Microsoft.SC-200.vFeb-2024.by.Powyraki.133q

Number: SC-200
Passing Score: 800
Time Limit: 120
File Version: 13.3

Exam Code: SC-200
Exam Name: Microsoft Security Operations Analyst

Case Study 02 - Mitigate threats using Azure Defender

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
```

QUESTION 1

You need to recommend a solution to meet the technical requirements for the Azure virtual machines.

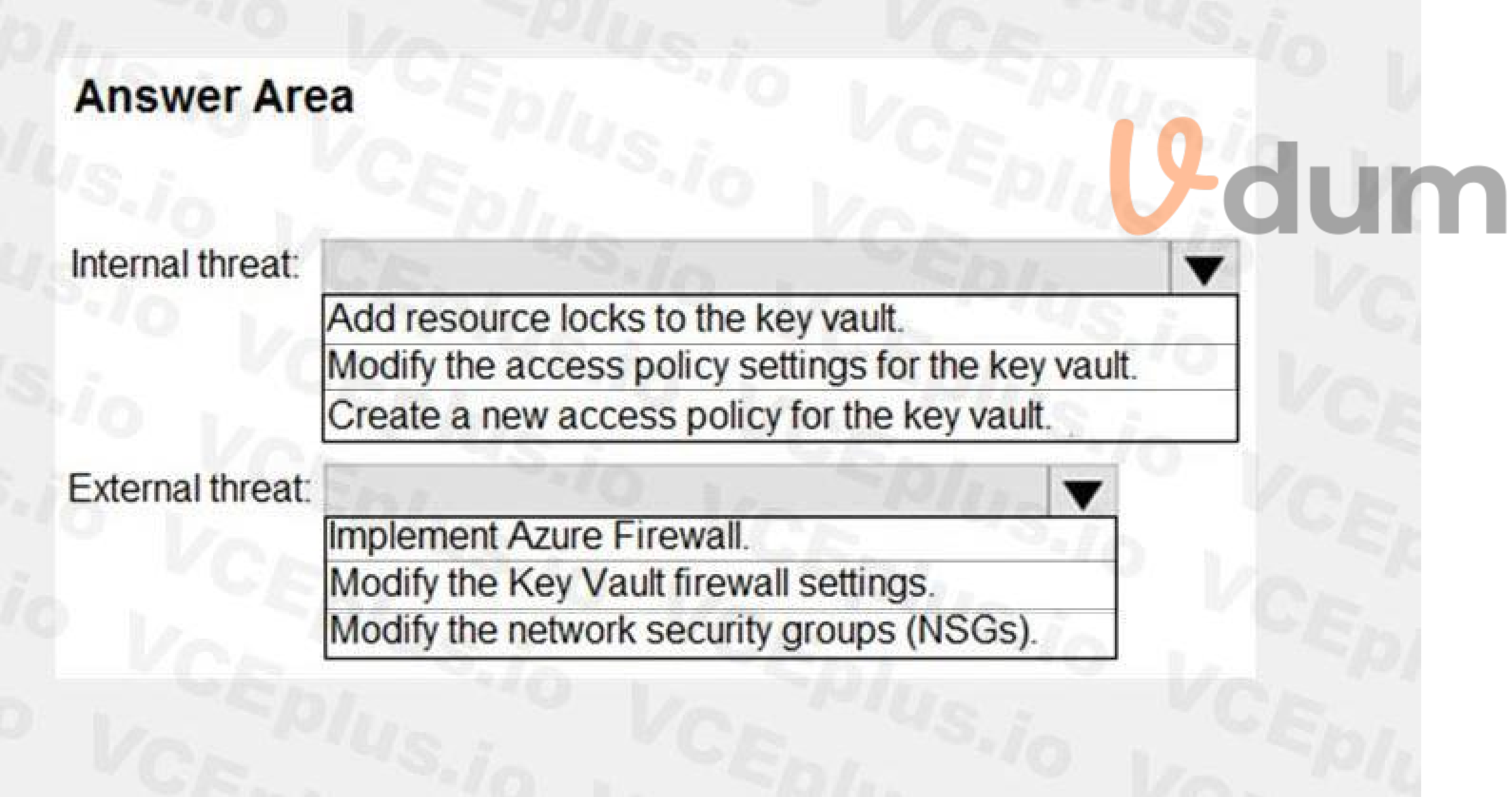
What should you include in the recommendation?

A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway

Correct Answer: B
Section:
Explanation:
Reference:
https://docsmicrosoft.com/en-us/azure/security-center/azure-defender

QUESTION 2
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:

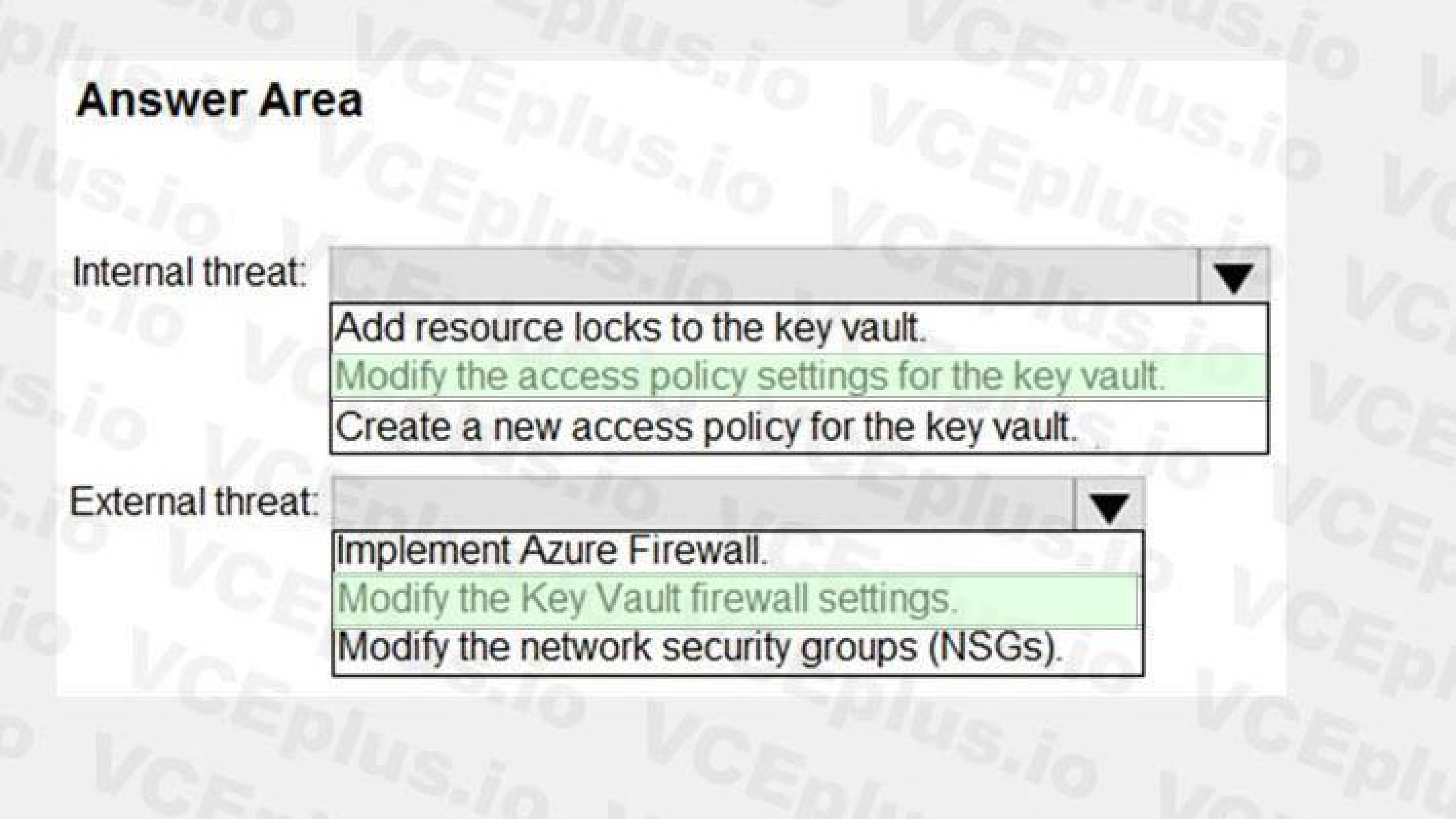


Answer Area

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).

Answer 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).

Section:
Explanation:
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:
Explanation:
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:
Explanation:
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:

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: A, D
Section:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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

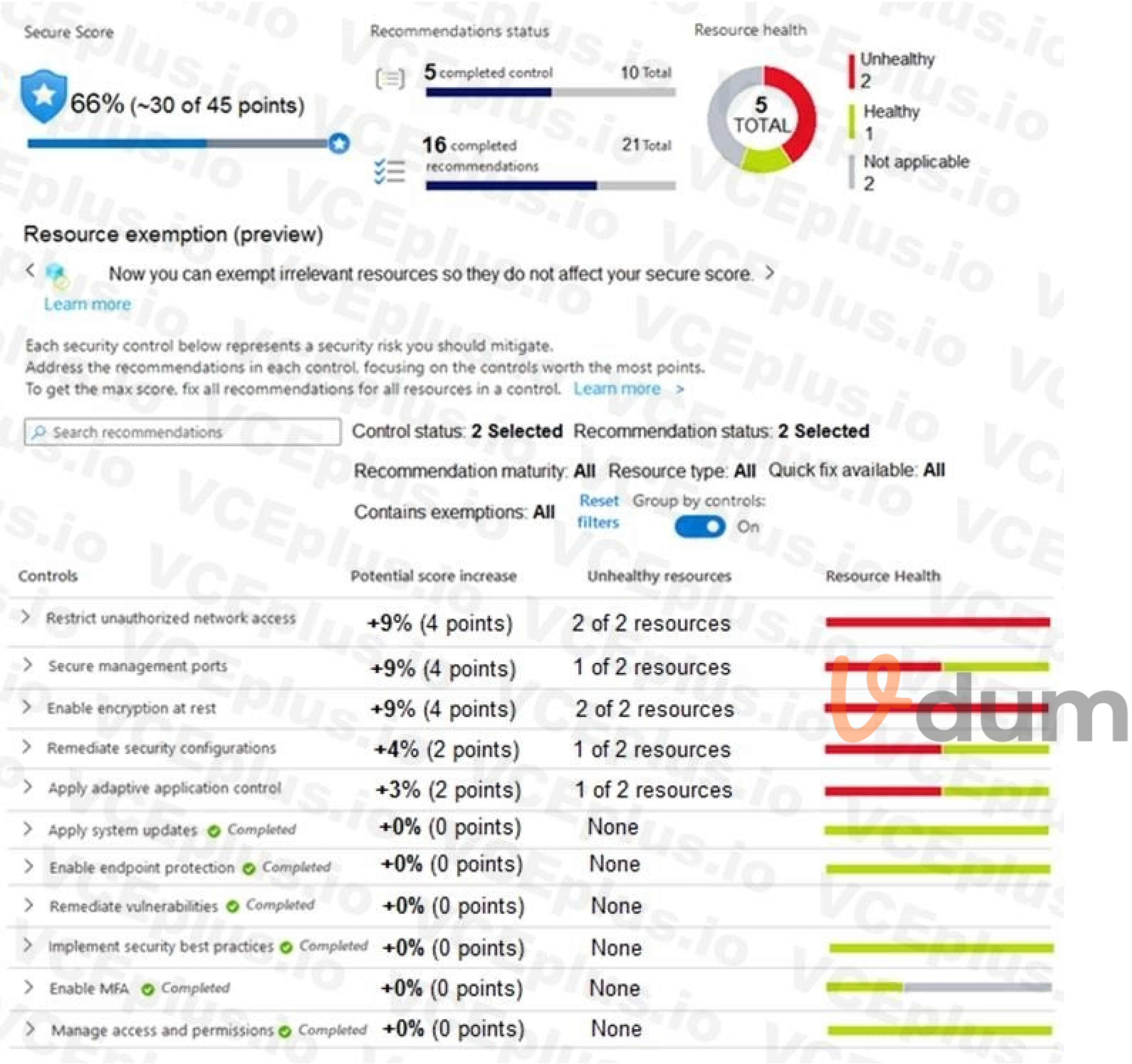
Correct Answer: A
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

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: A, C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/storaqe/common/azure-defender-storaqe-confiqure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

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

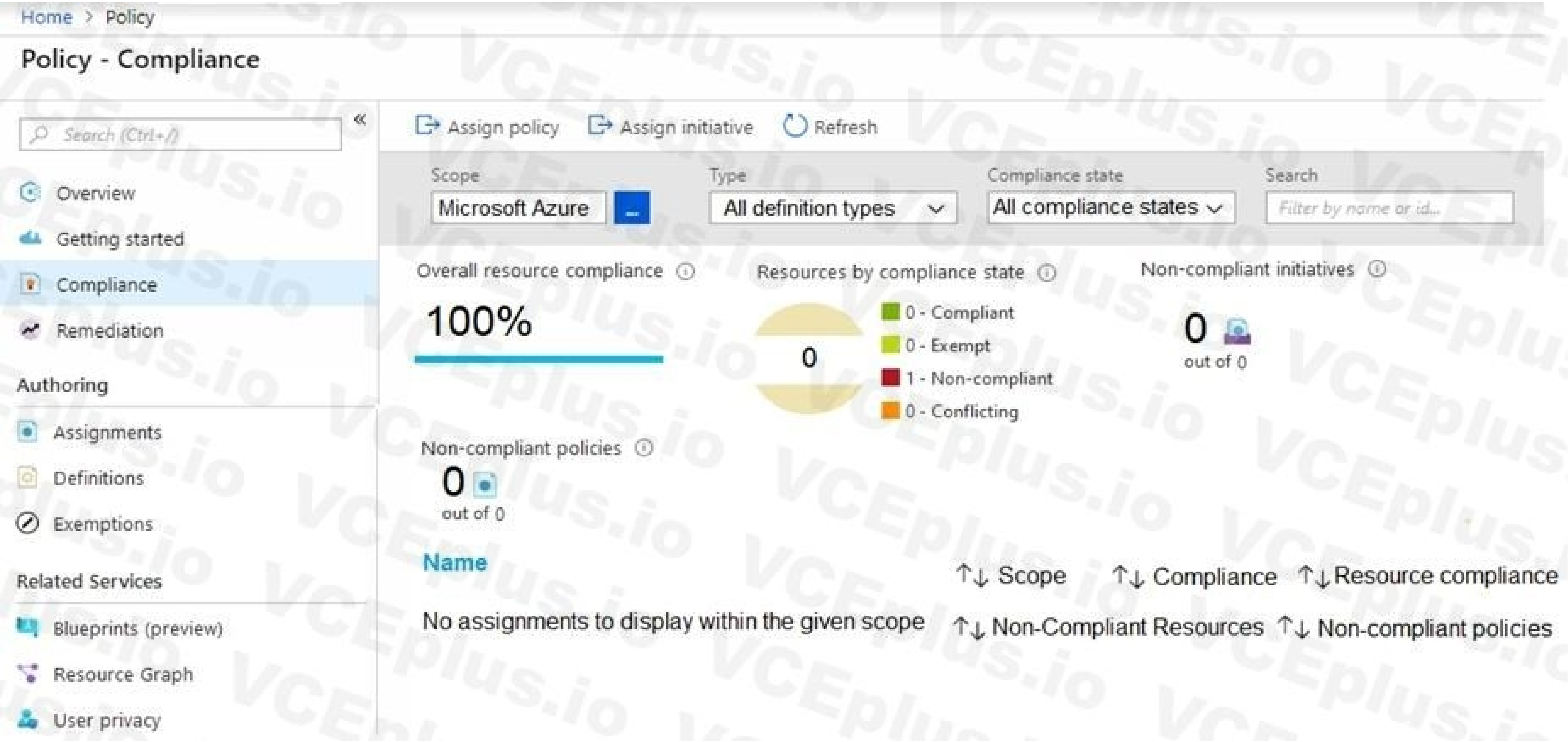
Control status: **2 Selected** Recommendation status: **2 Selected**

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.)



Home > Policy

Policy - Compliance

Search (Ctrl+/) «

Overview

Getting started

Compliance

Remediation

Authoring

Assignments

Definitions

Exemptions

Related Services

Blueprints (preview)

Resource Graph

User privacy

