Microsoft.VCEup.com.SC-200.2022-Aug-01.85q.vce

Number: SC-200
Passing Score: 800
Time Limit: 120 min

Exam Code: SC-200
Exam Name: Microsoft Security Operations Analyst
Certification Provider: Microsoft
Corresponding Certification: Microsoft Certified: Security Operations Analyst Associate
Website: www.vceup.com

01 - Mitigate threats using Microsoft 365 Defender

QUESTION 1
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 various 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
```

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive
B. sales
C. marketing

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 3
The issue for which team can be resolved by using Microsoft Defender for Office 365?

A. executive
B. marketing
C. security
D. sales

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoft. co m/en-us/microsoft-365/securitv/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

02 - Mitigate threats using Microsoft 365 Defender

QUESTION 1
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 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

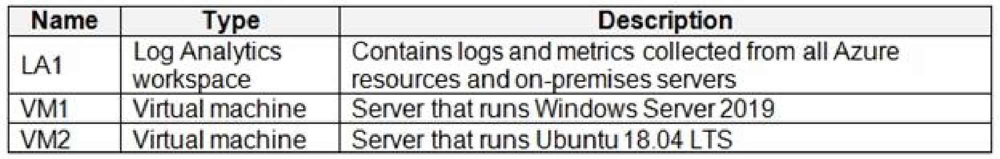
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

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.



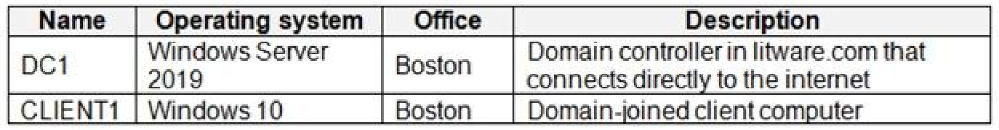
Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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

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.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 3
You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements.
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
Section: (none)
Explanation

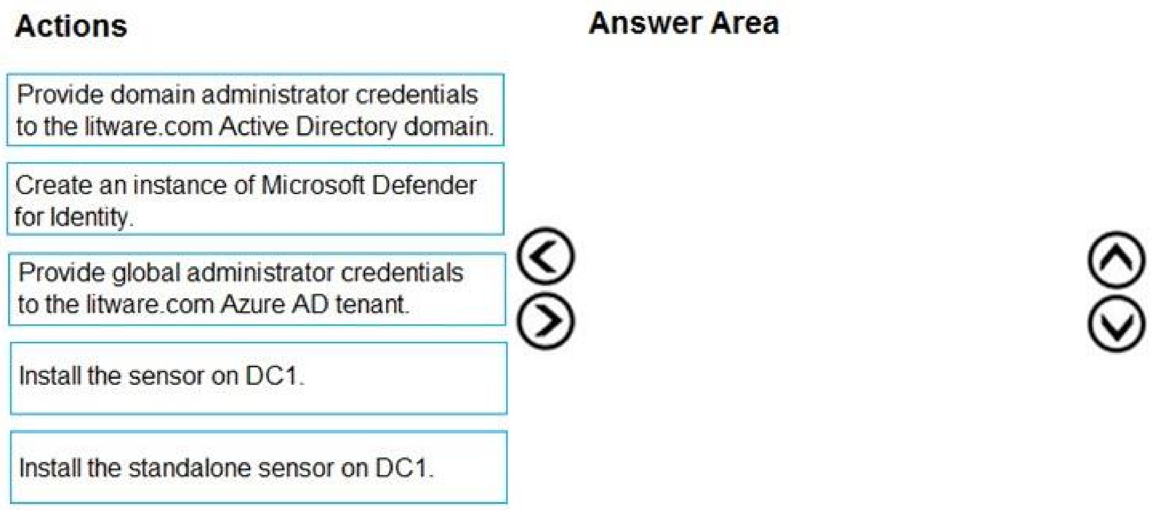
Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

QUESTION 4
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:



Actions

Provide domain administrator credentials to the litware.com Active Directory domain.

Create an instance of Microsoft Defender for Identity.

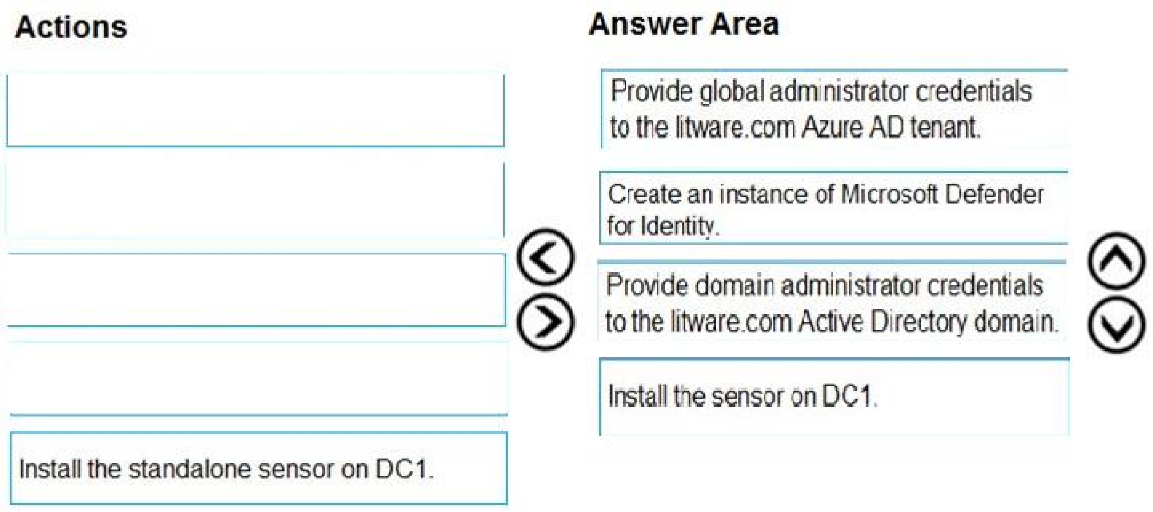
Provide global administrator credentials to the litware.com Azure AD tenant.

Install the sensor on DC1.

Install the standalone sensor on DC1.

Answer Area

Correct Answer:



Actions

Install the standalone sensor on DC1.

Answer Area

Provide global administrator credentials to the litware.com Azure AD tenant.

Create an instance of Microsoft Defender for Identity.

Provide domain administrator credentials to the litware.com Active Directory domain.

Install the sensor on DC1.

Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

03 - Mitigate threats using Microsoft 365 Defender

QUESTION 1
You need to receive a security alert when a user attempts to sign in from a location that was nevsr 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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomalv-detection-policy

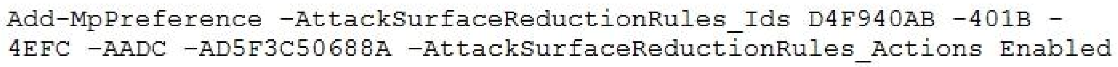
QUESTION 2
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents.
What should you use to detect which documents are sensitive?

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

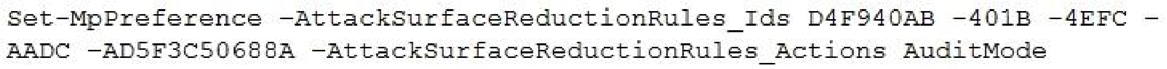
Correct Answer: C
Section: (none)
Explanation

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

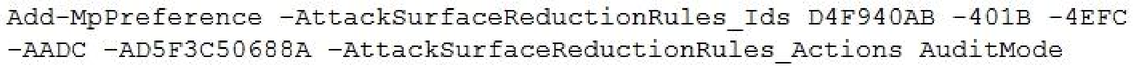
QUESTION 3
Your company uses line-of-business apps that contain Microsoft Office VBA macros.
You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.
You need to identify which Office VBA macros might be affected.
Which 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.


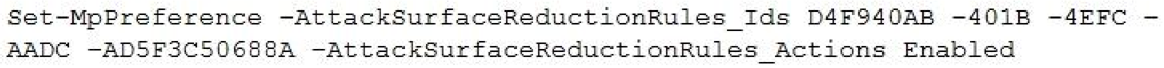
```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

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
Section: (none)
Explanation

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

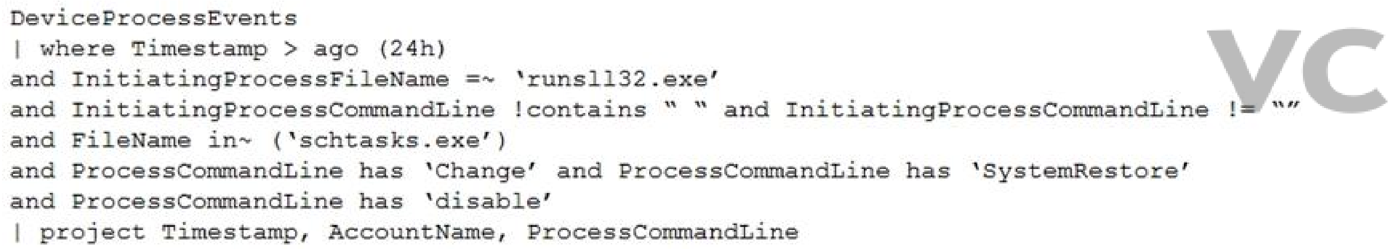
QUESTION 4
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/windows/securitv/threat-protection/microsoft-defender-atp/manaqe-alerts

QUESTION 5
You have the following advanced hunting query in Microsoft 365 Defender.



```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

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

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

NOTE: Each correct selection is worth one point.

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

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoftcom/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

QUESTION 6
You are investigating a potential attack that deploys a new ransomware strain.
You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.
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.
B. Add the device users to the admin role.
C. Add a tag to the machines.
D. Create a new device group that has a rank of 1.
E. Create a new admin role.
F. Create a new device group that has a rank of 4.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manaqe-access

QUESTION 7
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
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manaqe-sensitive-honeytoken-accounts

QUESTION 8
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 Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manaqe-sensitive-honeytoken-accounts

QUESTION 9

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manaqe-sensitive-honeytoken-accounts

QUESTION 10
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
B. Replace
C. Block and Enable redirect
D. Monitor and Enable redirect

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoft. co m/en-us/microsoft-365/securitv/office-365-security/safe-attachments?view=o365-worldwide

QUESTION 11
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
D. a certificate indicator that has Action set to Alert and block

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.eom/en-us/microsoft-365/securitv/defender-endpoint/i nd icator-file?view=o365-worldwide

QUESTION 12
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
C. the Security Administrator role in Azure Active Directory (Azure AD)
D. the Security Reader role in Azure Active Directory (Azure AD)

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoft. co m/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

QUESTION 13
DRAG DROP

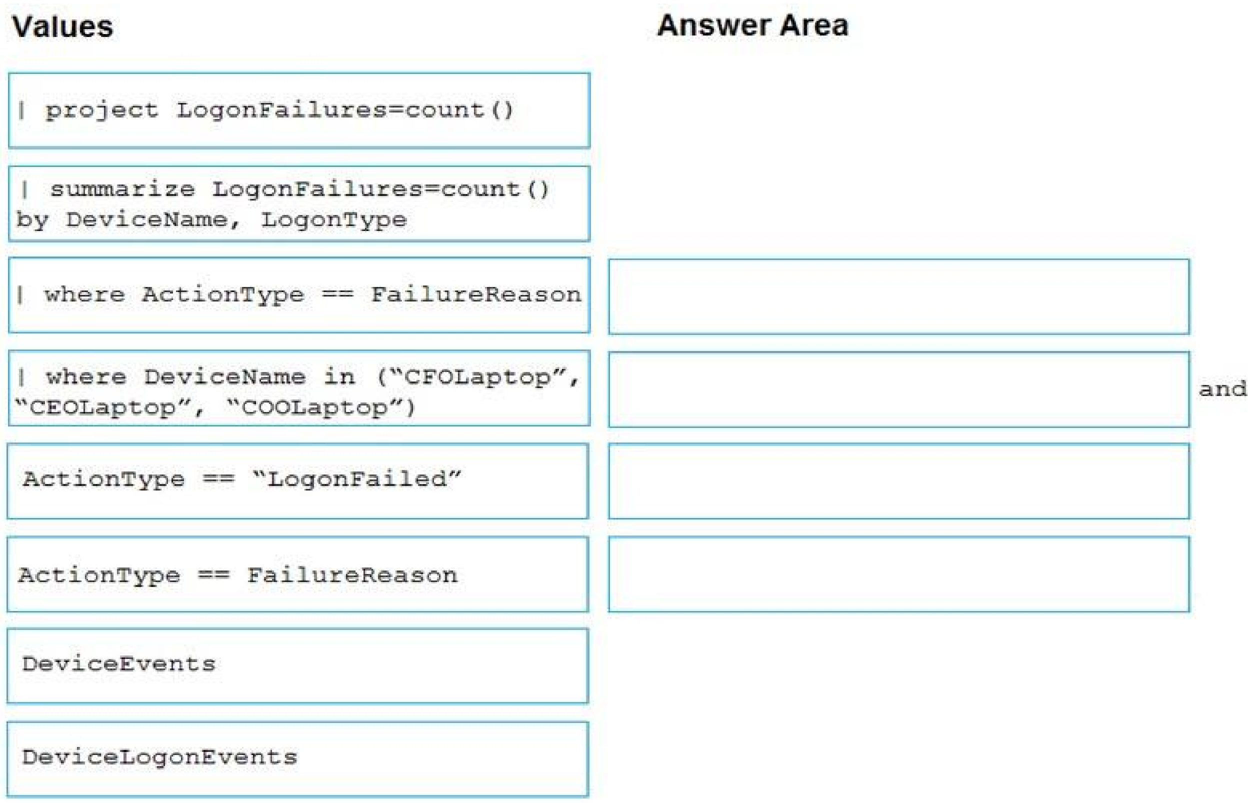
You are investigating an incident by using Microsoft 365 Defender.

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"
```

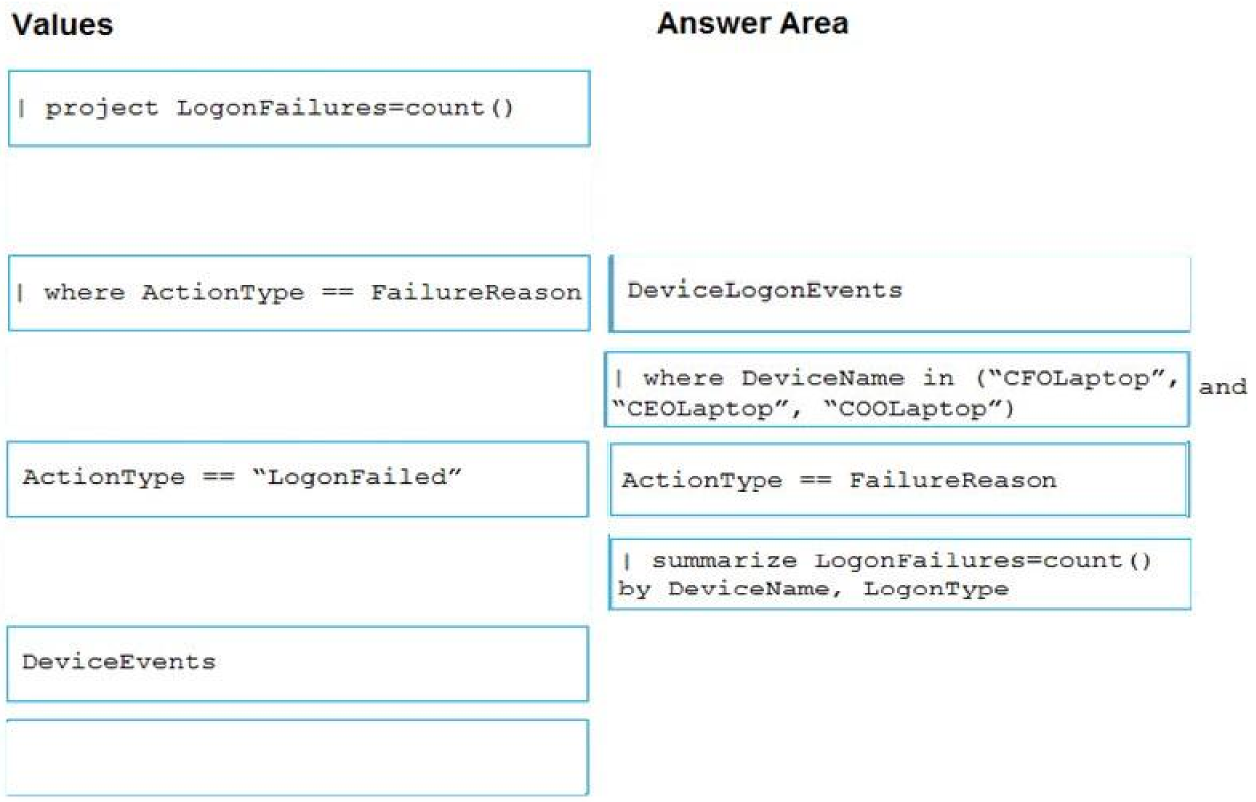
```
ActionType == FailureReason
```

```
DeviceEvents
```

```
DeviceLogonEvents
```

Answer Area

Correct Answer:



Values

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

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

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

```
DeviceEvents
```

Answer Area

```
DeviceLogonEvents
```

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

and

```
ActionType == FailureReason
```

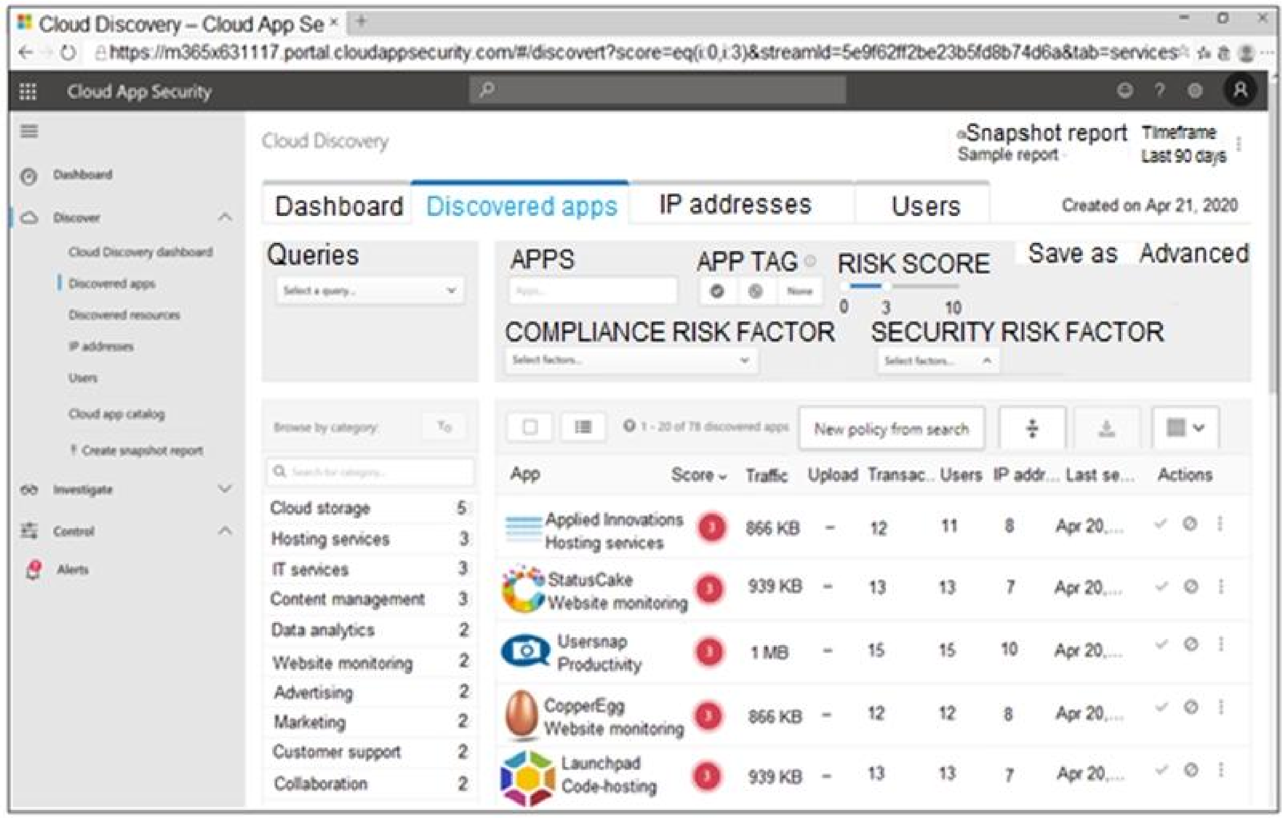
```
| summarize LogonFailures=count()
by DeviceName, LogonType
```

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
DRAG DROP

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



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

Created on Apr 21, 2020

1 - 20 of 78 discovered apps

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

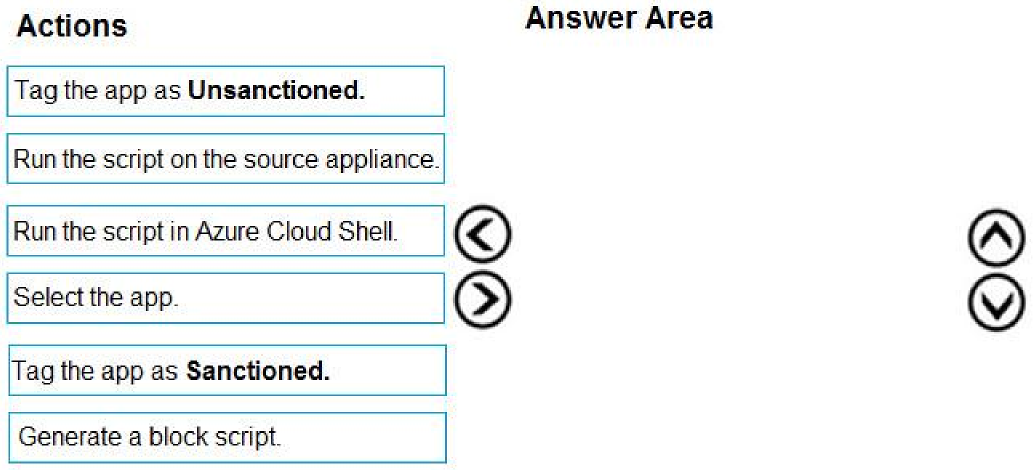
App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	3	866 KB	–	12	11	8	Apr 20,...	
StatusCake Website monitoring	3	939 KB	–	13	13	7	Apr 20,...	
Usersnap Productivity	3	1 MB	–	15	15	10	Apr 20,...	
CopperEgg Website monitoring	3	866 KB	–	12	12	8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

Your environment does NOT have Microsoft Defender for Endpoint enabled.

You need to remediate the risk for the Launchpad app.

