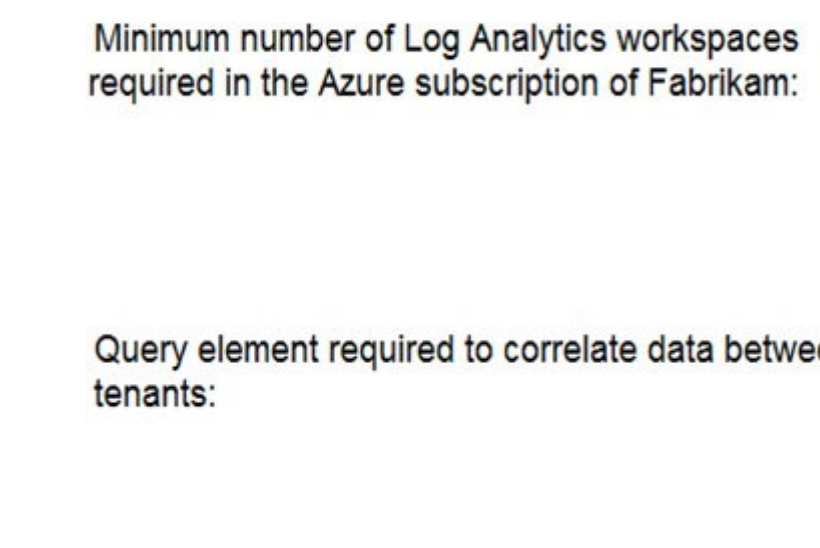
Use Azure Sentinel to reduce organizational risk by rapidly remediating active attacks on the environment.

Implement Azure Sentinel queries that correlate data across the Azure AD tenants of Contoso and Fabrikam.

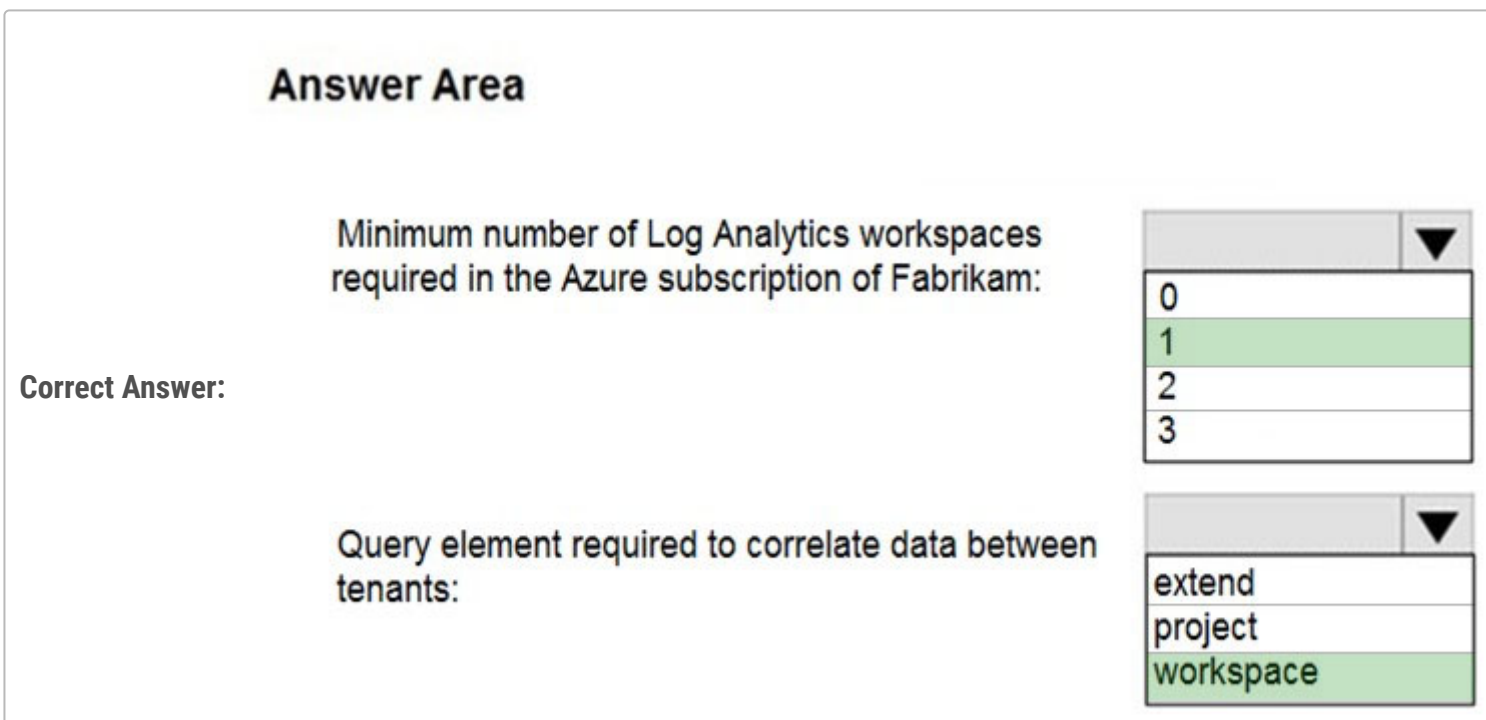
Develop a procedure to remediate Azure Defender for Key Vault alerts for Fabrikam in case of external attackers and a potential compromise of its own Azure
AD applications.
Identify all cases of users who failed to sign in to an Azure resource for the first time from a given country. A junior security administrator provides you with the following incomplete query.