Assign policy | Assign initiative | Refresh

Scope	Type	Compliance state	Search
Microsoft Azure ...	All definition types	All compliance states	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

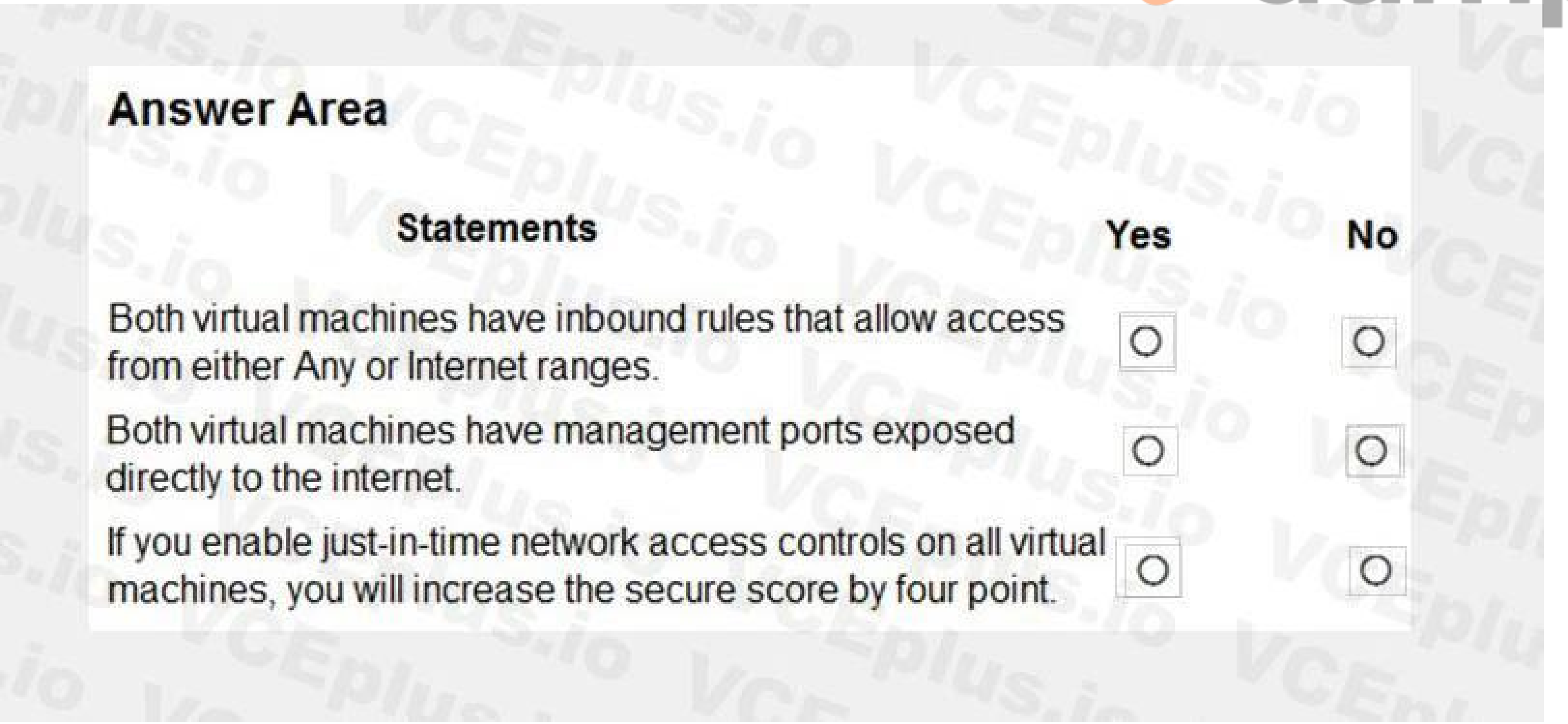
Non-compliant policies ⓘ

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.

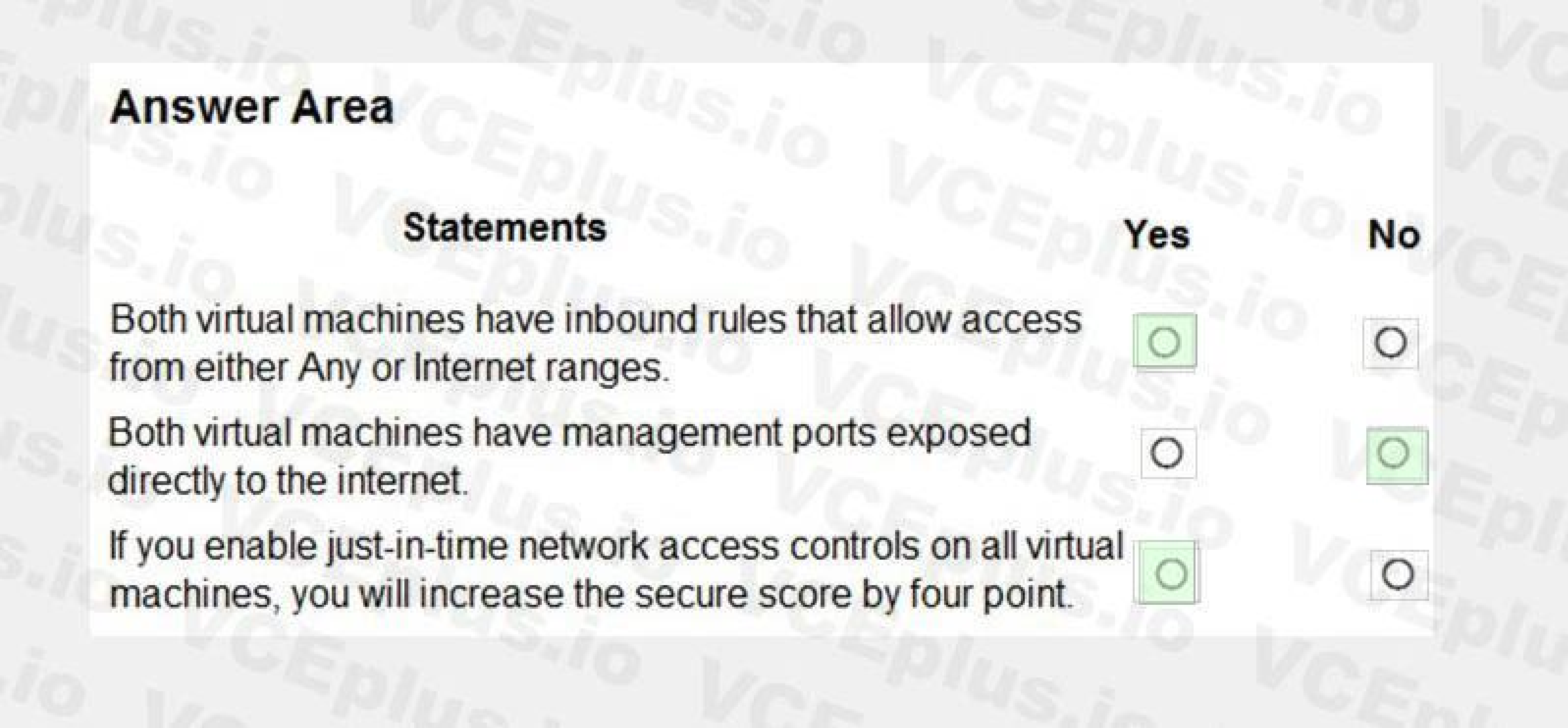
Hot Area:



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.	○	○

Answer Area:



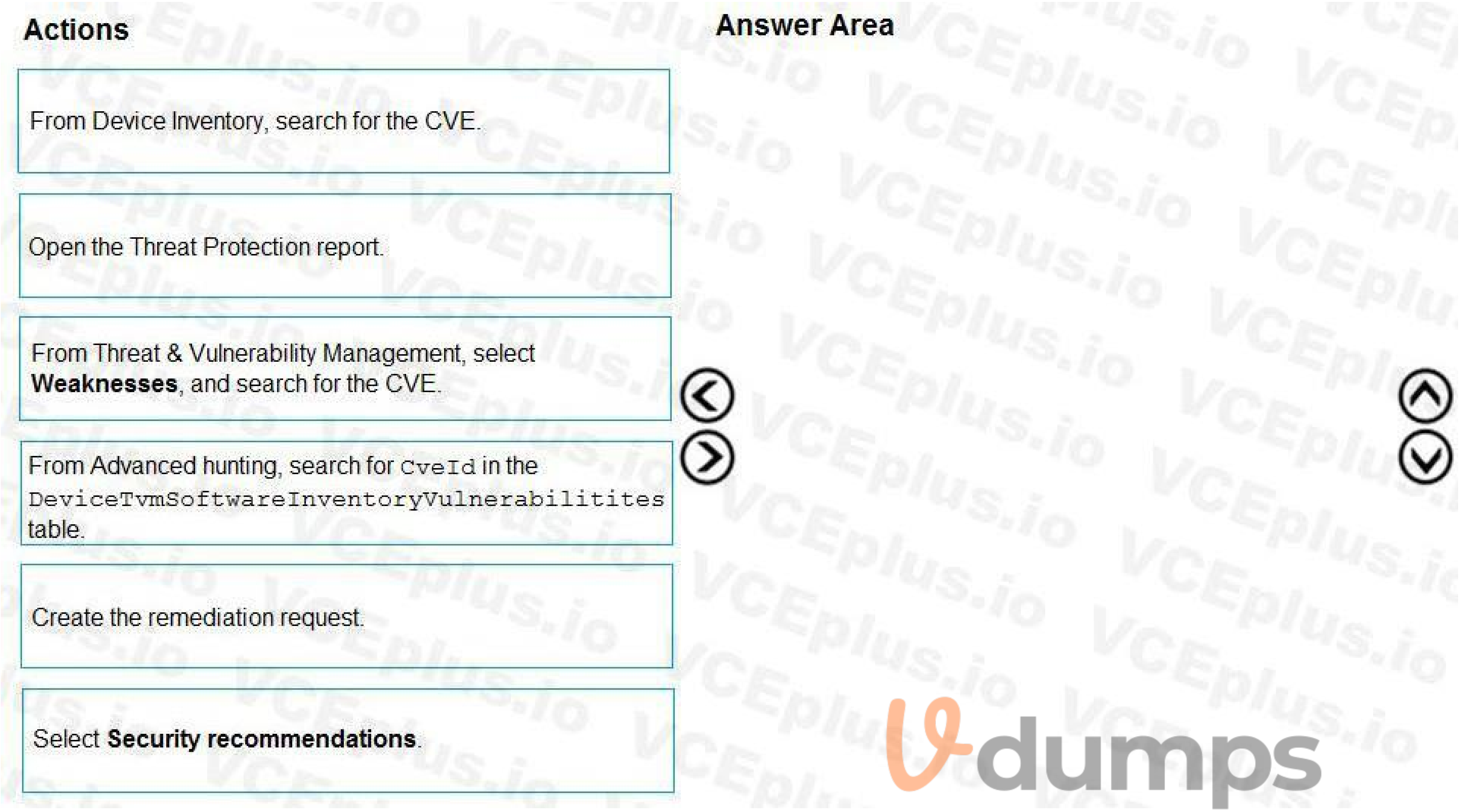
Answer Area

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.	[✓ ○]	○

Section:
Explanation:
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:

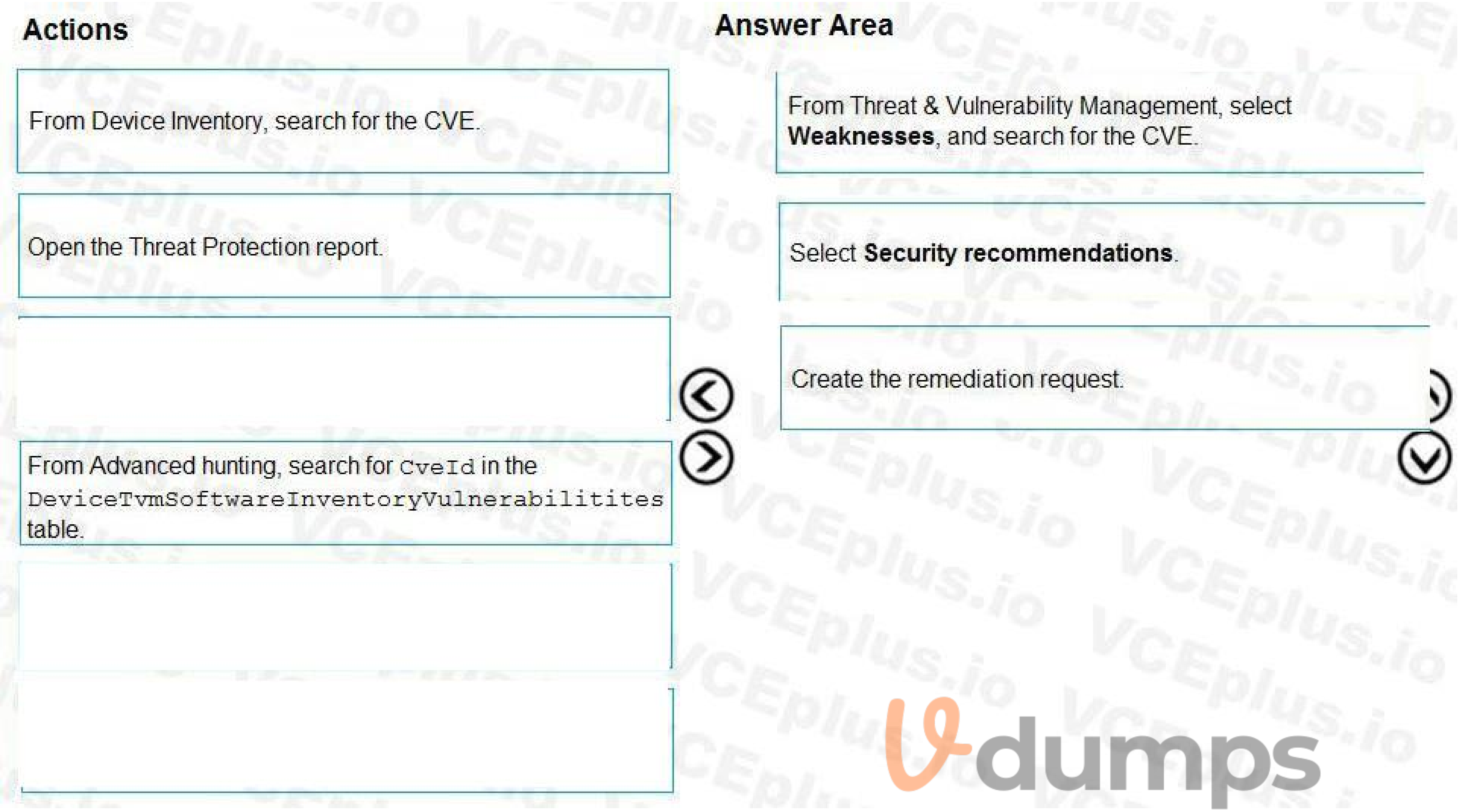


Actions

- 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.

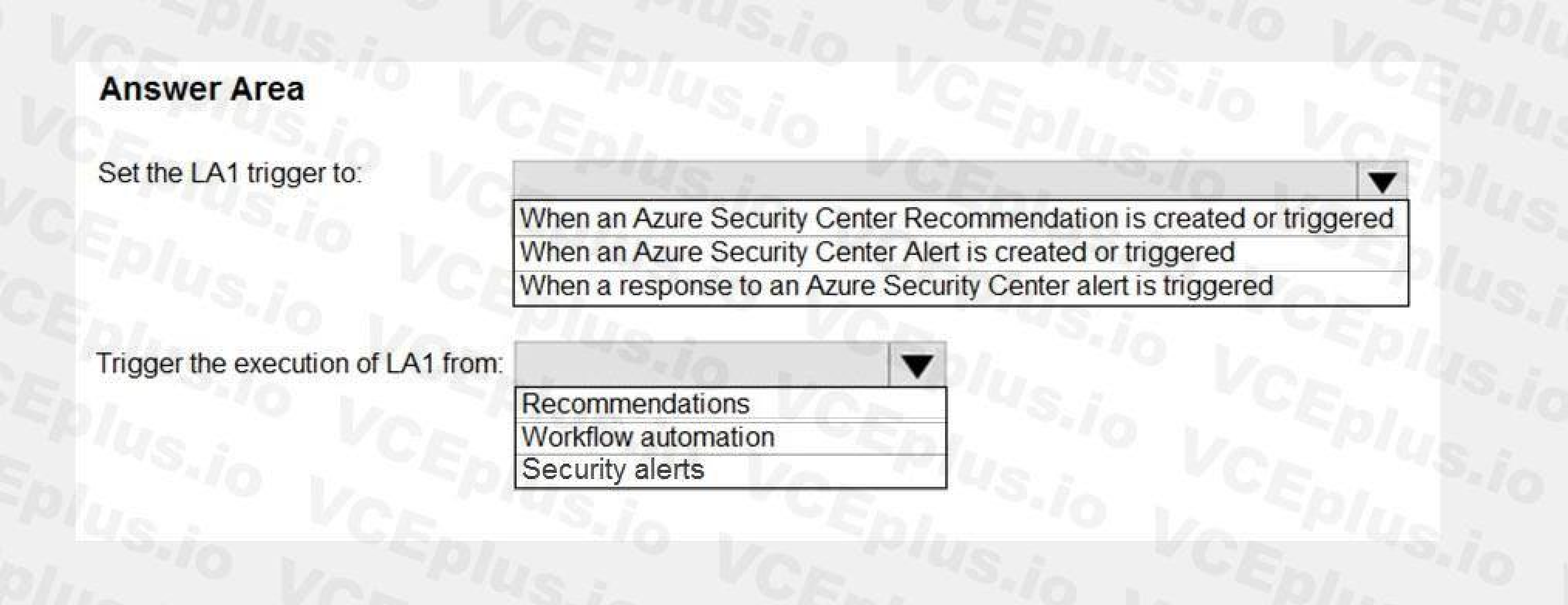
Select **Security recommendations**.

Create the remediation request.

Section:
Explanation:
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

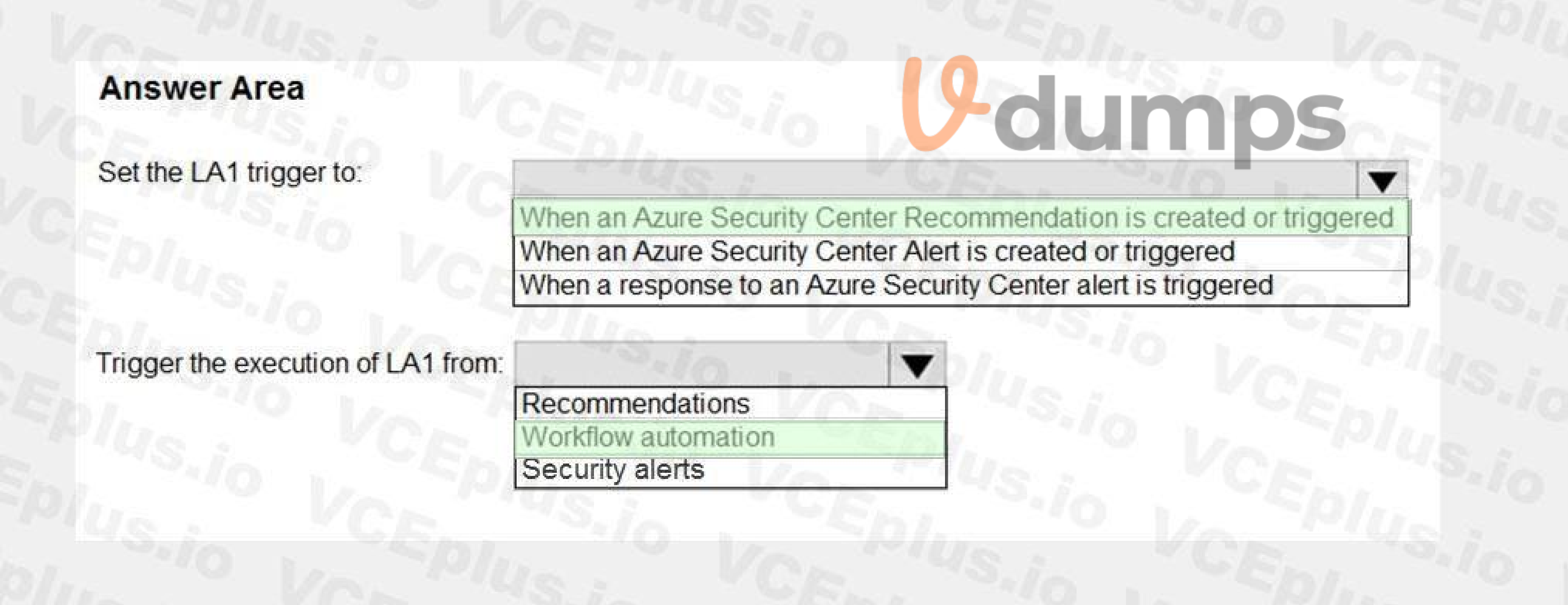
Set the LA1 trigger to:

- 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

Answer 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

Section:

Explanation:

Reference:

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

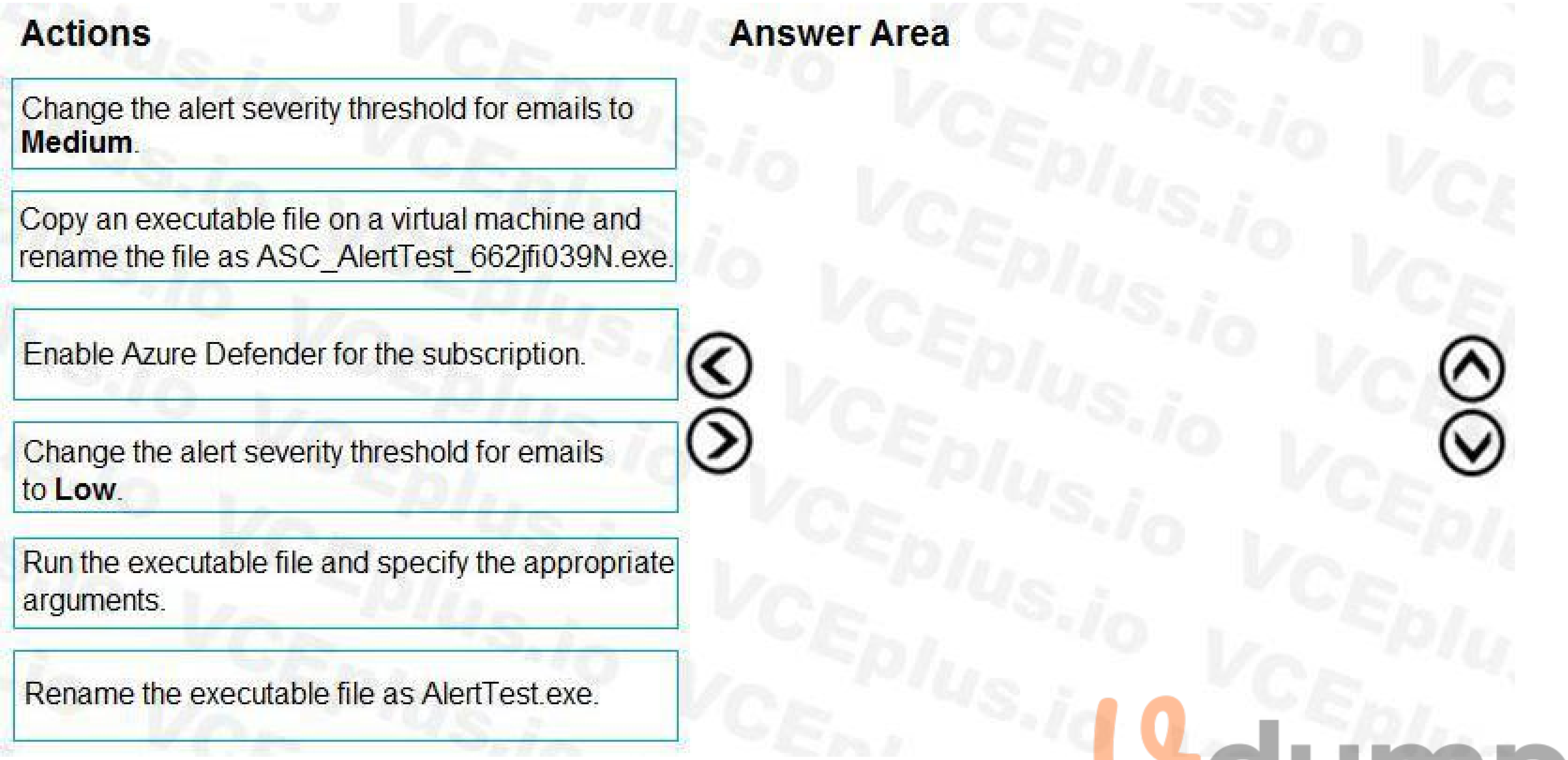
QUESTION 16

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:

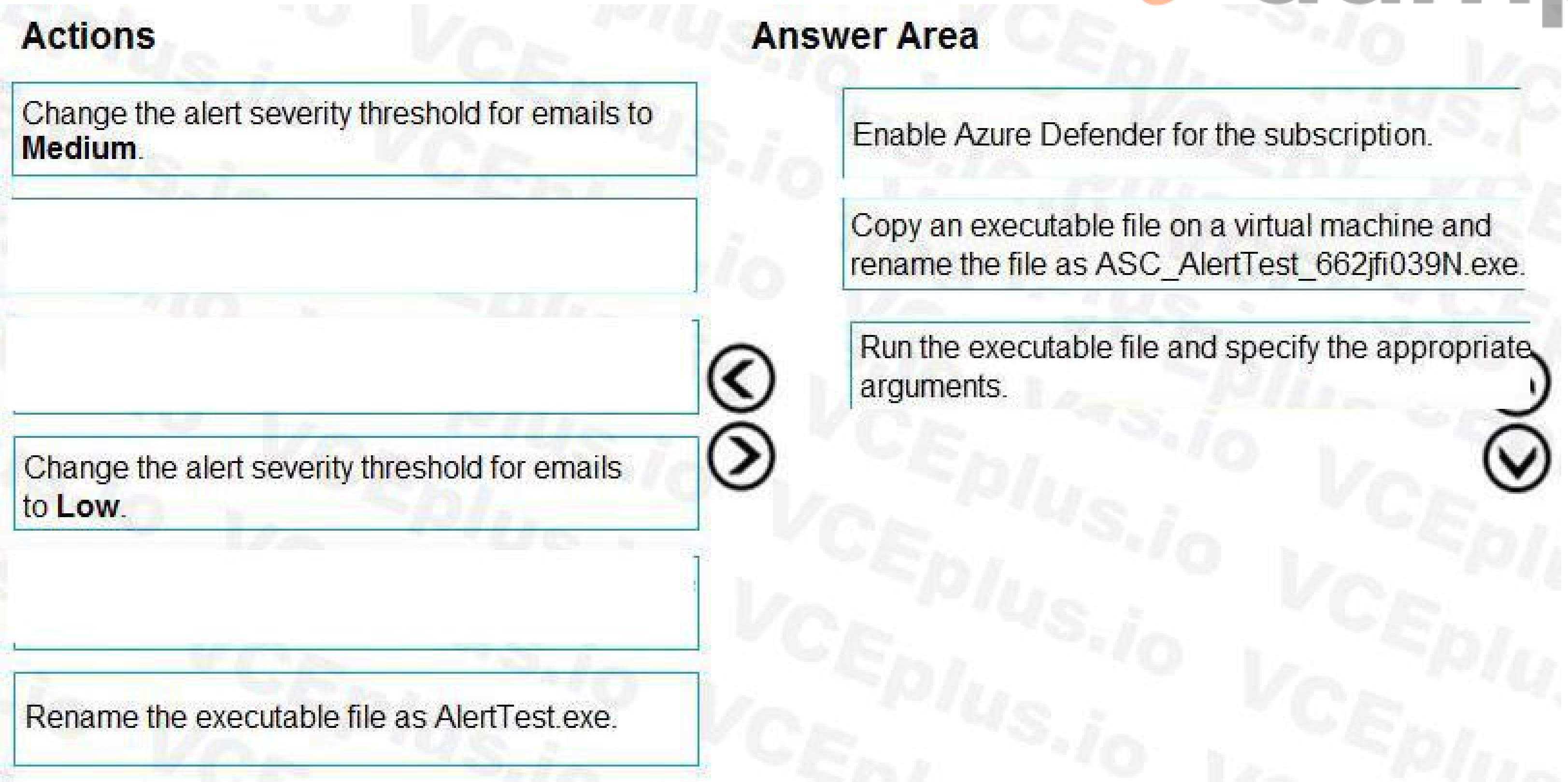


Actions

- 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

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

Section:
Explanation:
Reference:

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

QUESTION 17

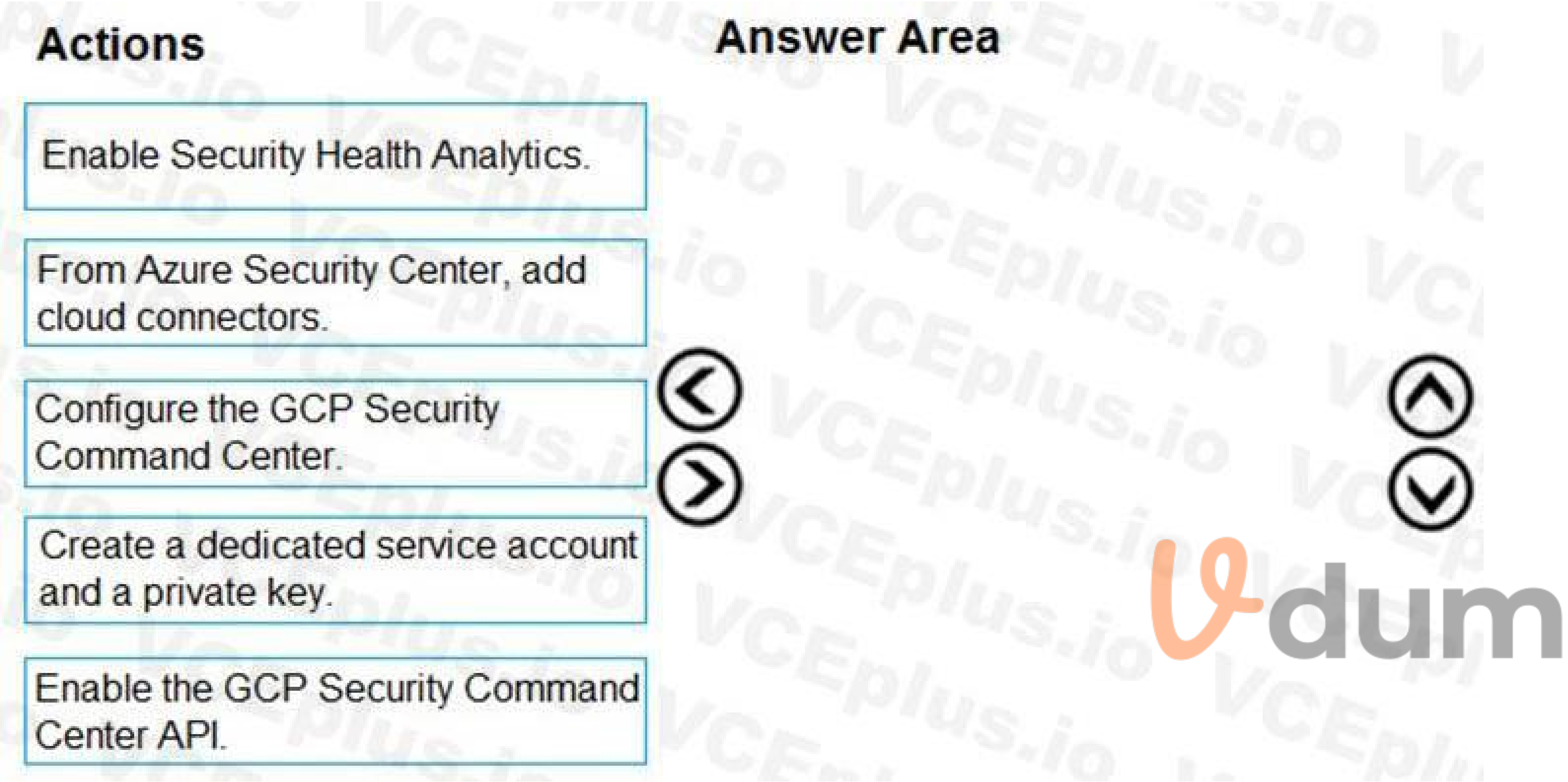
DRAG DROP

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:

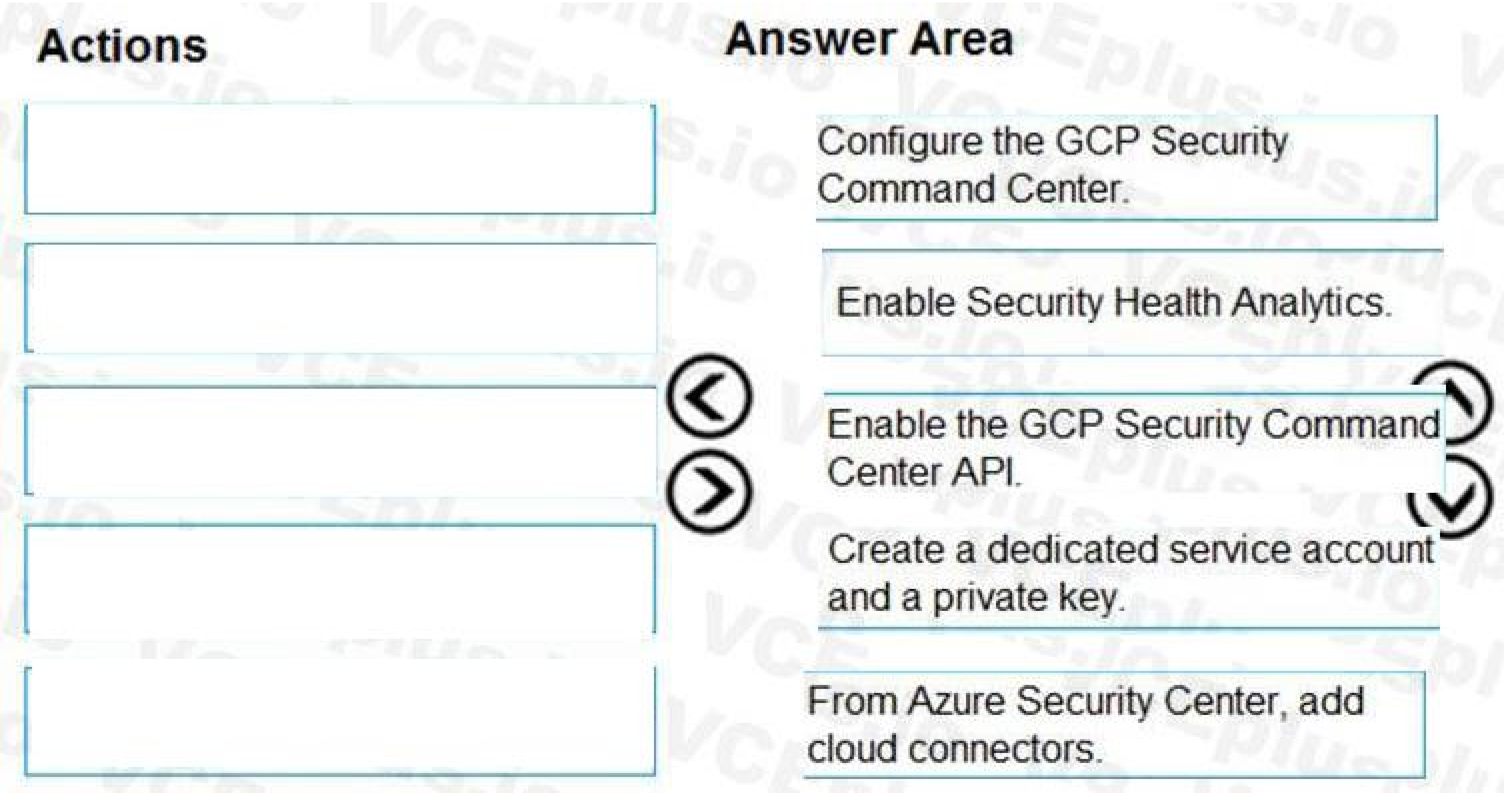


Actions

- 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.

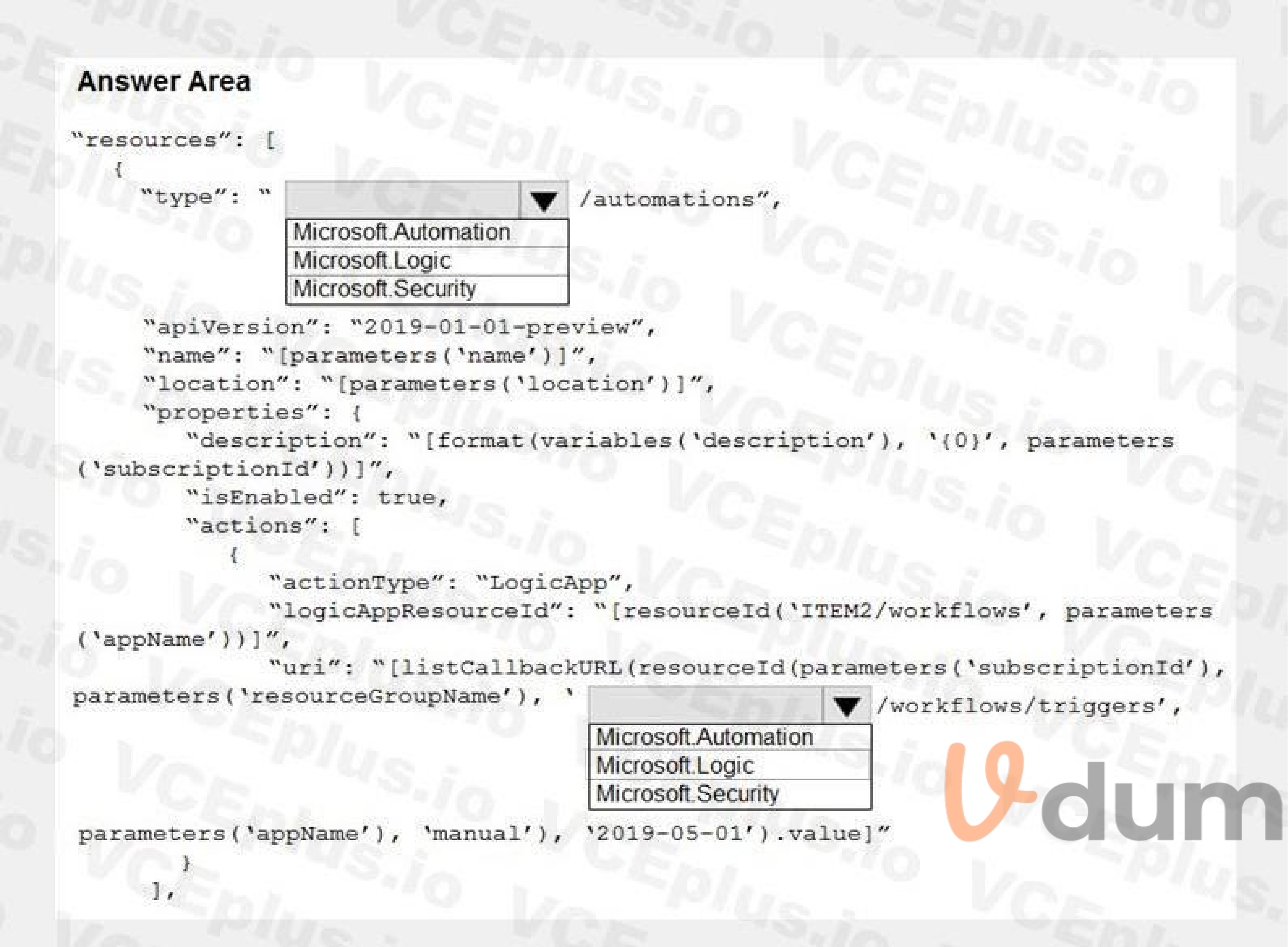
Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

Section:
Explanation:
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.

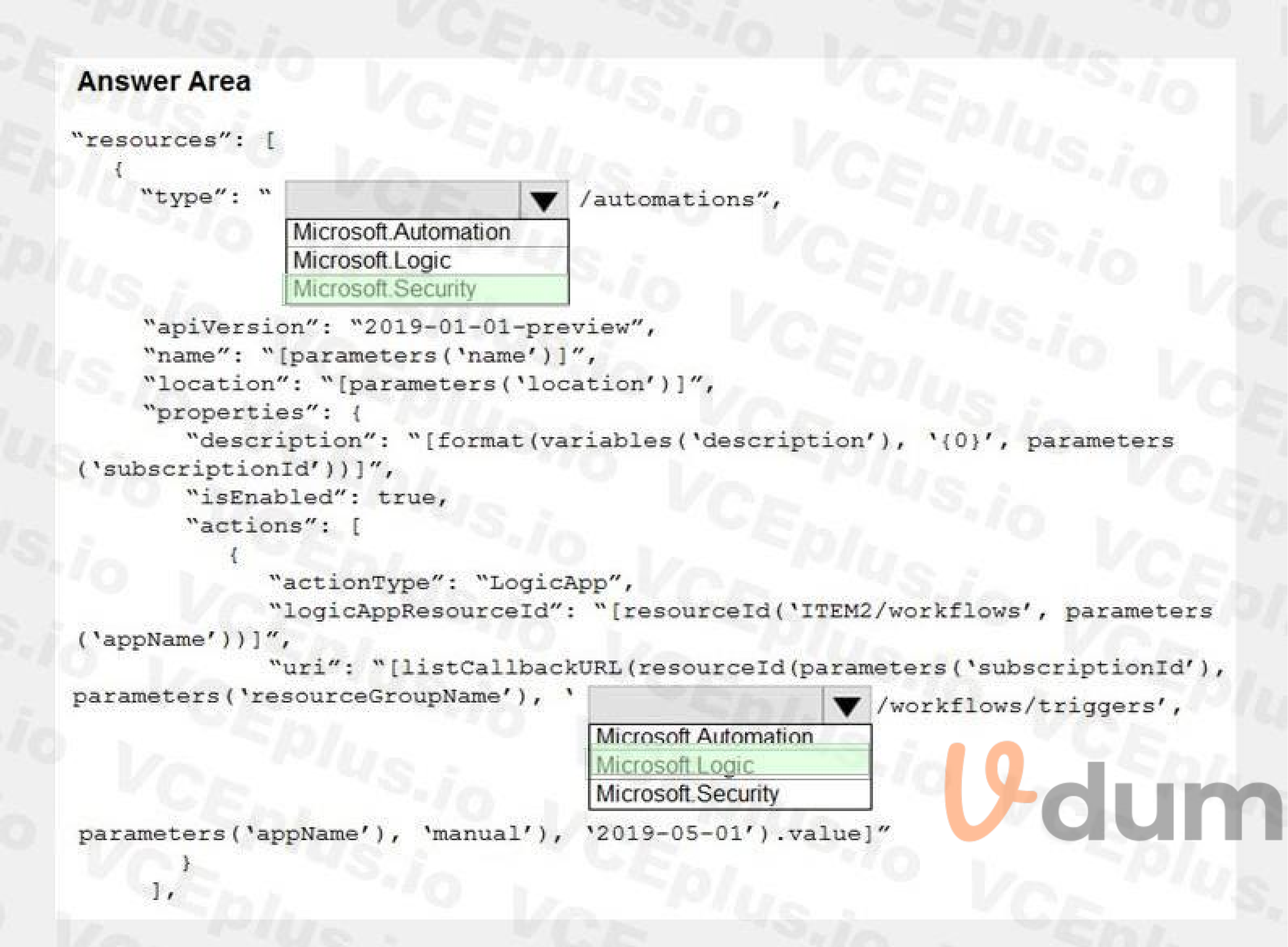
Hot Area:



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]”
           }
        ],
```