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

Select and Place:

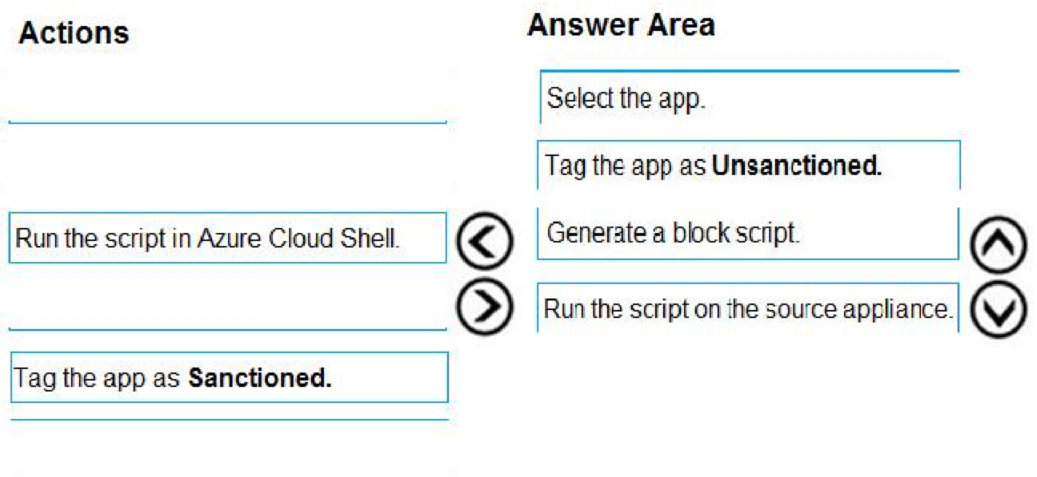


Actions

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

Answer Area

Correct Answer:



Actions

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned.**

Answer Area

Select the app.

Tag the app as **Unsanctioned.**

Generate a block script.

Run the script on the source appliance.

Section: (none)
Explanation

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

QUESTION 15
HOTSPOT

You have a Microsoft 365 E5 subscription.

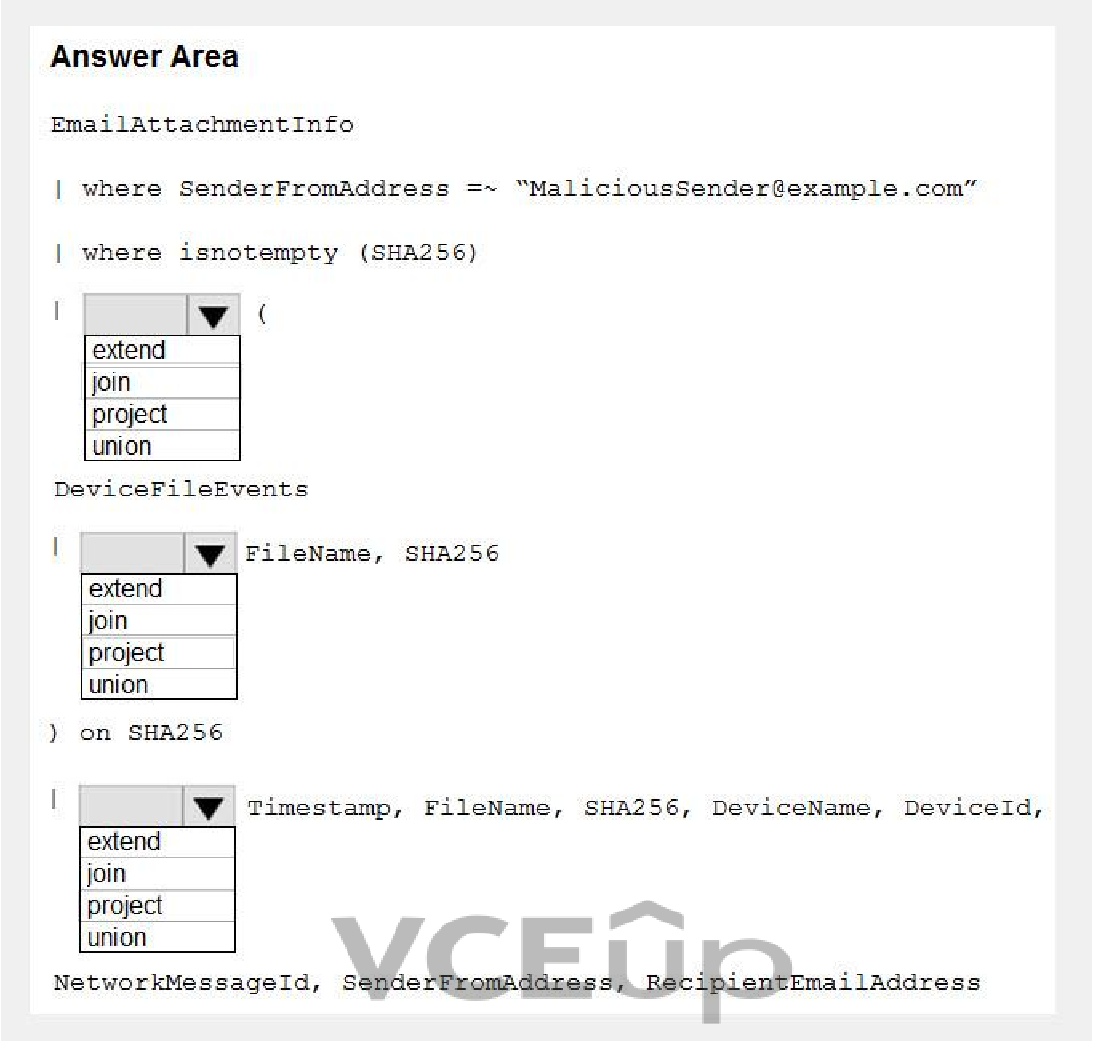
You plan to perform cross-domain investigations by using Microsoft 365 Defender.

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.

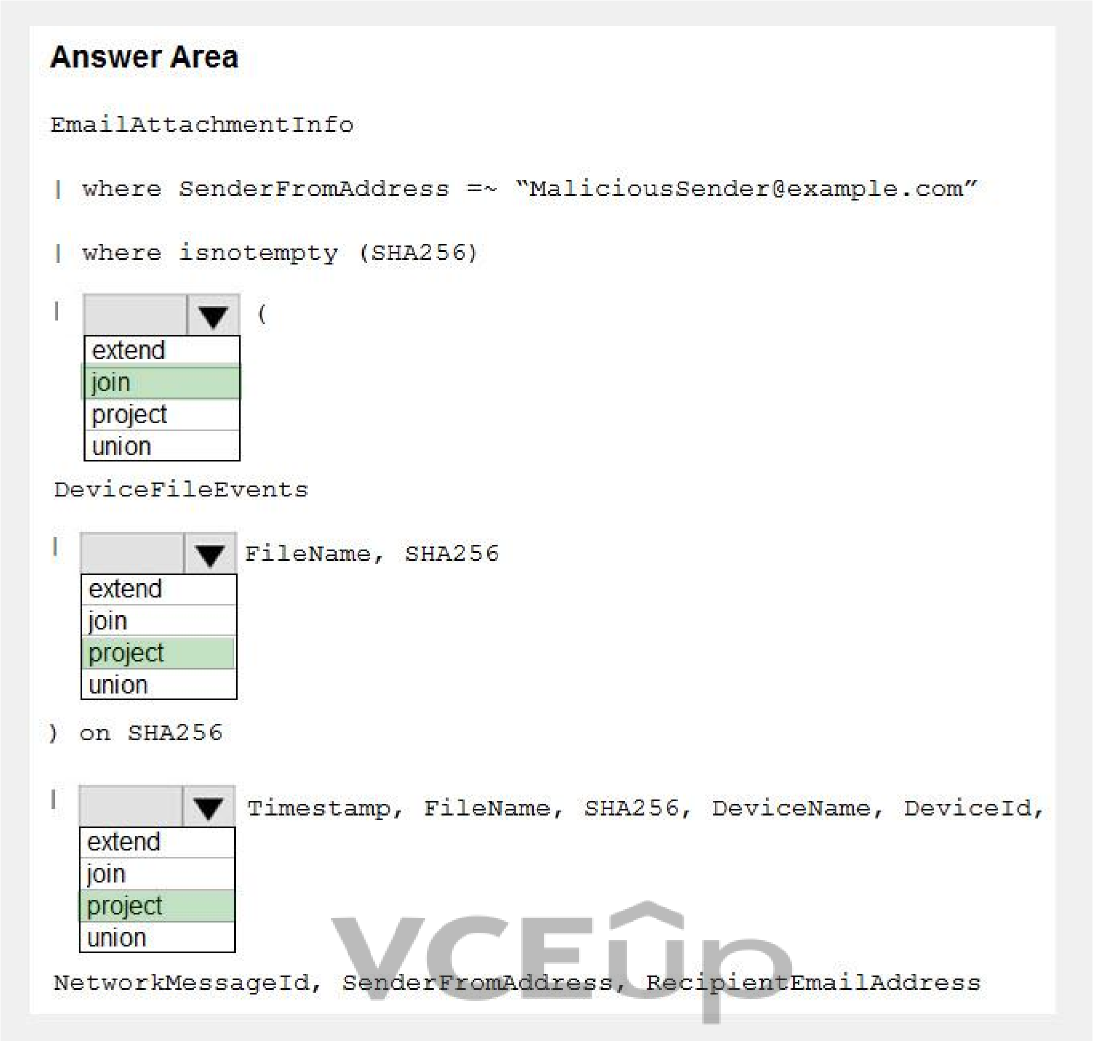
Hot Area:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [▼] (

DeviceFileEvents

| [▼] FileName, SHA256

) on SHA256

| [▼] Timestamp, FileName, SHA256, DeviceName, DeviceId,

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Correct Answer:



Answer Area

```
EmailAttachmentInfo

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

| where isnotempty (SHA256)

| ▼ (
    extend
    [✓ join]
    project
    union
DeviceFileEvents

| ▼ FileName, SHA256
    extend
    join
    [✓ project]
    union
) on SHA256

| ▼ Timestamp, FileName, SHA256, DeviceName, DeviceId,
    extend
    join
    [✓ project]
    union
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Section: (none)
Explanation

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

QUESTION 16
HOTSPOT

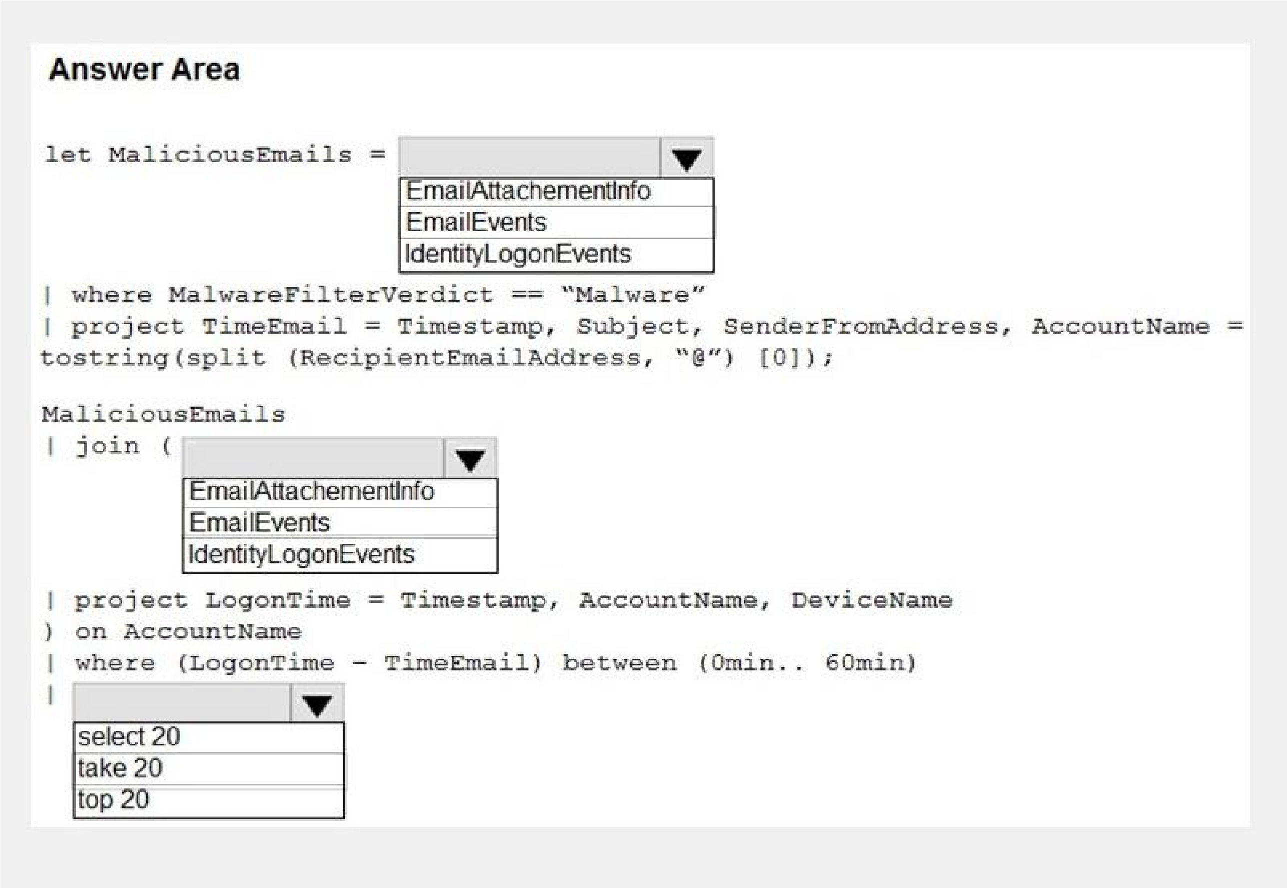
You are informed of an increase in malicious email being received by users.

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

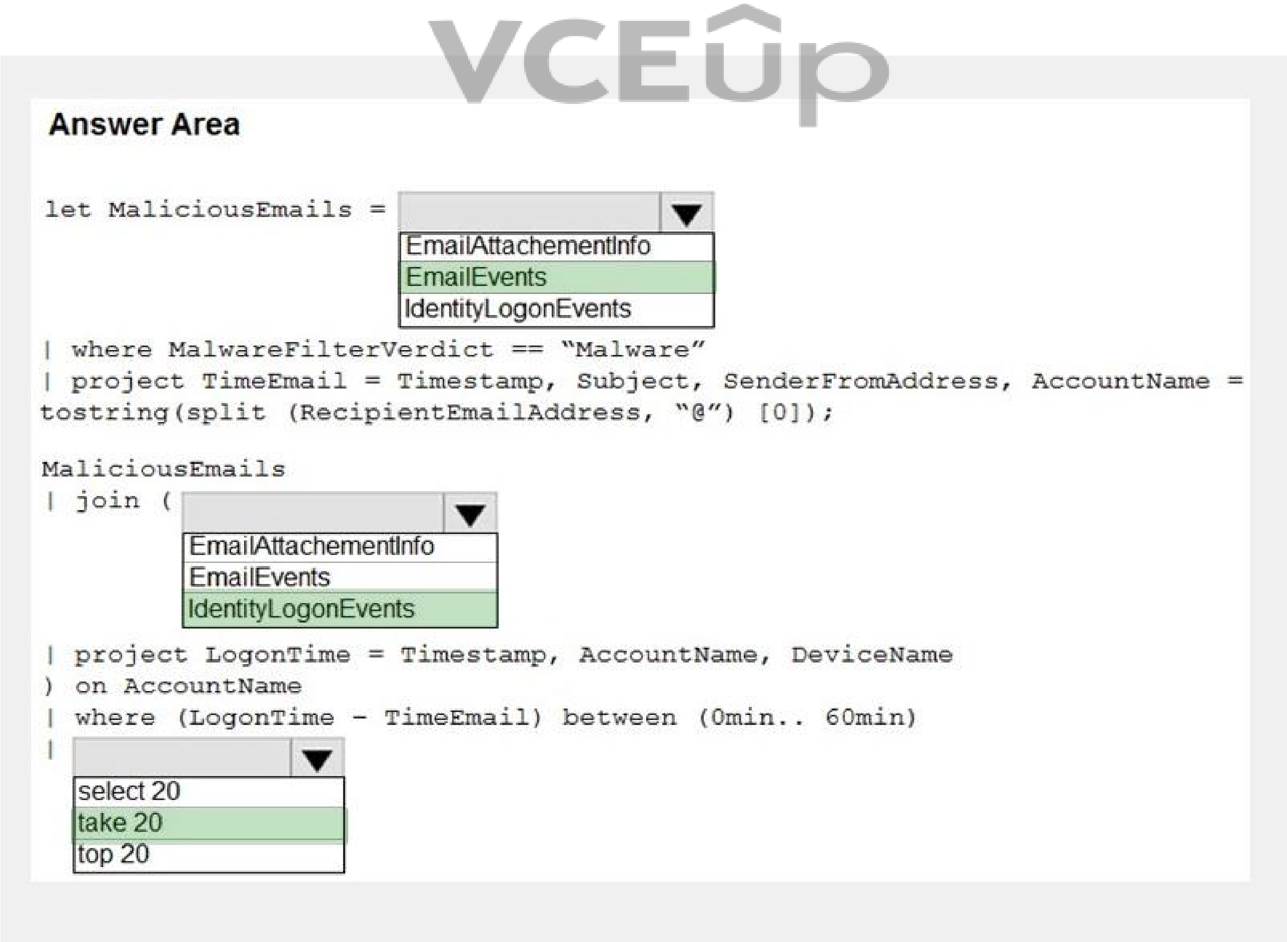
```
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join (
```

- EmailAttachementInfo
- EmailEvents
- IdentityLogonEvents

```
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
|
```

- select 20
- take 20
- top 20

Correct Answer:



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

Section: (none)

Explanation

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

QUESTION 17
HOTSPOT

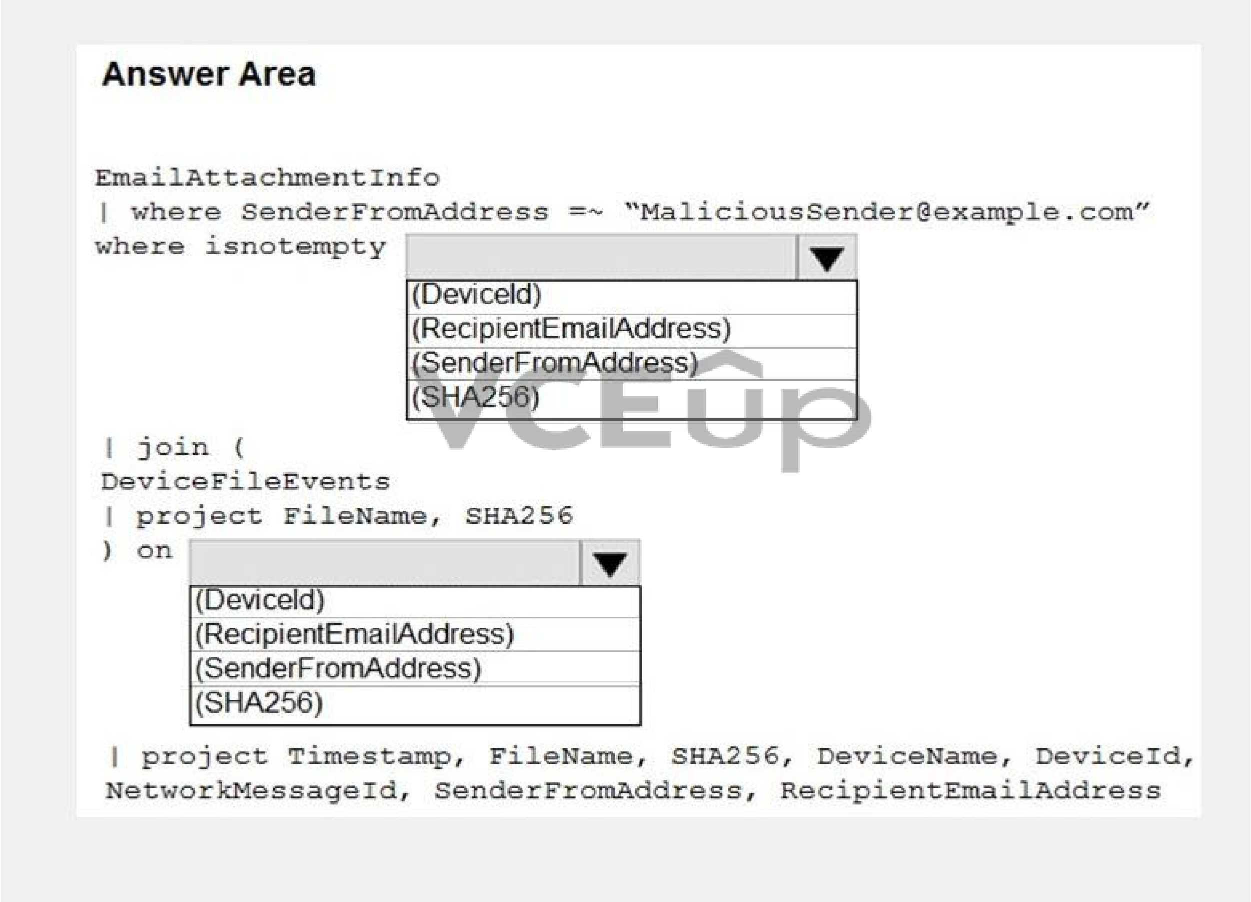
You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

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 [▼]
```

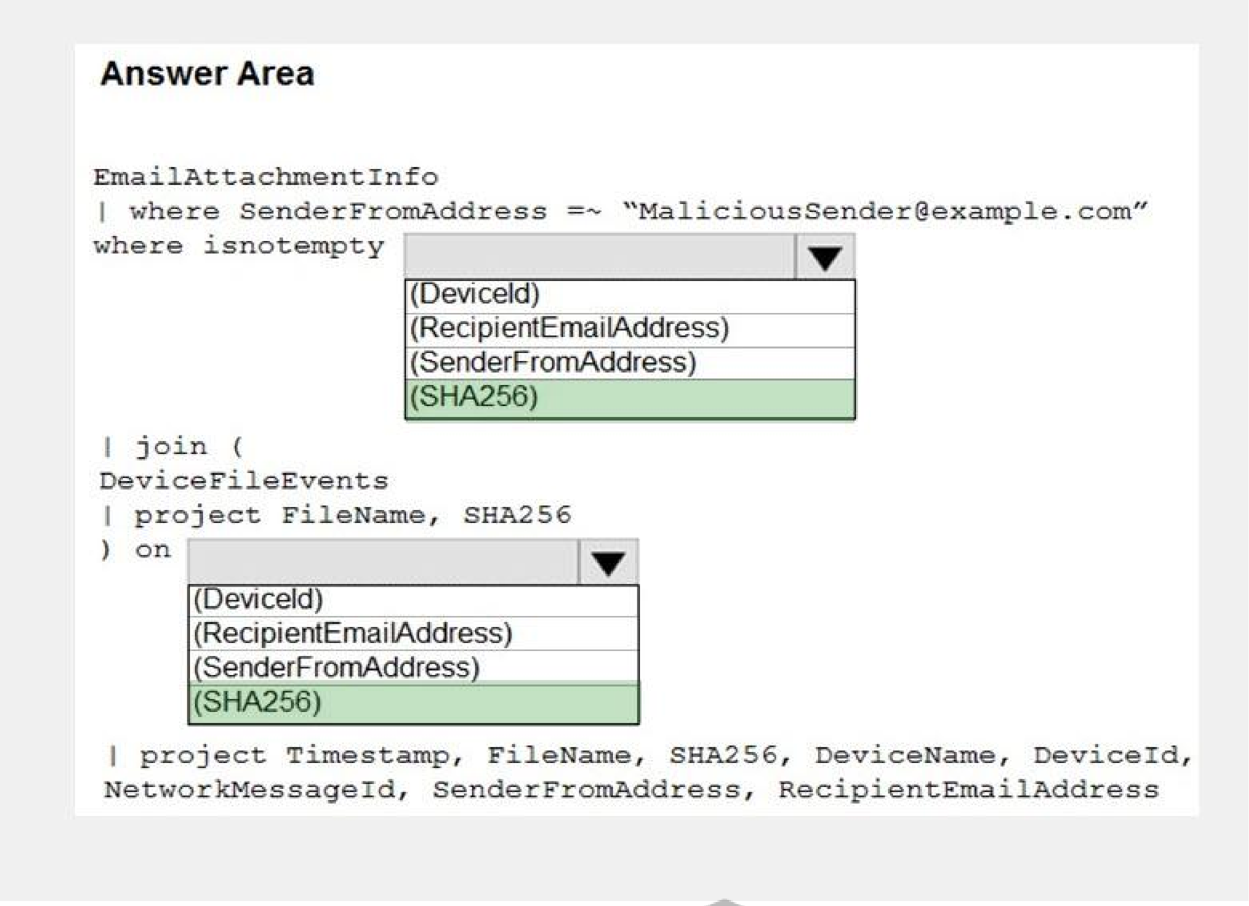
- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