BehaviorAnalytics -
| where ActivityType == "FailedLogOn"
| where _____ == True

Question
HOTSPOT -
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.
Hot Area:



Correct Answer:



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

Previous Questions
Next Questions

Topic 9 - Testlet 6

Question #1 *Topic 9*

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -
Litware plans to implement the following changes:
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center

B. Cloud App Security anomaly detection policies

C. Advanced features from Settings in Microsoft Defender Security Center Most Voted

D. the Cloud Discovery settings in Cloud App Security Most Voted

Correct Answer: *CD*
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

Community vote distribution
CD (100%)

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

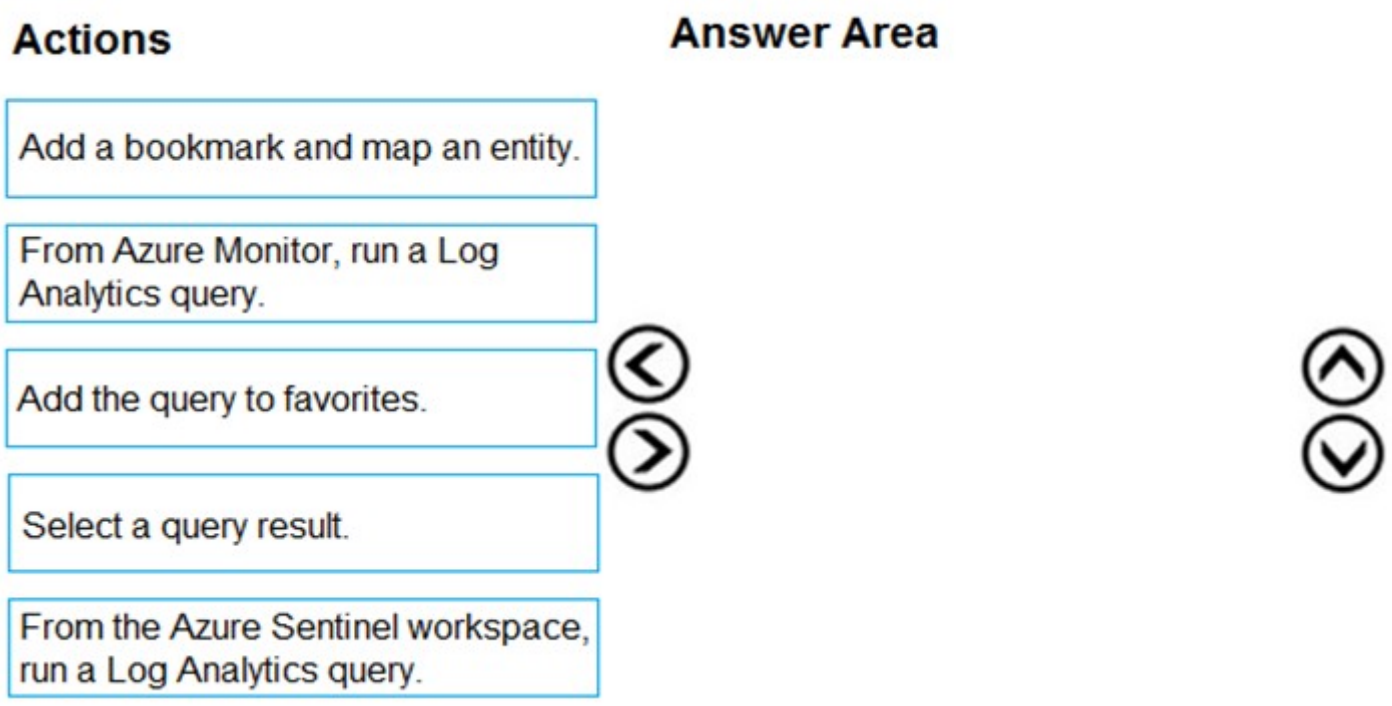
Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