Answer Area:



Answer Area

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

Section:
Explanation:
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:
Explanation:

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

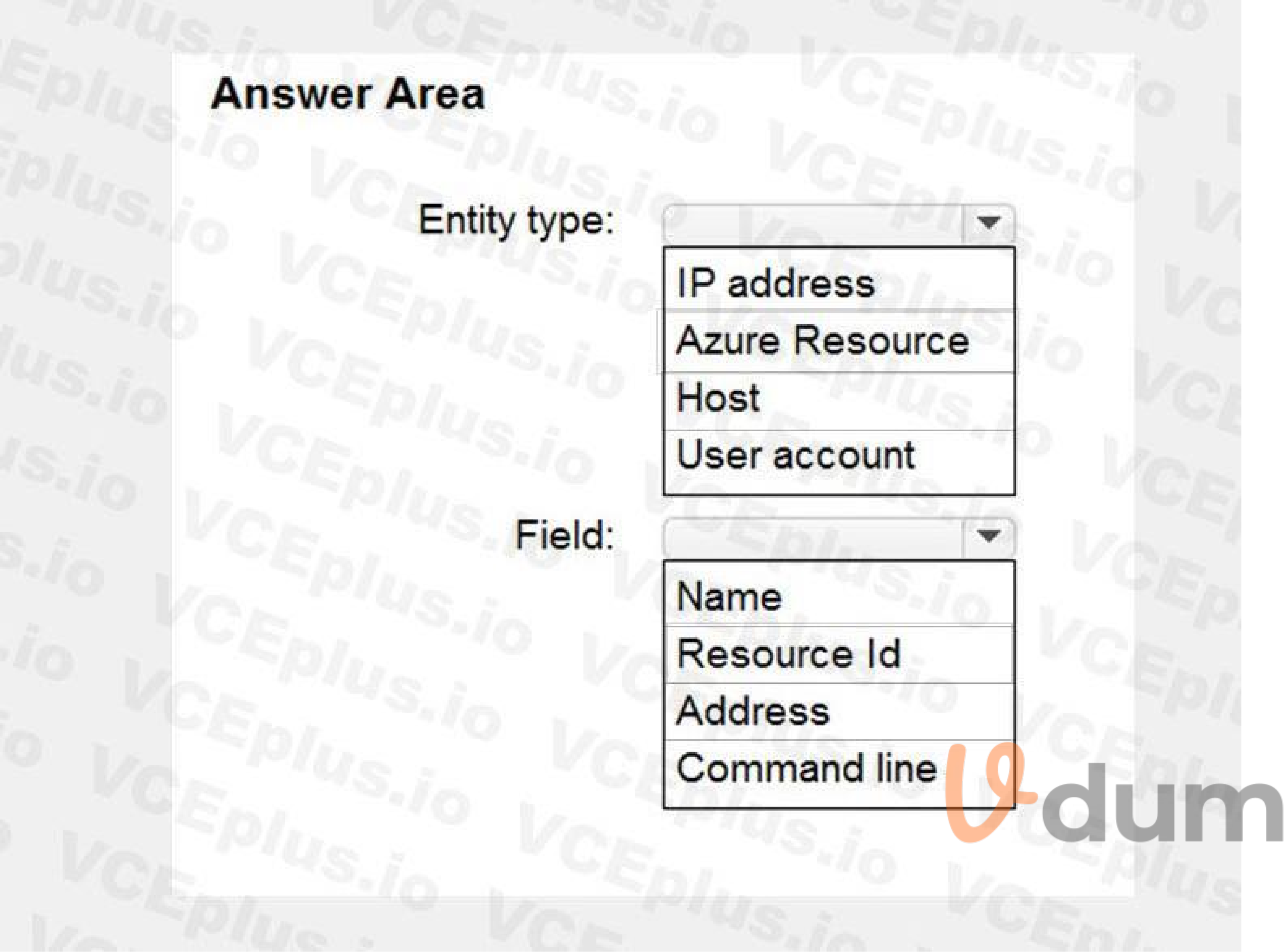
QUESTION 20
You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during 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:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

QUESTION 21
HOTSPOT
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.
You need to hide Azure Defender alerts for the storage account.
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

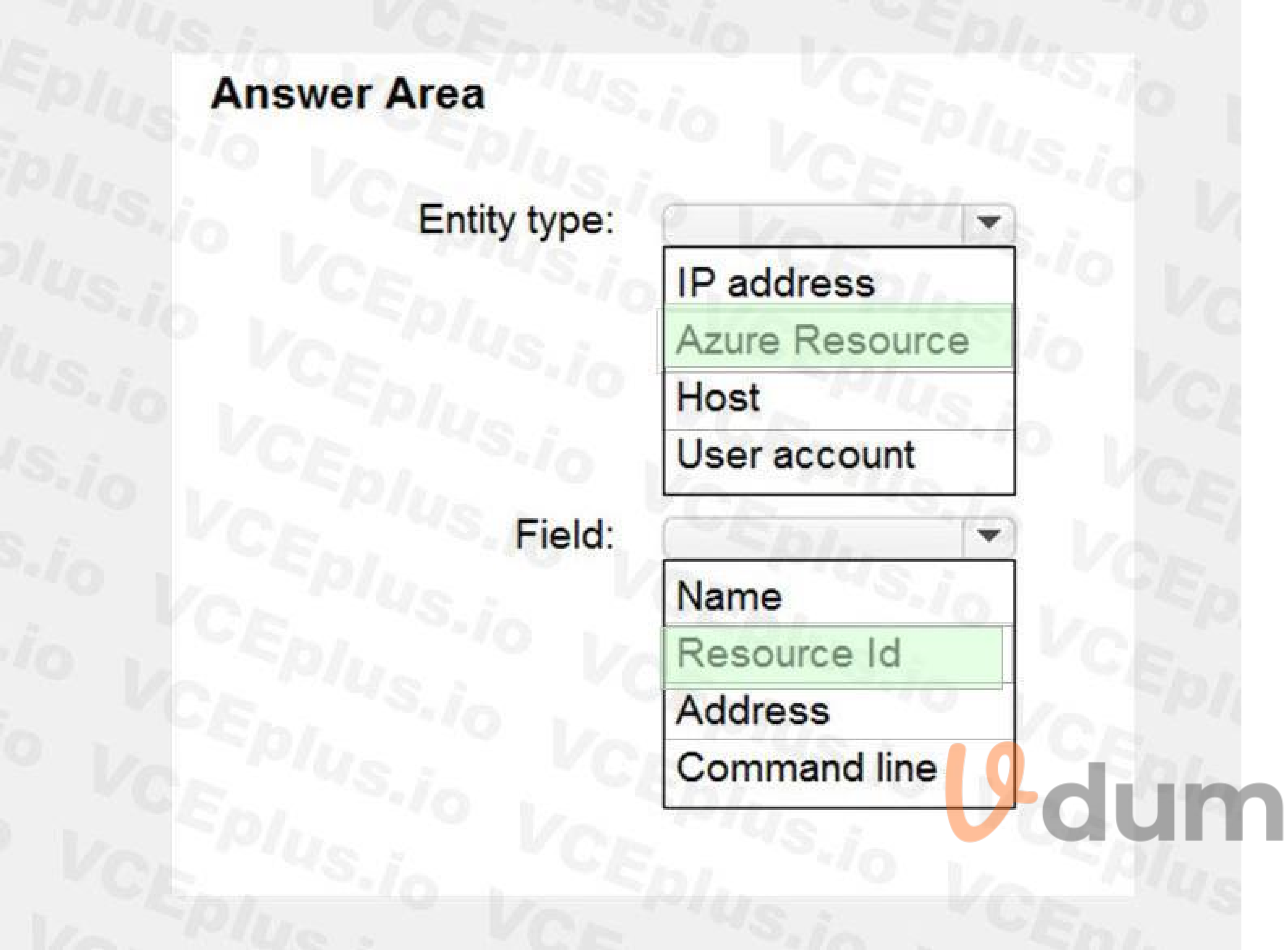
Entity type:

- IP address
- Azure Resource
- Host
- User account

Field:

- Name
- Resource Id
- Address
- Command line

Answer Area:



Answer Area

Entity type:

- IP address
- Azure Resource
- Host
- User account

Field:

- Name
- Resource Id
- Address
- Command line

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

QUESTION 22
You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers.
What should you do on the on-premises computers?

A. Install the Log Analytics agent.
B. Install the Dependency agent.
C. Configure the Hybrid Runbook Worker role.
D. Install the Connected Machine agent.

Correct Answer: A
Section:
Explanation:

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

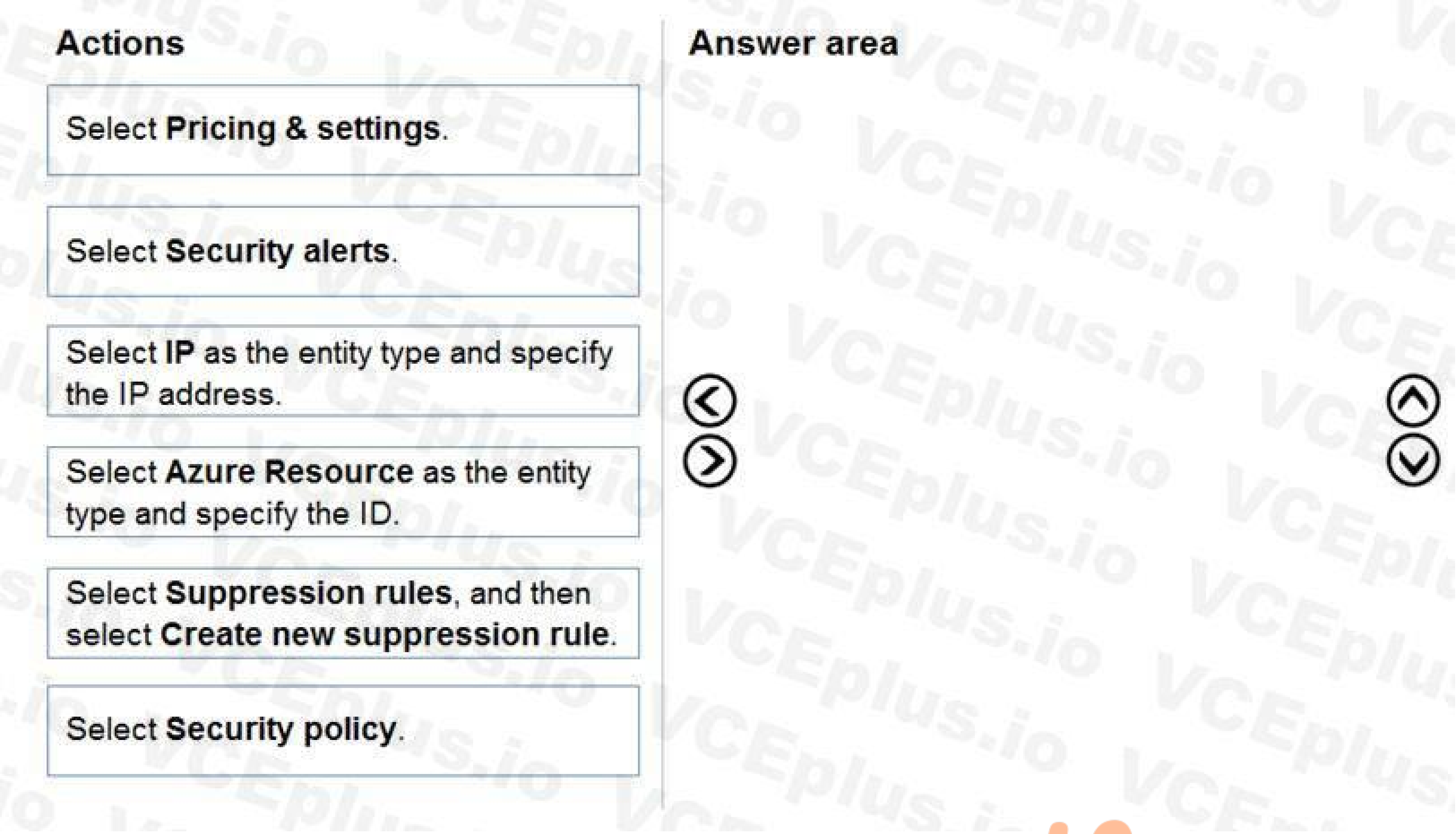
QUESTION 23
A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

A. the severity level of email notifications
B. a cloud connector
C. the Azure Defender plans
D. the integration settings for Threat detection

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

QUESTION 24
DRAG DROP
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.
You need to hide the alerts automatically in Security Center.
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

Select and Place:

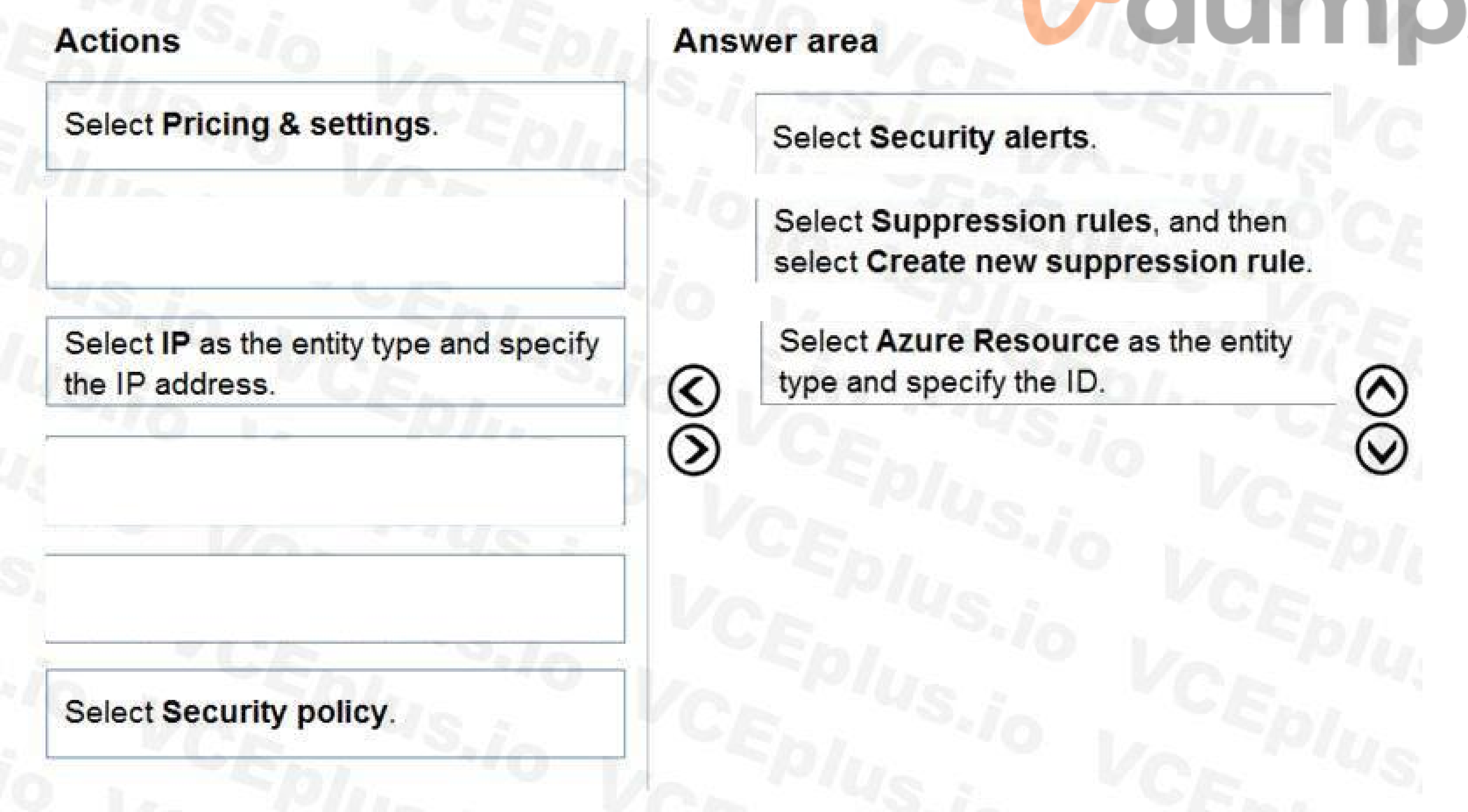


Actions

- Select **Pricing & settings**.
- Select **Security alerts**.
- Select **IP** as the entity type and specify the IP address.
- Select **Azure Resource** as the entity type and specify the ID.
- Select **Suppression rules**, and then select **Create new suppression rule**.
- Select **Security policy**.

Answer area

Correct Answer:



Actions

- Select **Pricing & settings**.
- Select **IP** as the entity type and specify the IP address.
- Select **Security policy**.

Answer area

1. Select **Security alerts**.
2. Select **Suppression rules**, and then select **Create new suppression rule**.
3. Select **Azure Resource** as the entity type and specify the ID.

Section:

Explanation:

Reference:

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

QUESTION 25

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

Enable and disable Azure Defender.

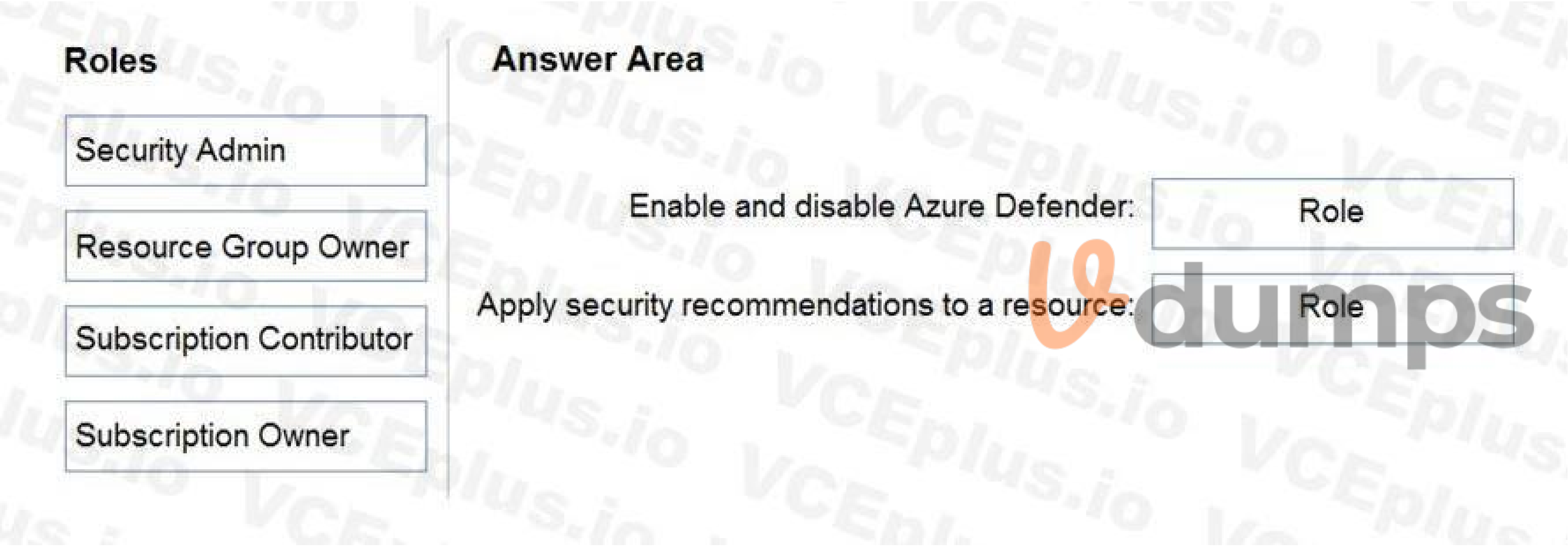
Apply security recommendations to resource.

The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Select and Place:



Roles

Security Admin

Resource Group Owner

Subscription Contributor

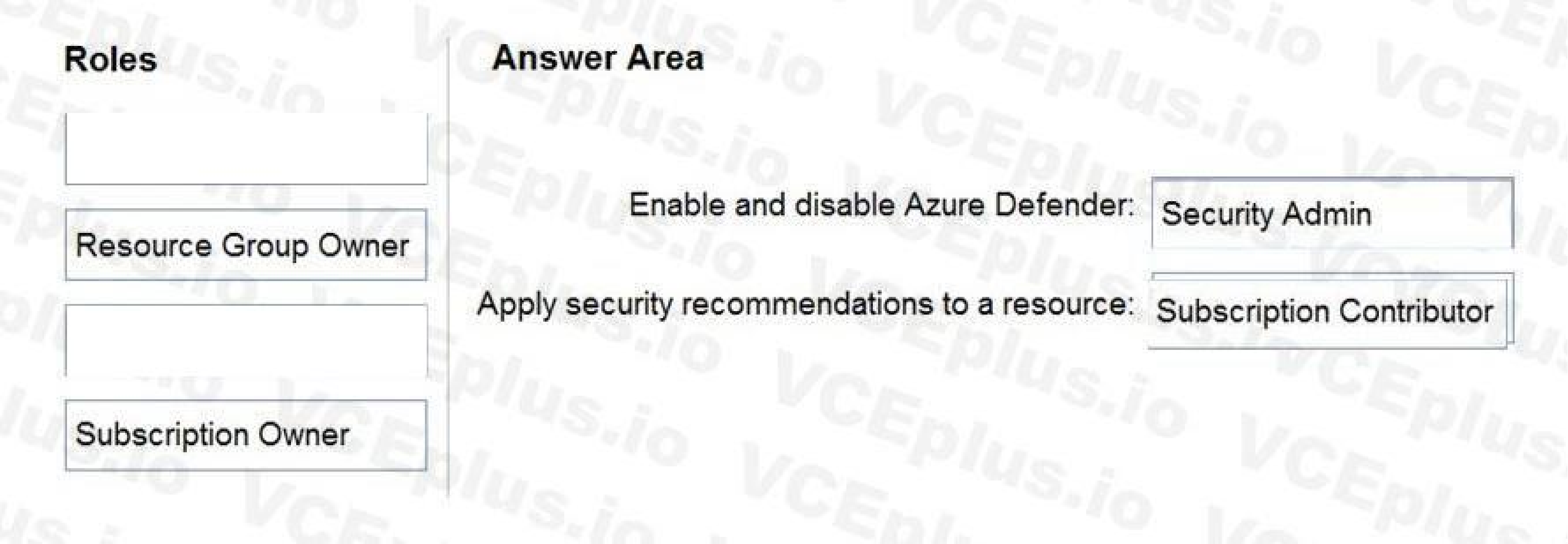
Subscription Owner

Answer Area

Enable and disable Azure Defender: Role

Apply security recommendations to a resource: Role

Correct Answer:



Roles

Resource Group Owner

Subscription Owner

Answer Area

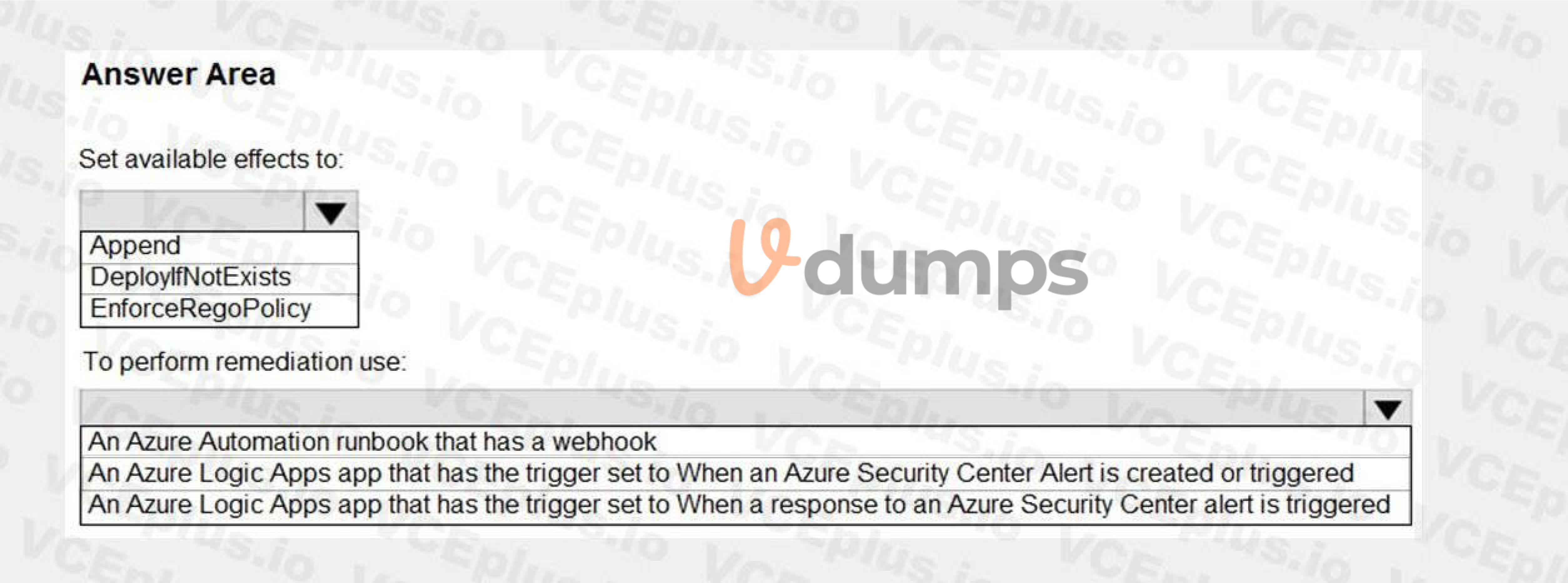
Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Subscription Contributor

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

QUESTION 26
HOTSPOT
You have an Azure subscription that uses Azure Defender.
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.
You need to create an Azure policy that will perform threat remediation automatically.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

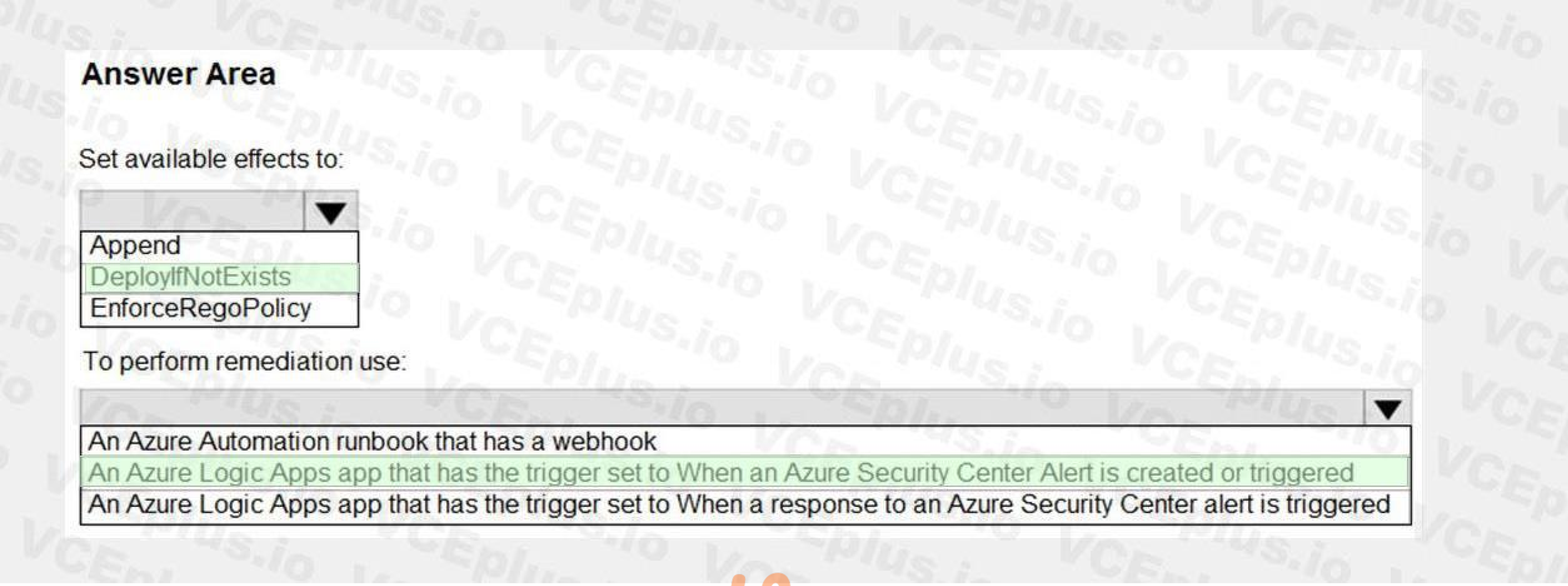
Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Answer Area:



Answer Area

Set available effects to:

- Append
- DeployIfNotExists
- EnforceRegoPolicy

To perform remediation use:

- An Azure Automation runbook that has a webhook
- An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
- An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

Section:

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

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

Case Study 01 - Mitigate threats using Azure Sentinel

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
```

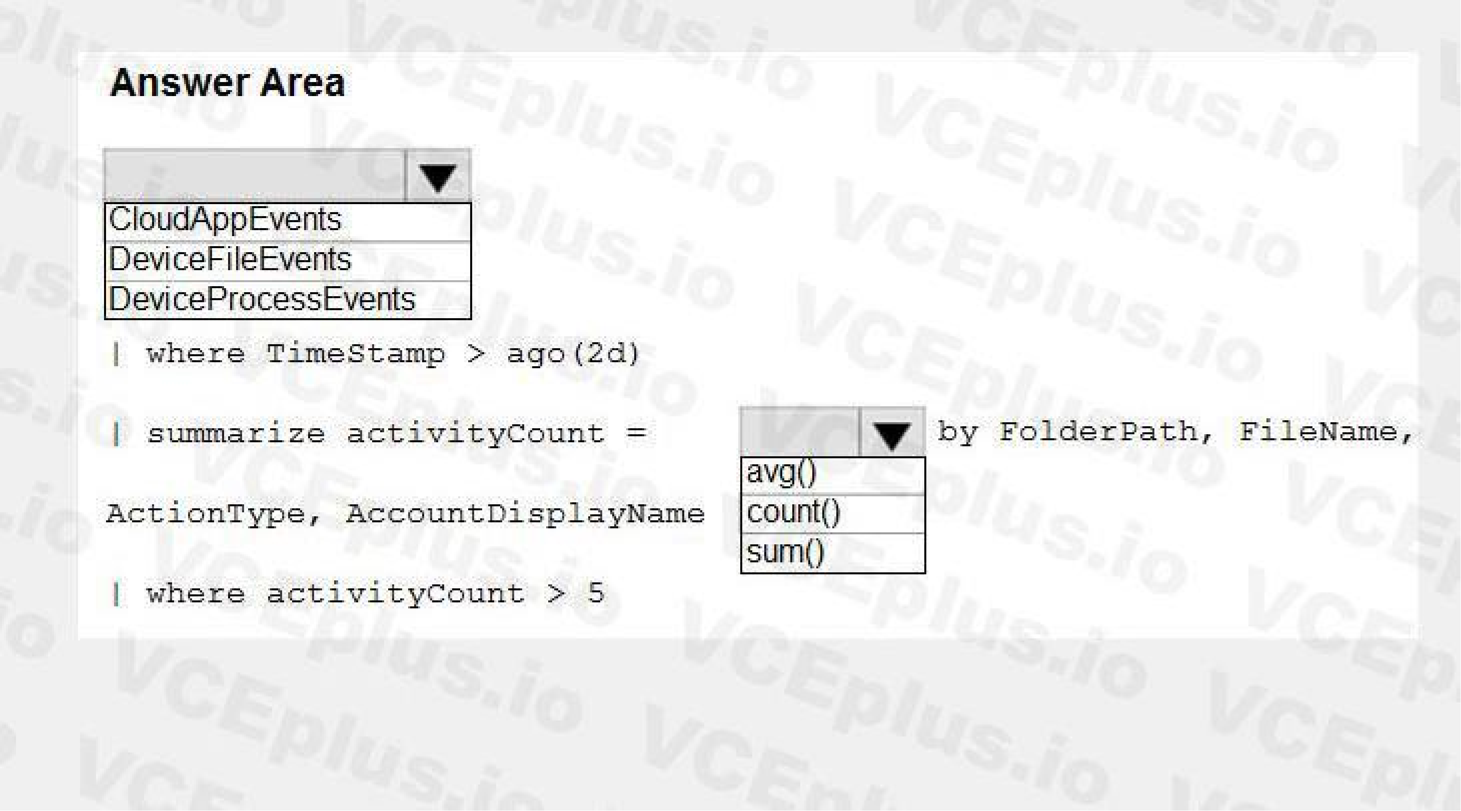
QUESTION 1
You need to remediate active attacks to meet the technical requirements.
What should you include in the solution?

A. Azure Automation runbooks
B. Azure Logic Apps
C. Azure Functions
D. Azure Sentinel livestreams

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

QUESTION 2
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

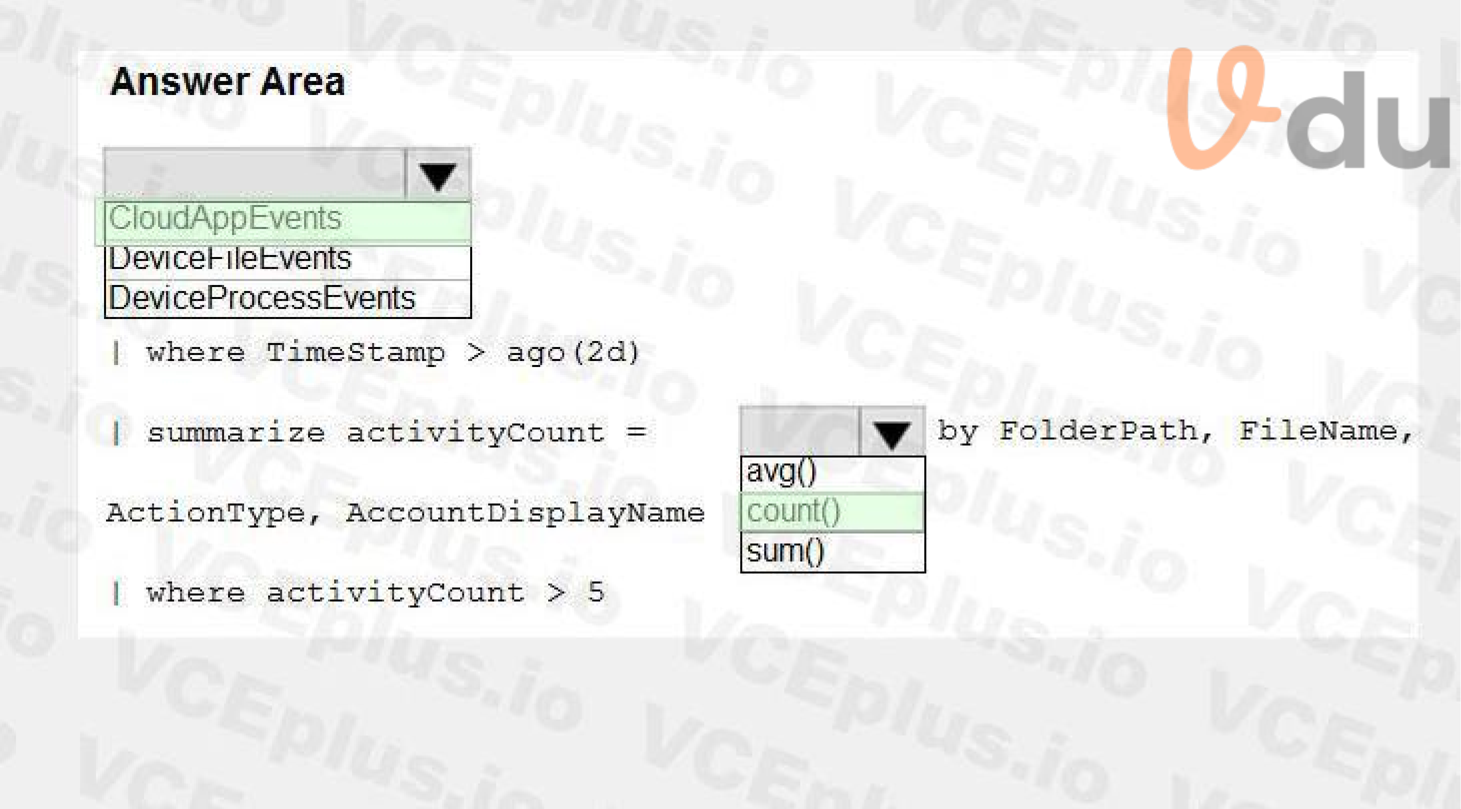
CloudAppEvents
DeviceFileEvents
DeviceProcessEvents

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

avg()
count()
sum()

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

Answer Area:



Answer Area

[✓ CloudAppEvents]
DeviceFileEvents
DeviceProcessEvents

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

avg()
[✓ count()]
sum()

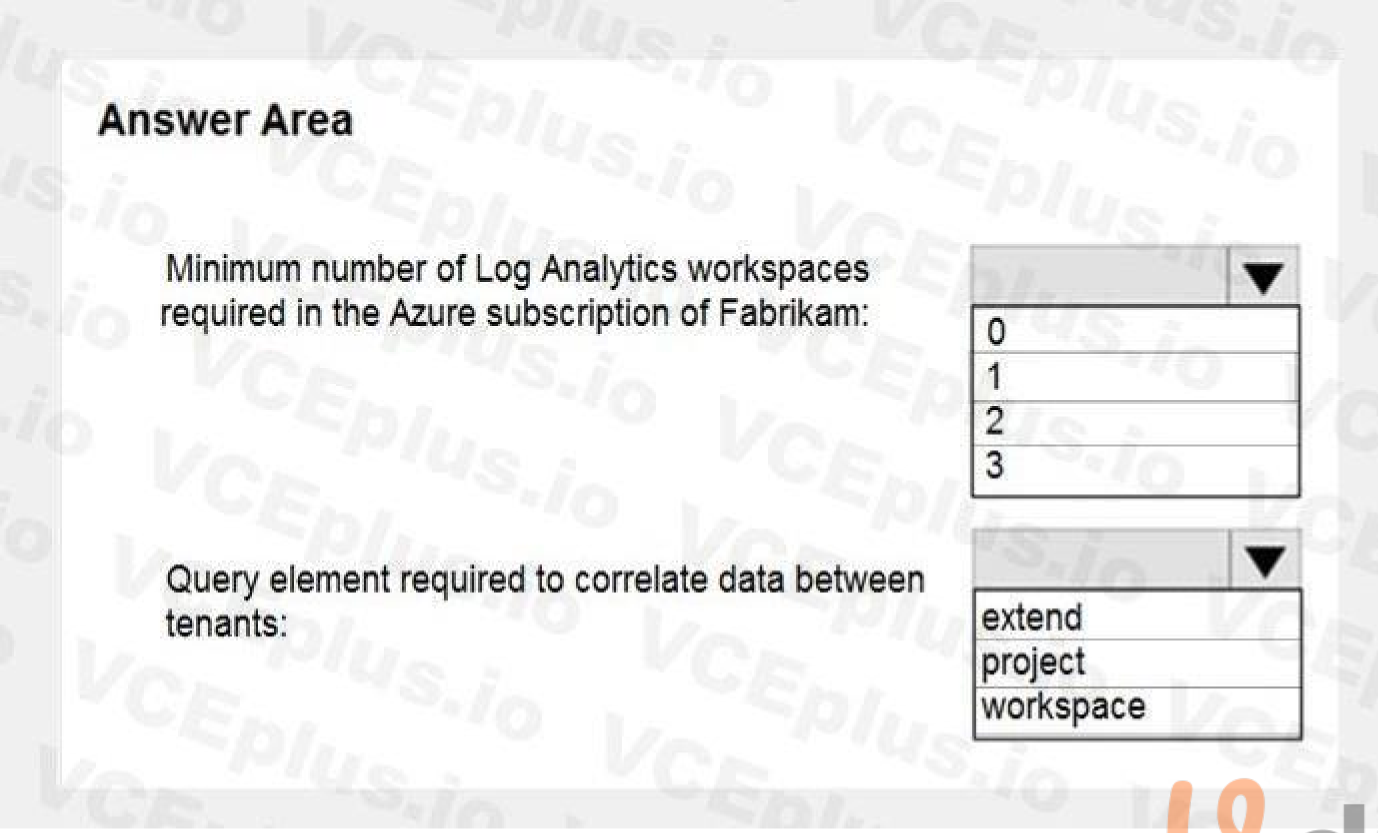
```
by FolderPath, FileName,
ActionType, AccountDisplayName
| where activityCount > 5
```

Section:
Explanation:

QUESTION 3
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

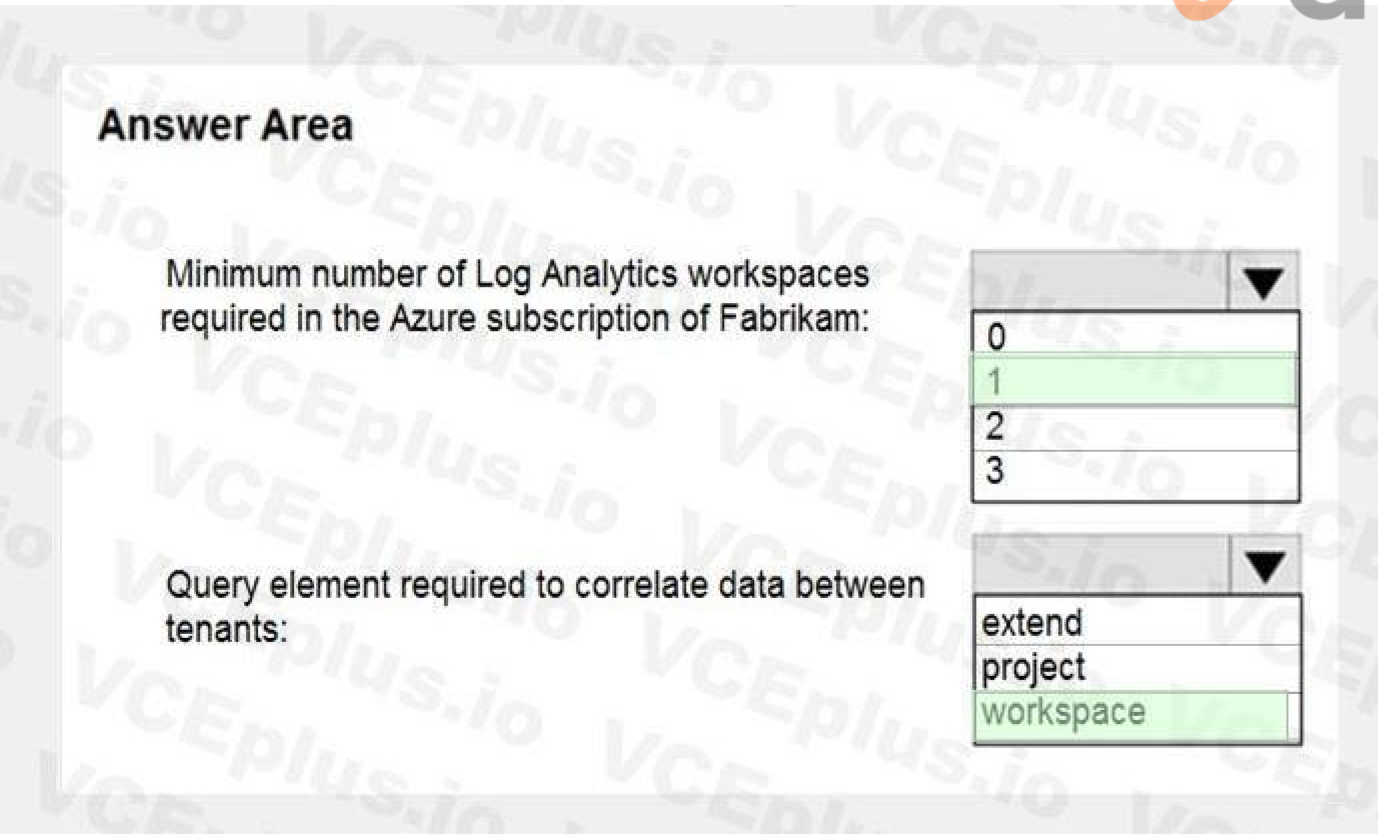
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Answer 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]

Section:

Explanation:

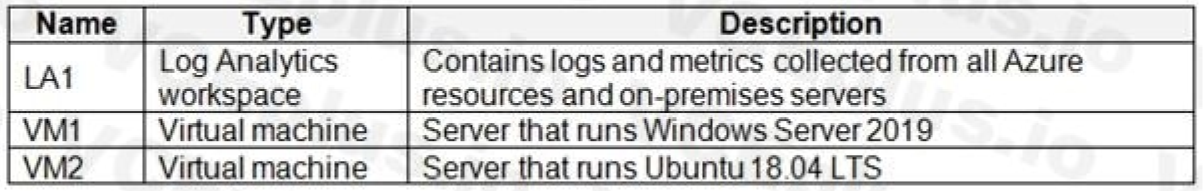
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

QUESTION 4
You need to complete the query for failed sign-ins to meet the technical requirements.
Where can you find the column name to complete the where clause?

A. Security alerts in Azure Security Center
B. Activity log in Azure
C. Azure Advisor
D. the query windows of the Log Analytics workspace

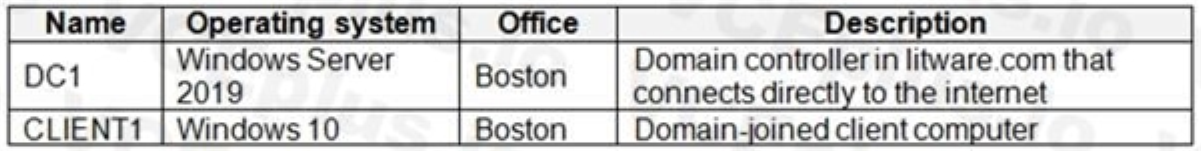
Correct Answer: D
Section:
Explanation:

Case Study 02 - Mitigate threats using Azure Sentinel
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 â€" Data discovery dashboard.

Microsoft Defender for Endpoint requirements

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Cloud App Security requirements

Cloud App Security must identify whether a user connection is anomalous based on tenant-level data.

Azure Defender Requirements

All servers must send logs to the same Log Analytics workspace.

Azure Sentinel Requirements

Litware must meet the following Azure Sentinel requirements:

Integrate Azure Sentinel and Cloud App Security.

Ensure that a user named admin1 can configure Azure Sentinel playbooks.

Create an Azure Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.

Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.

Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

QUESTION 1

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:

Explanation:

Reference:

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

QUESTION 2

You need to create the test rule to meet the Azure Sentinel requirements.

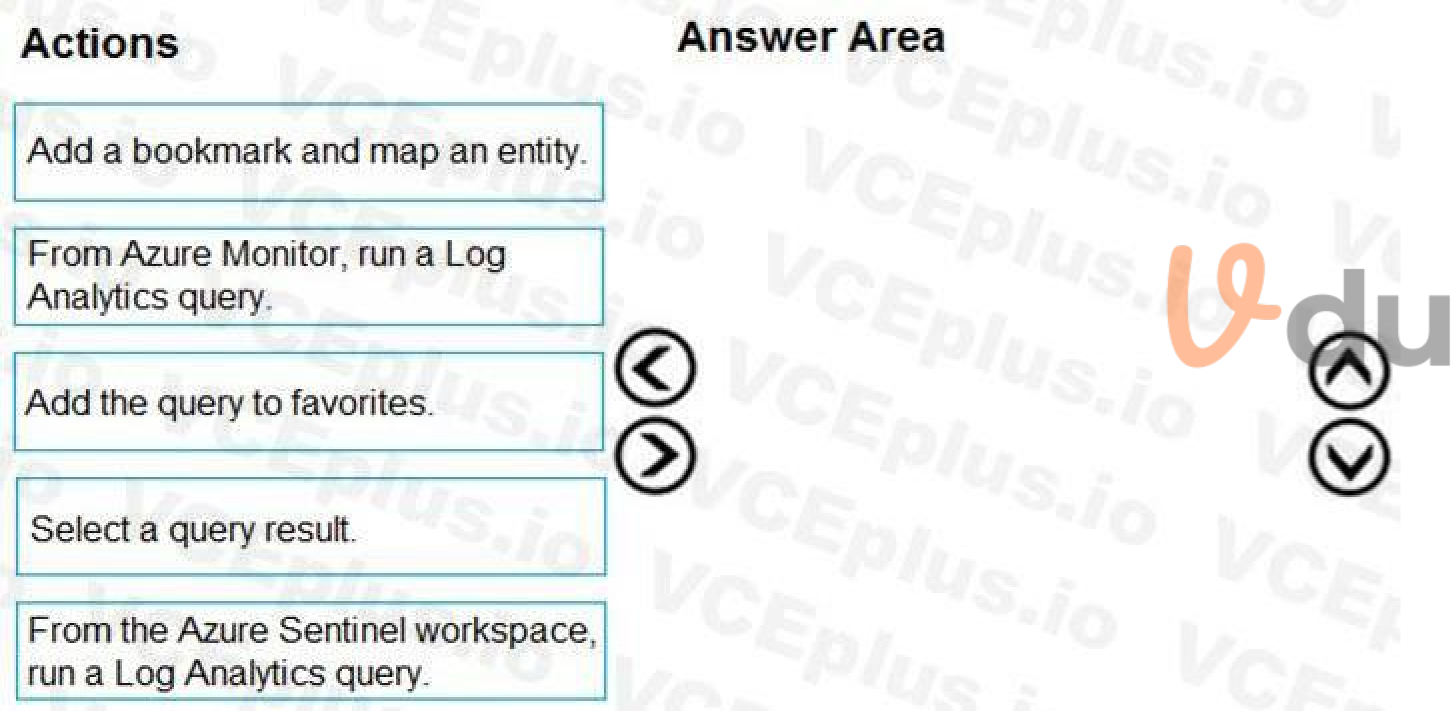
What should you do when you create the rule?

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

QUESTION 3
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.

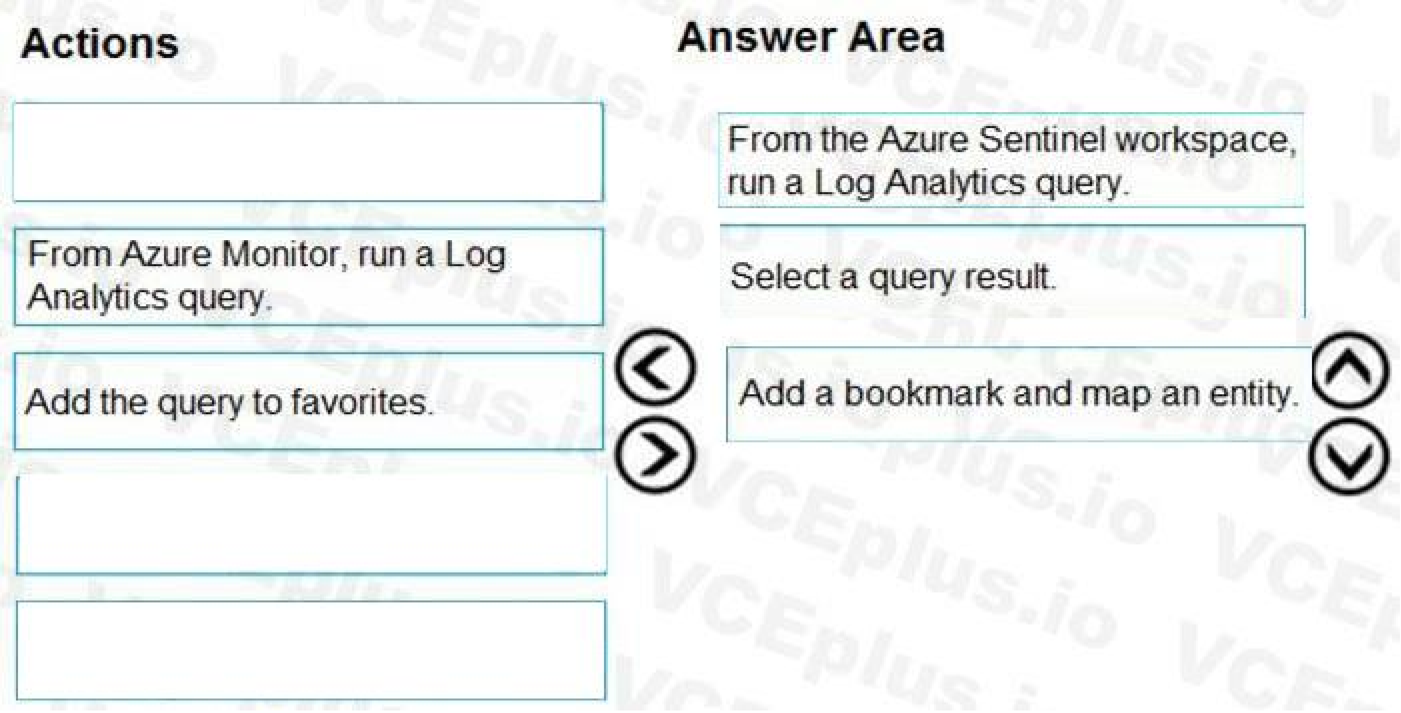
Add the query to favorites.

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:

Explanation:

Reference:

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

QUESTION 4

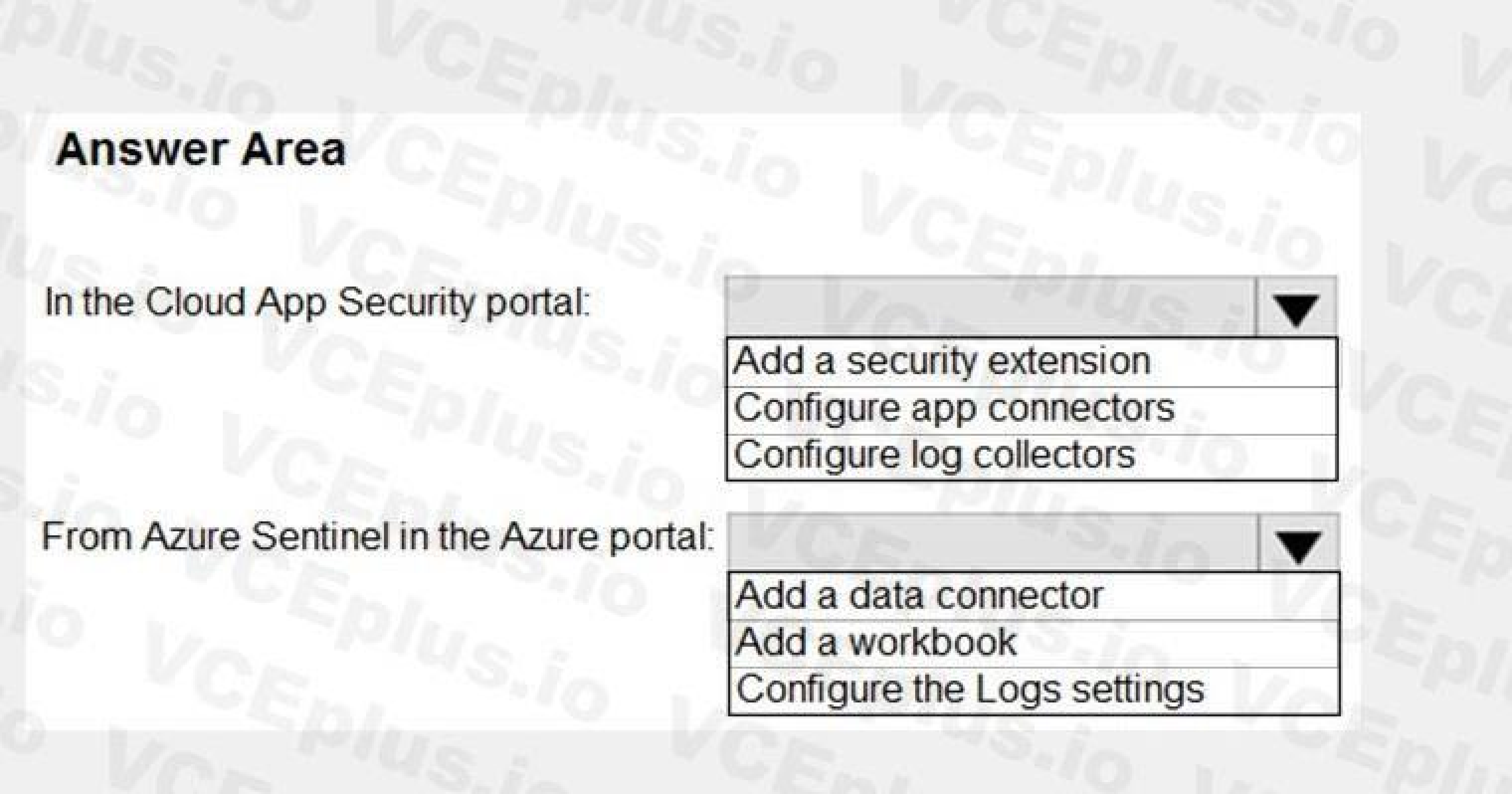
HOTSPOT

You need to configure the Azure Sentinel integration to meet the Azure Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:

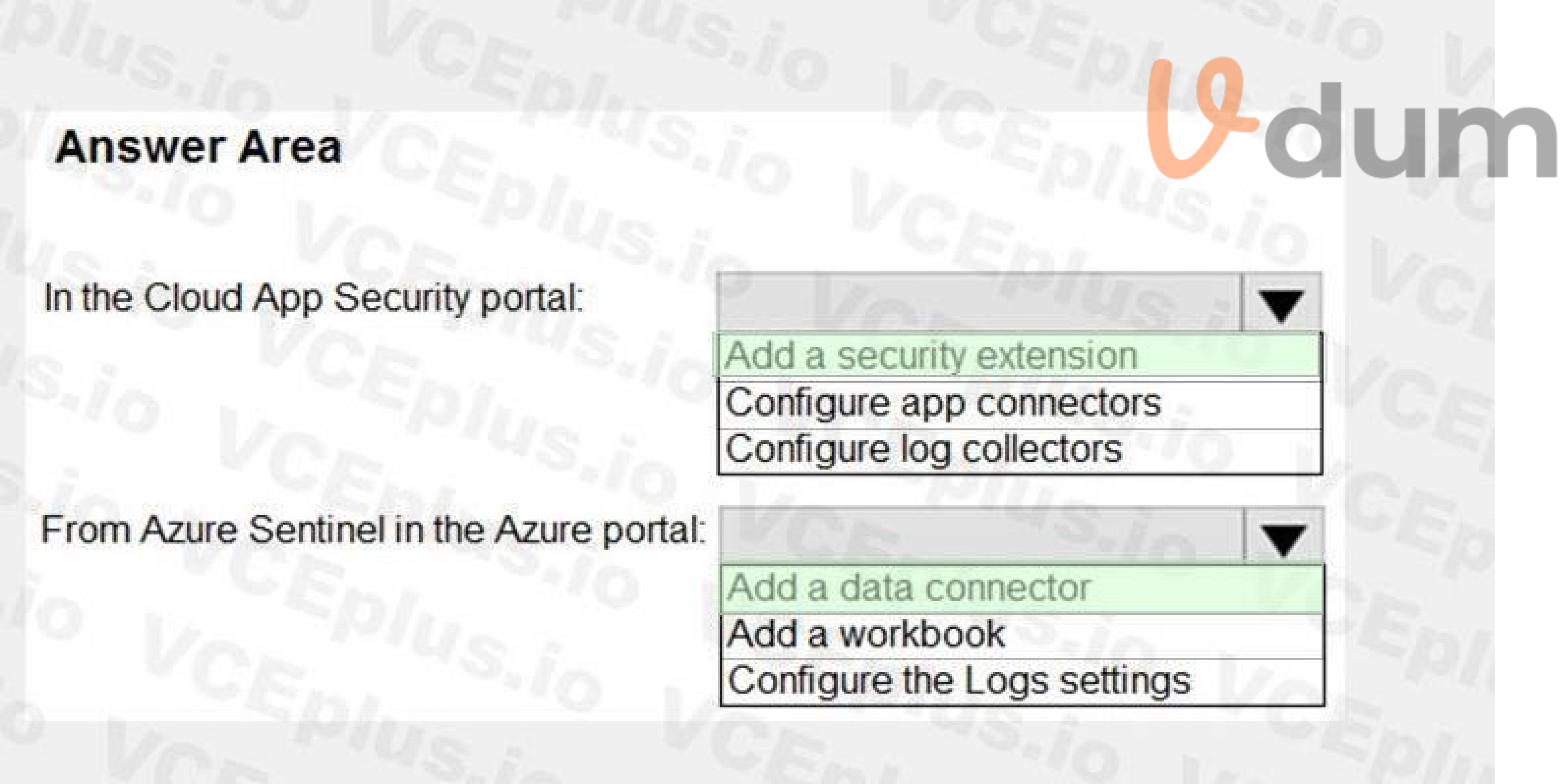


Answer Area

In the Cloud App Security portal:
- Add a security extension
- Configure app connectors
- Configure log collectors

From Azure Sentinel in the Azure portal:
- Add a data connector
- Add a workbook
- Configure the Logs settings

Answer Area:



Answer Area

In the Cloud App Security portal:
- [✓ Add a security extension]
- Configure app connectors
- Configure log collectors

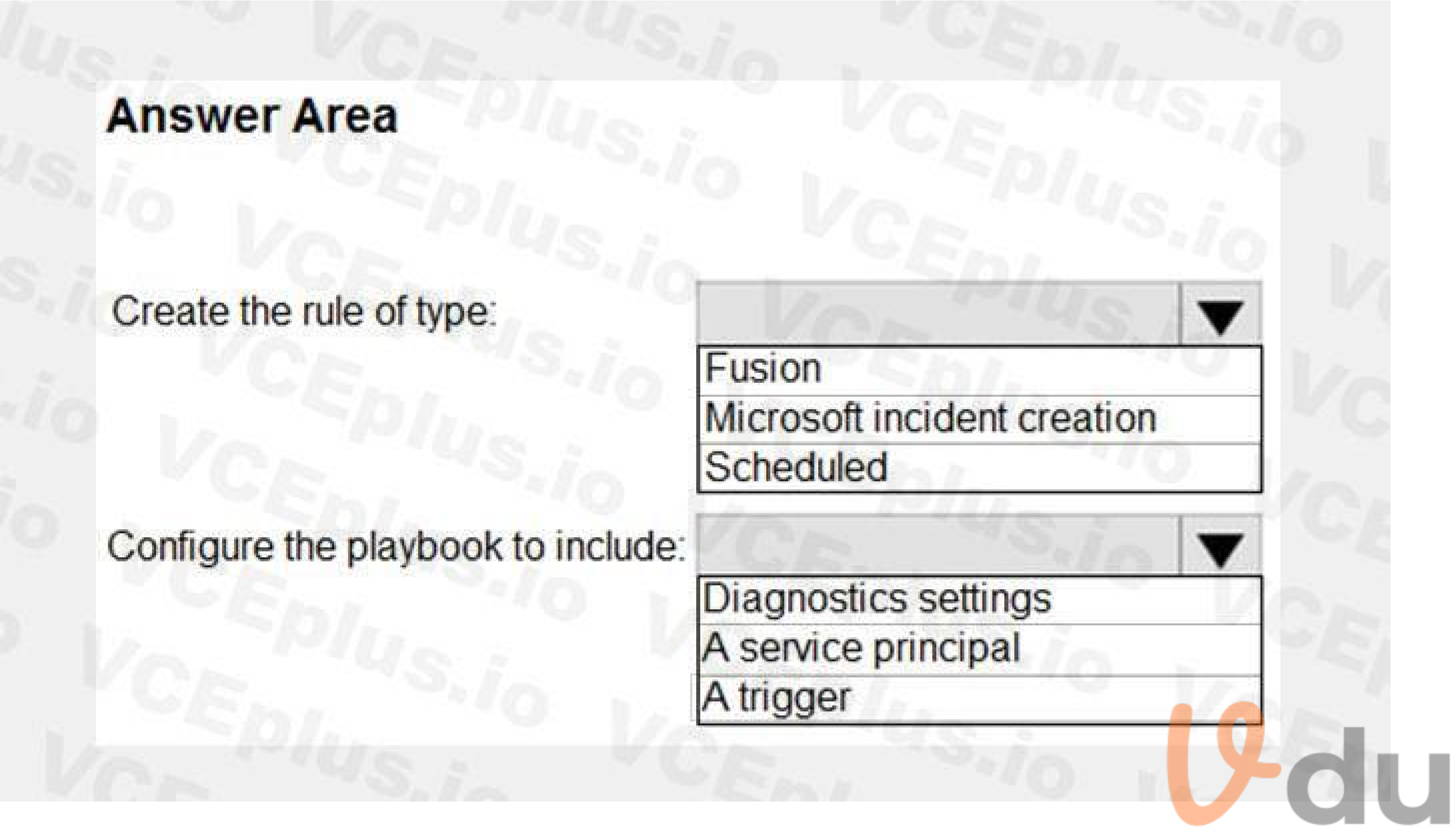
From Azure Sentinel in the Azure portal:
- [✓ Add a data connector]
- Add a workbook
- Configure the Logs settings

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

QUESTION 5
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:

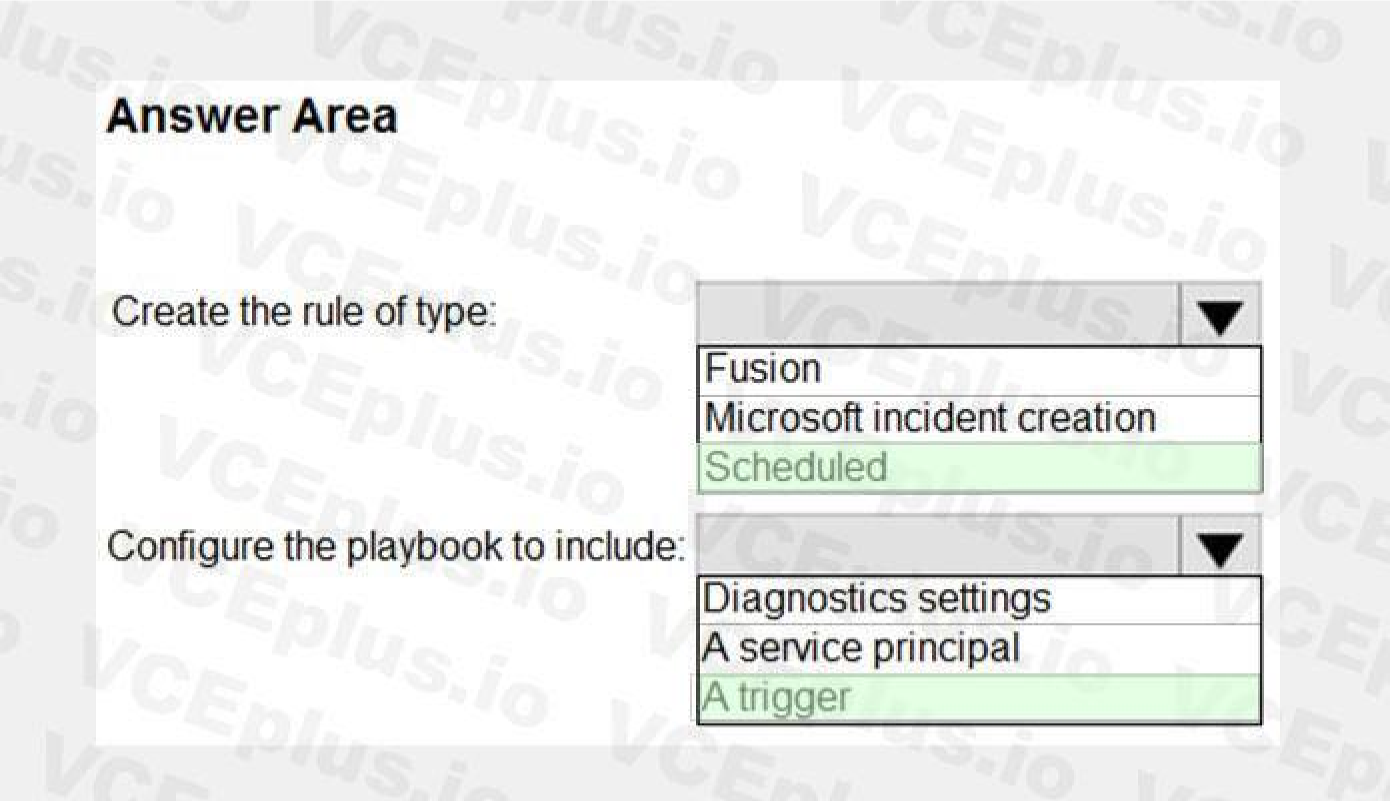


Answer Area

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

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

Answer 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]

Section:
Explanation:

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

QUESTION 6

You need to restrict cloud apps running on CLIENT1 to meet the Microsoft Defender for Endpoint requirements.
Which two configurations should you modify? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. the Onboarding settings from Device management in Microsoft Defender Security Center
B. Cloud App Security anomaly detection policies
C. Advanced features from Settings in Microsoft Defender Security Center