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

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

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

Correct Answer:



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
```

Section: (none)
Explanation

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

QUESTION 18
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**.
E. From Settings, select **Information Protection**, select **Files**, and then enable file monitoring.
F. Select **Investigate files**, and then filter File Type to **Document**.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp

https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

QUESTION 19
HOTSPOT

You purchase a Microsoft 365 subscription.

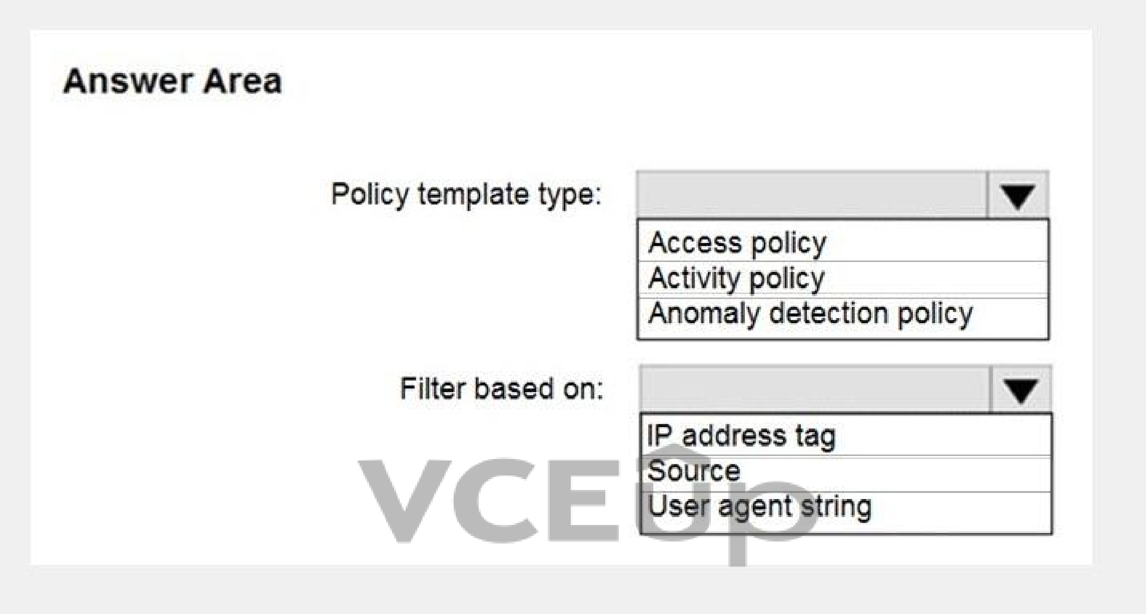
You plan to configure Microsoft Cloud App Security.

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:

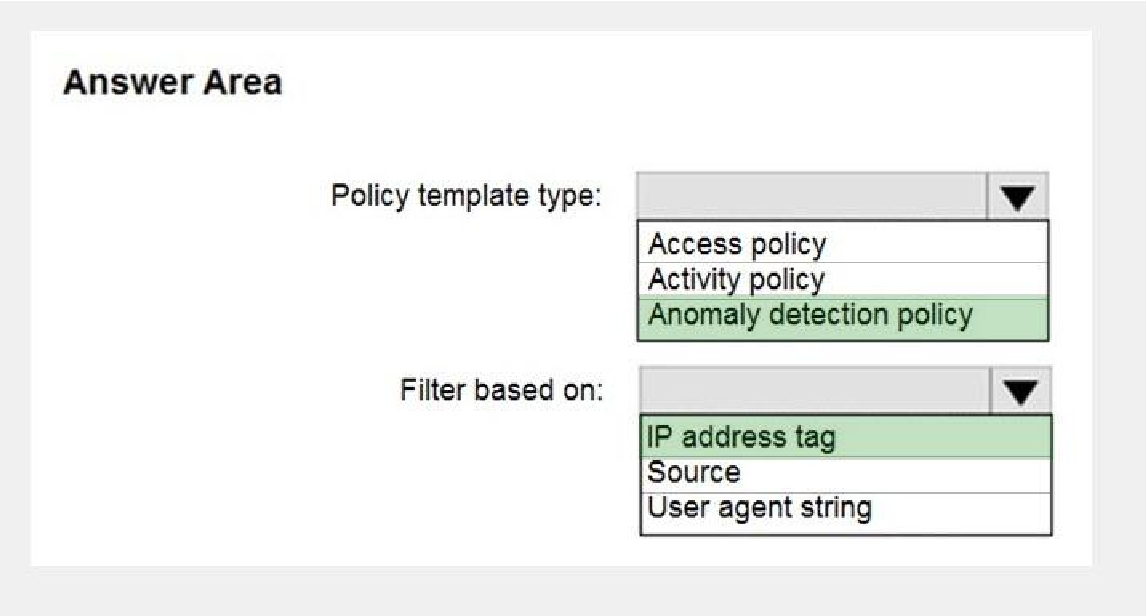


Answer Area

Policy template type:
- Access policy
- Activity policy
- Anomaly detection policy

Filter based on:
- IP address tag
- Source
- User agent string

Correct Answer:



Answer Area

Policy template type:
- Access policy
- Activity policy
- [✓ Anomaly detection policy]

Filter based on:
- [✓ IP address tag]
- Source
- User agent string

Section: (none)
Explanation

Explanation/Reference:

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

01 - Mitigate threats using Azure Defender

QUESTION 1
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 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

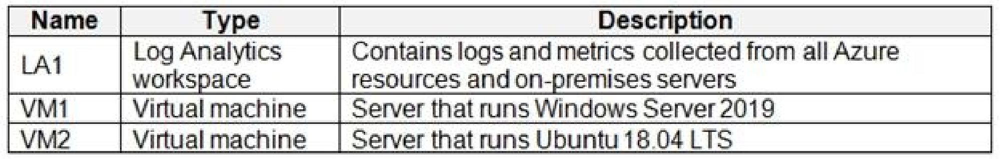
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

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.



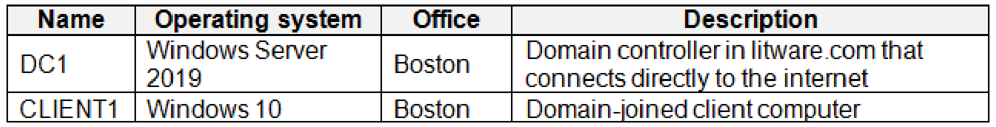
Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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

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.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

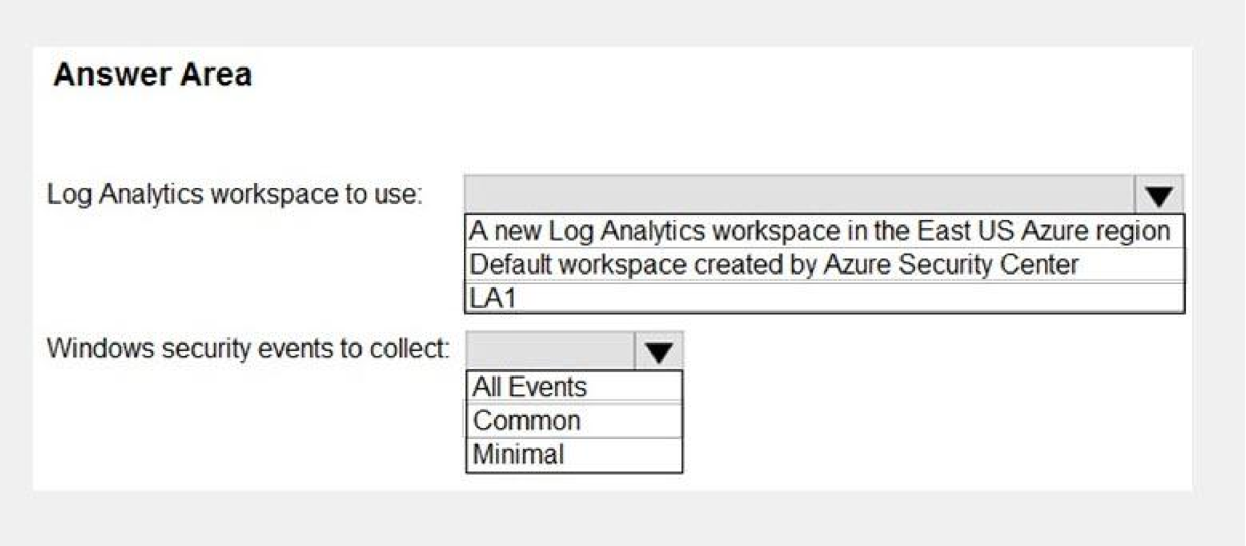
QUESTION 2
HOTSPOT

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:

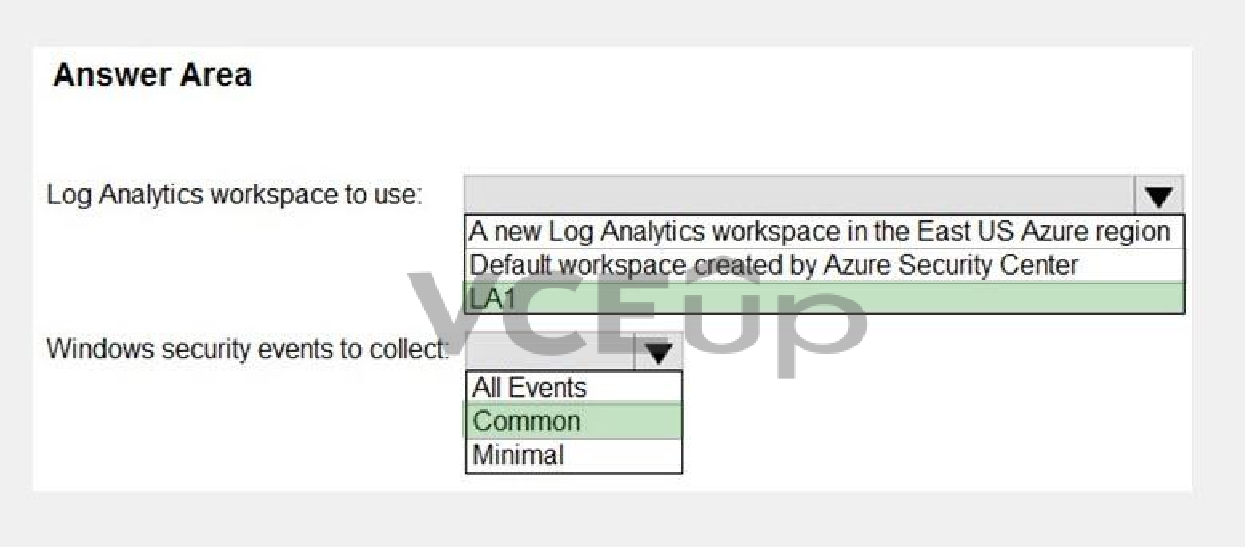


Answer Area

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

Correct Answer:



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

Section: (none)
Explanation

Explanation/Reference:

02 - Mitigate threats using Azure Defender

QUESTION 1
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 various 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
```

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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
C. Azure Firewall
D. Azure Application Gateway

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docsmicrosoft.com/en-us/azure/security-center/azure-defender

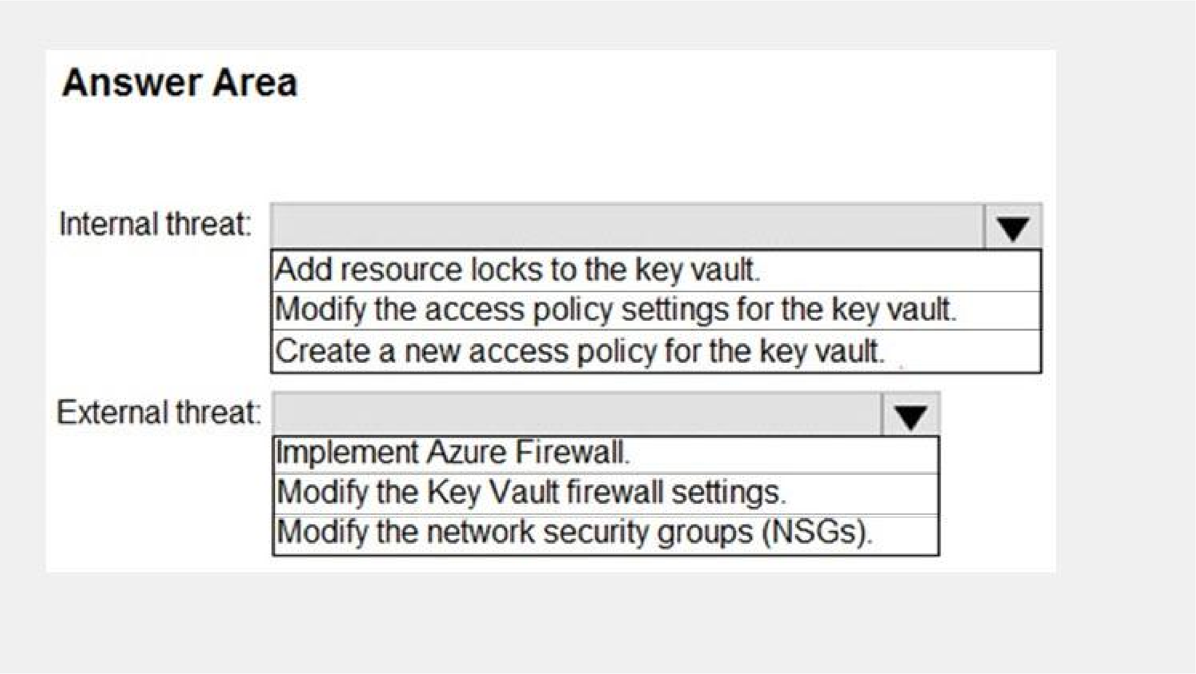
QUESTION 3
HOTSPOT

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:



Answer Area

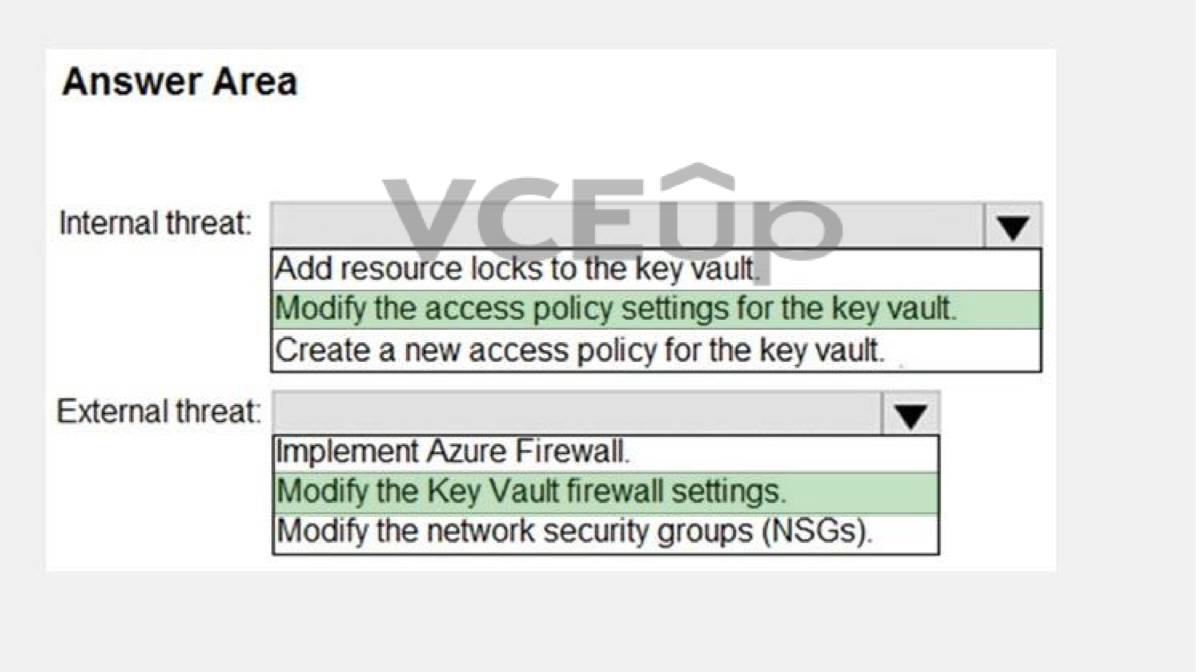
Internal threat:

- Add resource locks to the key vault.
- Modify the access policy settings for the key vault.
- Create a new access policy for the key vault.

External threat:

- Implement Azure Firewall.
- Modify the Key Vault firewall settings.
- Modify the network security groups (NSGs).

Correct Answer:



Answer Area

Internal threat:

- Add resource locks to the key vault.
- [✓ Modify the access policy settings for the key vault.]
- Create a new access policy for the key vault.

External threat:

- Implement Azure Firewall.
- [✓ Modify the Key Vault firewall settings.]
- Modify the network security groups (NSGs).

Section: (none)
Explanation

Explanation/Reference:
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

03 - Mitigate threats using Azure Defender

QUESTION 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 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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-manaqinq-and-respondinq-alerts

QUESTION 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.
C. Create an application security group.
D. Modify the access policy for the key vault.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/security-center/defender-for-kev-vault-usaQe

QUESTION 3
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 Sec Adm in 1.
You need to ensure that SecAdminl 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 SecAdminl?

A. the Security Reader role for the subscription
B. the Contributor for the subscription
C. the Contributor role for RG1
D. the Owner role for RG1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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`
B. `./alerttest testing eicar pipe`
C. `cp /bin/echo ./alerttest`
D. `./asc_alerttest_662jfi039n testing eicar pipe`

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoft.com/en-us/azure/securitv-center/security-c enter-ale rt-validation#simulate-alerts-on-your-azure-vms-linux-

QUESTION 5
You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace*!.
You enable Azure Security Center and configure Security Center to use workspace*!.
You need to colect security event logs from the Azure virtual machines that report to workspace 1.
What should you do?

A. From Security Center, enable data colection
B. In sub*!, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace*!, create a workbook.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-colection

QUESTION 6
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
D. Security alerts
E. Azure Defender

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/securitv-center/securitv-center-provide-security-contact-details

QUESTION 7

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
Section: (none)
Explanation

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

QUESTION 8
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
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-manaqinq-and-respondinq-alerts

QUESTION 9
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.mic rosoft. co m/en-us/azure/security-center/continuous-export?tabs=azure-portal

QUESTION 10
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 firewals 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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/qeneral/network-security

QUESTION 11
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://do cs. microsoft.com/en-us/azu re/sec urit y-center/e na bl e-azu re-defender

QUESTION 12
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.
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.
D. Create an Azure logic app that has an HTTP trigger.
E. From Azure Active Directory (Azure AD), add an app registration.

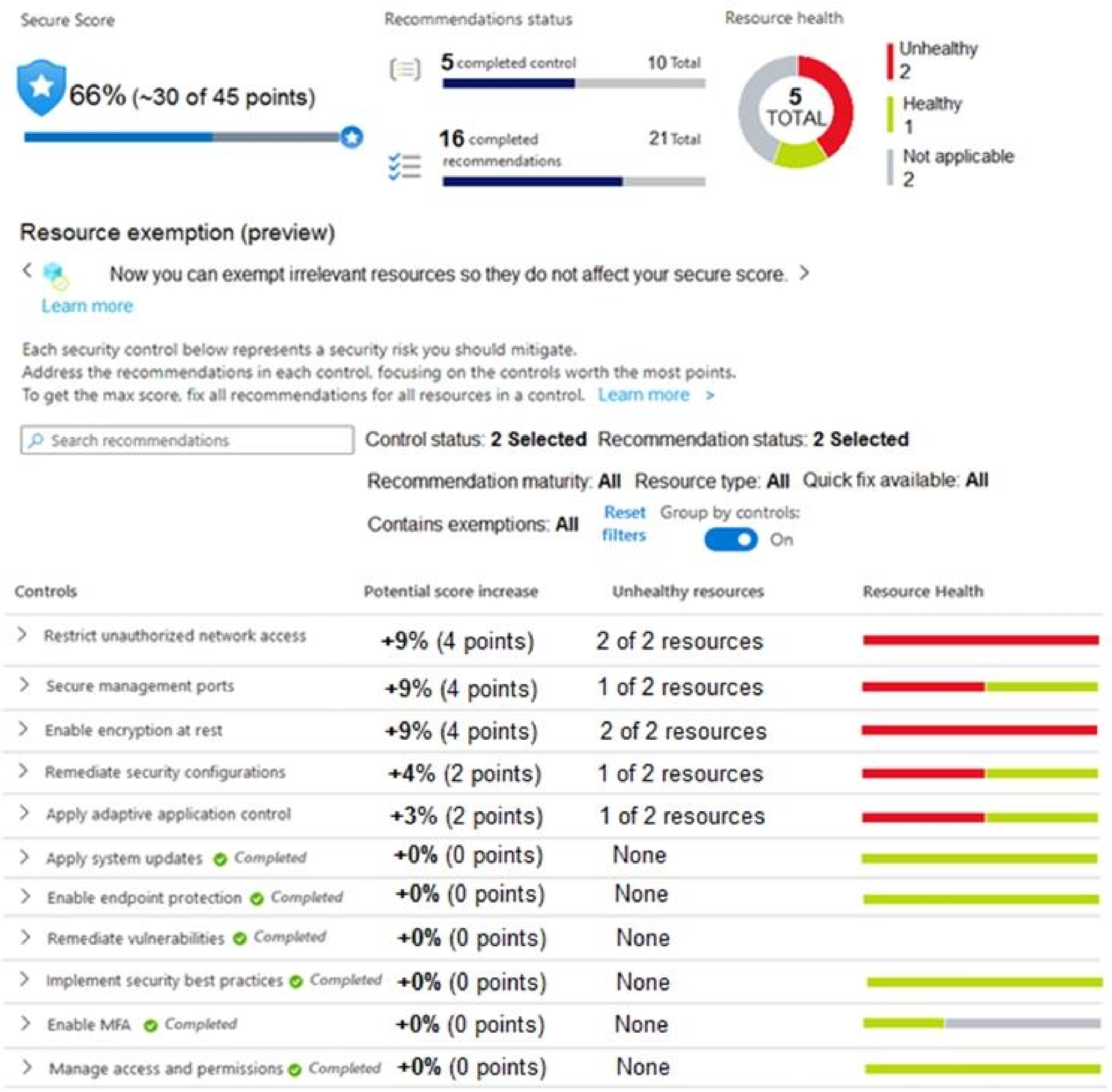
Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/storaqe/common/azure-defender-storaqe-confiqure?tabs=azure-security-center
https: //docs. m ic rosoft. com/en -us/azu re/sec urity-ce rite r/workflow-a uto mation

QUESTION 13
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.)