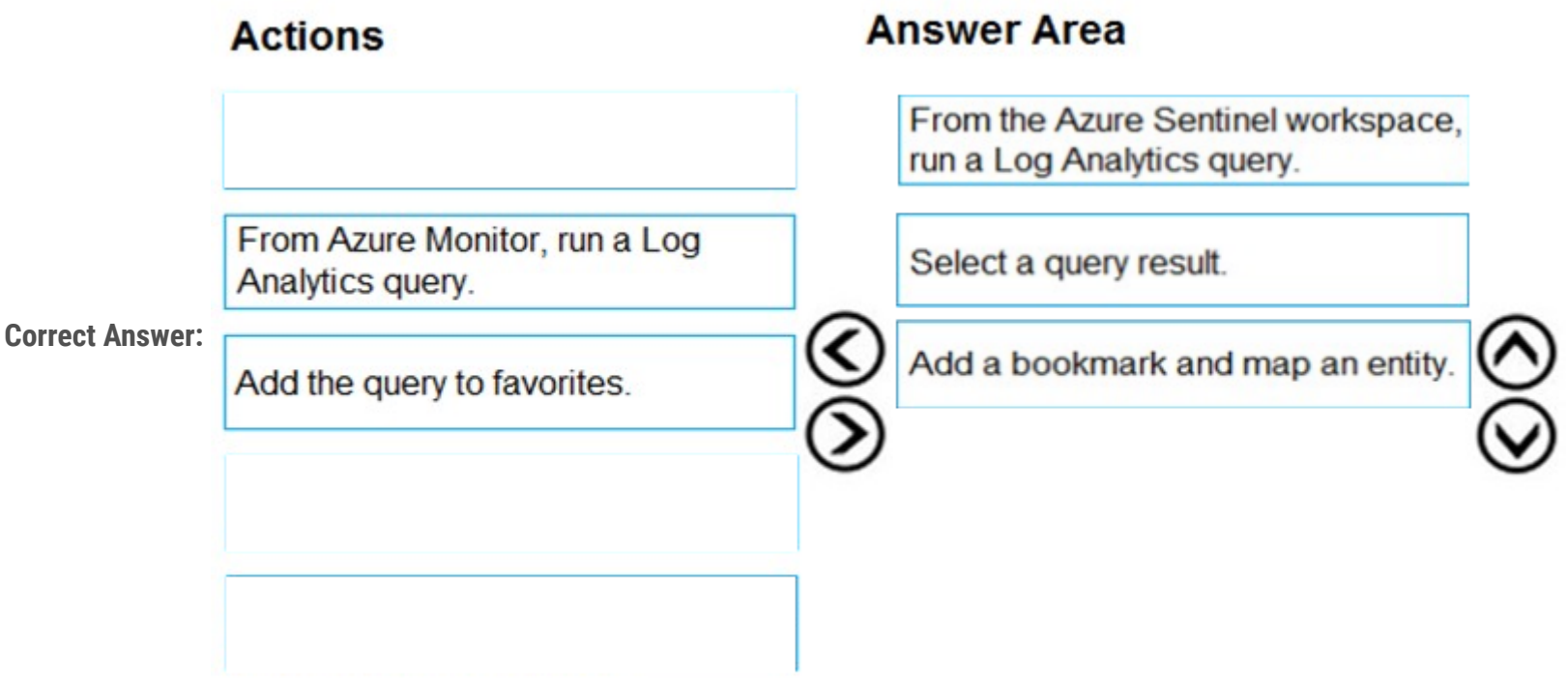
Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
DRAG DROP -
You need to add notes to the events to meet the Azure Sentinel requirements.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.
Select and Place:



Correct Answer:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
HOTSPOT -
You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

In the Cloud App Security portal:

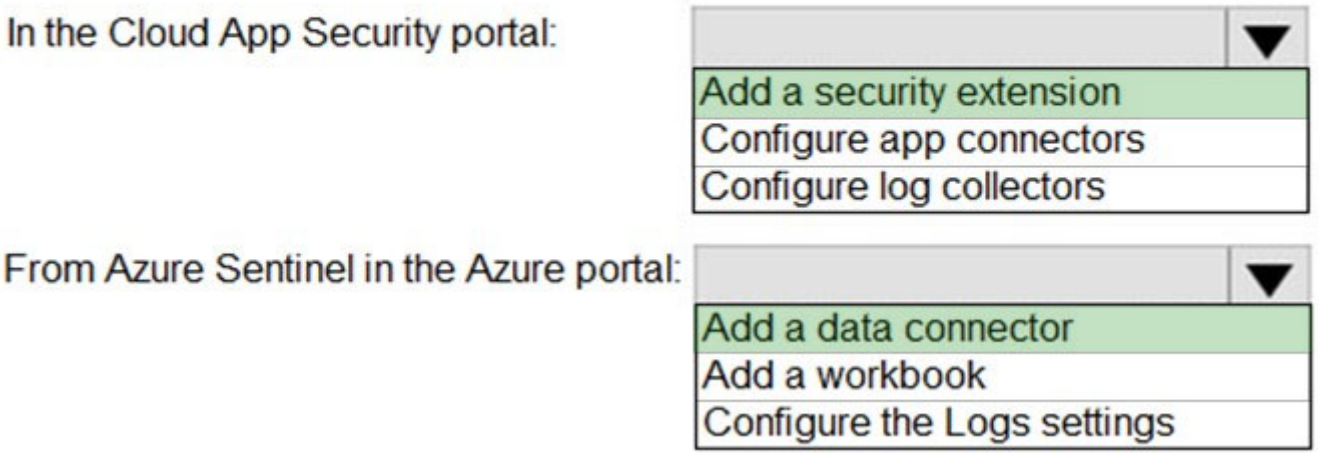
- Add a security extension
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal:

- Add a data connector
- Add a workbook
- Configure the Logs settings

Answer Area

Correct Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A. Automation Operator
B. Automation Runbook Operator
C. Azure Sentinel Contributor Most Voted
D. Azure Sentinel Responder

Correct Answer: *C*
Litware must meet the following requirements:
☞ Ensure that a user named admin1 can configure Azure Sentinel playbooks.
☞ The principle of least privilege must be used whenever possible.
Azure Sentinel Contributor can view data, incidents, workbooks, and other Azure Sentinel resources, manage incidents (assign, dismiss, etc.), create and edit workbooks, analytics rules, and other Azure Sentinel resources.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Community vote distribution
C (100%)

Previous Questions
Next Questions

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

Question
Which rule setting should you configure to meet the Azure Sentinel requirements?

A. From Set rule logic, turn off suppression.

B. From Analytics rule details, configure the tactics.

C. From Set rule logic, map the entities. Most Voted

D. From Analytics rule details, configure the severity.

Correct Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

Community vote distribution
C (100%)

Introductory Info

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment -

Identity Environment -

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment -

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run

Windows 10. All Microsoft Cloud App Security built-in anomaly detection policies are enabled.

Azure Environment -

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment -

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment -

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current problems -

Cloud App Security frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes -

Litware plans to implement the following changes:

Create and configure Azure Sentinel in the Azure subscription.
Validate Azure Sentinel functionality by using Azure AD test user accounts.