D. the Cloud Discovery settings in Cloud App Security

Correct Answer: C, D
Section:
Explanation:

All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

QUESTION 7

You need to restrict cloud apps running on CUENT1 to meet the Microsoft Defender for Endpoint requirements. Which two configurations should you modify? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

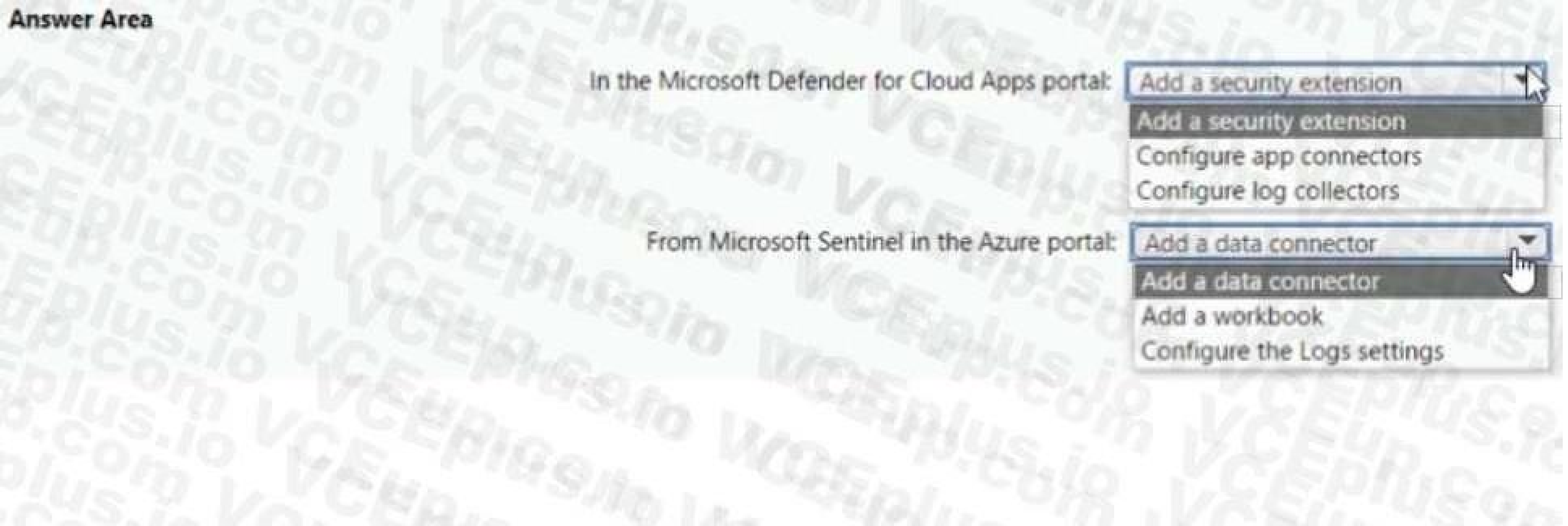
A. the Cloud Discovery settings in Microsoft Defender for Cloud Apps
B. the Onboarding settings from Device management in Settings in Microsoft 365 Defender portal
C. Microsoft Defender for Cloud Apps anomaly detection policies
D. Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal

Correct Answer: A, D
Section:

QUESTION 8

HOTSPOT
You need to configure the Microsoft Sentinel integration to meet the Microsoft 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

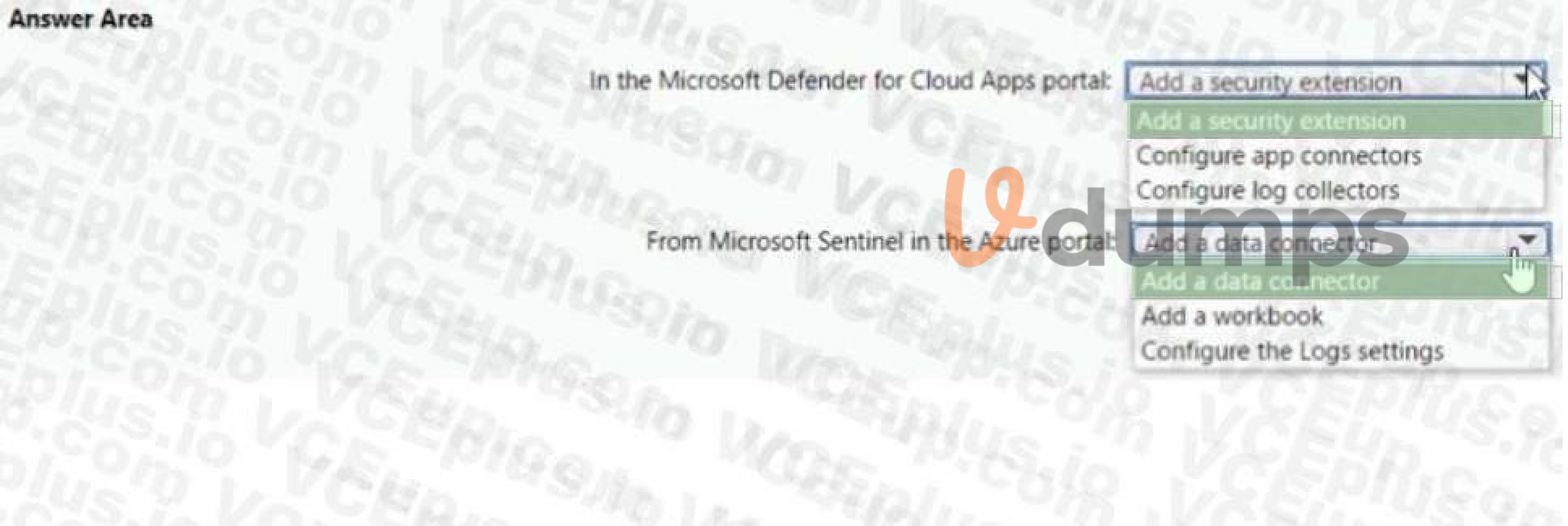
In the Microsoft Defender for Cloud Apps portal: Add a security extension

- Add a security extension
- Configure app connectors
- Configure log collectors

From Microsoft Sentinel in the Azure portal: Add a data connector

- Add a data connector
- Add a workbook
- Configure the Logs settings

Answer Area:



Answer Area

In the Microsoft Defender for Cloud Apps portal: Add a security extension

- Add a security extension
- Configure app connectors
- Configure log collectors

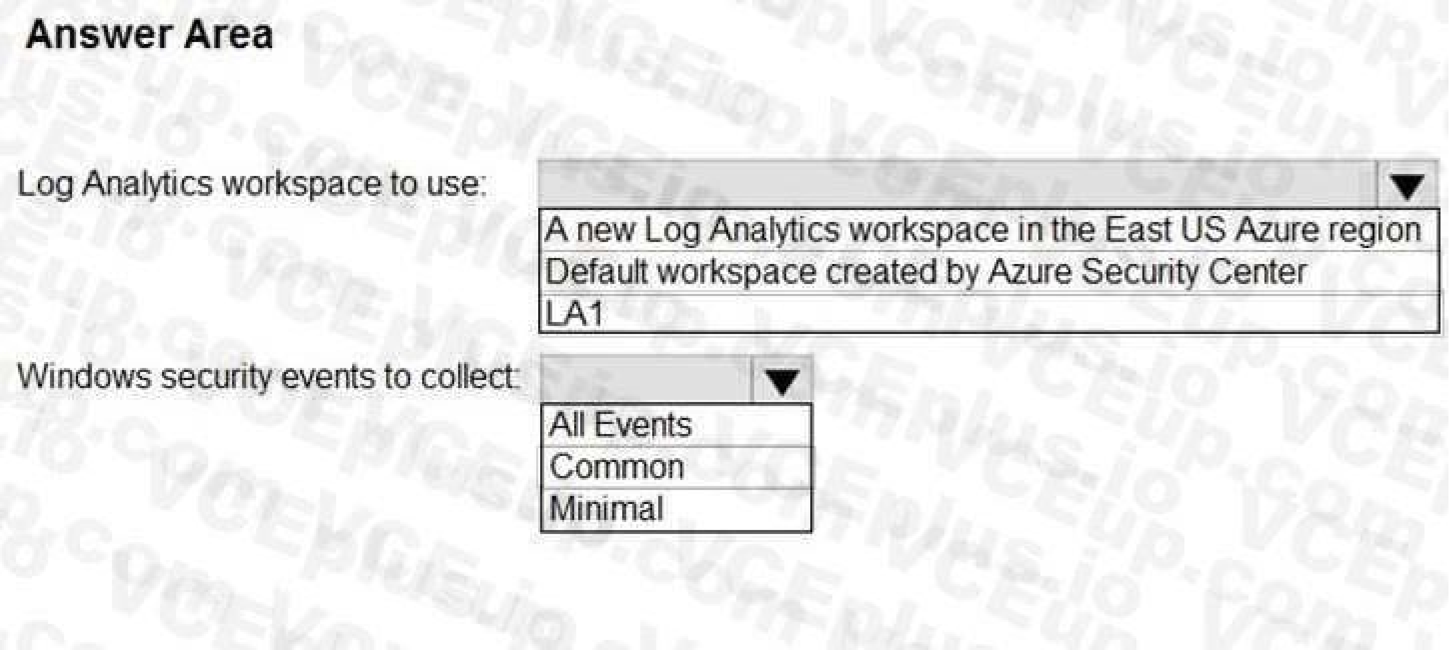
From Microsoft Sentinel in the Azure portal: Add a data connector

- Add a data connector
- Add a workbook
- Configure the Logs settings

Section:
Explanation:

QUESTION 9
HOTSPOT
You need to implement Microsoft Defender for Cloud to meet the Microsoft Defender for Cloud requirements and the business requirements. What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

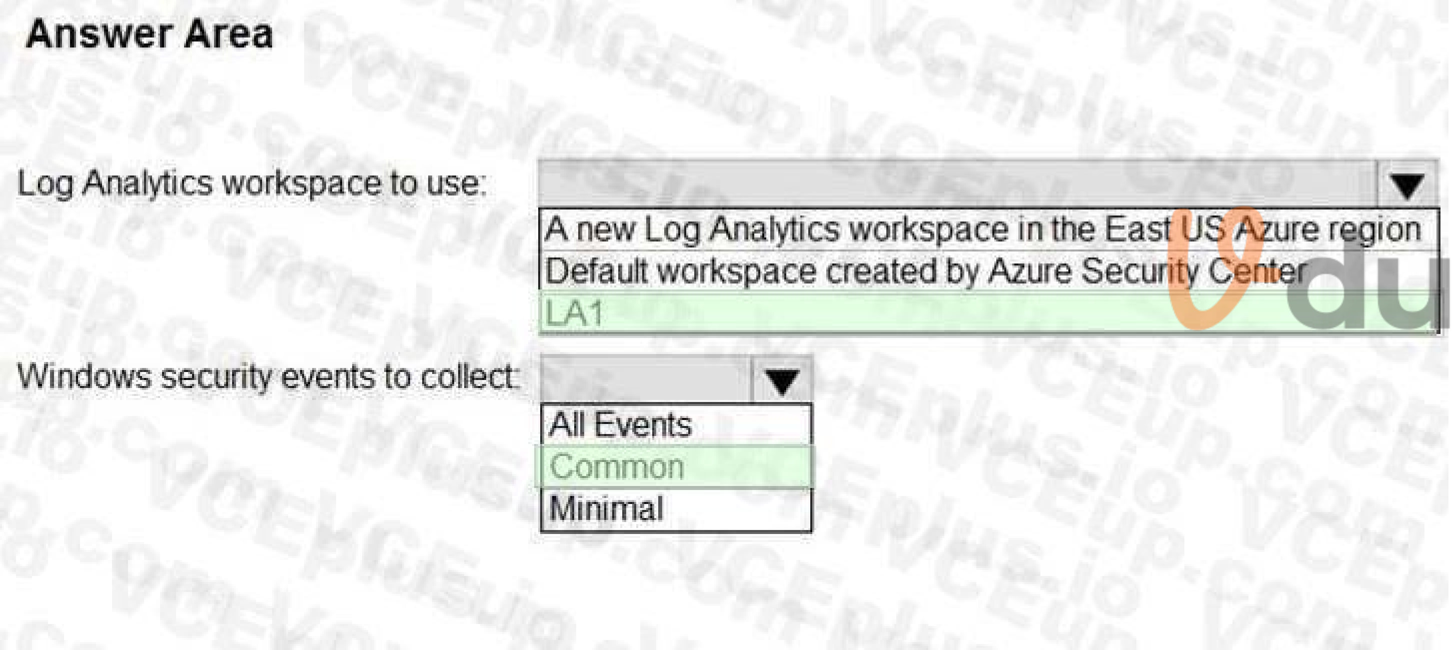
Log Analytics workspace to use:

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

Windows security events to collect:

- All Events
- Common
- Minimal

Answer Area:



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:
Explanation:

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:
Explanation:
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: A, B
Section:
Explanation:
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:
Explanation:
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: B
Section:
Explanation:

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: B, C
Section:
Explanation:
B: To add a data connector, you would use the Azure Sentinel data connectors feature to connect to your Azure subscription and to configure log data collection for Azure Storage account key enumeration events.C: After adding the data connector, you need to create an analytics rule to analyze the log data from the Azure storage connector, looking for the specific event of Azure storage account keys enumeration. This rule will trigger an alert when it detects the specific event, allowing you to take immediate action.

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:

QUESTION 7
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning. What should you include in the recommendation?

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

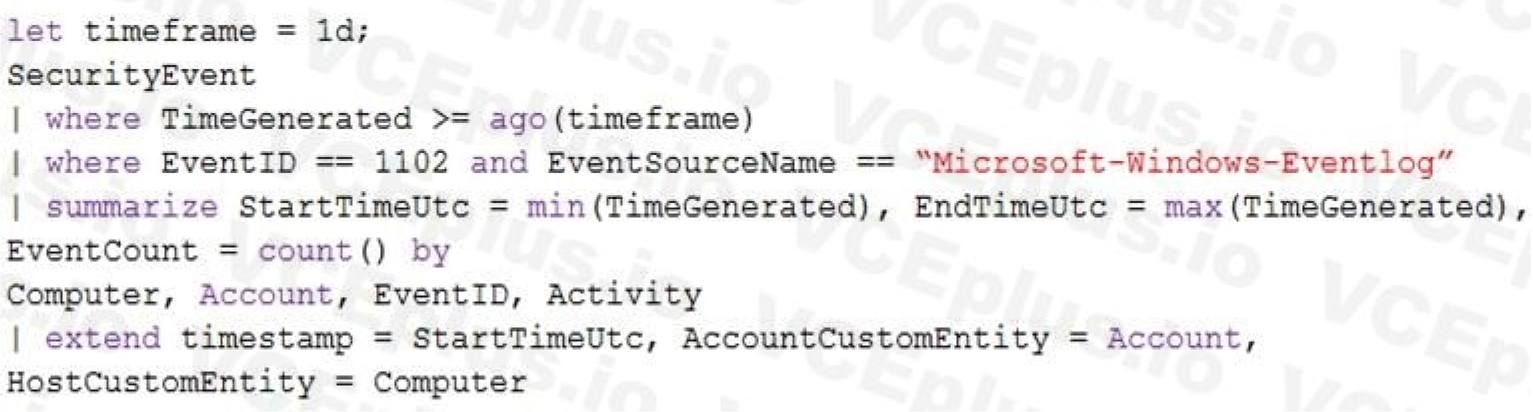
Correct Answer: C
Section:
Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

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 an alert and modify the action.

Correct Answer: D
Section:
Explanation:
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: C, D

Section:

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: B, E
Section:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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:
Explanation:
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 Microsoft Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.

Correct Answer: C
Section:
Explanation:
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: A, D
Section:
Explanation:
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:
Explanation:
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:
Explanation:
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?

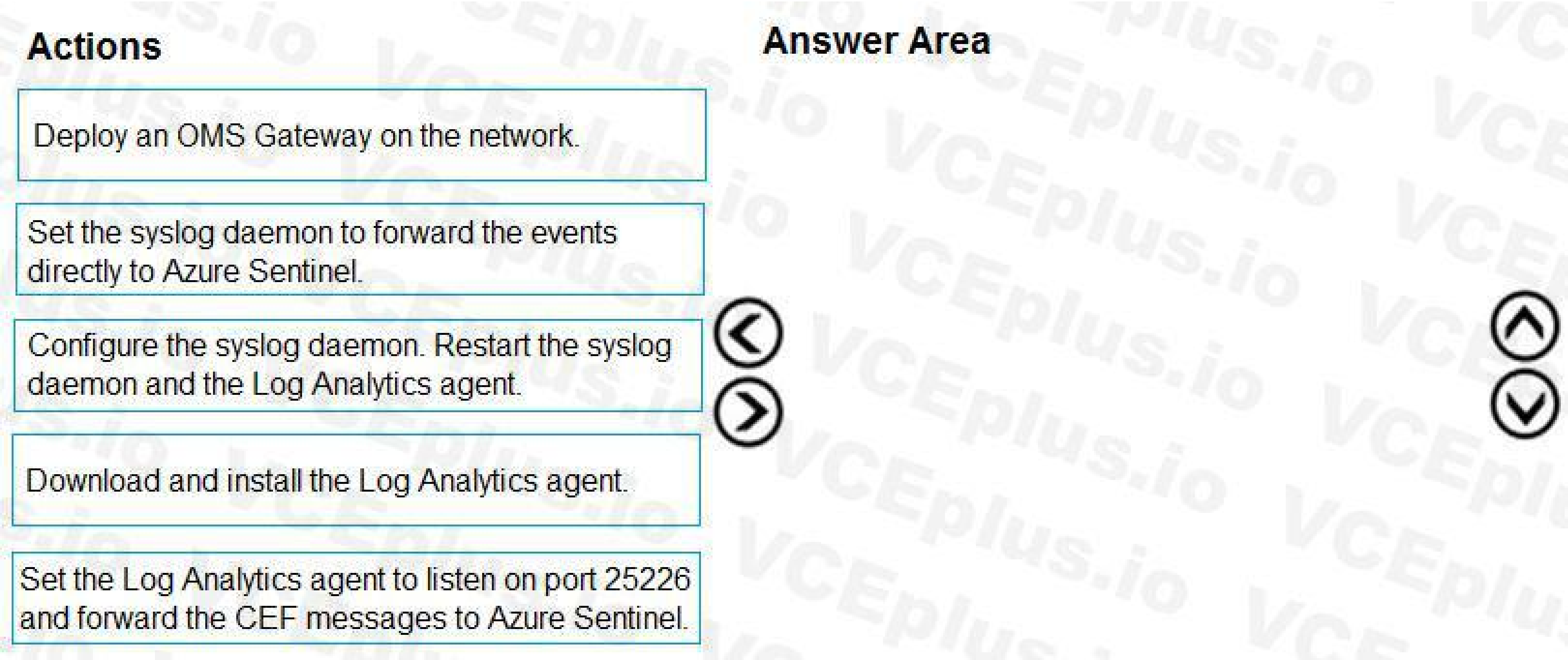
A. Yes
B. No

Correct Answer: A
Section:
Explanation:
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:

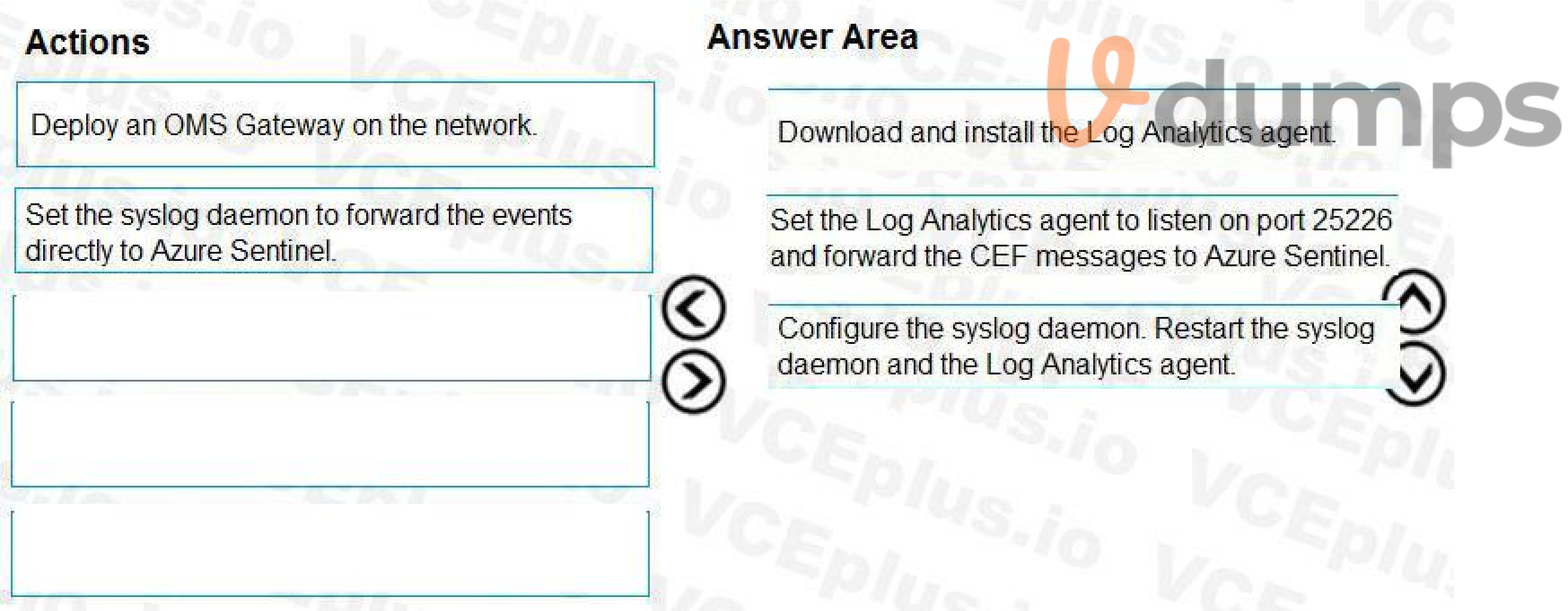


Actions

- 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

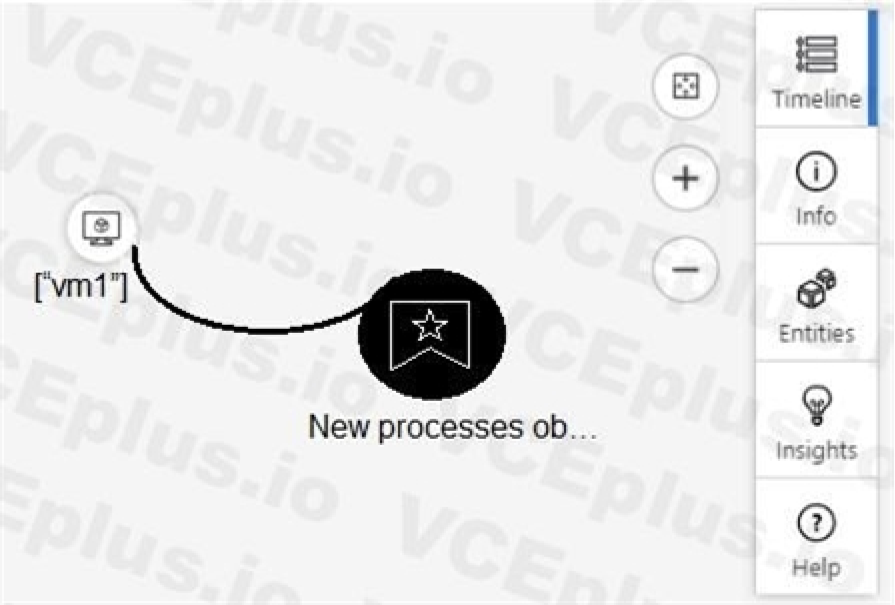
- Deploy an OMS Gateway on the network.
- Set the syslog daemon to forward the events directly to Azure Sentinel.

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

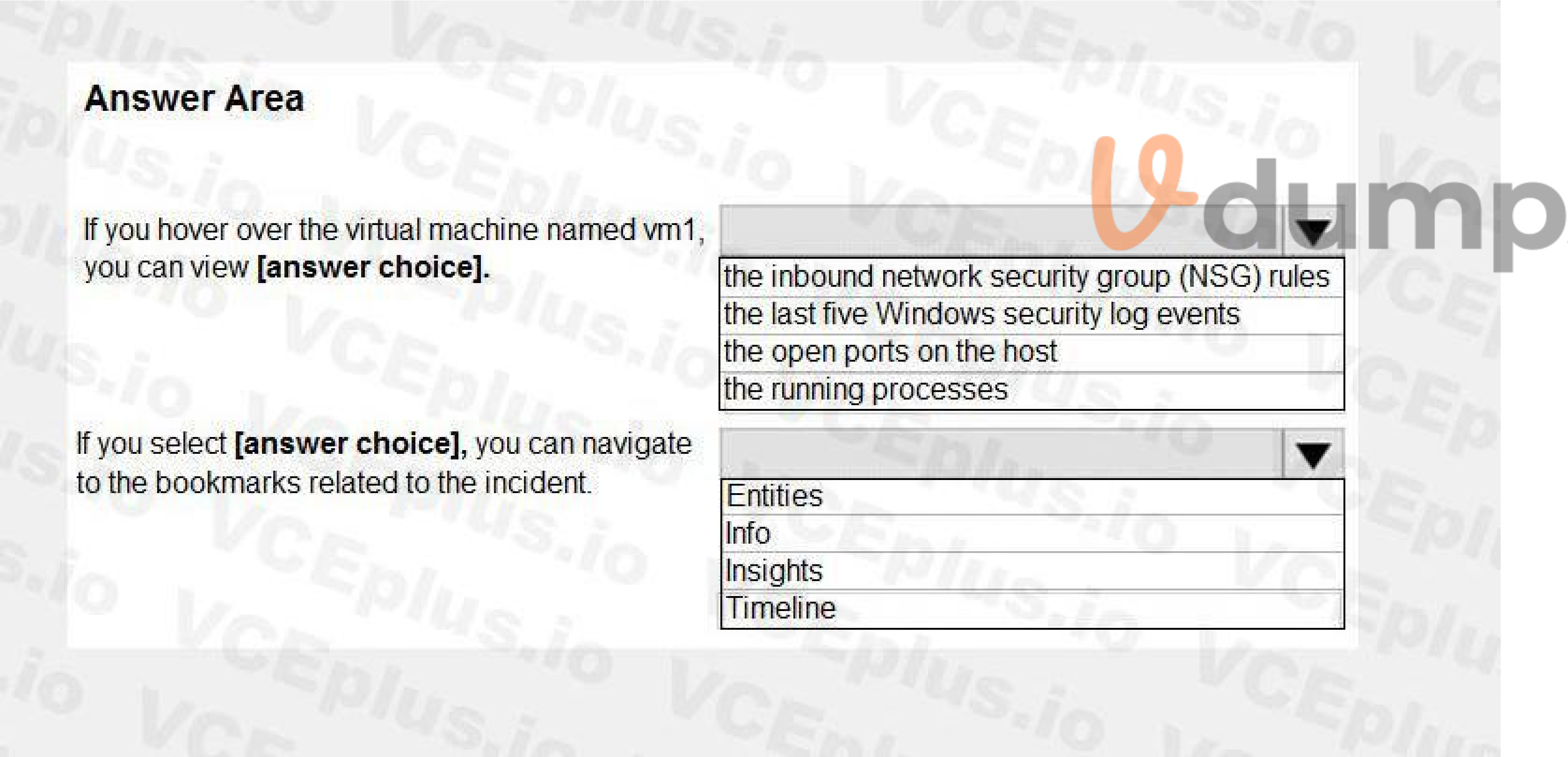
QUESTION 22
HOTSPOT
From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



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

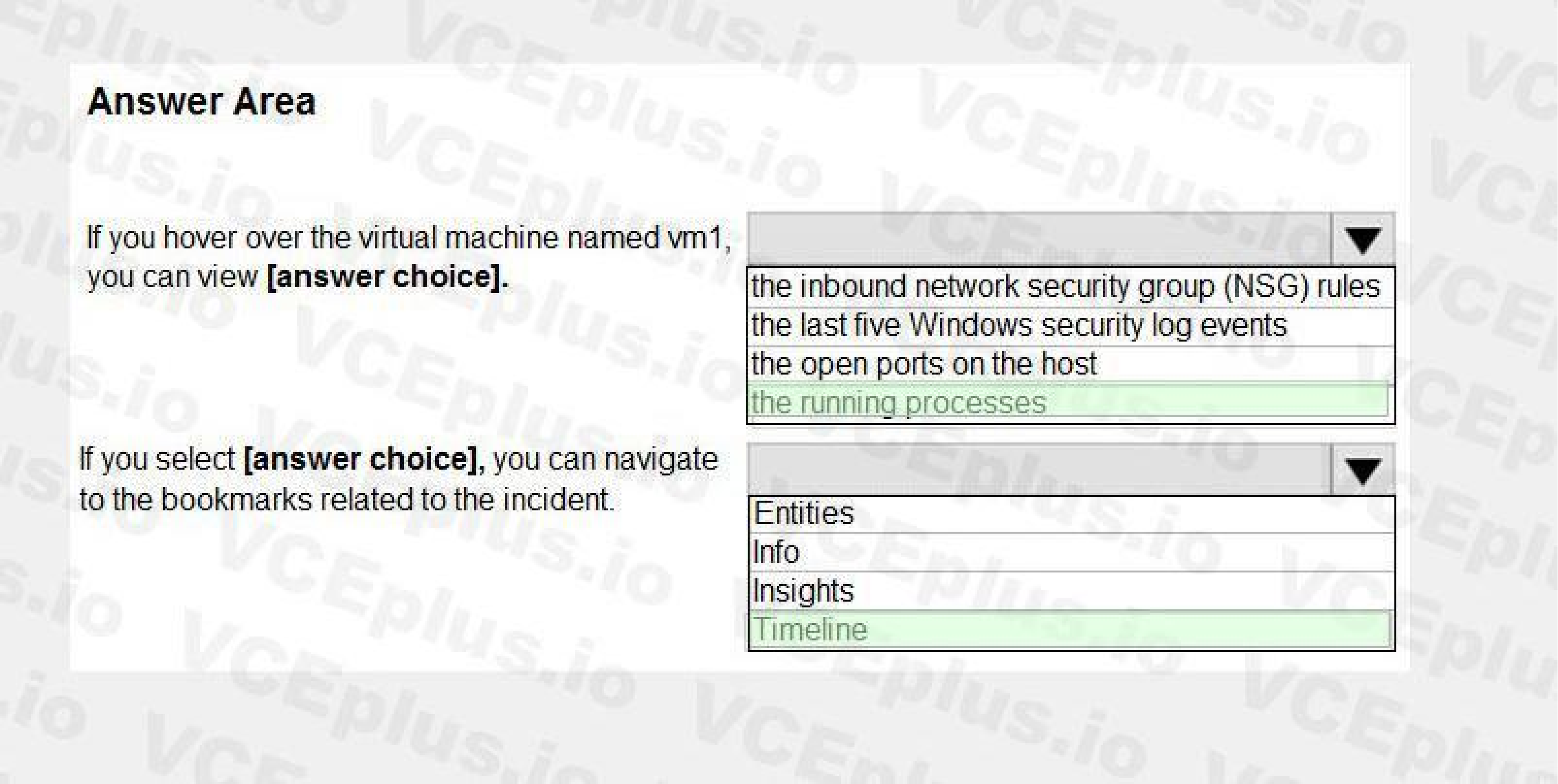
If you hover over the virtual machine named vm1, you can view **[answer choice].**