Secure Score

66% (~30 of 45 points)

Recommendations status

5 completed control 10 Total

16 completed recommendations 21 Total

Resource health

5 TOTAL

Unhealthy 2

Healthy 1

Not applicable 2

Resource exemption (preview)

Now you can exempt irrelevant resources so they do not affect your secure score.

Learn more

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

Search recommendations

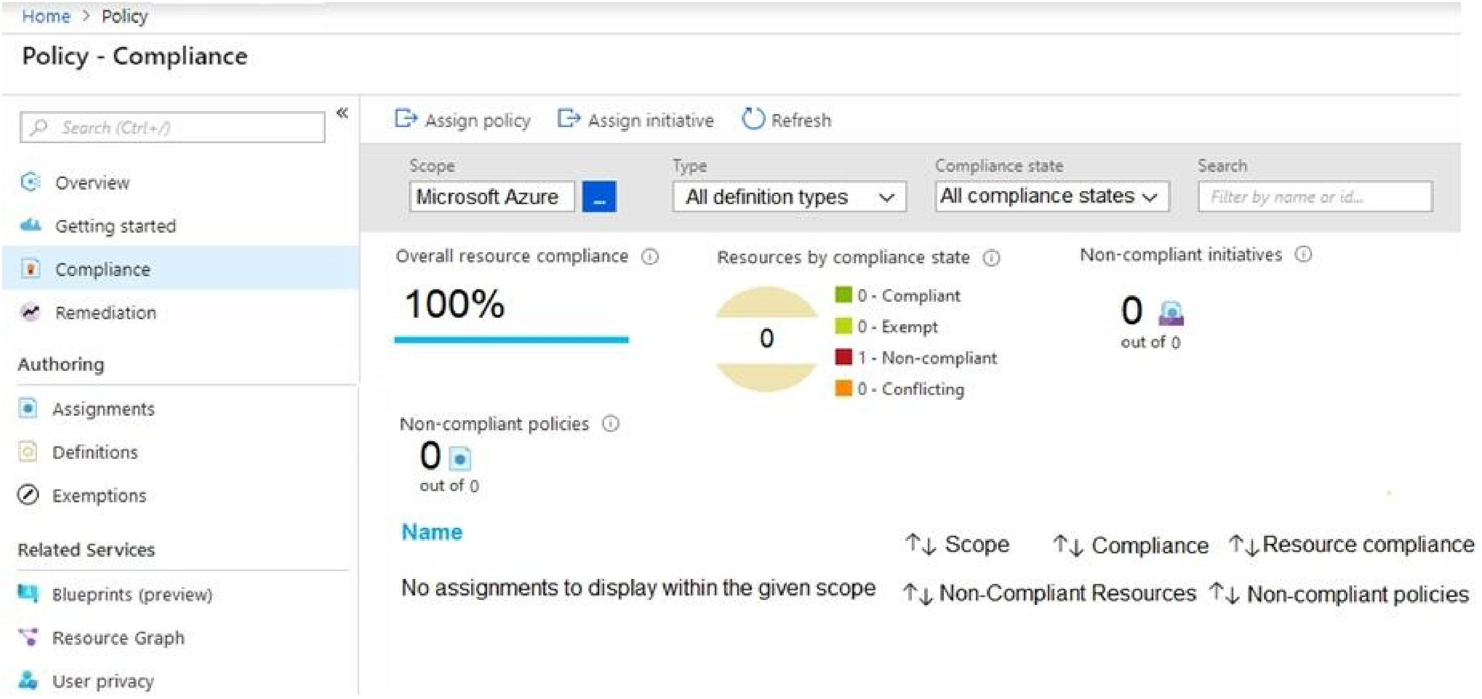
Control status: **2 Selected** Recommendation status: **2 Selected**

Recommendation maturity: **All** Resource type: **All** Quick fix available: **All**

Contains exemptions: **All** Reset filters Group by controls: On

Controls	Potential score increase	Unhealthy resources	Resource Health
Restrict unauthorized network access	+9% (4 points)	2 of 2 resources	🟥🟥
Secure management ports	+9% (4 points)	1 of 2 resources	🟥🟩
Enable encryption at rest	+9% (4 points)	2 of 2 resources	🟥🟥
Remediate security configurations	+4% (2 points)	1 of 2 resources	🟥🟩
Apply adaptive application control	+3% (2 points)	1 of 2 resources	🟥🟩
Apply system updates ✓ Completed	+0% (0 points)	None	🟩🟩
Enable endpoint protection ✓ Completed	+0% (0 points)	None	🟩🟩
Remediate vulnerabilities ✓ Completed	+0% (0 points)	None	
Implement security best practices ✓ Completed	+0% (0 points)	None	🟩🟩
Enable MFA ✓ Completed	+0% (0 points)	None	🟩⬜
Manage access and permissions ✓ Completed	+0% (0 points)	None	🟩🟩

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



Policy - Compliance

Scope: Microsoft Azure

Type: All definition types

Compliance state: All compliance states

Search: Filter by name or id...

Overall resource compliance: 100%

Resources by compliance state: 0

- 🟩 0 - Compliant
- 🟨 0 - Exempt
- 🟥 1 - Non-compliant
- 🟧 0 - Conflicting

Non-compliant initiatives: 0 out of 0

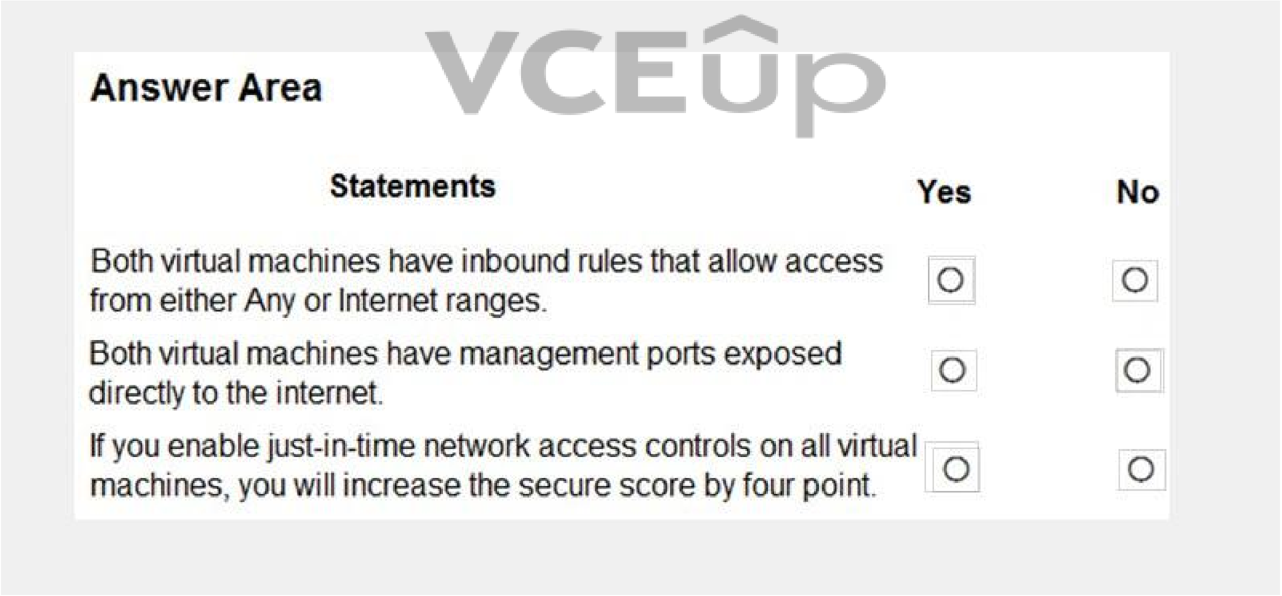
Non-compliant policies: 0 out of 0

Name	↑↓ Scope	↑↓ Compliance	↑↓ Resource compliance	↑↓ Non-Compliant Resources	↑↓ Non-compliant policies
No assignments to display within the given scope					

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

NOTE: Each correct selection is worth one point.

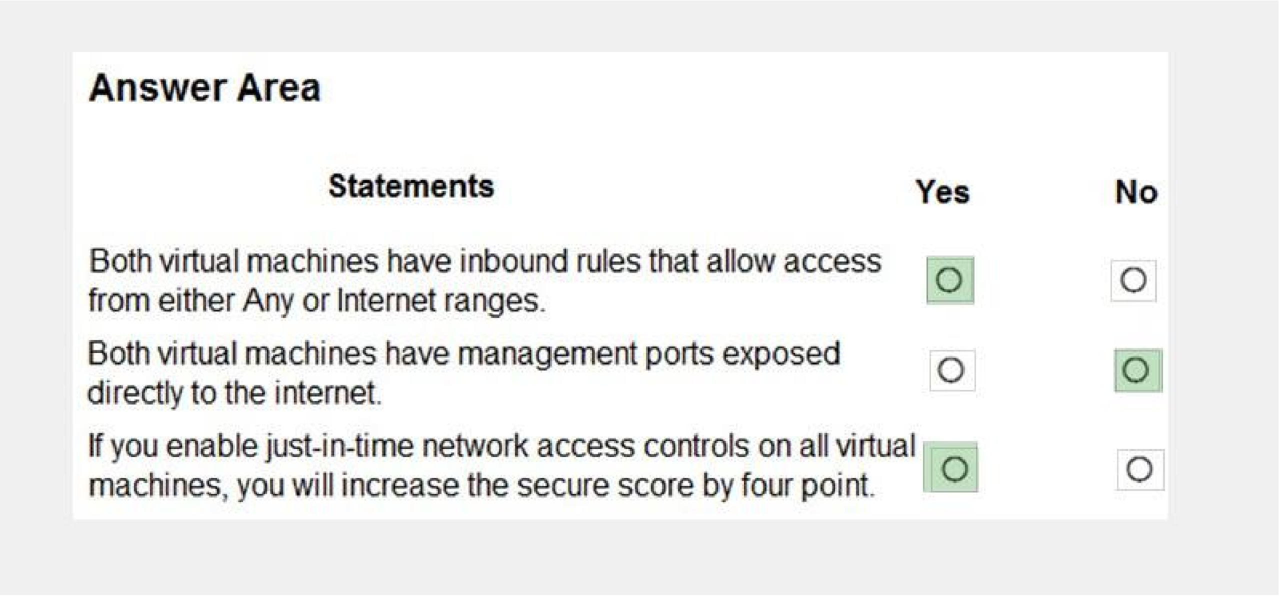
Hot Area:



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.	○	○

Correct Answer:



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.	●	○

Section: (none)
Explanation

Explanation/Reference:
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

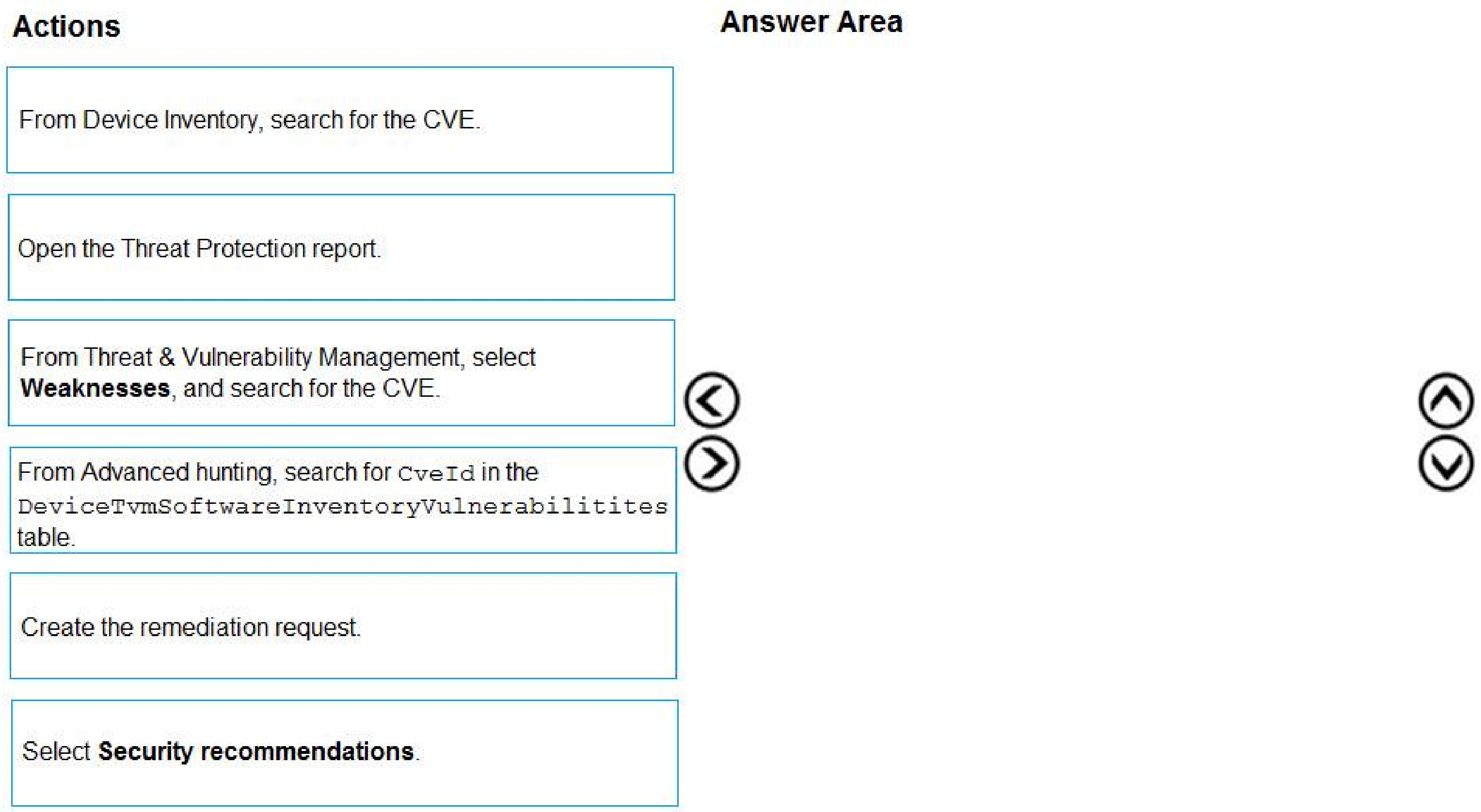
QUESTION 14
DRAG DROP

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:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

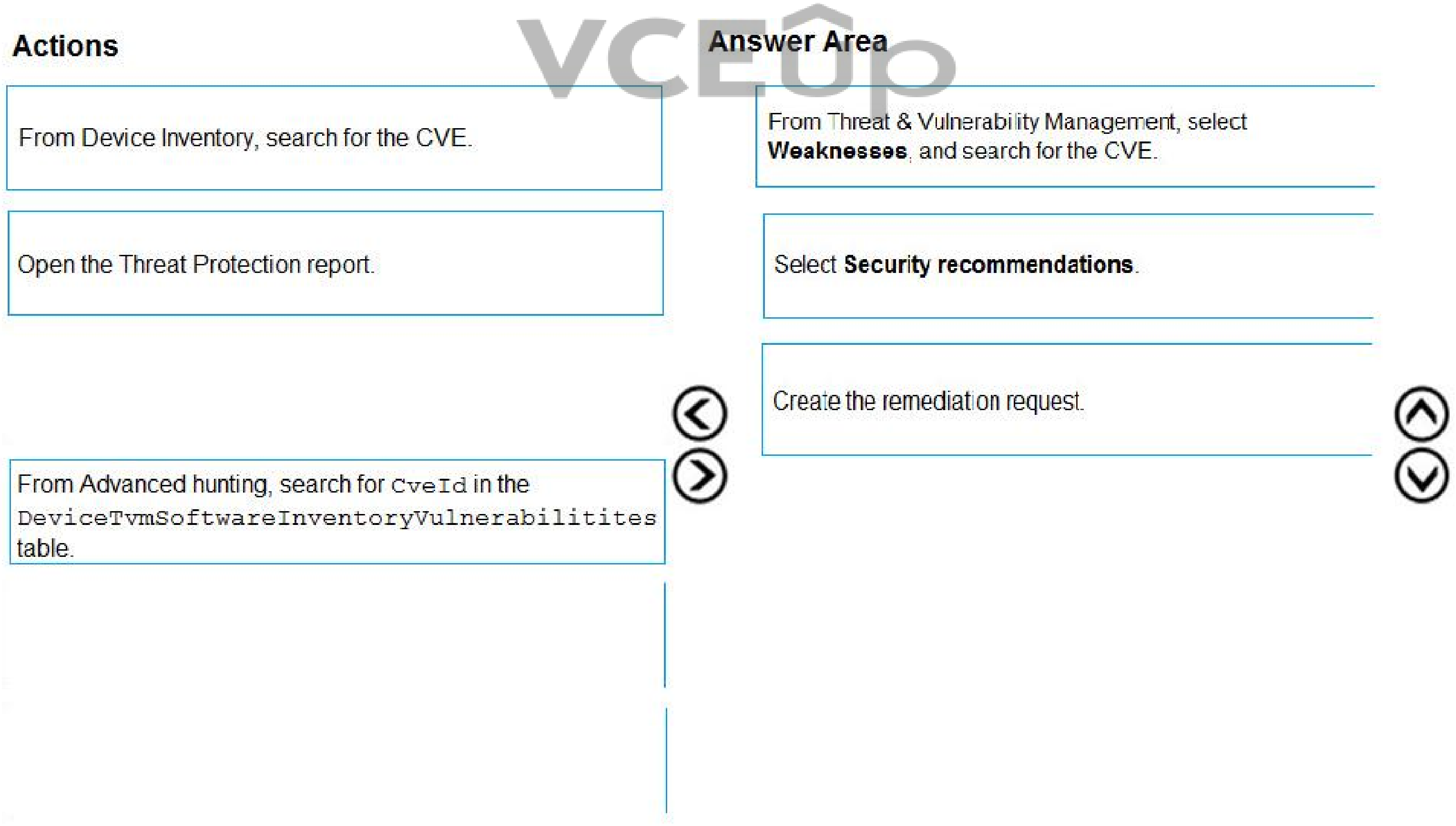
From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

Correct Answer:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for `cveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Answer Area

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 15
HOTSPOT

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

You create an Azure logic app named LA1.

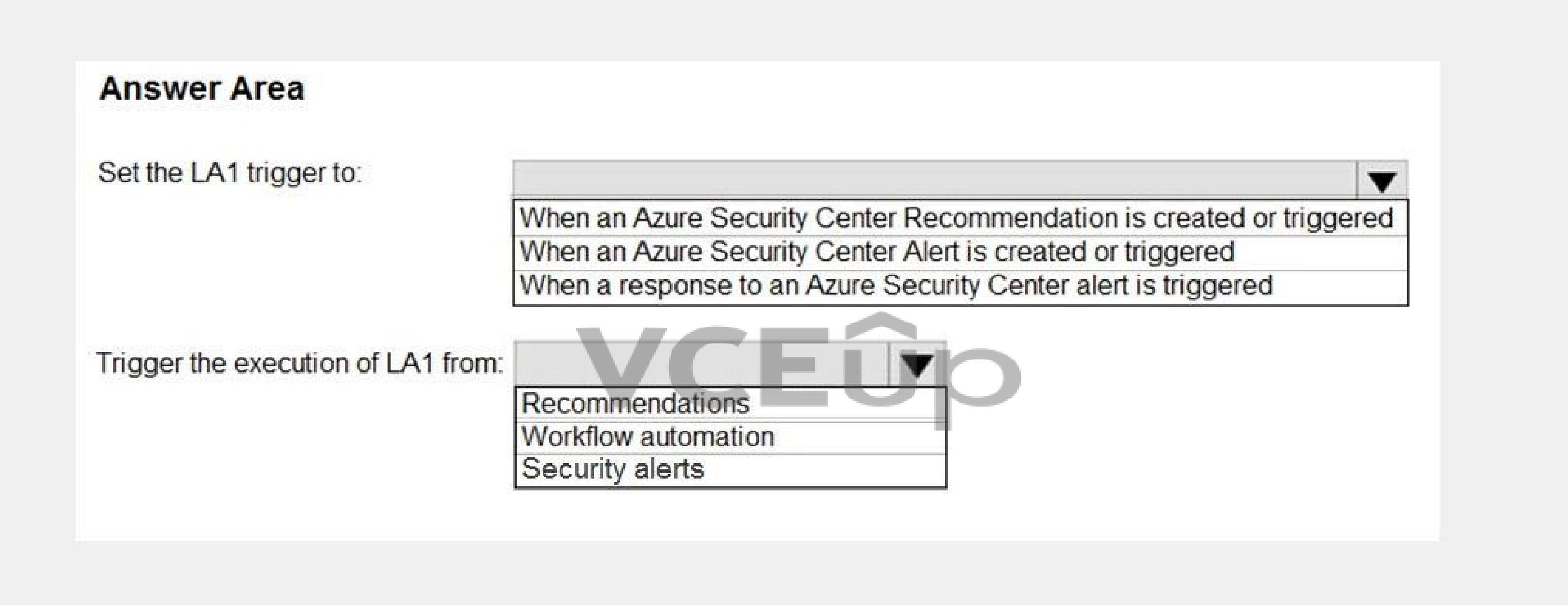
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

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:

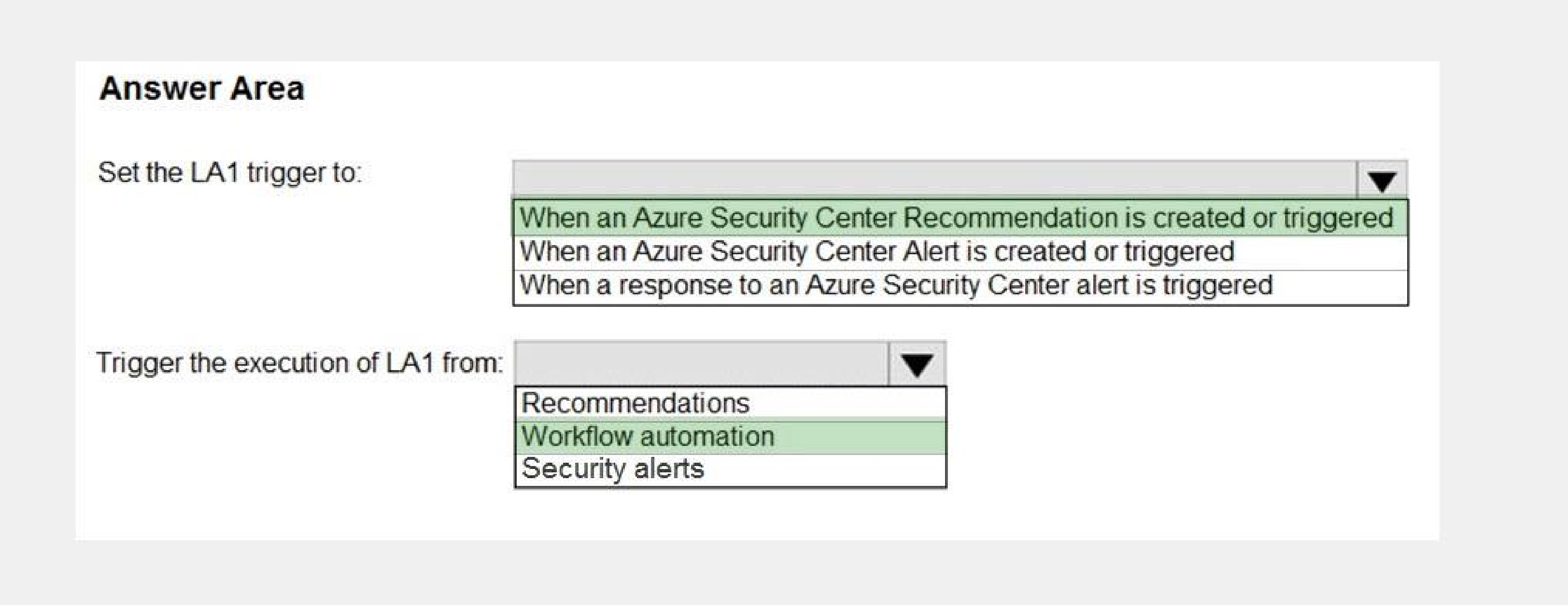


Answer Area

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

Section: (none)
Explanation

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

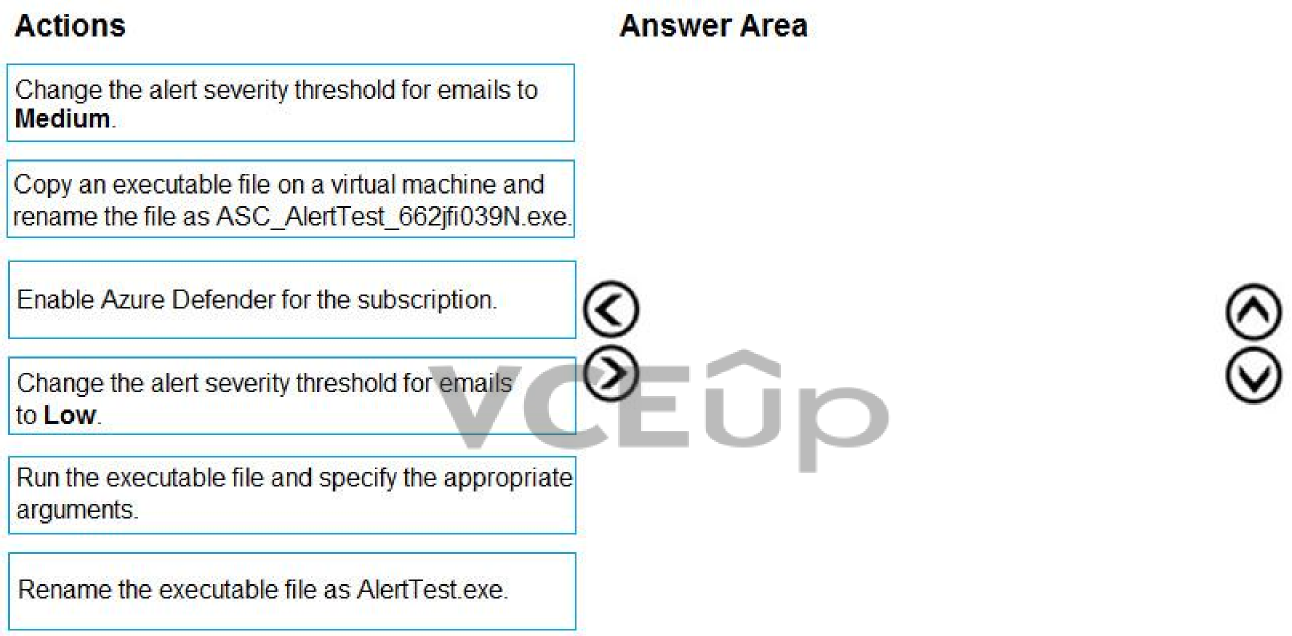
QUESTION 16
DRAG DROP

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:

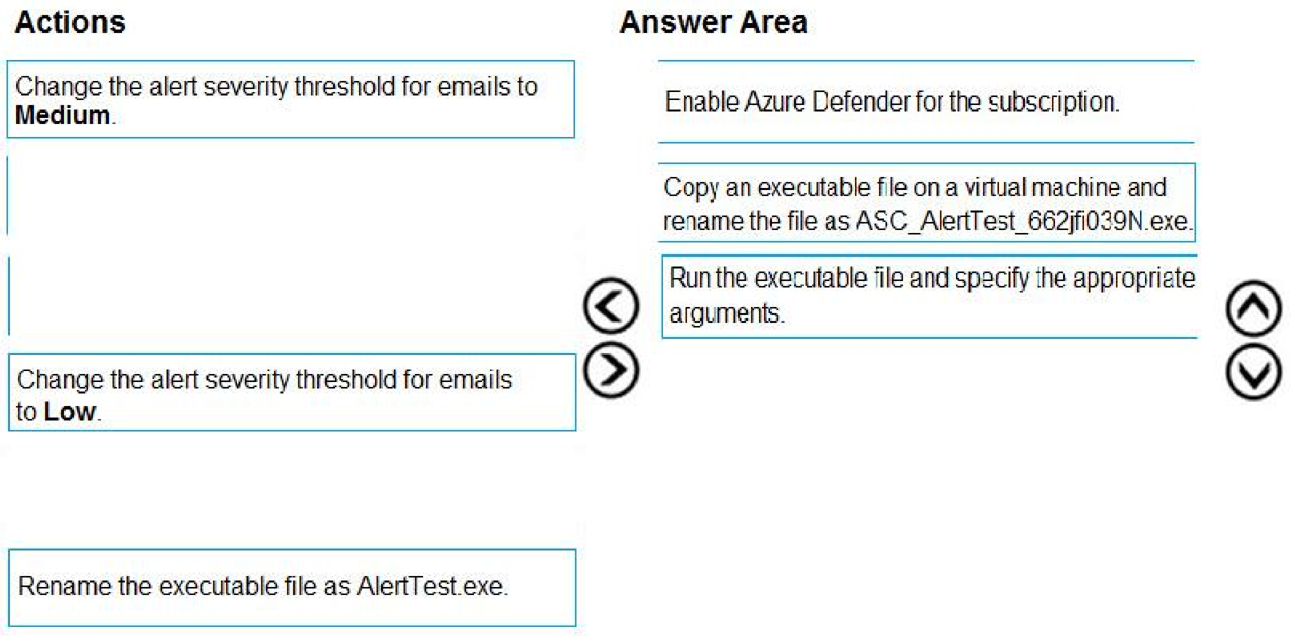


Actions

- 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.

Answer Area

Correct Answer:



Actions

- Change the alert severity threshold for emails to **Medium**.
- Change the alert severity threshold for emails to **Low**.
- Rename the executable file as AlertTest.exe.

Answer Area

1. Enable Azure Defender for the subscription.
2. Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.
3. Run the executable file and specify the appropriate arguments.

Section: (none)
Explanation

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

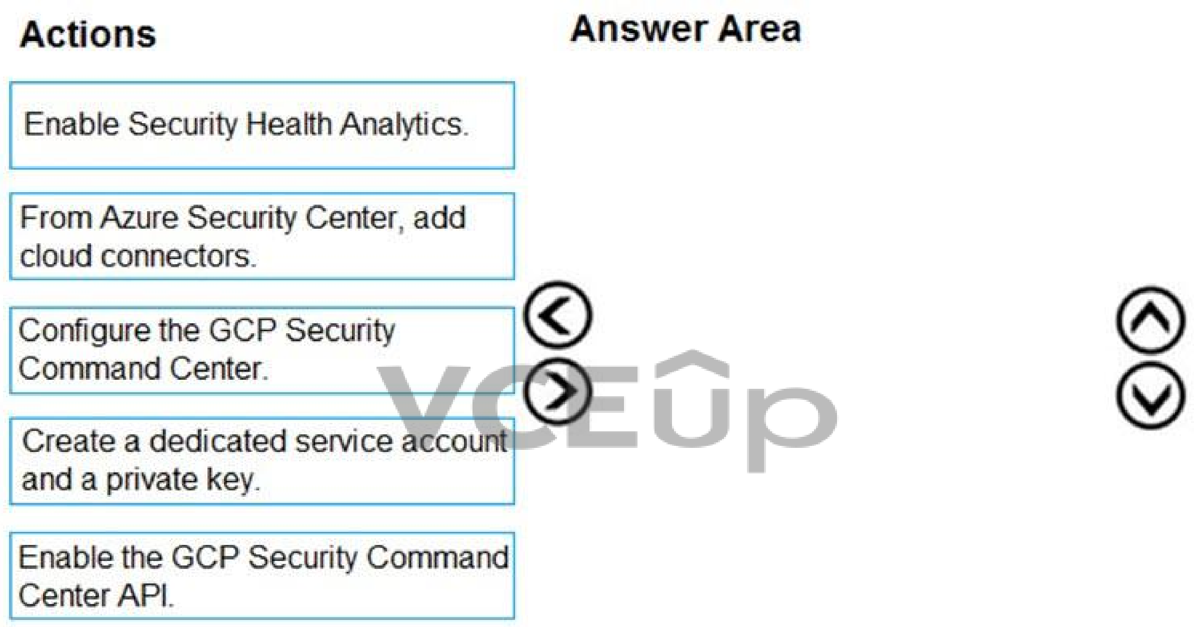
QUESTION 17
DRAG DROP

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:



Actions

Enable Security Health Analytics.

From Azure Security Center, add cloud connectors.

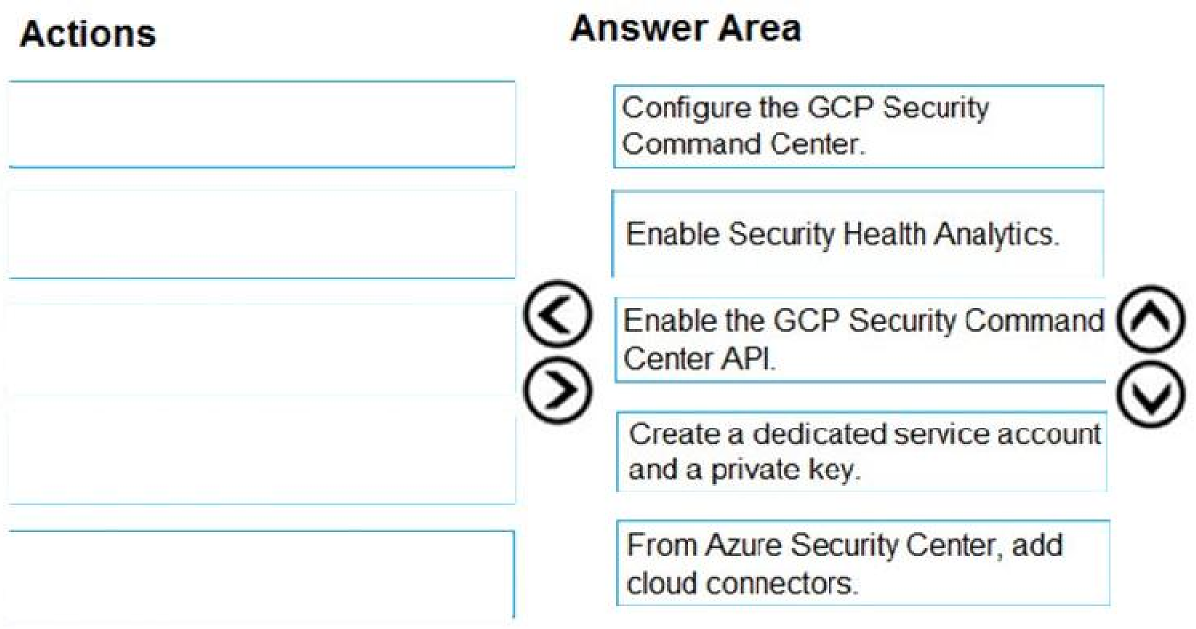
Configure the GCP Security Command Center.

Create a dedicated service account and a private key.

Enable the GCP Security Command Center API.

Answer Area

Correct Answer:



Actions

Answer Area

Configure the GCP Security Command Center.

Enable Security Health Analytics.

Enable the GCP Security Command Center API.

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Section: (none)
Explanation

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

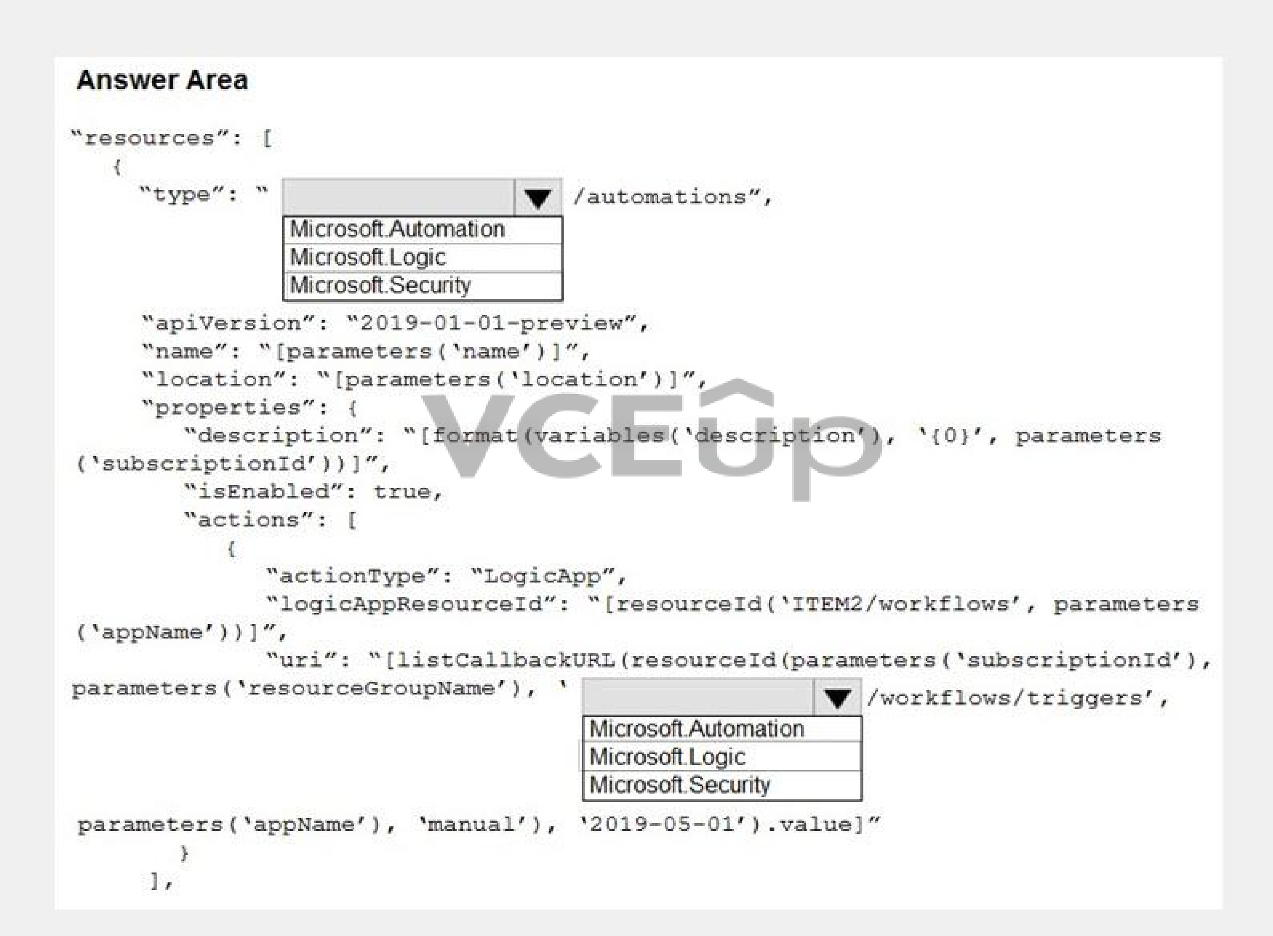
QUESTION 18
HOTSPOT

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.

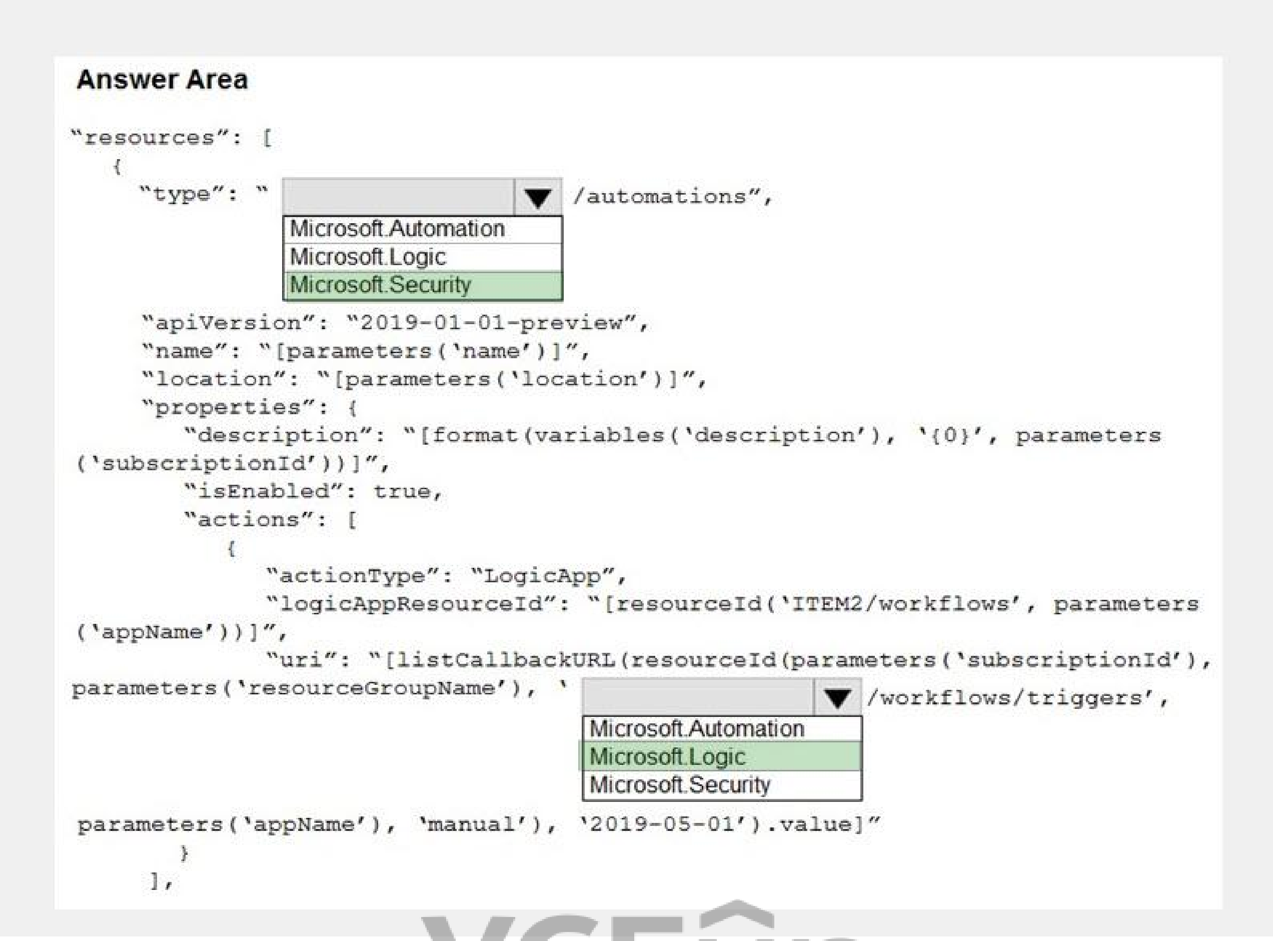
Hot Area:



Answer Area

```
"resources": [
   {
     "type": "  [ ▼ ] /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
     "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',
                                    Microsoft.Automation
                                    Microsoft.Logic
                                    Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ],
```

Correct Answer:



Answer Area

```
"resources": [
  {
    "type": "                    /automations",
              Microsoft.Automation
              Microsoft.Logic
              Microsoft.Security
    "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',
                                   Microsoft.Automation
                                   Microsoft.Logic
                                   Microsoft.Security

parameters('appName'), 'manual'), '2019-05-01').value]"
       }
     ],
```

Section: (none)
Explanation

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

QUESTION 19
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.
C. From Regulatory compliance, download the report.
D. From Recommendations, download the CSV report.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 20
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.
D. View the Windows event logs on the virtual machines.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

01 - Mitigate threats using Azure Sentinel

QUESTION 1
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 various 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
```

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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
Section: (none)
Explanation

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

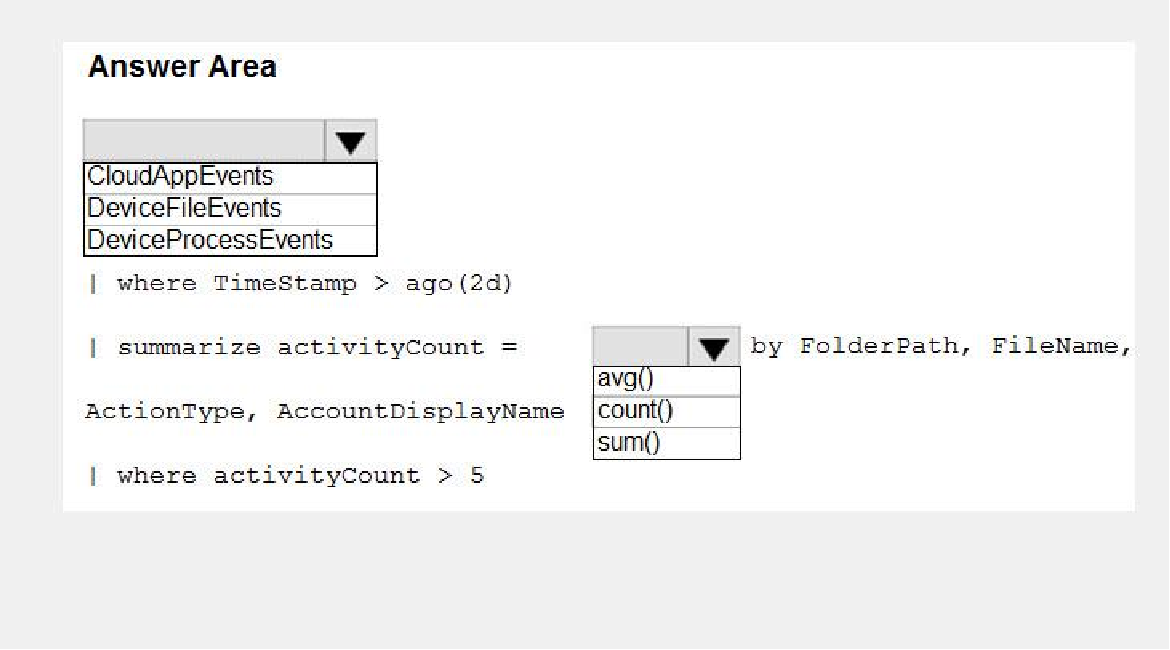
QUESTION 3
HOTSPOT

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

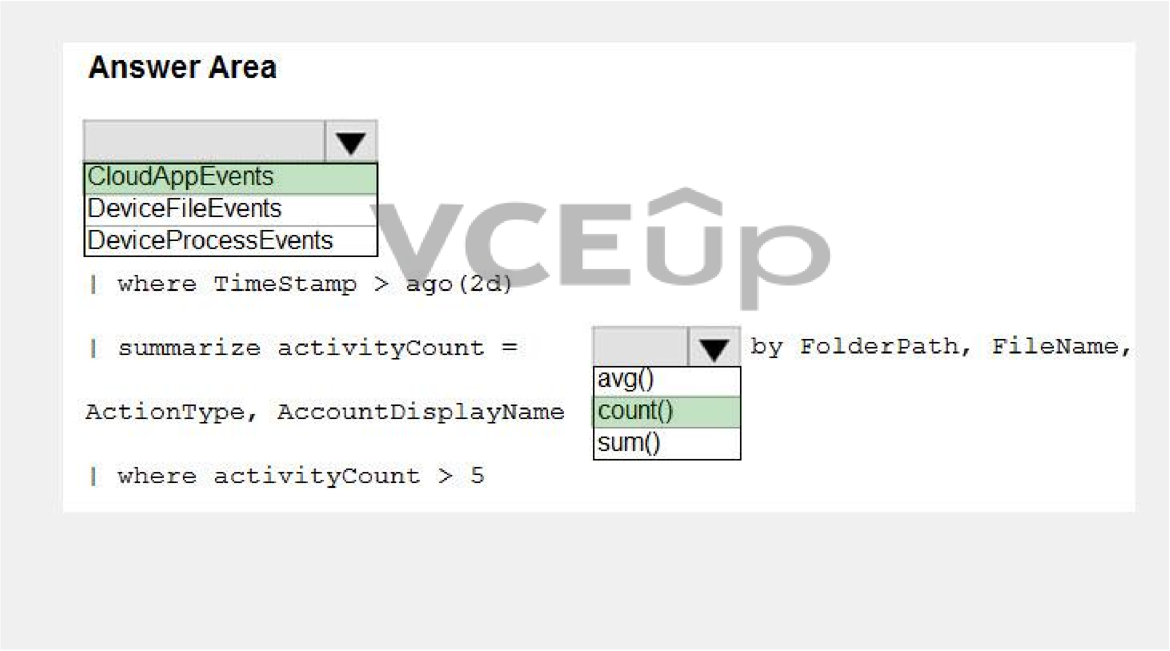
- CloudAppEvents
- DeviceFileEvents
- DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount =
```