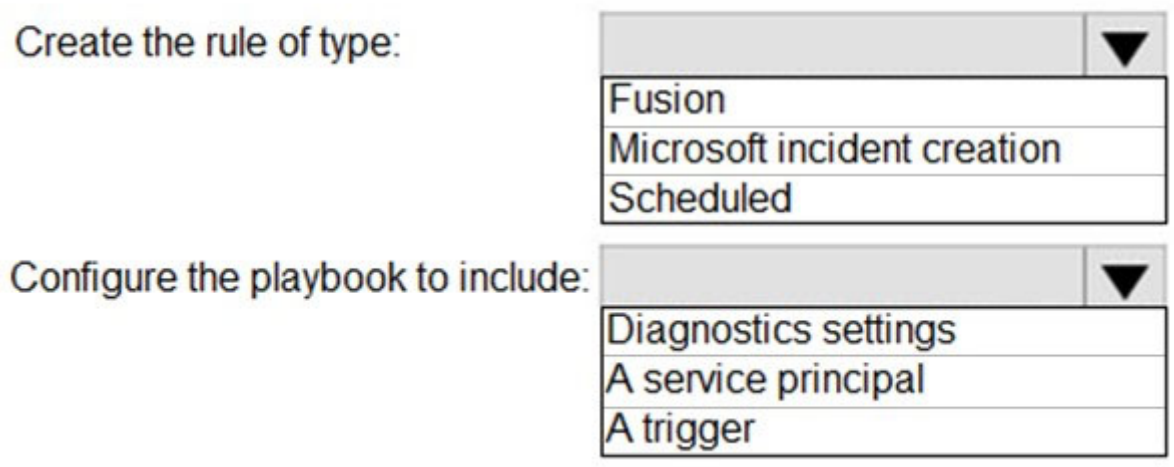
Business Requirements -
Litware identifies the following business requirements:
The principle of least privilege must be used whenever possible.
Costs must be minimized, as long as all other requirements are met.
Logs collected by Log Analytics must provide a full audit trail of user activities.
All domain controllers must be protected by using Microsoft Defender for Identity.
Azure Information Protection Requirements
All files that have security labels and are stored on the Windows 10 computers must be available from the Azure Information Protection `" Data discovery dashboard.
Microsoft Defender for Endpoint requirements
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Microsoft Cloud App Security requirements
Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements -
All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements -
Litware must meet the following Azure Sentinel requirements:
Integrate Azure Sentinel and Cloud App Security.
Ensure that a user named admin1 can configure Azure Sentinel playbooks.
Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

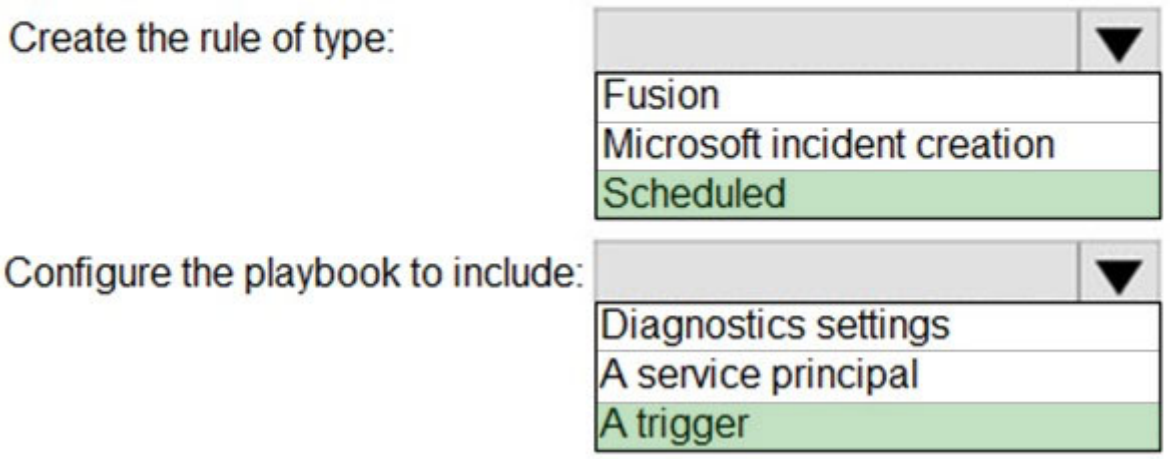
Question
HOTSPOT -
You need to create the analytics rule to meet the Azure Sentinel requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area



Answer Area

Correct Answer:



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

Previous Questions