- 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

Answer 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]

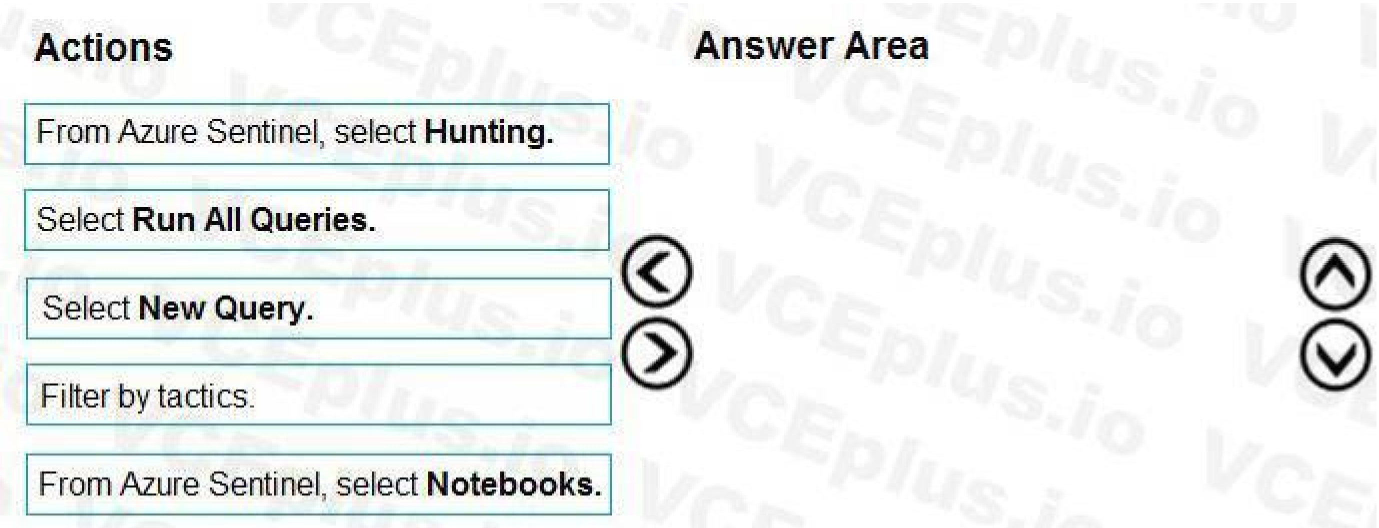
If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- [✓ Timeline]

Section:
Explanation:
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:

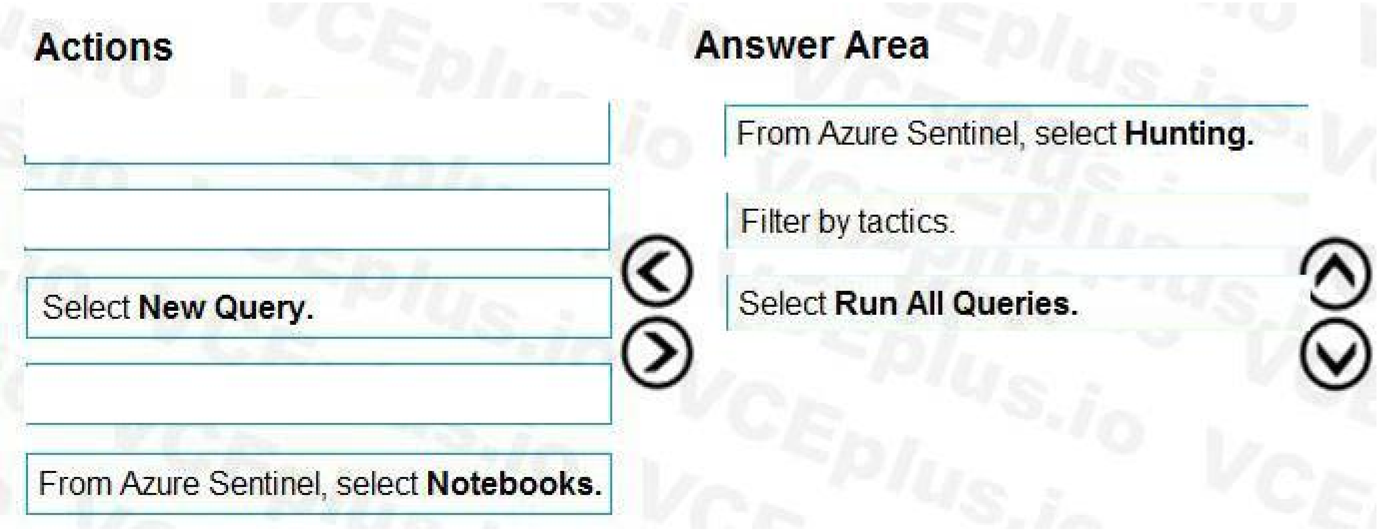


Actions

- 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.**

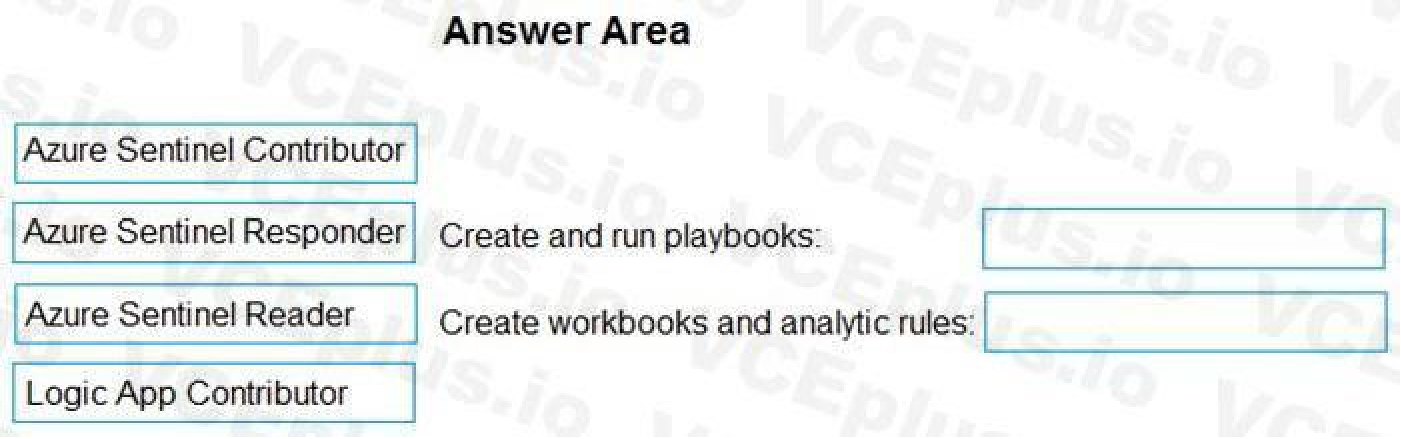
Filter by tactics.

Select **Run All Queries.**

Section:
Explanation:
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

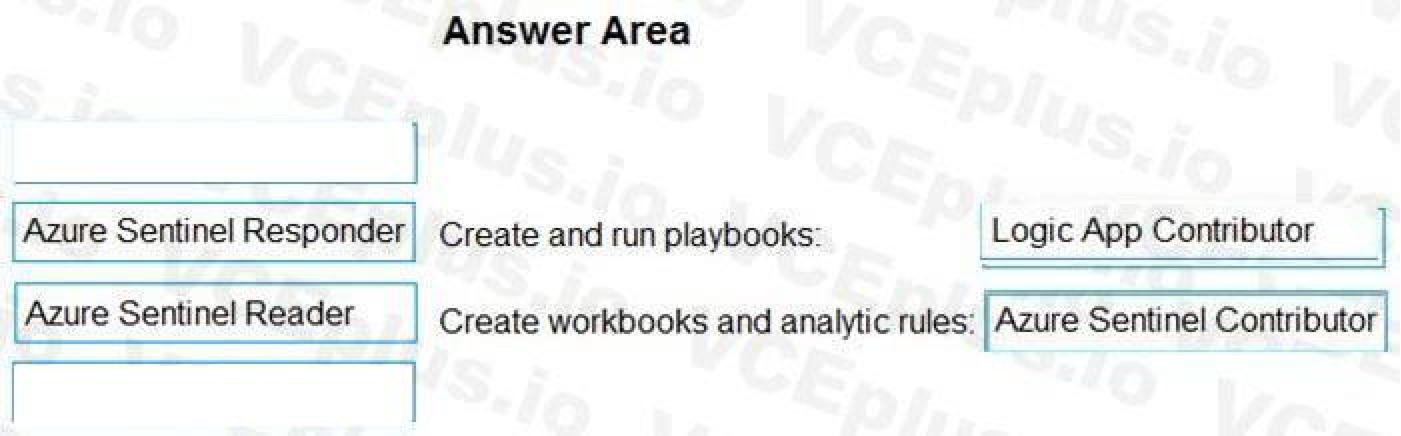
Azure Sentinel Reader

Logic App Contributor

Create and run playbooks:

Create workbooks and analytic rules:

Correct Answer:



Answer Area

Azure Sentinel Responder

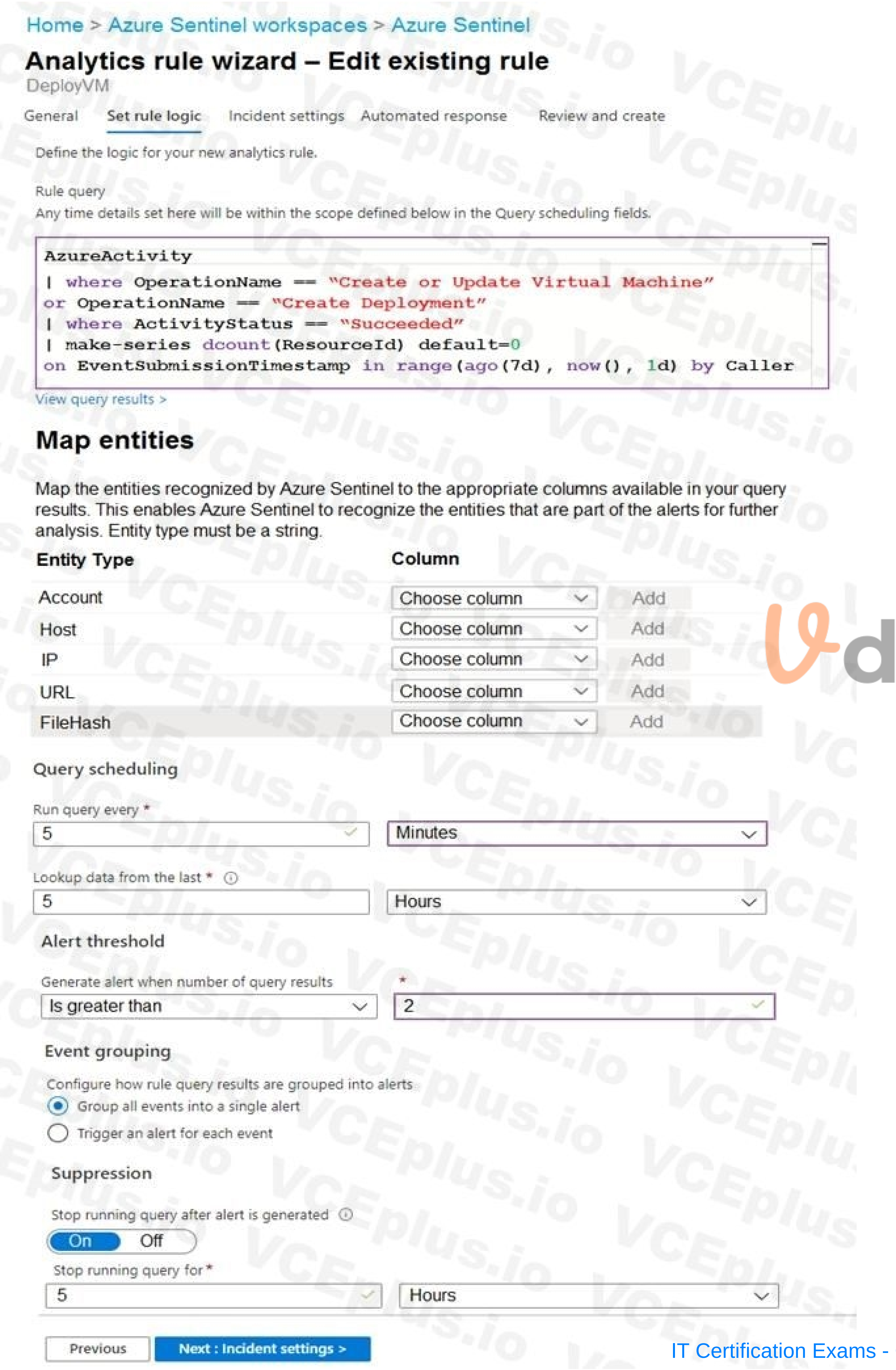
Azure Sentinel Reader

Create and run playbooks: Logic App Contributor

Create workbooks and analytic rules: Azure Sentinel Contributor

Section:
Explanation:
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

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

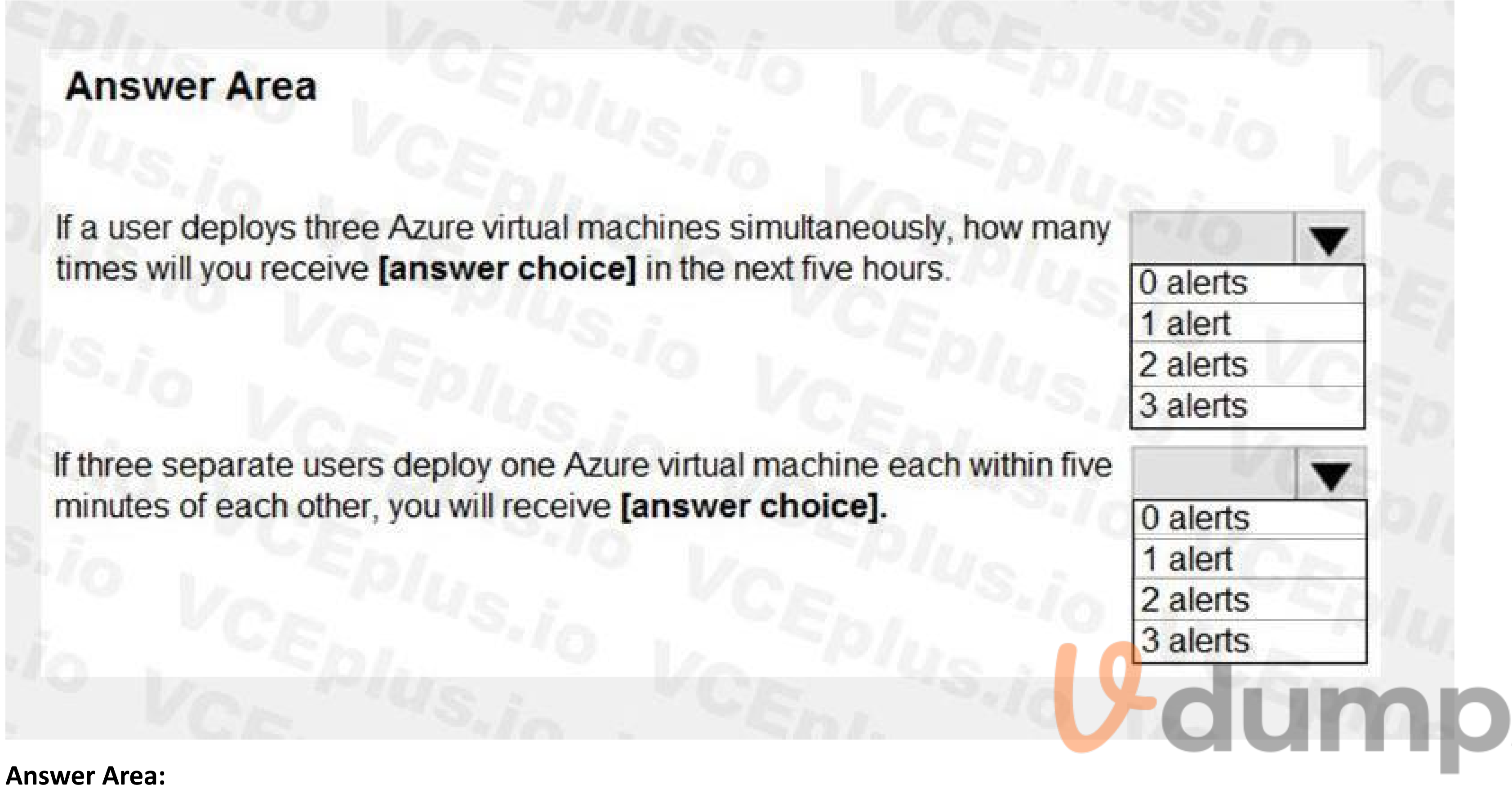
Stop running query after alert is generated

[✓ 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

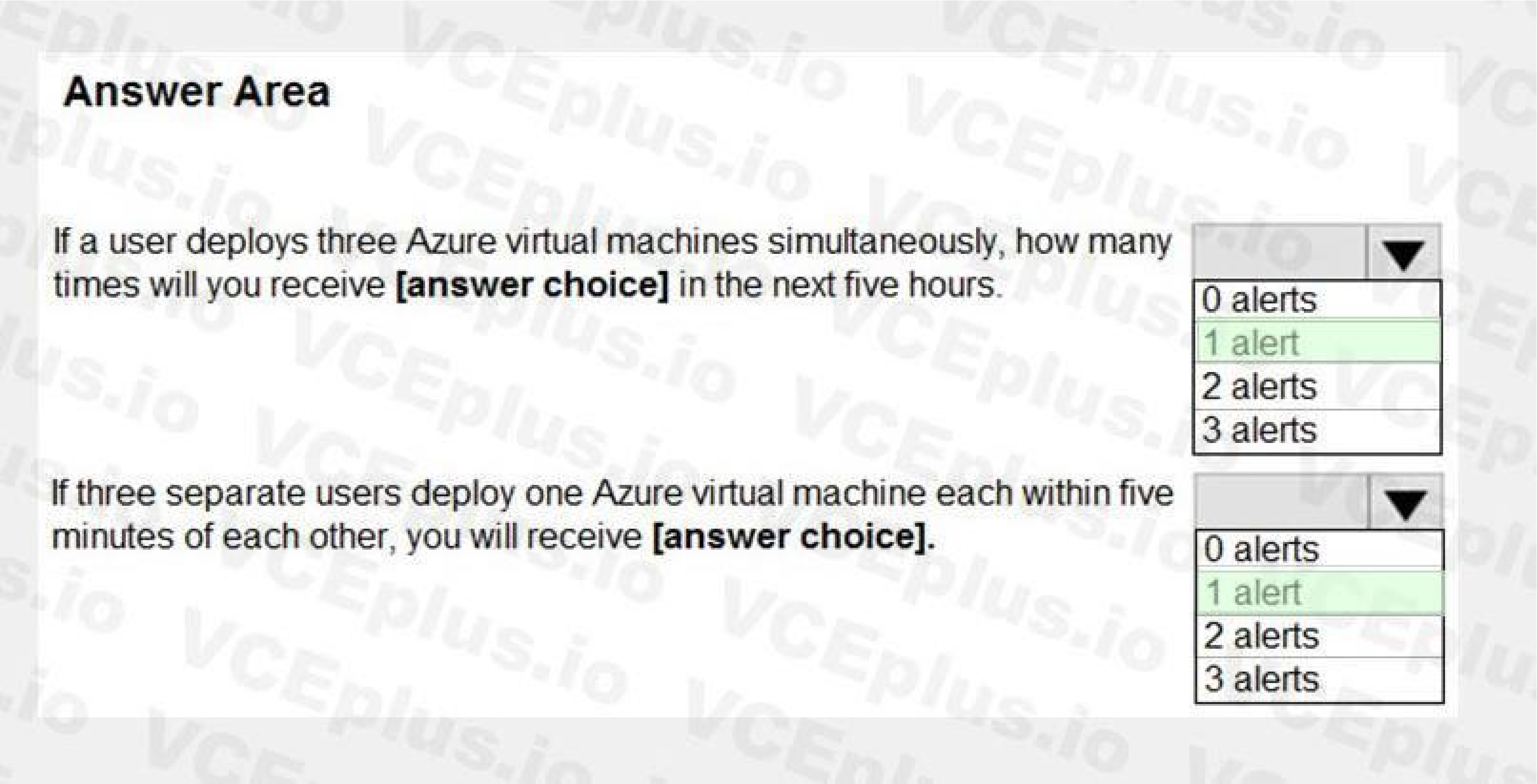
If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 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

Answer 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]**.

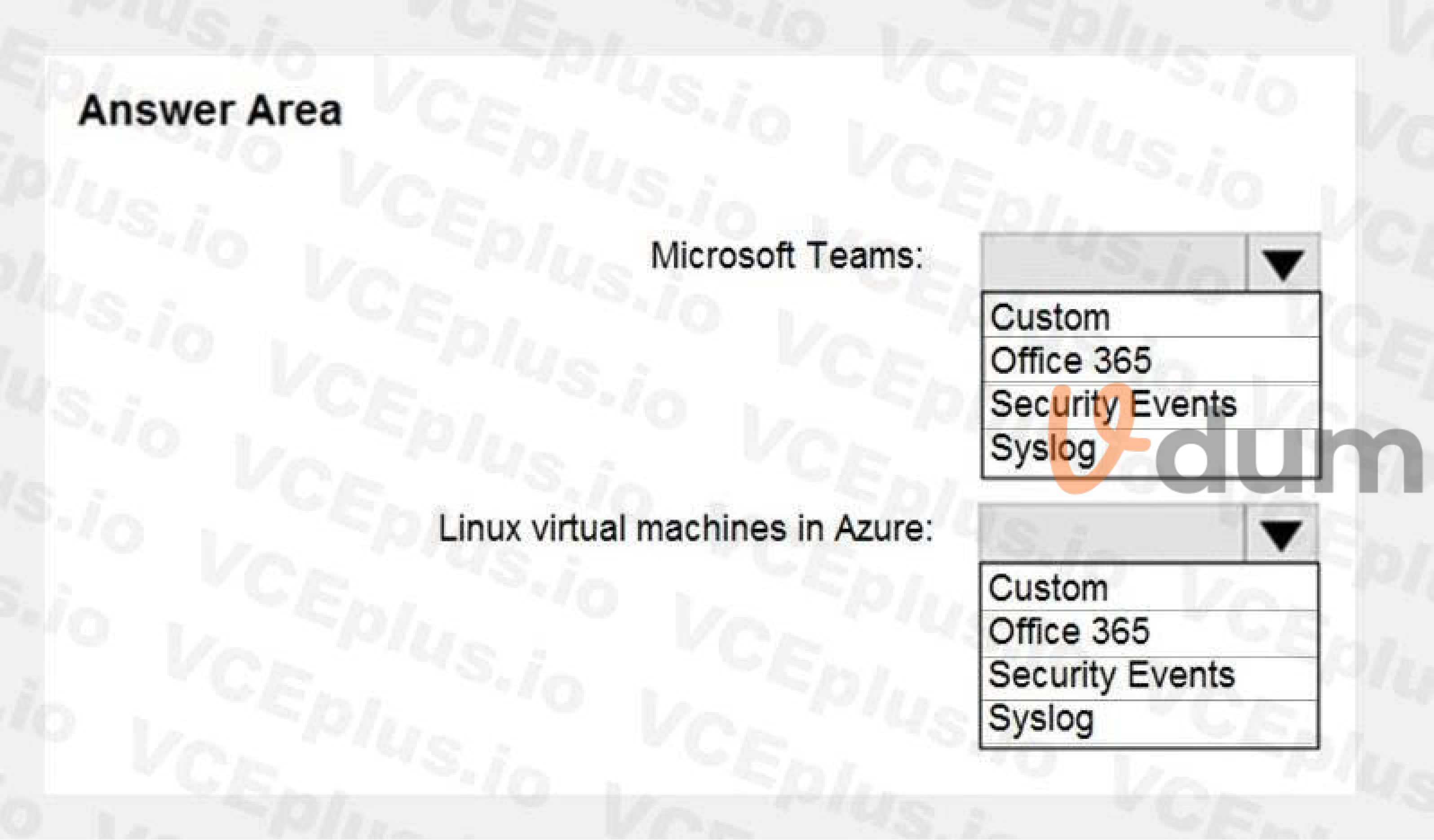
- 0 alerts
- [✓ 1 alert]
- 2 alerts
- 3 alerts

Section:

Explanation:
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:

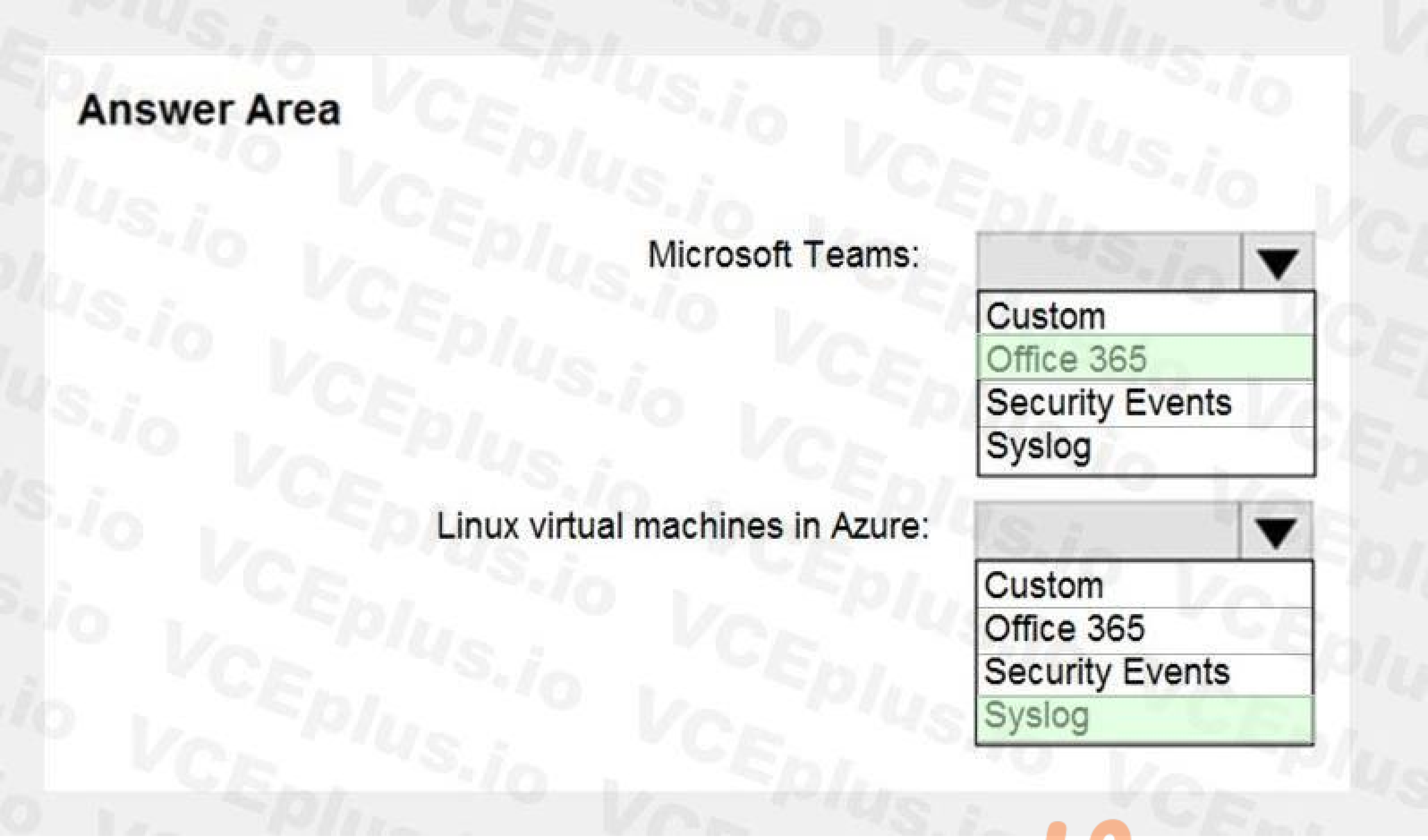


Answer Area

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

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

Answer Area:



Answer Area

Microsoft Teams:

- Custom
- [✓ Office 365]
- Security Events
- Syslog

Linux virtual machines in Azure:

- Custom
- Office 365
- Security Events
- [✓ Syslog]

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

QUESTION 28
You are configuring Azure Sentinel.

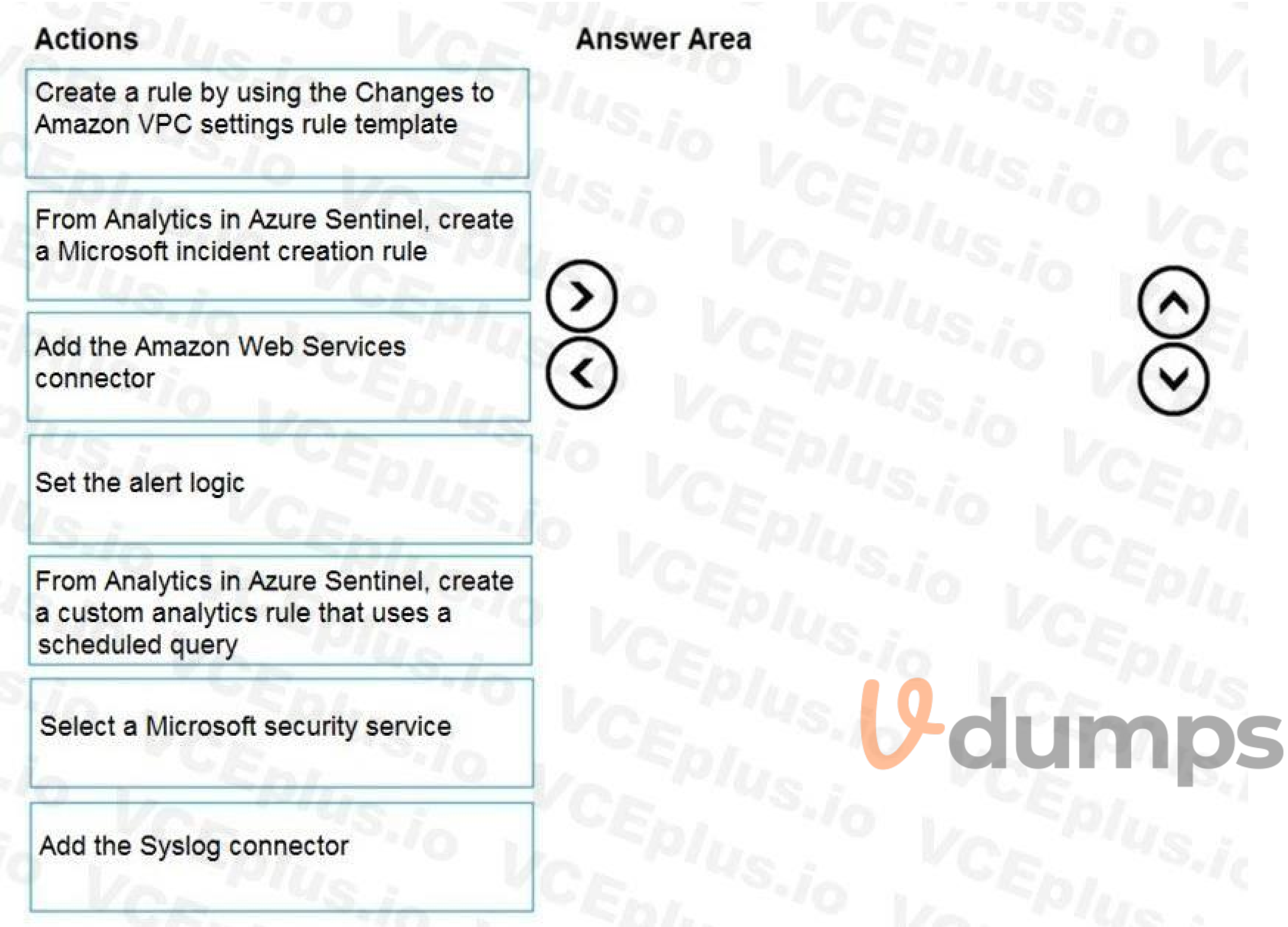
You need to send a Microsoft Teams message to a channel whenever an incident representing a sign-in risk event is activated in Azure Sentinel.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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: A, B
Section:
Explanation:
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:

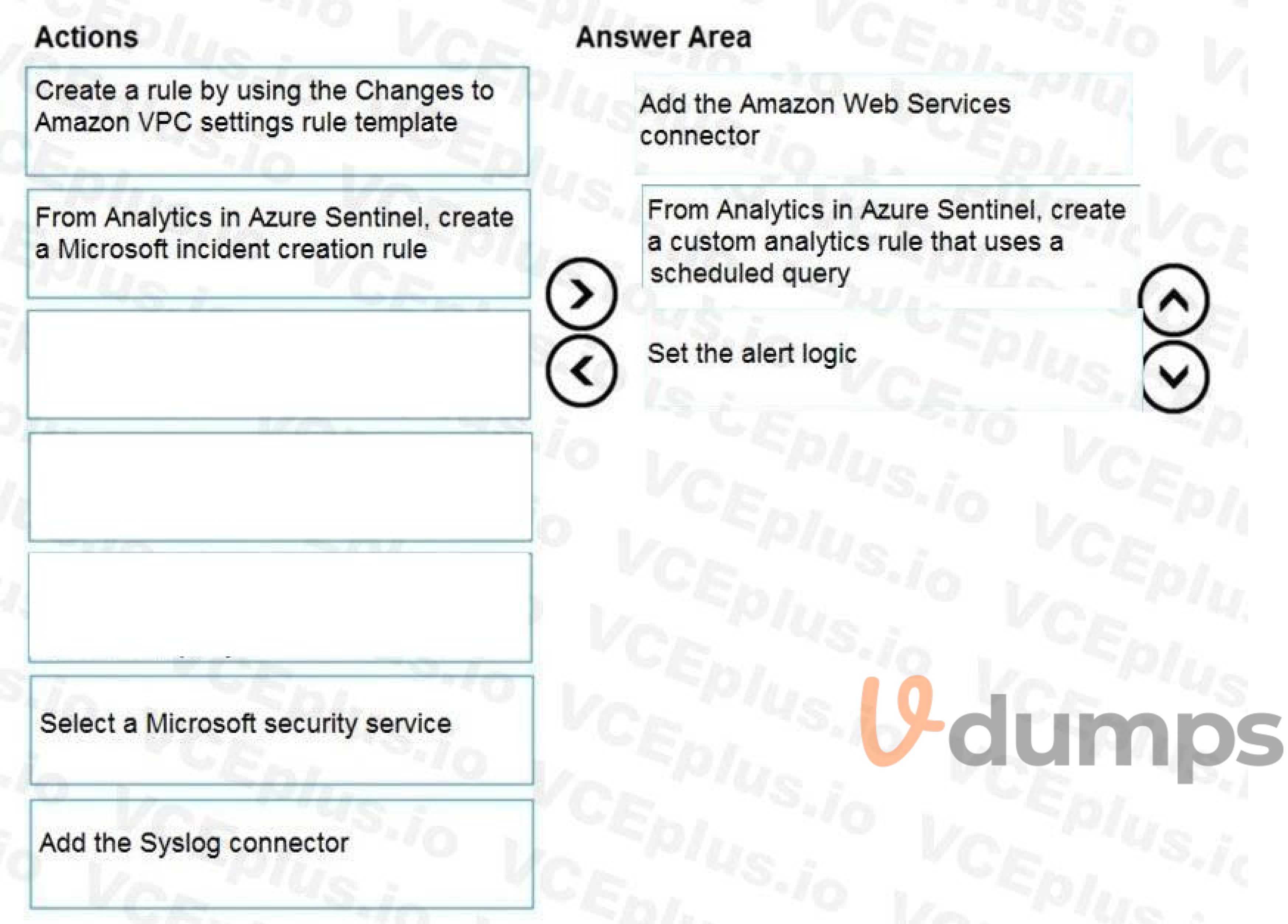


Actions

- 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:

Explanation:

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: A, D
Section:
Explanation:
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

QUESTION 31
You use Azure Sentinel.
You need to use a built-in role to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Contributor

B. Security Administrator

C. Azure Sentinel Responder

D. Logic App Contributor

Correct Answer: C
Section:
Explanation:

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

QUESTION 32
You create a hunting query in Azure Sentinel.
You need to receive a notification in the Azure portal as soon as the hunting query detects a match on the query. The solution must minimize effort.
What should you use?

A. a playbook

B. a notebook

C. a livestream

D. a bookmark

Correct Answer: C
Section:
Explanation:

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

QUESTION 33

You have an Azure subscription named Sub1 and a Microsoft 365 subscription. Sub1 is linked to an Azure Active Directory (Azure AD) tenant named contoso.com.
You create an Azure Sentinel workspace named workspace1. In workspace1, you activate an Azure AD connector for contoso.com and an Office 365 connector for the Microsoft 365 subscription.
You need to use the Fusion rule to detect multi-staged attacks that include suspicious sign-ins to contoso.com followed by anomalous Microsoft Office 365 activity.
Which two actions should you perform? Each correct answer present part of the solution.
NOTE: Each correct selection is worth one point.

A. Create custom rule based on the Office 365 connector templates.
B. Create a Microsoft incident creation rule based on Microsoft Defender for Cloud.
C. Create a Microsoft Cloud App Security connector.
D. Create an Azure AD Identity Protection connector.

Correct Answer: A, B
Section:
Explanation:

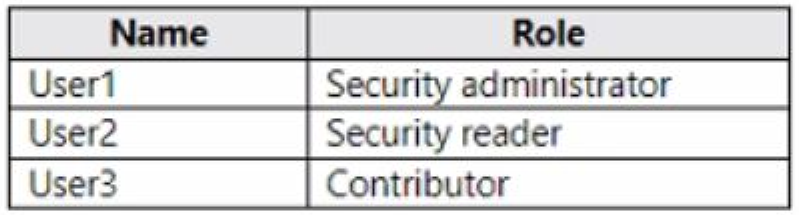
QUESTION 34
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a livestream from a query.
Does this meet the goal?

A. Yes
B. No

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

Exam F

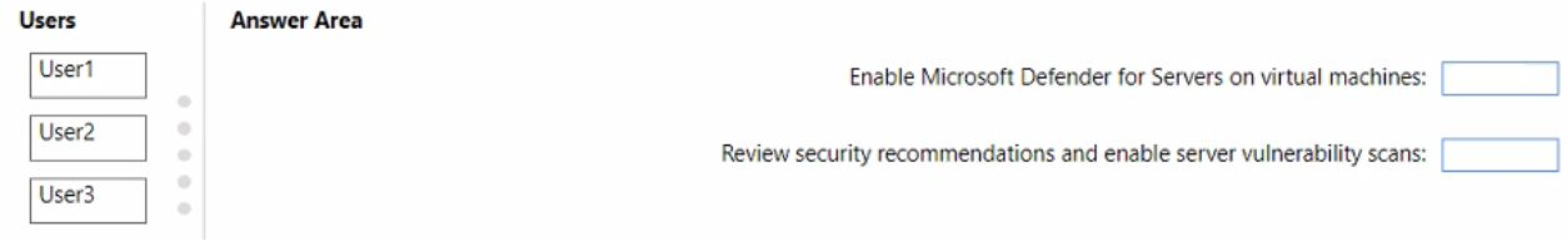
QUESTION 1
DRAG DROP
You have an Azure subscription that contains the users shown in the following table.



Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

You need to delegate the following tasks:
* Enable Microsoft Defender for Servers on virtual machines.
* Review security recommendations and enable server vulnerability scans.