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

```
by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Correct Answer:



Answer Area

- [✓ CloudAppEvents]
- DeviceFileEvents
- DeviceProcessEvents

```
| where TimeStamp > ago(2d)
| summarize activityCount =
```

- avg()
- [✓ count()]
- sum()

```
by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Section: (none)
Explanation

Explanation/Reference:

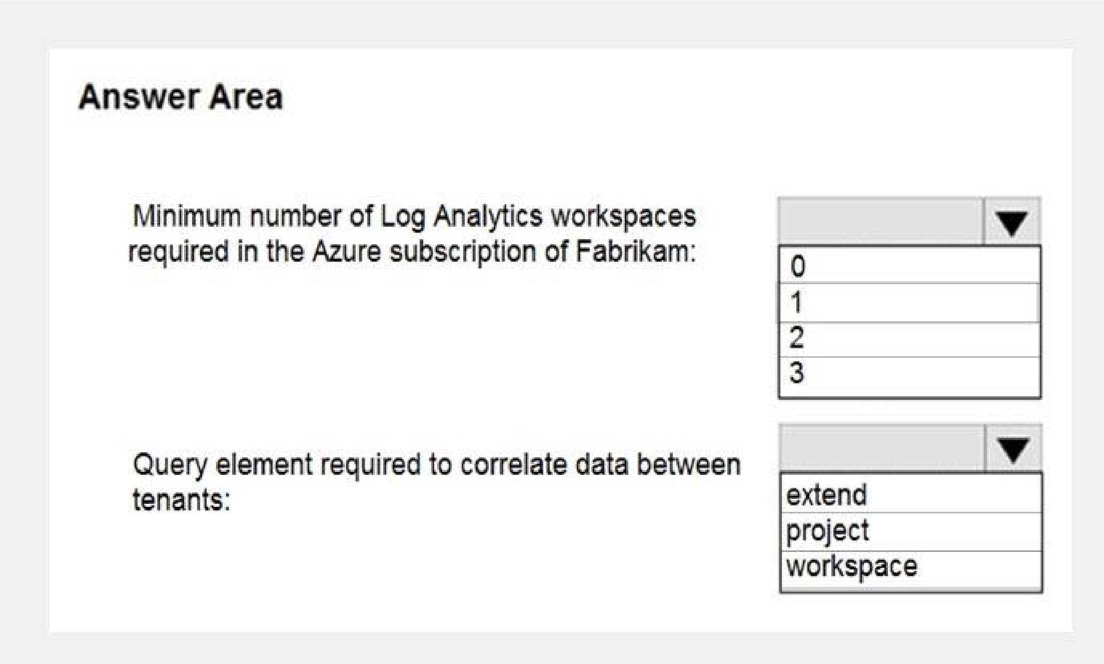
QUESTION 4
HOTSPOT

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:



Answer Area

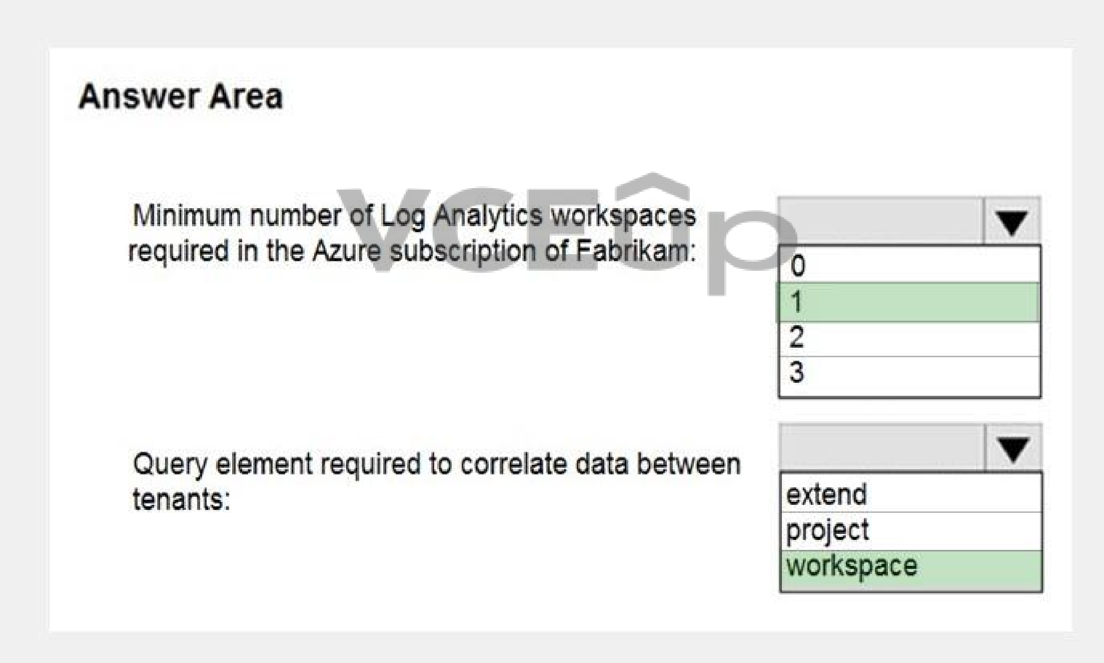
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Correct Answer:



Answer Area

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

- 0
- [✓ 1]
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- [✓ workspace]

Section: (none)
Explanation

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

02 - Mitigate threats using Azure Sentinel

QUESTION 1
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 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

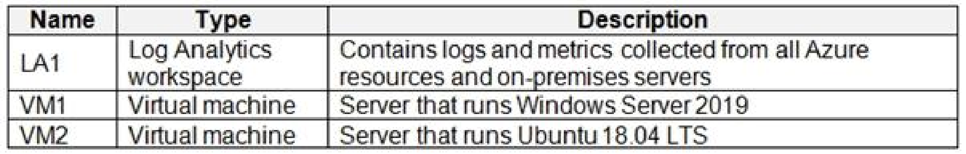
The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

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.



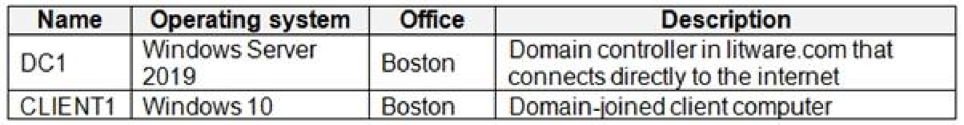
Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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

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.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You need to assign a role-based access control (RBAC) role to admin! to meet the Azure Sentinel requirements and the business requirements.
Which role should you assign?

A. Automation Operator

B. Automation Run book Operator

C. Azure Sentinel Contributor

D. Logic App Contributor

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 3
You need to create the test rule to meet the Azure Sentinel requirements.
What should you do when you create the rule?

A. From Set rule logic, turn off suppression.
B. From Analytics rule details, configure the tactics.
C. From Set rule logic, map the entities.
D. From Analytics rule details, configure the severity.

Correct Answer: C
Section: (none)
Explanation

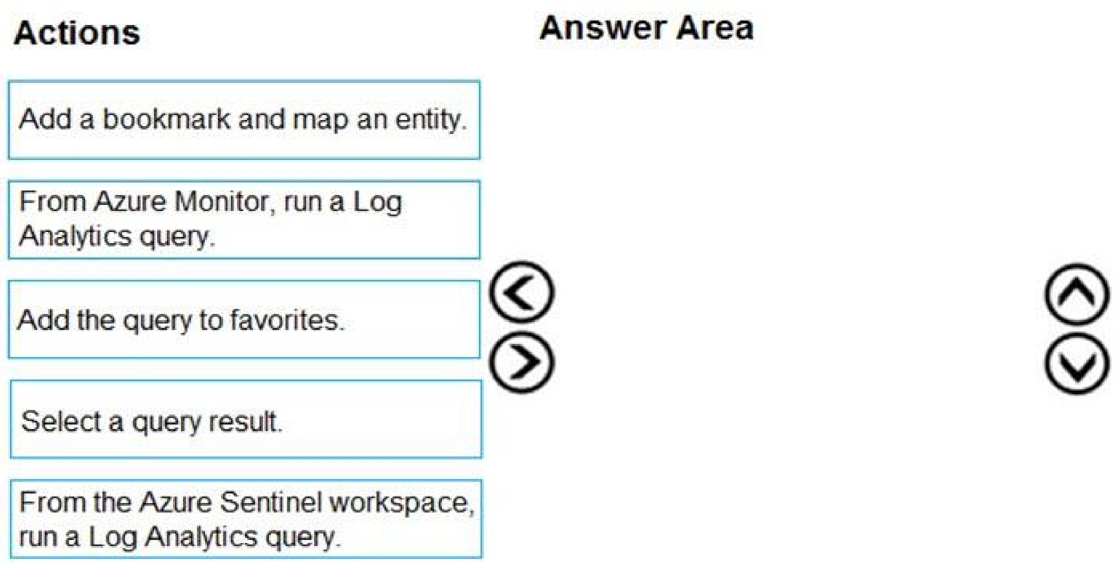
Explanation/Reference:
Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 4
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:

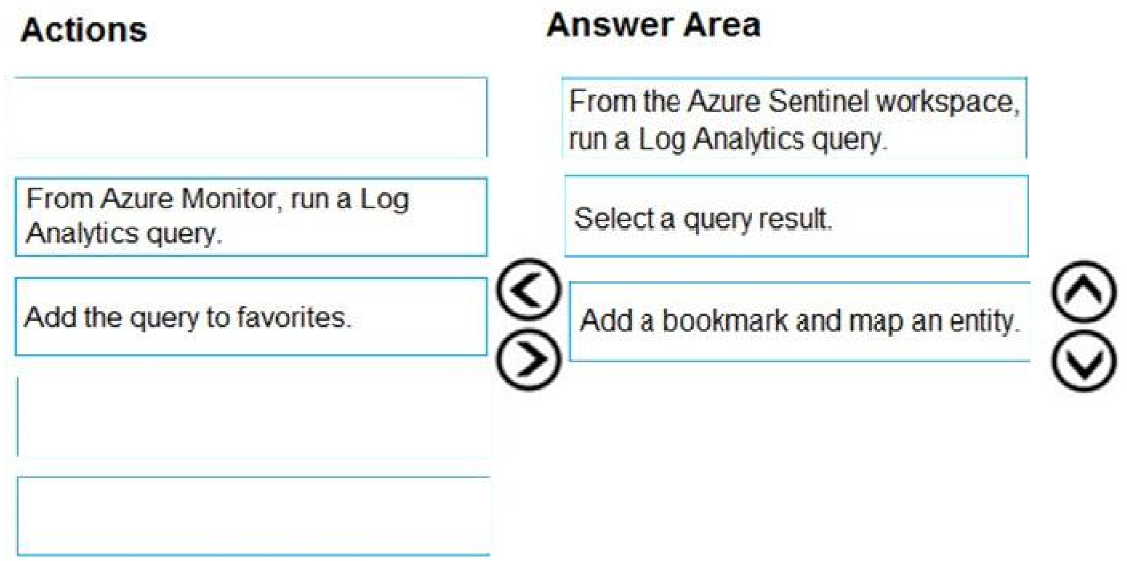


Actions

- Add a bookmark and map an entity.
- From Azure Monitor, run a Log Analytics query.
- Add the query to favorites.
- Select a query result.
- From the Azure Sentinel workspace, run a Log Analytics query.

Answer Area

Correct Answer:



Actions

From Azure Monitor, run a Log Analytics query.

Add the query to favorites.

Answer Area

From the Azure Sentinel workspace, run a Log Analytics query.

Select a query result.

Add a bookmark and map an entity.

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

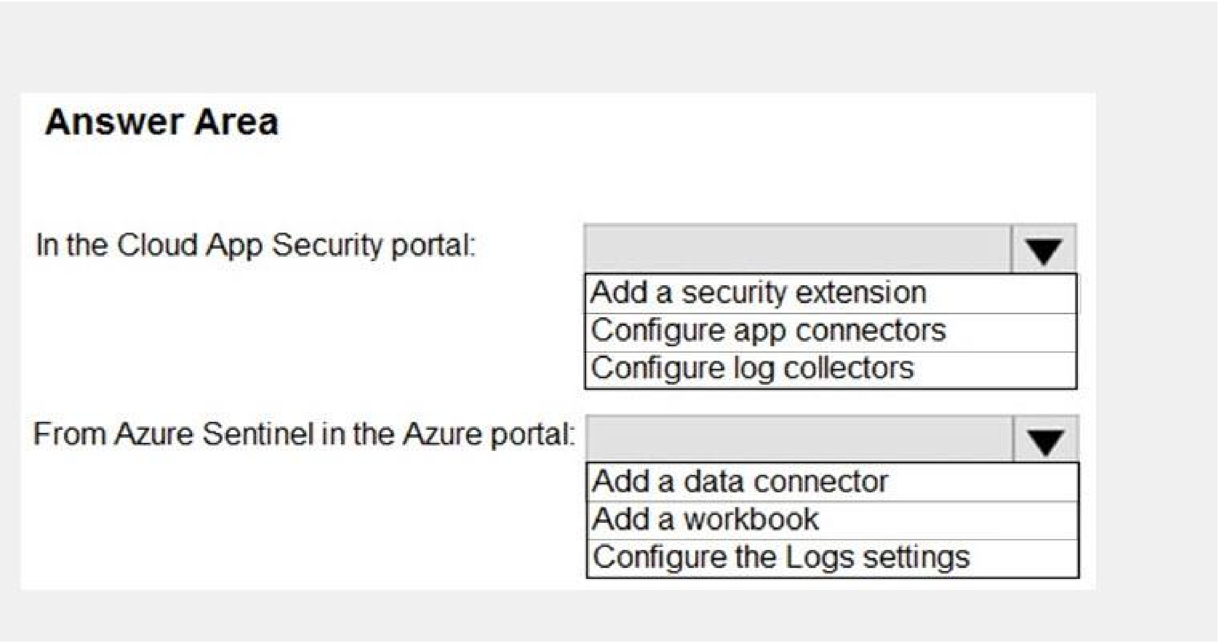
QUESTION 5
HOTSPOT

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:

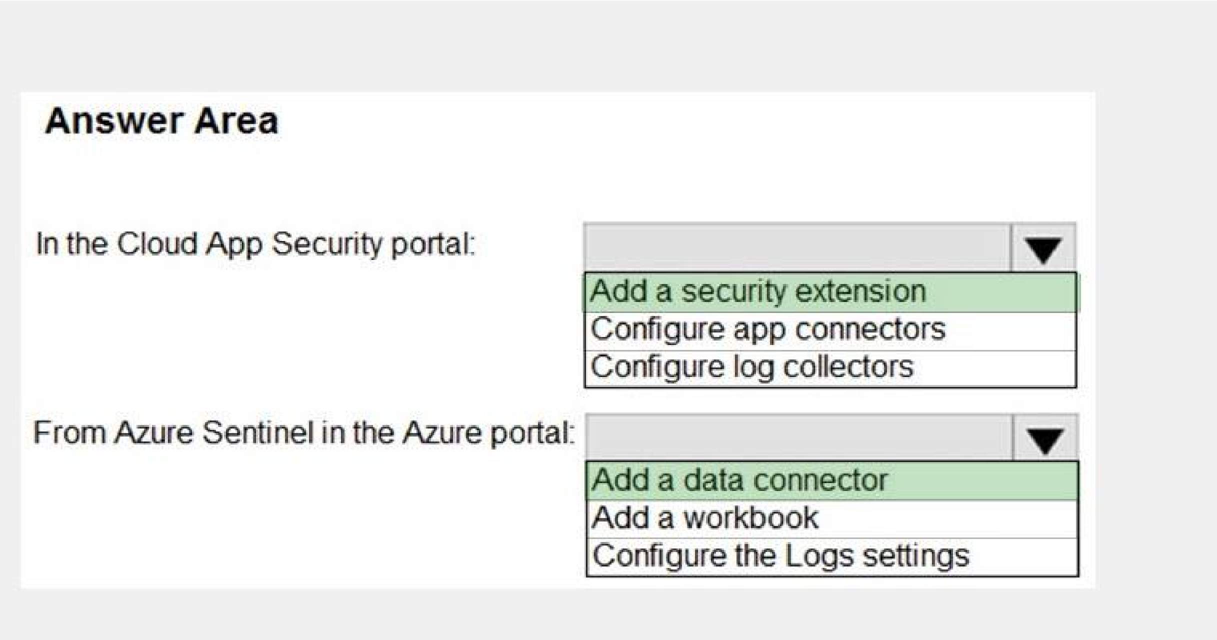


Answer Area

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

Correct Answer:



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

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

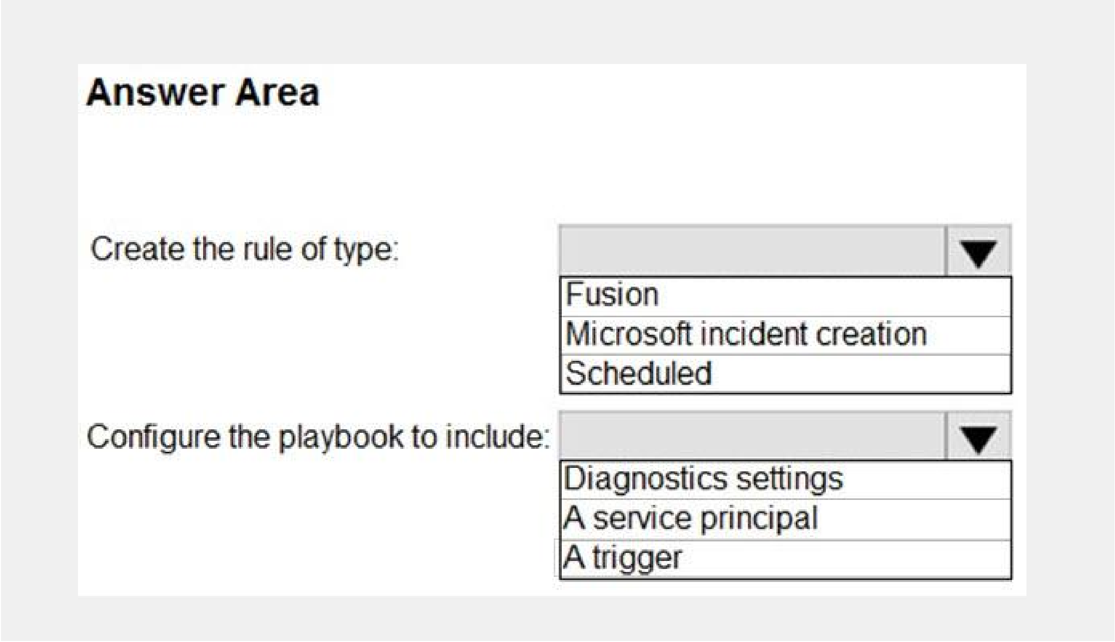
QUESTION 6
HOTSPOT

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

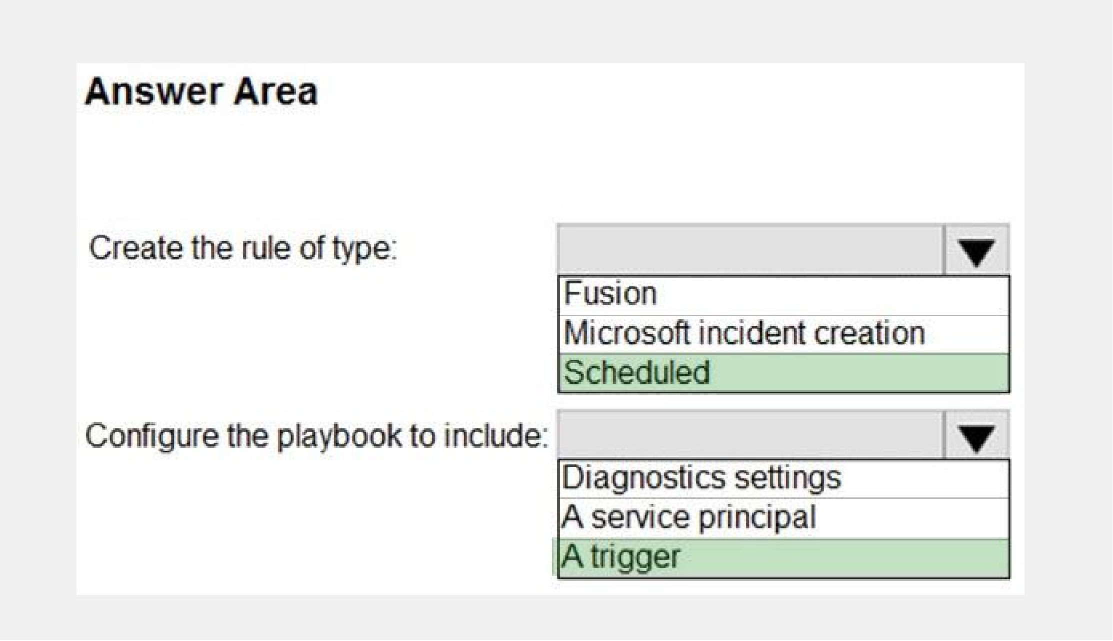
Create the rule of type:

- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include:

- Diagnostics settings
- A service principal
- A trigger

Correct Answer:



Answer Area

Create the rule of type:
- Fusion
- Microsoft incident creation
- [✓ Scheduled]

Configure the playbook to include:
- Diagnostics settings
- A service principal
- [✓ A trigger]

Section: (none)
Explanation

Explanation/Reference:
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

03 - Mitigate threats using Azure Sentinel

QUESTION 1
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/loqs/qet-started-queries

QUESTION 2
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Correct Answer: AB
Section: (none)
Explanation

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

QUESTION 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
Section: (none)
Explanation

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

QUESTION 4
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
Section: (none)
Explanation

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

QUESTION 5
You use Azure Sentinel.
You need to receive an immediate alert whenever Azure Storage account keys are enumerated.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Create a livestream
B. Add a data connector
C. Create an analytics rule
D. Create a hunting query.
E. Create a bookmark.

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 6
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Your company uses Azure Sentinel to manage alerts from more than 10,000 loT 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
Section: (none)
Explanation

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

QUESTION 8
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

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

Correct Answer: D
Section: (none)
Explanation

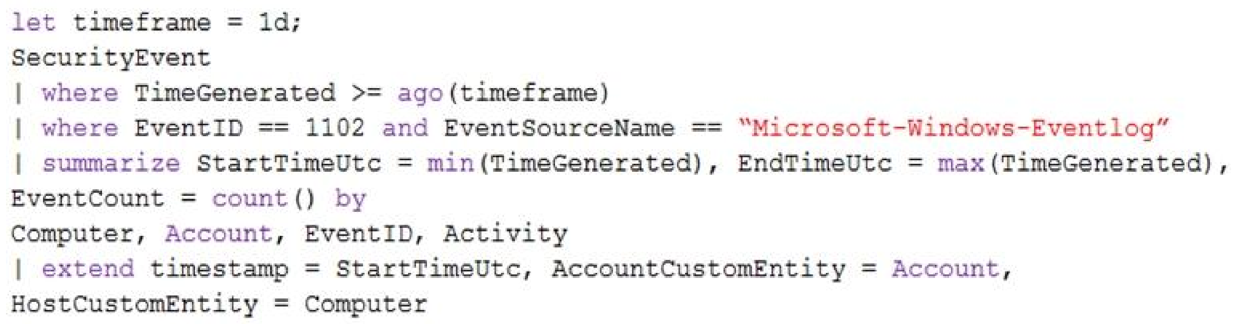
Explanation/Reference:
Expl anation/Refere nee:
Reference:
https://azsec.azu rewebsites .net/202(y01/19/notifv-azure-sentinel-alert-to-vour-email-automaticallv/

QUESTION 9
You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.



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

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address

D. computer

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Correct Answer: BE
Section: (none)
Explanation

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

QUESTION 11
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
Section: (none)
Explanation

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

QUESTION 12
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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https: //doc s. m ic rosoft. co m/en-u s/azu re/se ntine l/tutorial-detect-th reats-c ustom

QUESTION 13
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
B. Logic App Contributor
C. Azure Sentinel Contributor
D. Azure Sentinel Reader

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 14
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.micrQsoft.com/en-us/azure/sentinekconnect-data-sources

QUESTION 15
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
Section: (none)
Explanation

Explanation/Reference:

Reference:
https://docs.microsoftcom/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION 16
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
Section: (none)
Explanation

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

QUESTION 17
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.
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

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Incorrect Answers:
B: This would cause it to fail everytime, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

QUESTION 18
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
Section: (none)
Explanation

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

QUESTION 19
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-securitv-center

QUESTION 20
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azu re/sentinel/connect-azu re-security-center

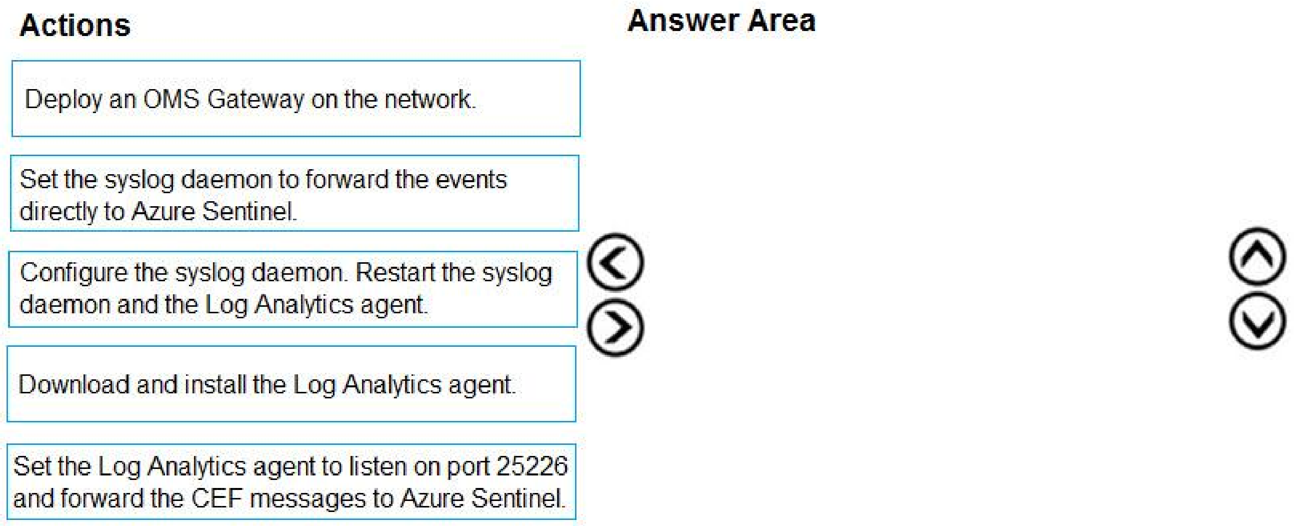
QUESTION 21
DRAG DROP

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:



Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

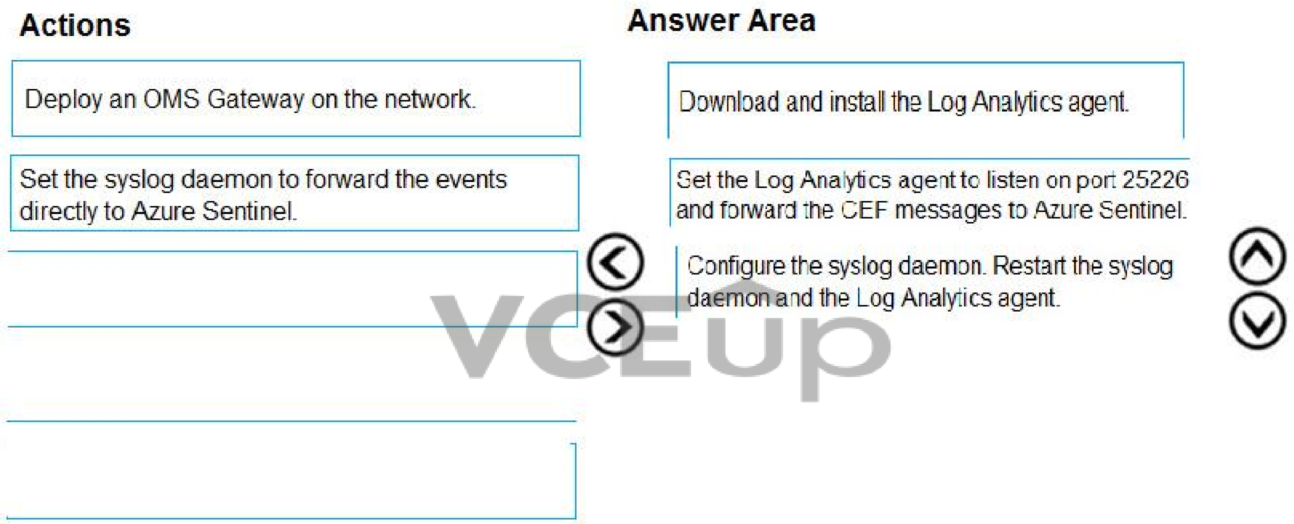
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

Answer Area

Correct Answer:



Actions

Deploy an OMS Gateway on the network.

Set the syslog daemon to forward the events directly to Azure Sentinel.

Answer Area

Download and install the Log Analytics agent.

Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.

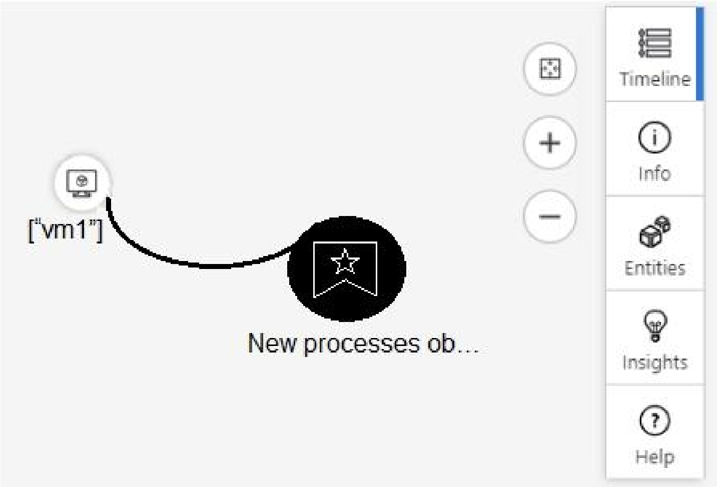
Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent.

Section: (none)
Explanation

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

QUESTION 22
HOTSPOT

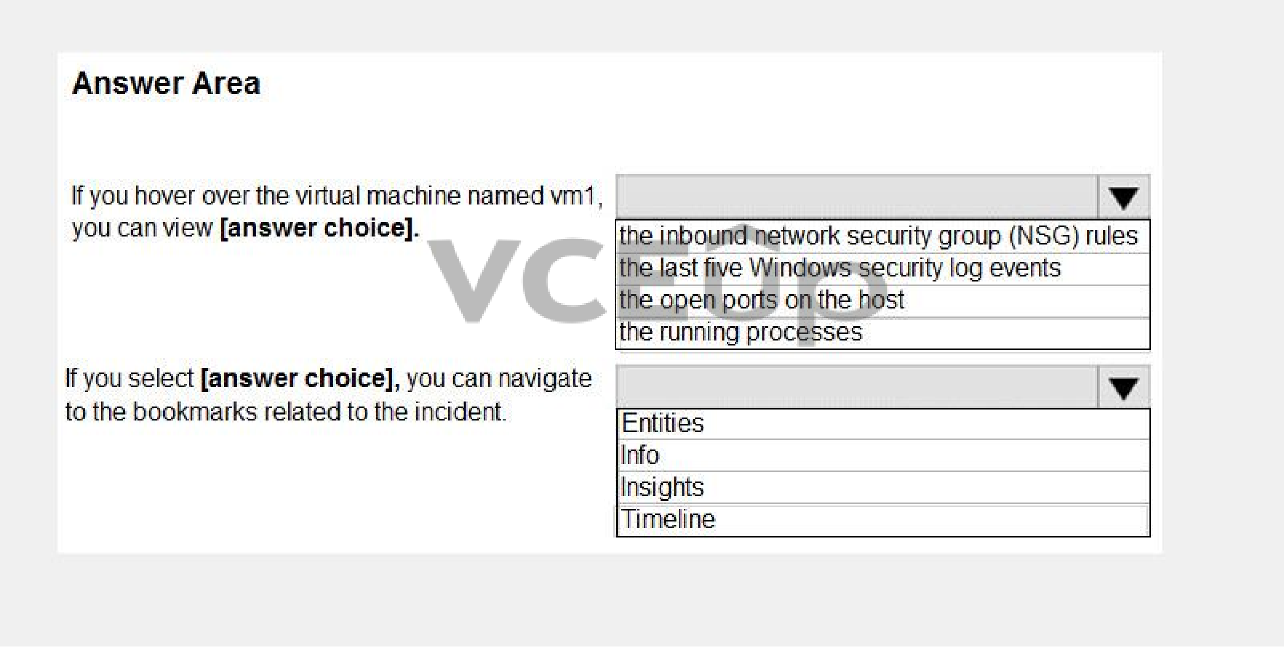
From Azure Sentinel, you open the **Investigation** pane for a high-severity incident as shown in the following exhibit.



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

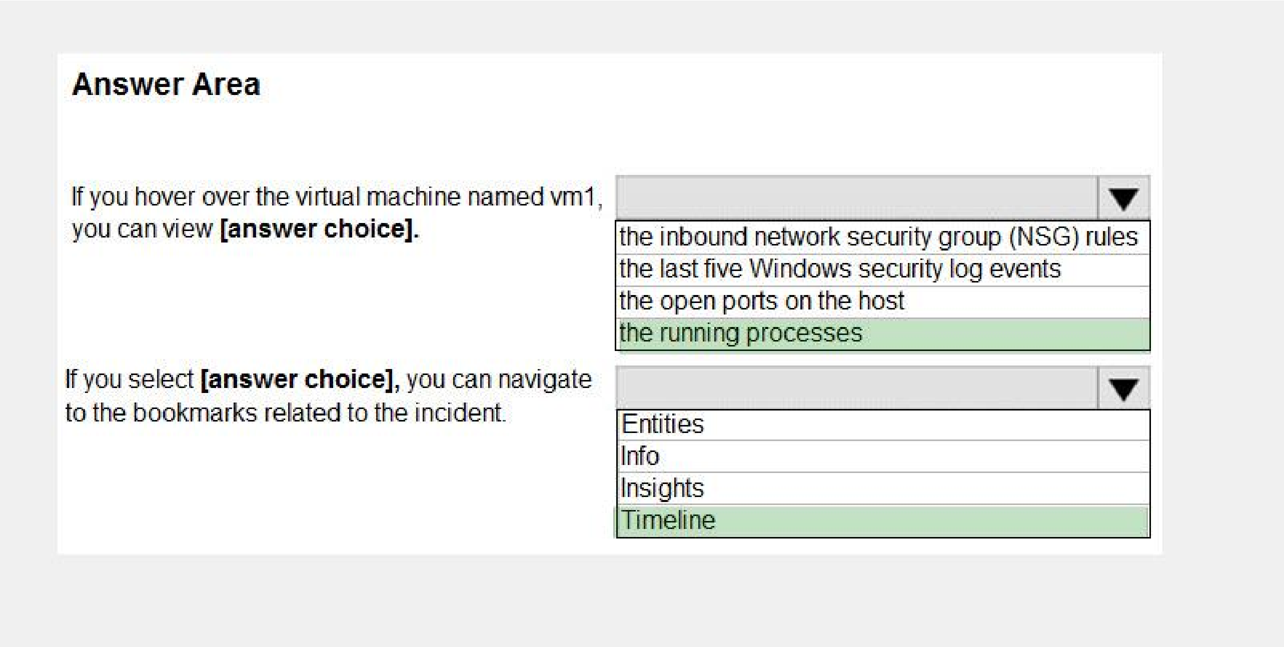
If you hover over the virtual machine named vm1, you can view **[answer choice].**

- 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 bookmarks 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 bookmarks related to the incident.

- Entities
- Info
- Insights
- [✓ Timeline]

Section: (none)
Explanation

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

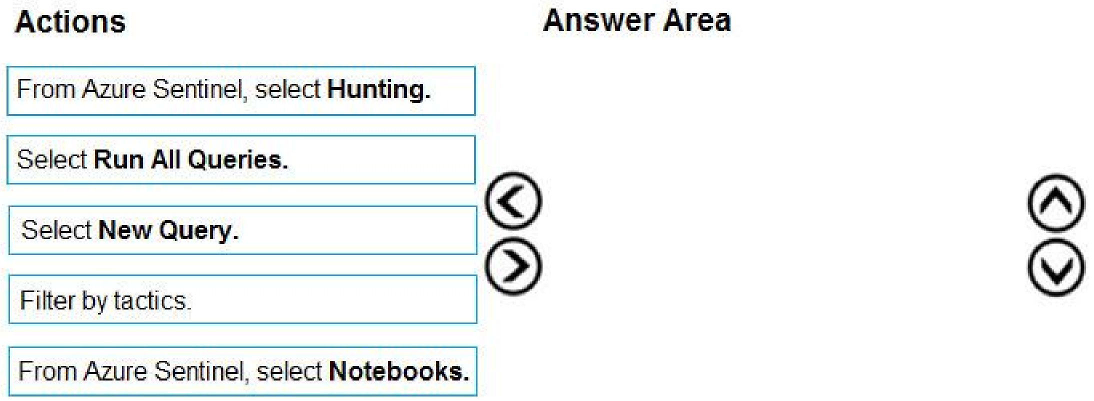
QUESTION 23
DRAG DROP

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:

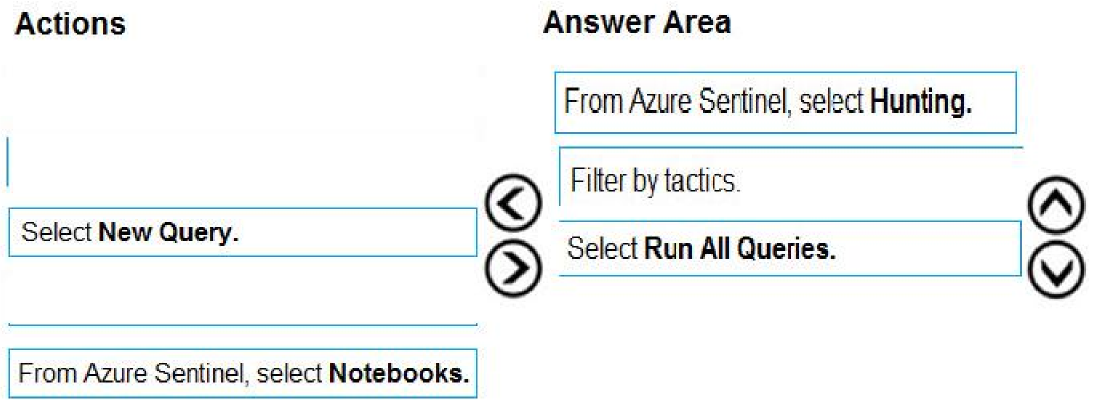


Actions

- From Azure Sentinel, select **Hunting.**
- Select **Run All Queries.**
- Select **New Query.**
- Filter by tactics.
- From Azure Sentinel, select **Notebooks.**

Answer Area

Correct Answer:



Actions

Select **New Query.**

From Azure Sentinel, select **Notebooks.**

Answer Area

From Azure Sentinel, select **Hunting.**

Filter by tactics.

Select **Run All Queries.**

Section: (none)
Explanation

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

QUESTION 24
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:

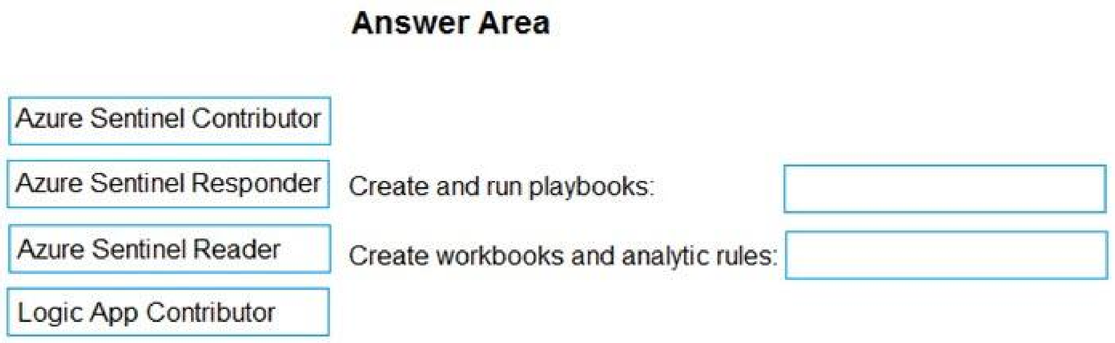
- Create and run playbooks
- Create workbooks and analytic rules.

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:



Answer Area

Azure Sentinel Contributor

Azure Sentinel Responder

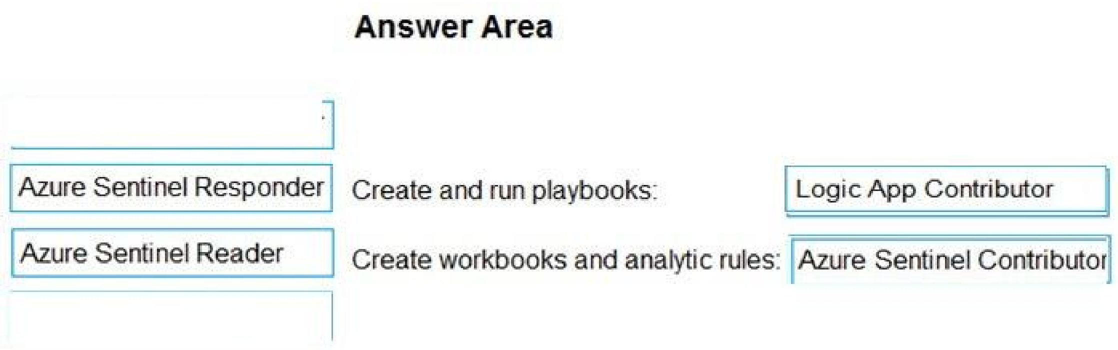
Azure Sentinel Reader

Logic App Contributor

Create and run playbooks:

Create workbooks and analytic rules:

Correct Answer:



Answer Area

Azure Sentinel Responder

Azure Sentinel Reader

Create and run playbooks: Logic App Contributor

Create workbooks and analytic rules: Azure Sentinel Contributor

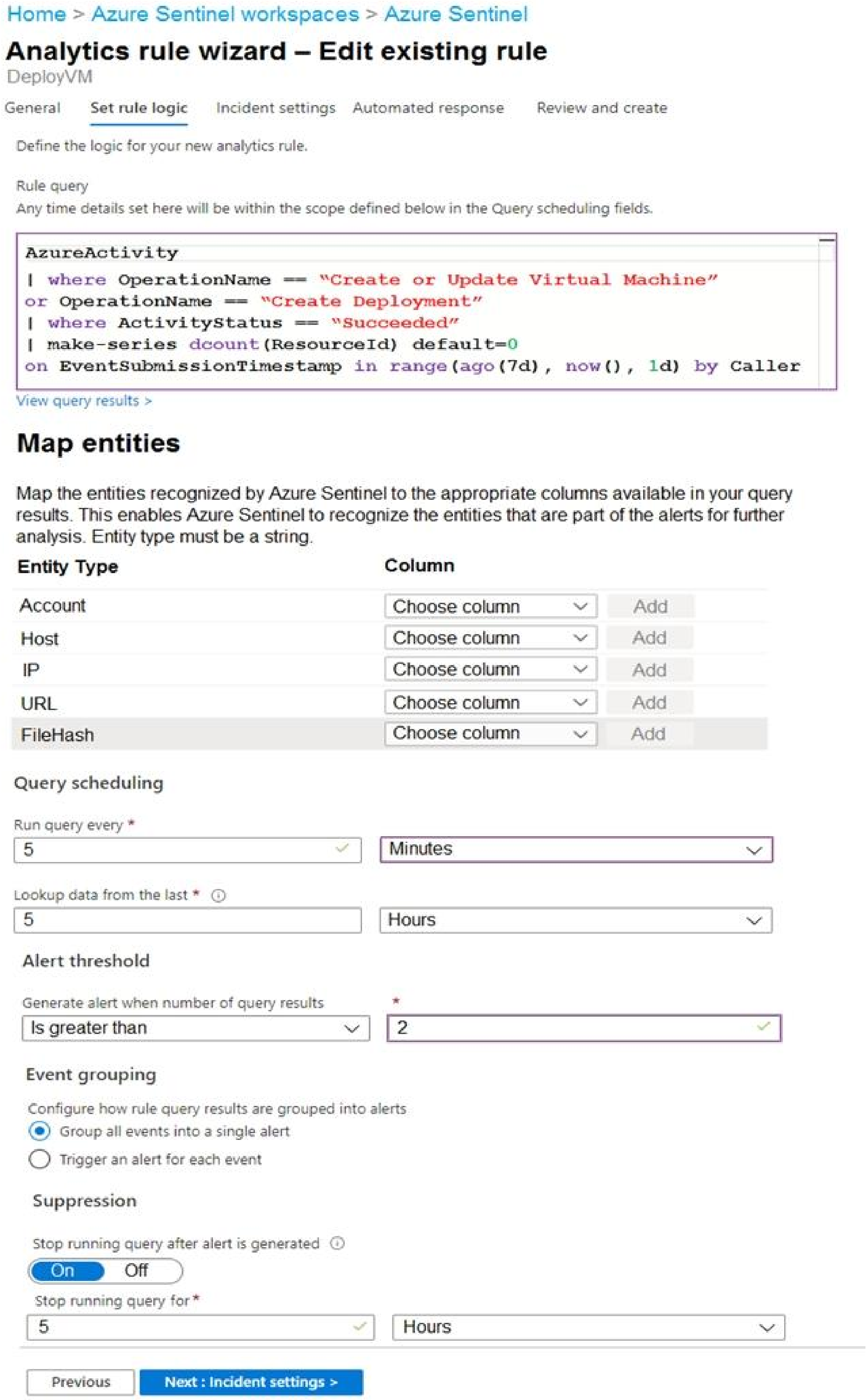
Section: (none)
Explanation

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

QUESTION 25
HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.