The solution must use the principle of least privilege.

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



Users

User1

User2

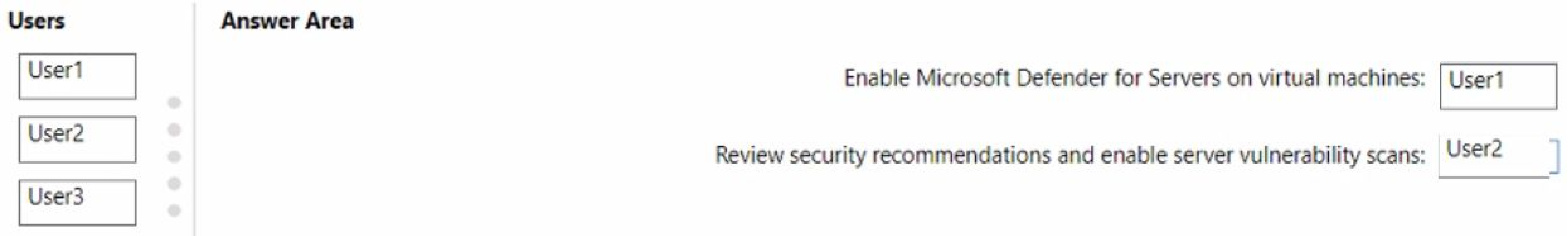
User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines:

Review security recommendations and enable server vulnerability scans:

Answer:



Users

User1

User2

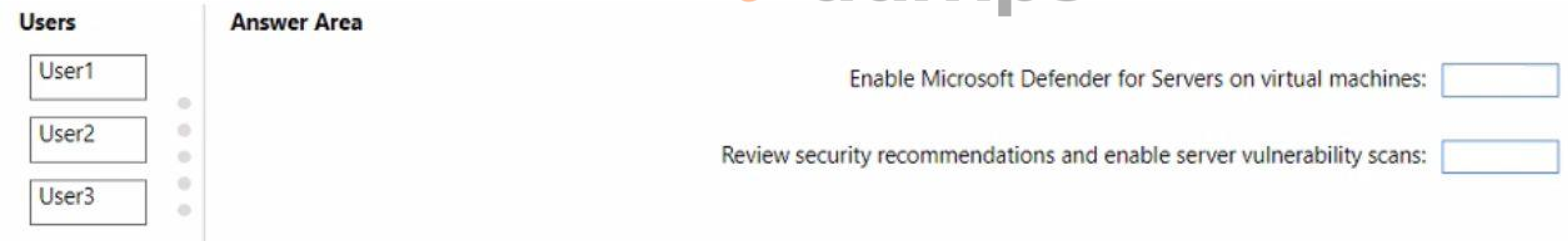
User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines: User1

Review security recommendations and enable server vulnerability scans: User2

Select and Place:



Users

User1

User2

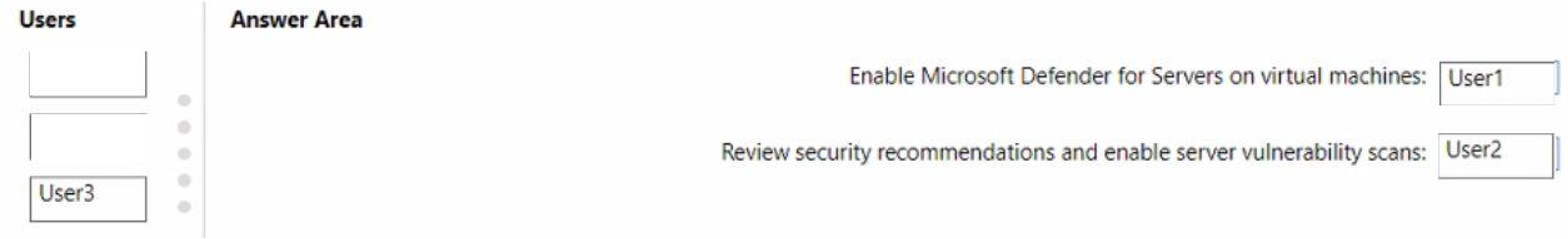
User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines:

Review security recommendations and enable server vulnerability scans:

Correct Answer:



Users

User3

Answer Area

Enable Microsoft Defender for Servers on virtual machines: User1

Review security recommendations and enable server vulnerability scans: User2

Section:

Explanation:

QUESTION 2
You have 50 Microsoft Sentinel workspaces.
You need to view all the incidents from all the workspaces on a single page in the Azure portal. The solution must minimize administrative effort.
Which page should you use in the Azure portal?

A. Microsoft Sentinel - Incidents
B. Microsoft Sentinel - Workbooks
C. Microsoft Sentinel
D. Log Analytics workspaces

Correct Answer: D
Section:

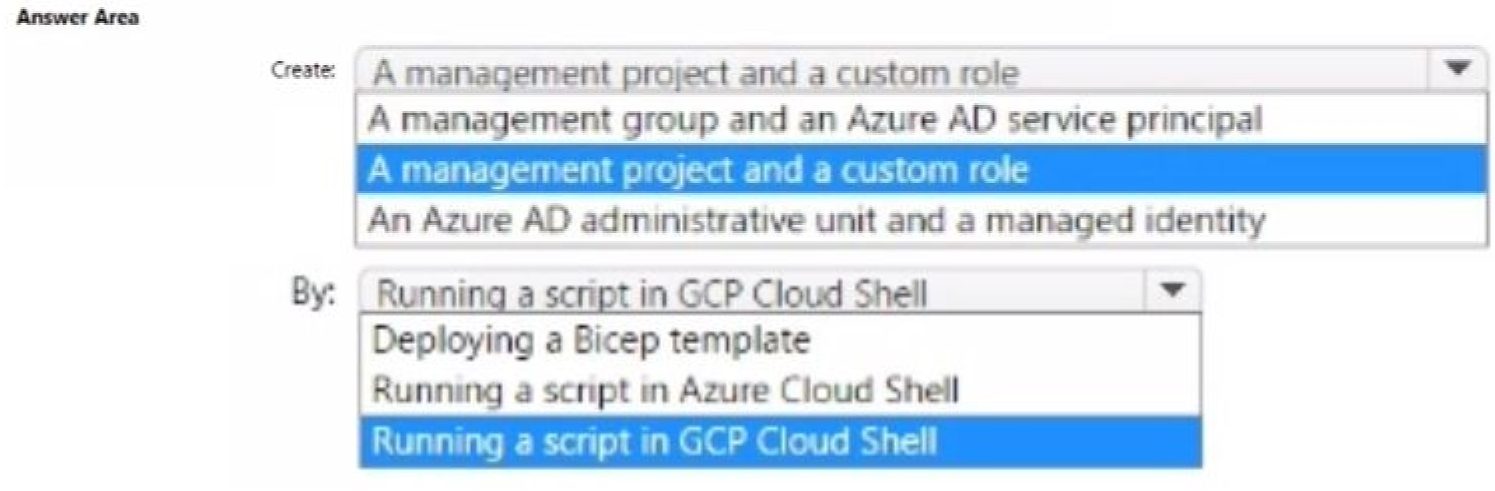
QUESTION 3
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.
What should you use in the Microsoft 365 Defender portal?

A. Incidents
B. Investigations
C. Advanced hunting
D. Remediation

Correct Answer: A
Section:

QUESTION 4
HOTSPOT
You have an Azure subscription that uses Microsoft Defender for Cloud.
You create a Google Cloud Platform (GCP) organization named GCP1.
You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.
What should you include in the solution? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

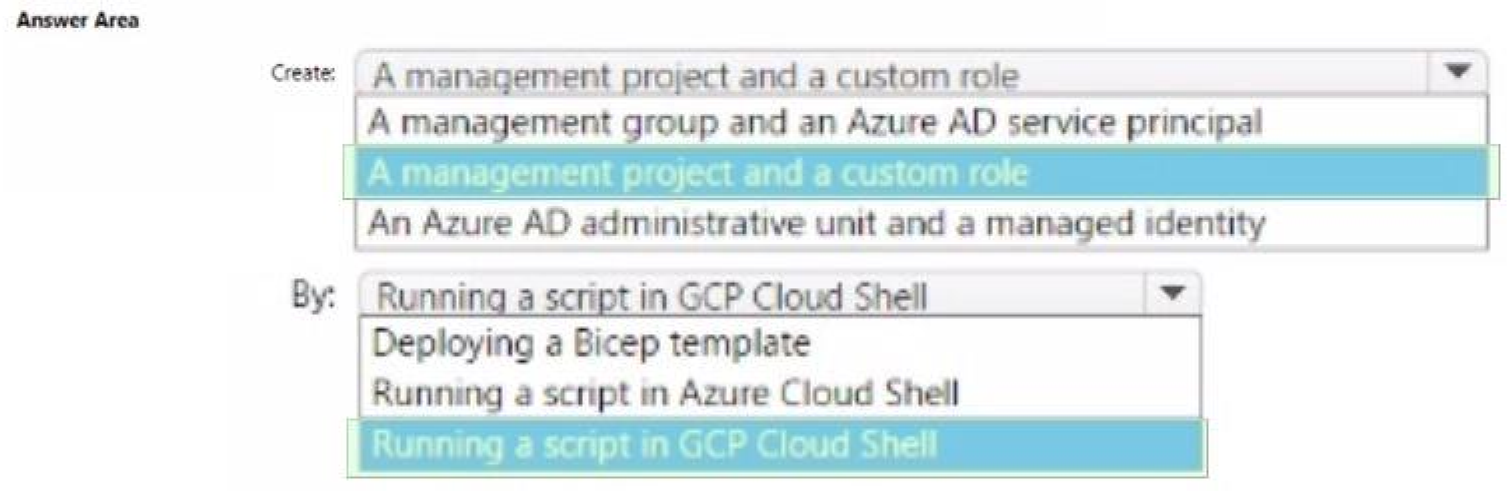


Answer Area

Create: A management project and a custom role
- A management group and an Azure AD service principal
- A management project and a custom role
- An Azure AD administrative unit and a managed identity

By: Running a script in GCP Cloud Shell
- Deploying a Bicep template
- Running a script in Azure Cloud Shell
- Running a script in GCP Cloud Shell

Answer Area:



Answer Area

Create: A management project and a custom role

- A management group and an Azure AD service principal
- A management project and a custom role
- An Azure AD administrative unit and a managed identity

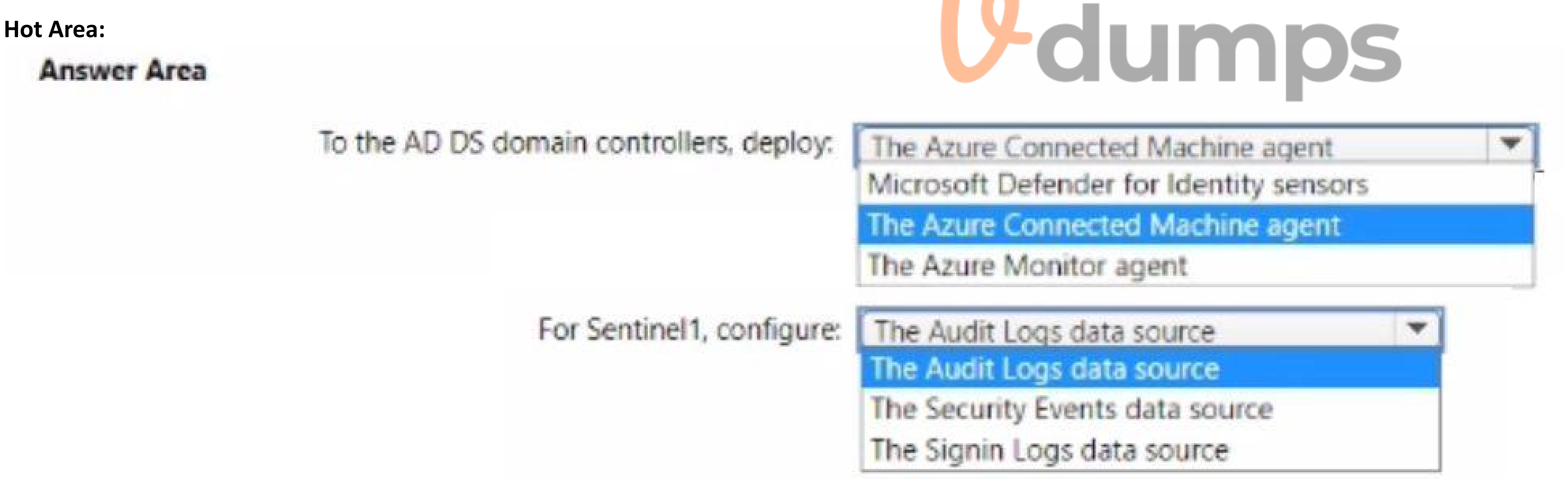
By: Running a script in GCP Cloud Shell

- Deploying a Bicep template
- Running a script in Azure Cloud Shell
- Running a script in GCP Cloud Shell

Section:
Explanation:

QUESTION 5
HOTSPOT
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.
You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel 1 and configure UEBA to use data collected from Active Directory Domain Services (AD OS).
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

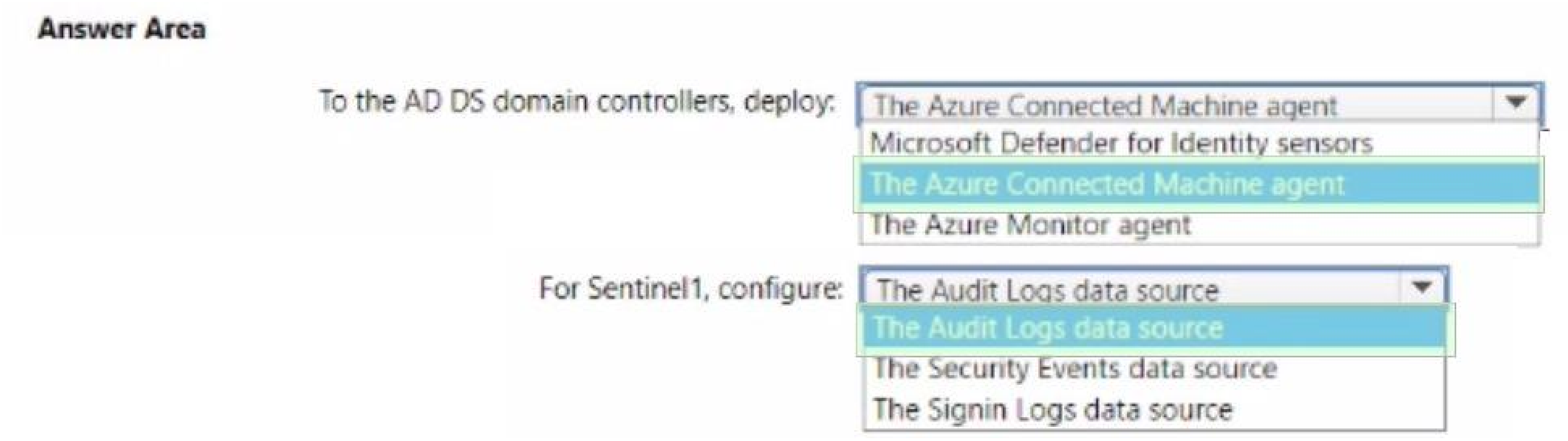
To the AD DS domain controllers, deploy: The Azure Connected Machine agent

- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent
- The Azure Monitor agent

For Sentinel1, configure: The Audit Logs data source

- The Audit Logs data source
- The Security Events data source
- The Signin Logs data source

Answer Area:



Answer Area

To the AD DS domain controllers, deploy: The Azure Connected Machine agent

- Microsoft Defender for Identity sensors
- [✓ The Azure Connected Machine agent]
- The Azure Monitor agent

For Sentinel1, configure: The Audit Logs data source

- [✓ The Audit Logs data source]
- The Security Events data source
- The Signin Logs data source

Section:
Explanation:

QUESTION 6
You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You plan to create a hunting query from Microsoft Defender.
You need to create a custom tracked query that will be used to assess the threat status of the subscription.
From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Policies & rules
B. Explorer
C. Threat analytics
D. Advanced Hunting

Correct Answer: D
Section:

QUESTION 7
You have an Azure subscription that has Microsoft Defender for Cloud enabled.
You have a virtual machine named Server! that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).
You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.
What should you install first on Server1?

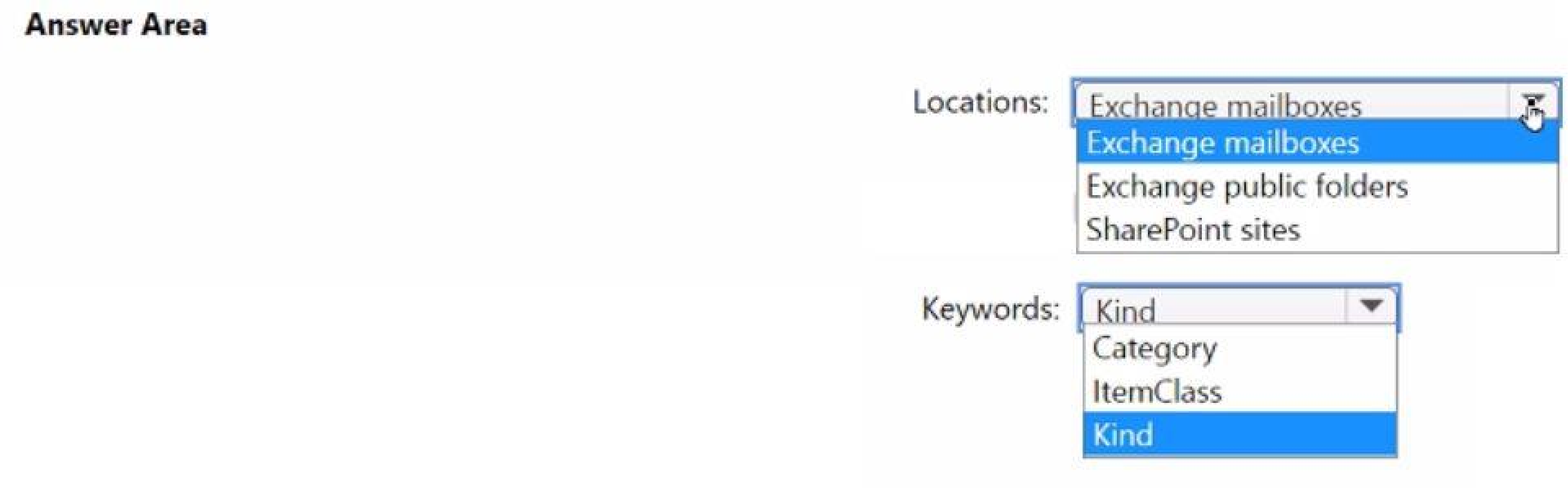
A. the Microsoft Monitoring Agent
B. the Azure Arc agent
C. the Azure Monitor agent
D. the Azure Pipelines agent

Correct Answer: C
Section:

QUESTION 8
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.
You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

How should you configure the content search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

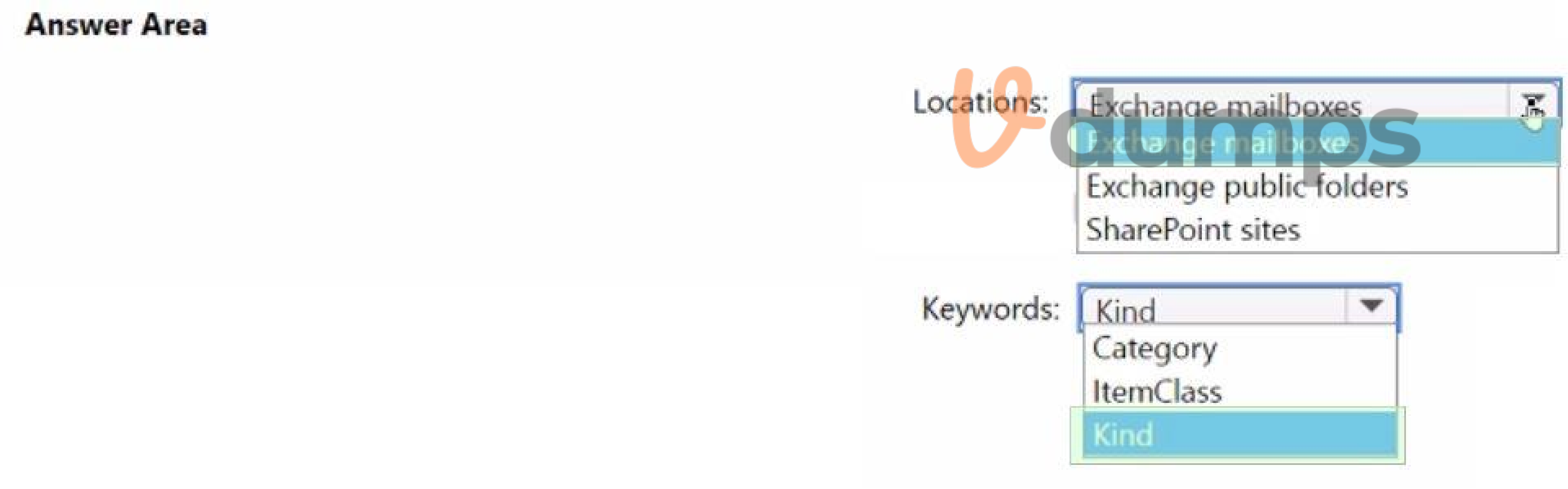


Answer Area

Locations: Exchange mailboxes

Keywords: Kind

Answer Area:



Answer Area