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



Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

General | Set rule logic | Incident settings | Automated response | Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every * 5 Minutes

Lookup data from the last * 5 Hours

Alert threshold

Generate alert when number of query results * Is greater than 2

Event grouping

Configure how rule query results are grouped into alerts

● Group all events into a single alert

○ Trigger an alert for each event

Suppression

Stop running query after alert is generated

On Off

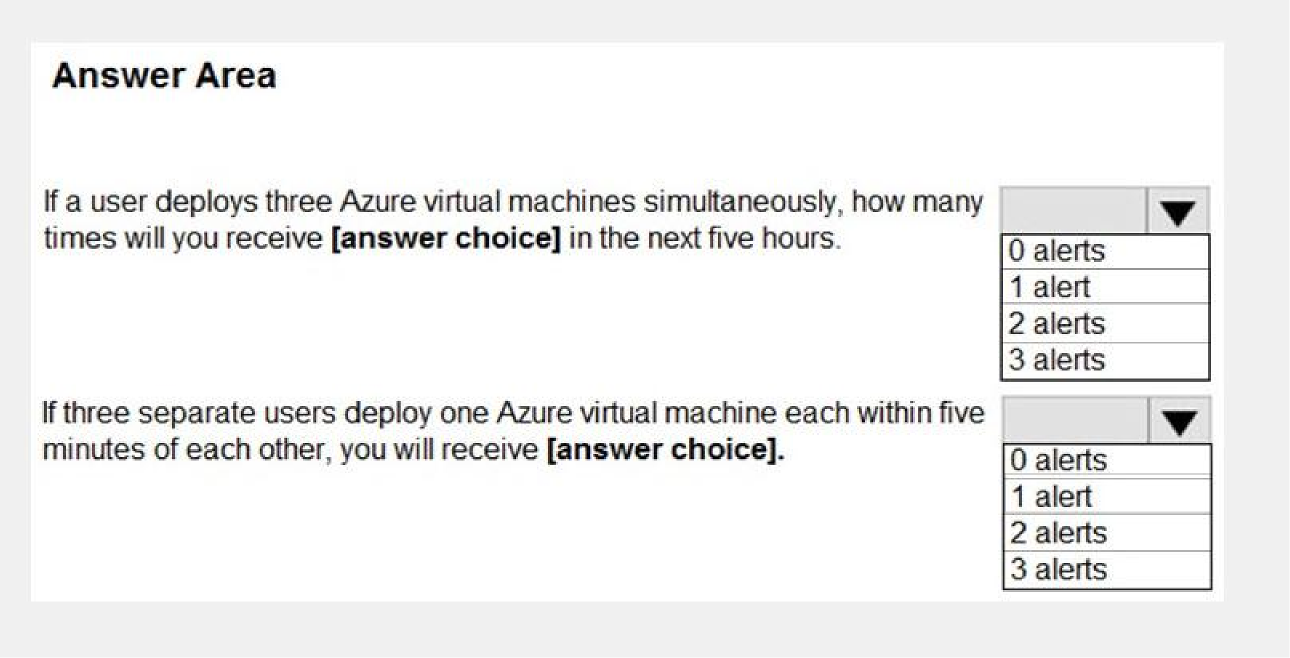
Stop running query for * 5 Hours

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

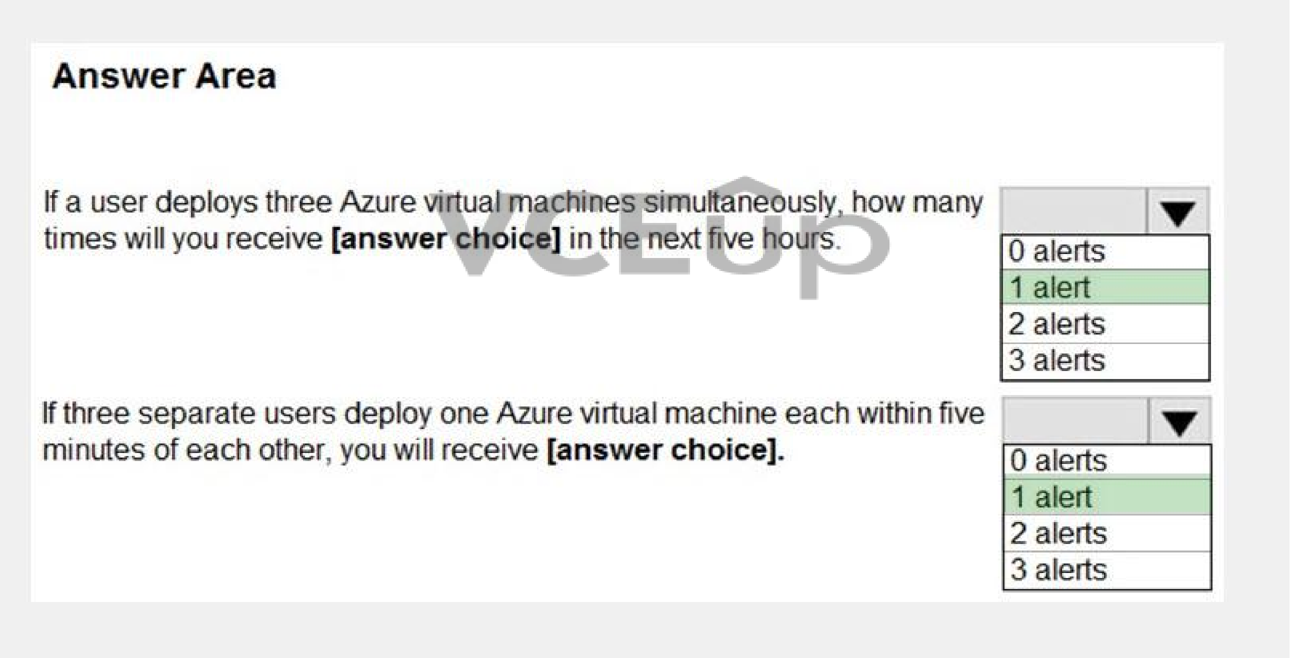
If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 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

Section: (none)
Explanation

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

QUESTION 26
HOTSPOT

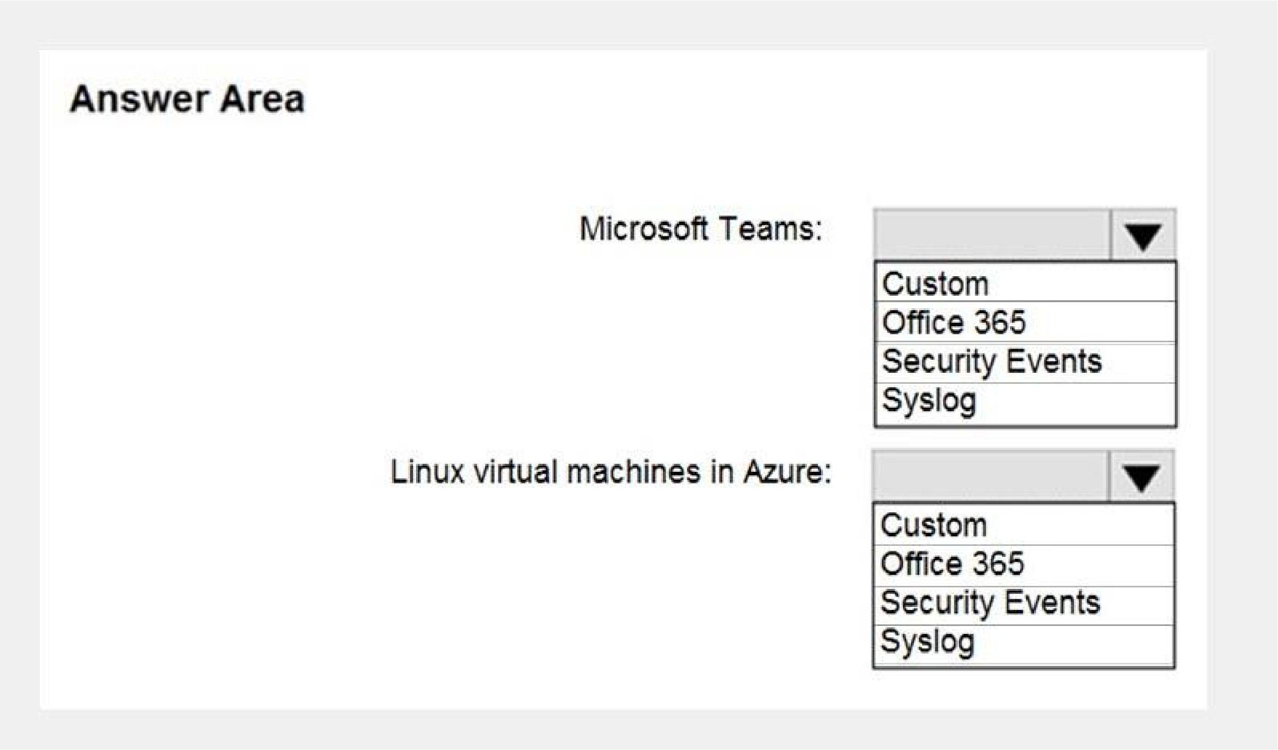
You deploy Azure Sentinel.

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:

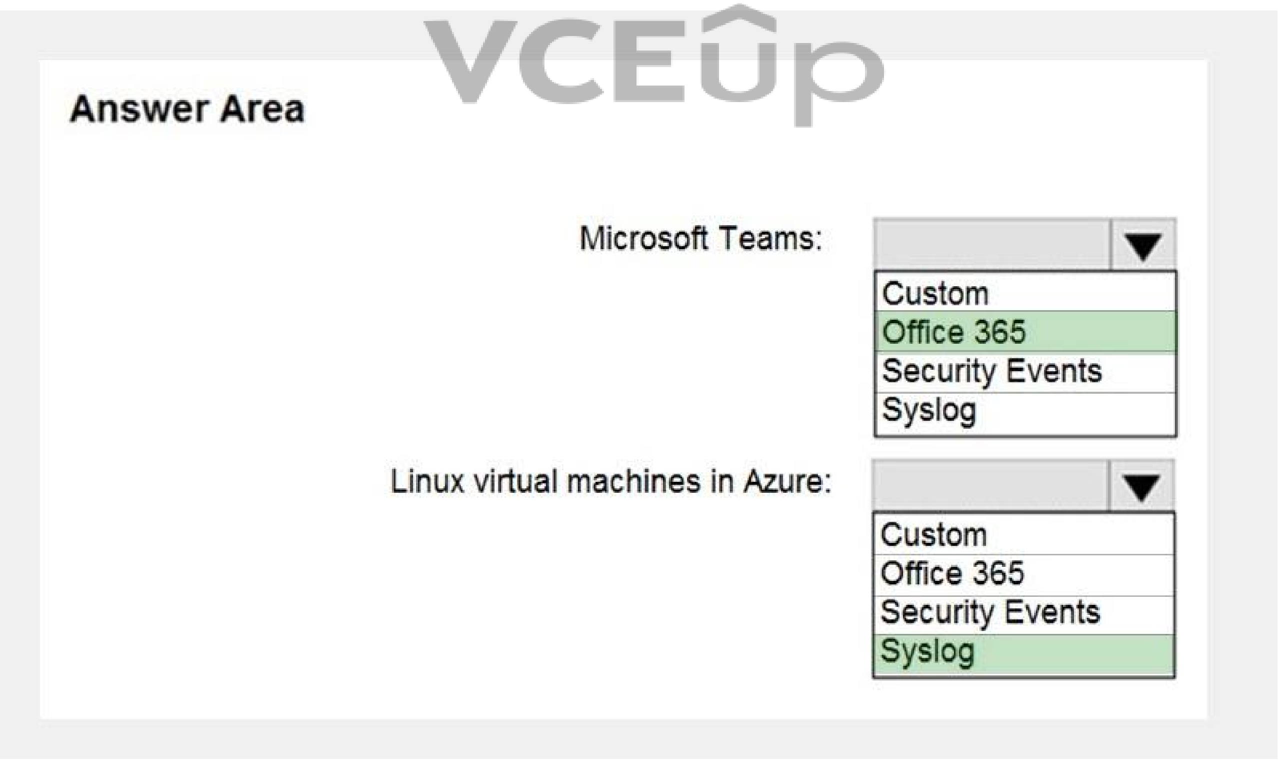


Answer Area

Microsoft Teams:
- Custom
- Office 365
- Security Events
- Syslog

Linux virtual machines in Azure:
- Custom
- Office 365
- Security Events
- Syslog

Correct Answer:



Answer Area

Microsoft Teams:
- Custom
- [✓ Office 365]
- Security Events
- Syslog

Linux virtual machines in Azure:
- Custom
- Office 365
- Security Events
- [✓ Syslog]

Section: (none)
Explanation

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

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

QUESTION 27
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
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

QUESTION 28
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.
C. Enable the Fusion rule.
D. Add a playbook.
E. Create a workbook.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics

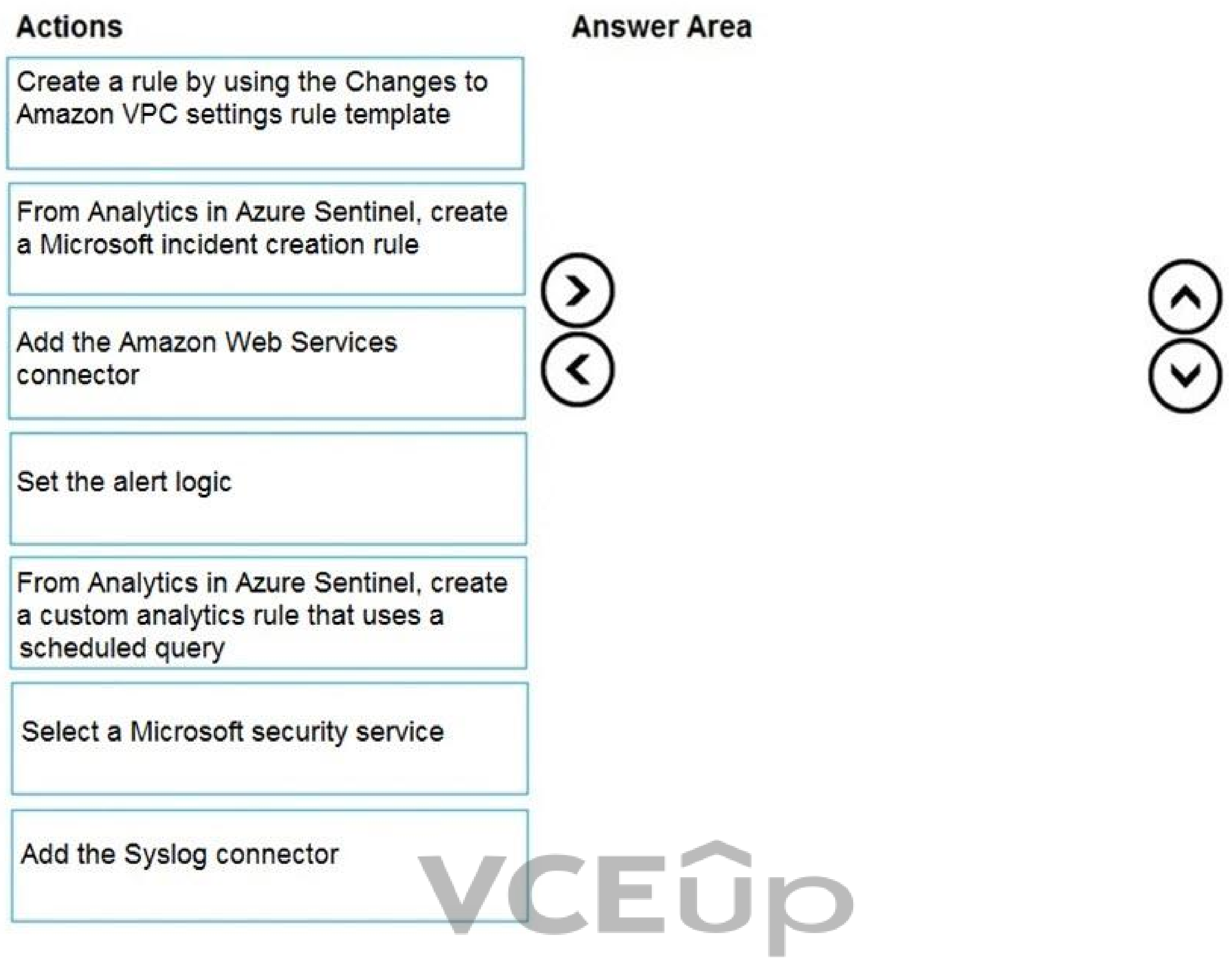
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

QUESTION 29
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:

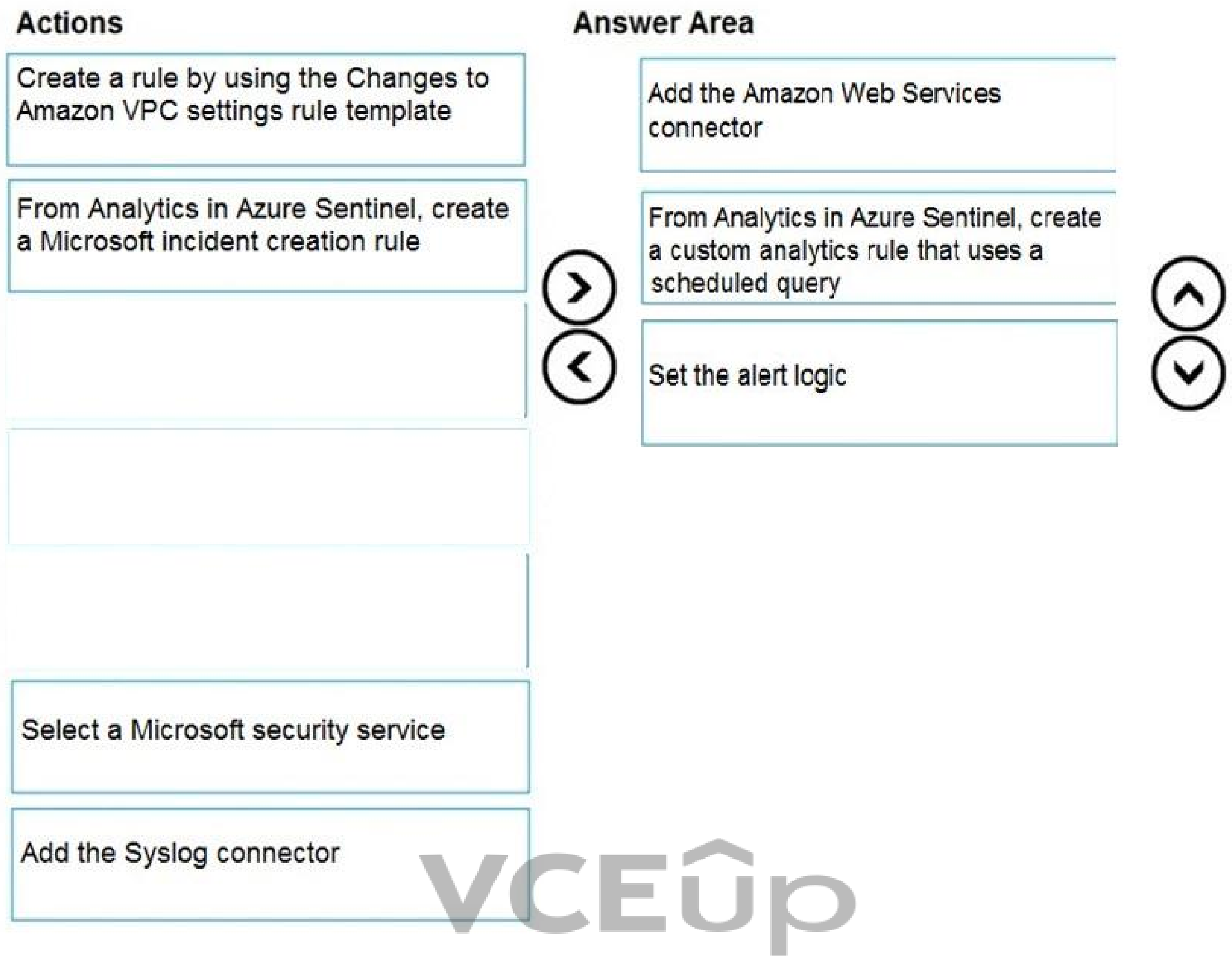


Actions

- Create a rule by using the Changes to Amazon VPC settings rule template
- From Analytics in Azure Sentinel, create a Microsoft incident creation rule
- Add the Amazon Web Services connector
- Set the alert logic
- From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query
- Select a Microsoft security service
- Add the Syslog connector

Answer Area

Correct Answer:



Actions

Create a rule by using the Changes to Amazon VPC settings rule template

From Analytics in Azure Sentinel, create a Microsoft incident creation rule

Select a Microsoft security service

Add the Syslog connector

Answer Area

Add the Amazon Web Services connector

From Analytics in Azure Sentinel, create a custom analytics rule that uses a scheduled query

Set the alert logic

Section: (none)
Explanation

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

QUESTION 30
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
Section: (none)
Explanation

Explanation/Reference:
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