Locations: Exchange mailboxes

Keywords: Kind

Section:
Explanation:

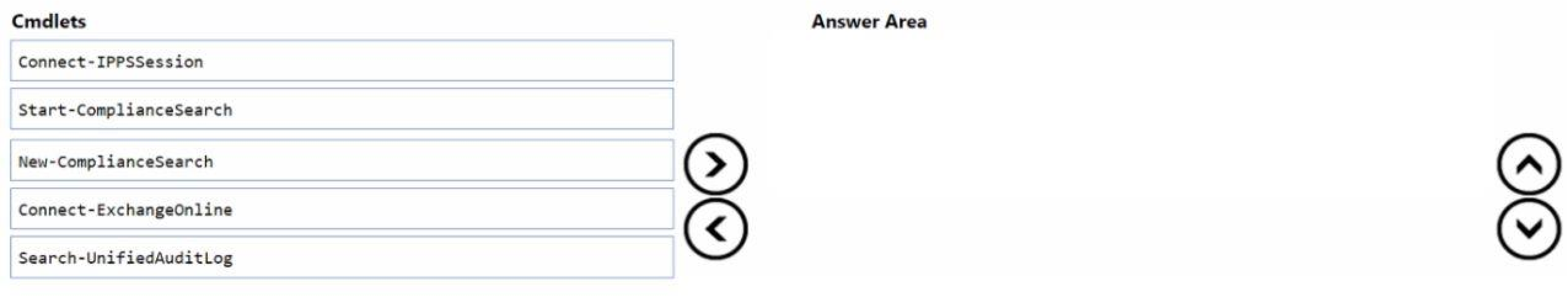
QUESTION 9
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint
You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.
Which operator should you use?

A. join kind = inner
B. evaluate hint. Remote =
C. search *
D. union kind = inner

Correct Answer: A
Section:

QUESTION 10
DRAG DROP
You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.
You need to identify phishing email messages.
Which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Select and Place:

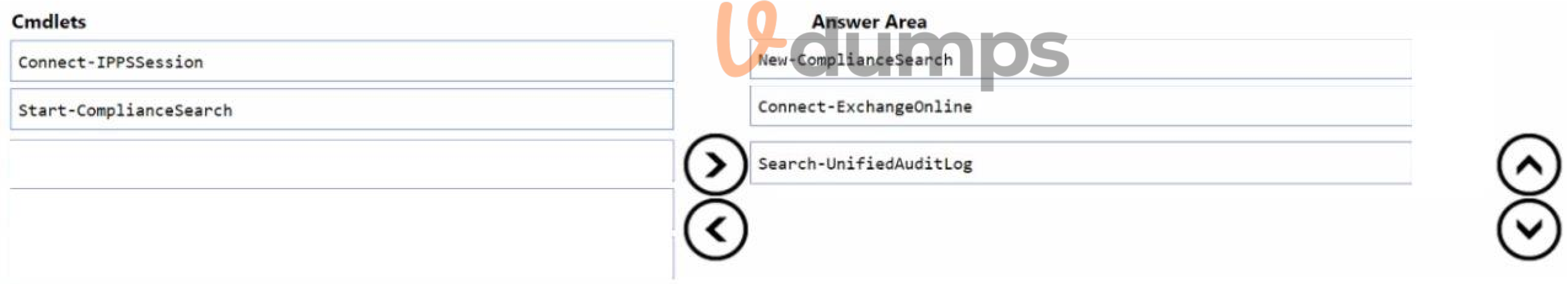


Cmdlets

Connect-IPPSSession
Start-ComplianceSearch
New-ComplianceSearch
Connect-ExchangeOnline
Search-UnifiedAuditLog

Answer Area

Correct Answer:



Cmdlets

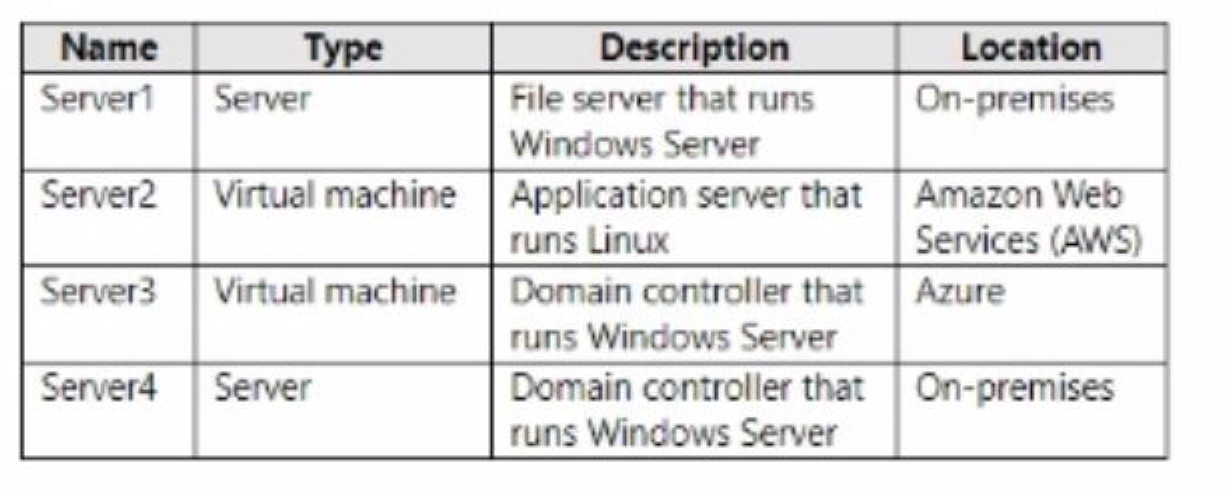
Connect-IPPSSession
Start-ComplianceSearch

Answer Area

New-ComplianceSearch
Connect-ExchangeOnline
Search-UnifiedAuditLog

Section:
Explanation:
New-ComplianceSearch
Connect-ExchangeOnline
Search-UnifiedAuditLog

QUESTION 11
You haw the resources shown in the following Table.



Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to enable Microsoft Defender lot Servers on each resource.
Which resources will require the installation of the Azure Arc agent?

A. Server 3 only

B. Server1 and 5erver4 only

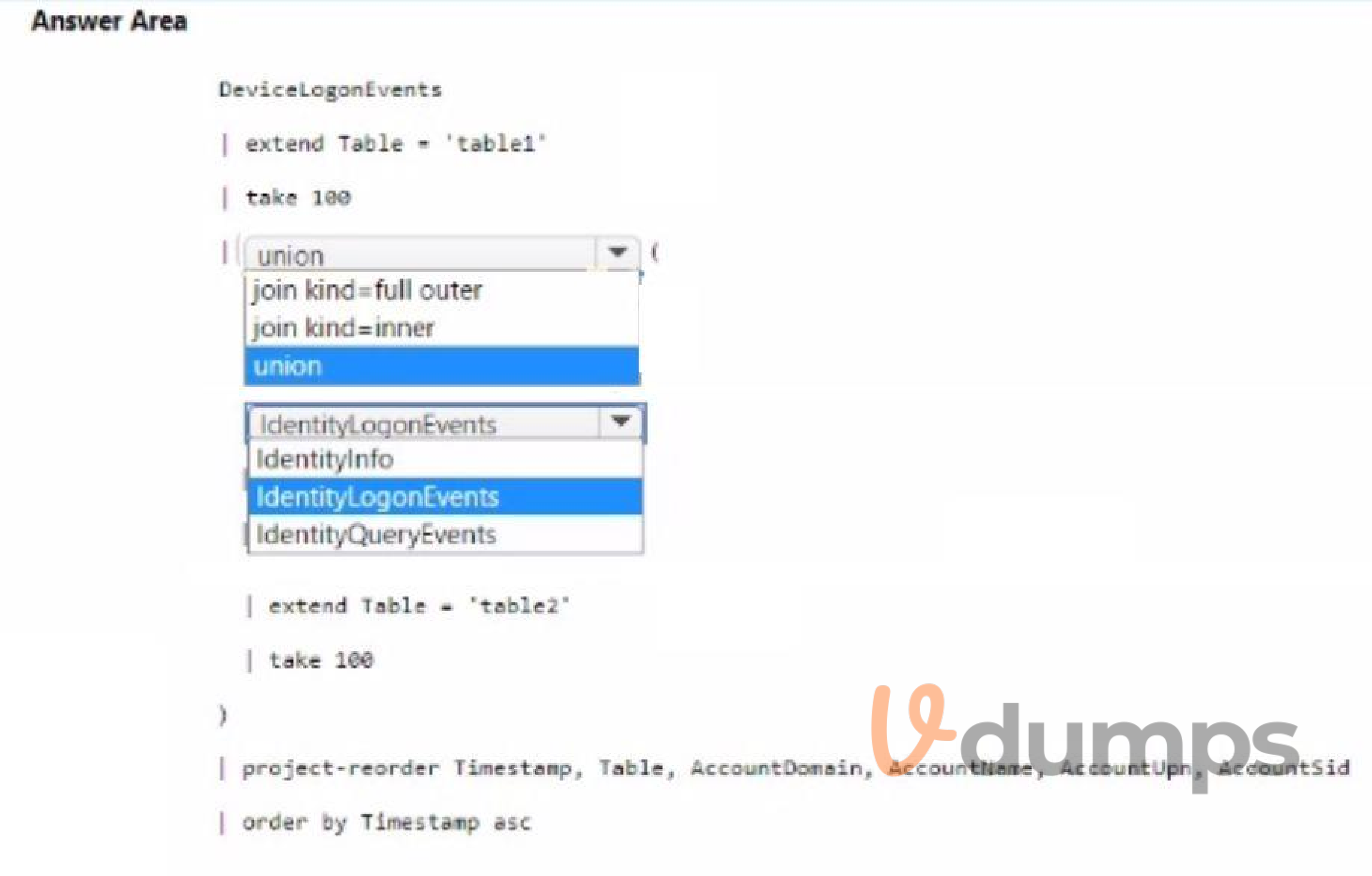
C. Server 1. Server2. arid Server4 only

D. Server 1, Servec2, Server3. and Seiver4

Correct Answer: B
Section:

QUESTION 12
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 36S.
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.
You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.
How should you complete The KQL query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

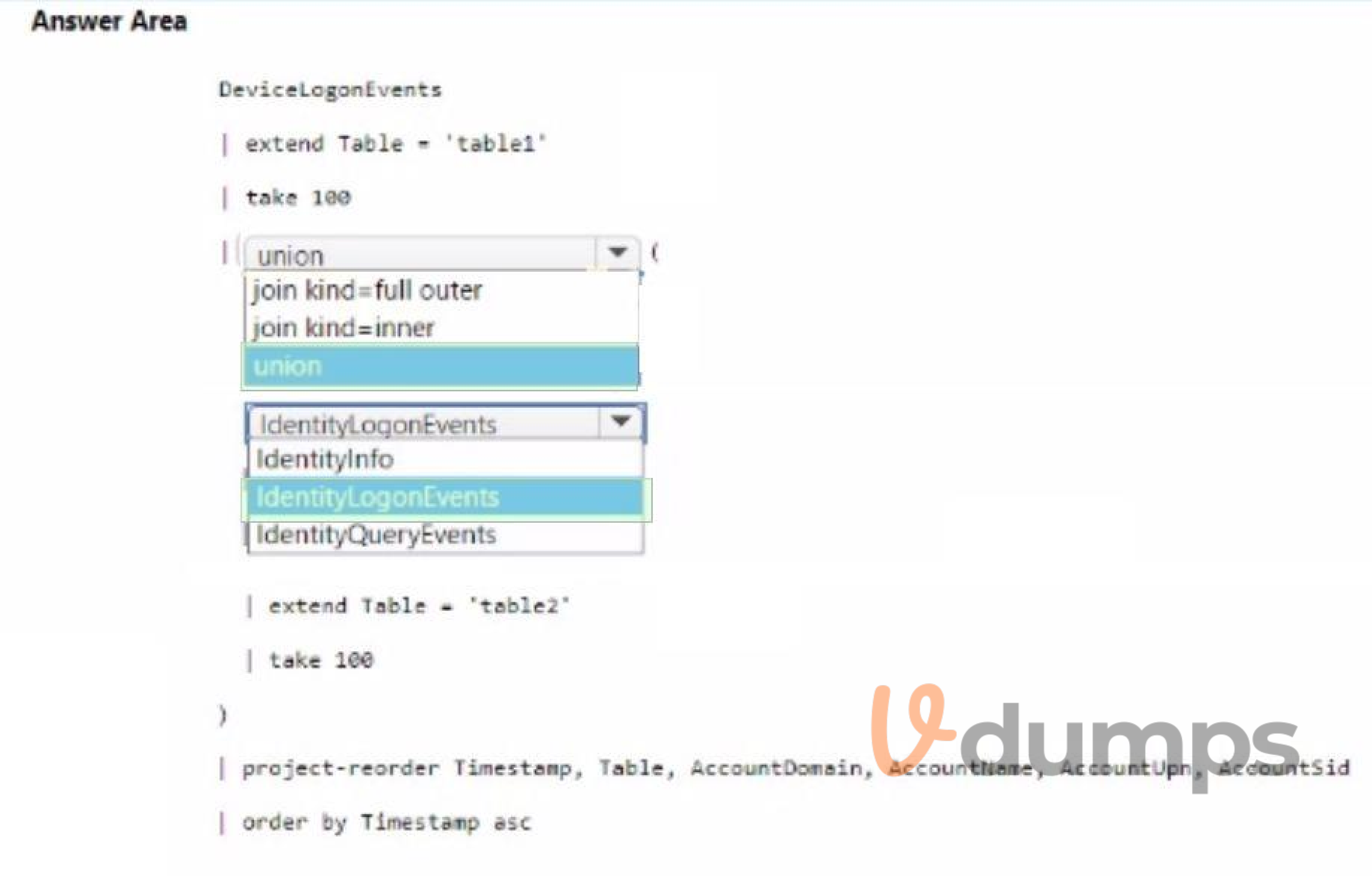
Hot Area:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Answer Area:



Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| union (
    IdentityLogonEvents
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Section:
Explanation:

QUESTION 13
You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent
B. the Log Analytics agent
C. the Azure Connected Machine agent
D. the Guest Configuration extension

Correct Answer: B
Section:
Explanation:

Defender for Cloud depends on the Log Analytics agent.

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

QUESTION 14
You have an Azure subscription that uses Microsoft Sentinel.
You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.
Which two features should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

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

Correct Answer: C, E
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threatsplaybook?tabs=LAC

QUESTION 15
You have a Microsoft Sentinel workspace named workspace1 that contains custom Kusto queries.
You need to create a Python-based Jupyter notebook that will create visuals. The visuals will display the results of the queries and be pinned to a dashboard. The solution must minimize development effort.
What should you use to create the visuals?

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

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

QUESTION 16

You have a Microsoft Sentinel workspace that contains the following incident.
Brute force attack against Azure Portal analytics rule has been triggered.
You need to identify the geolocation information that corresponds to the incident.
What should you do?

A. From Overview, review the Potential malicious events map.
B. From Incidents, review the details of the iPCustomEntity entity associated with the incident.
C. From Incidents, review the details of the AccouncCuscomEntity entity associated with the incident.
D. From Investigation, review insights on the incident entity.

Correct Answer: A
Section:
Explanation:

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

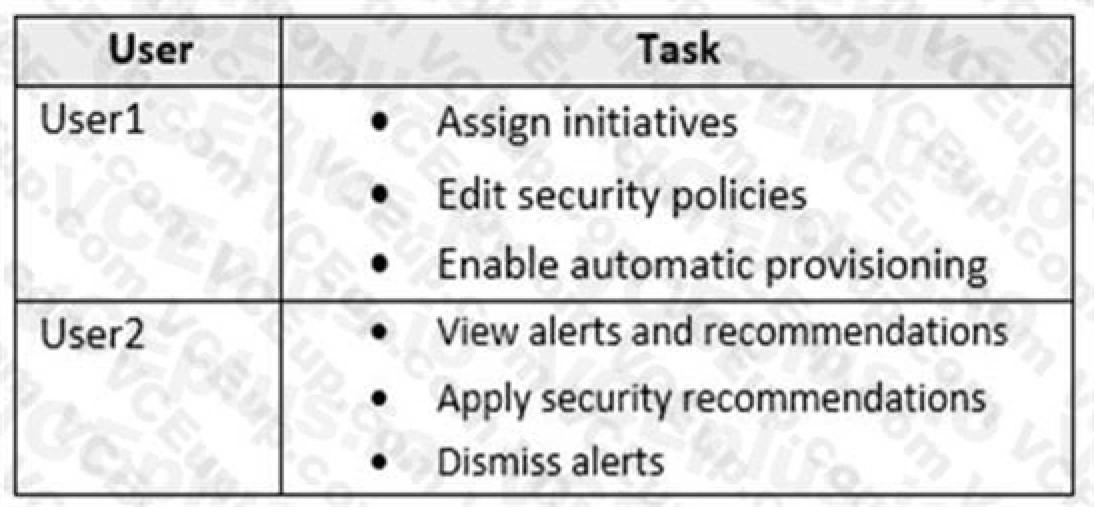
QUESTION 17
You have two Azure subscriptions that use Microsoft Defender for Cloud.
You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.
What should you do in the Azure portal?

A. Create an Azure Policy assignment.
B. Modify the Workload protections settings in Defender for Cloud.
C. Create an alert rule in Azure Monitor.
D. Modify the alert settings in Defender for Cloud.

Correct Answer: D
Section:
Explanation:

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

QUESTION 18
DRAG DROP
You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.
You plan to deploy Azure Defender.
You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

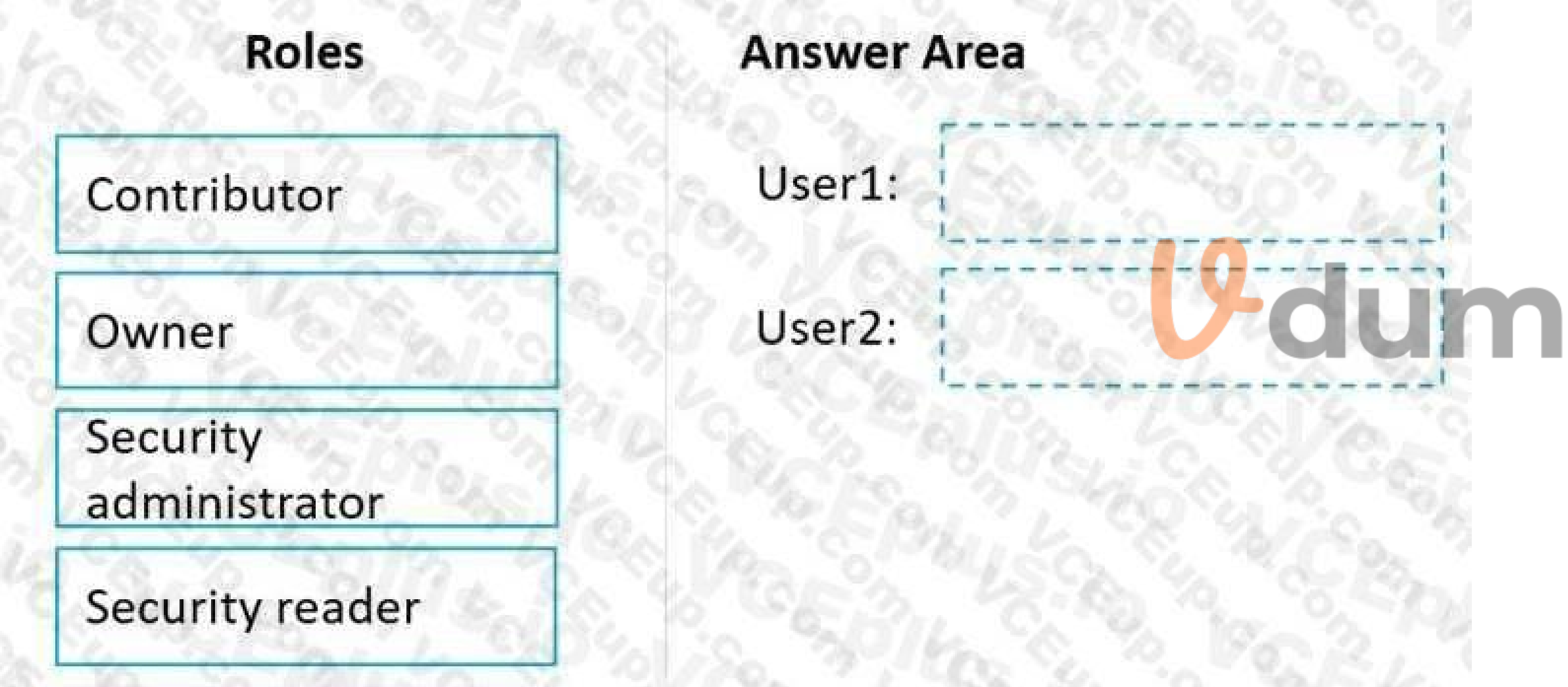


User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.

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

Select and Place:



Roles

Contributor

Owner

Security administrator

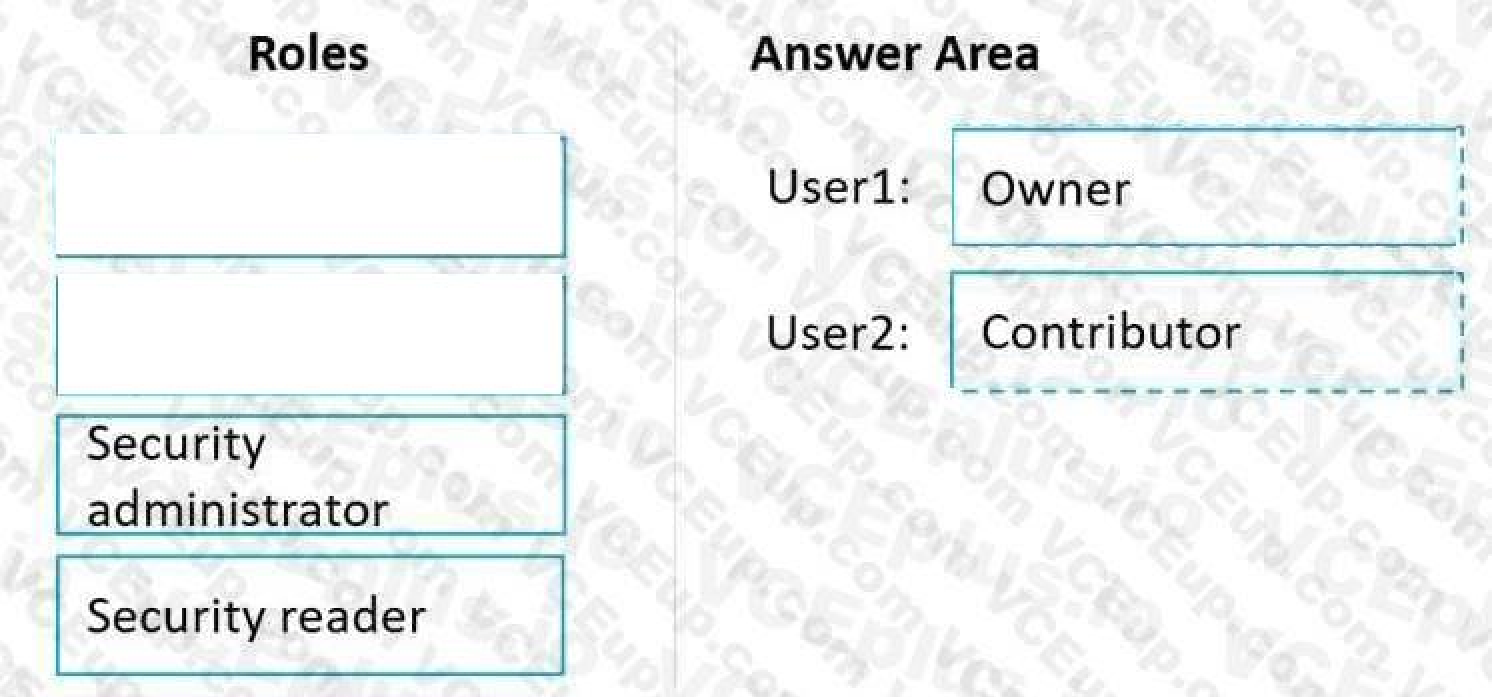
Security reader

Answer Area

User1:

User2:

Correct Answer:



Roles

Security administrator

Security reader

Answer Area

User1: Owner

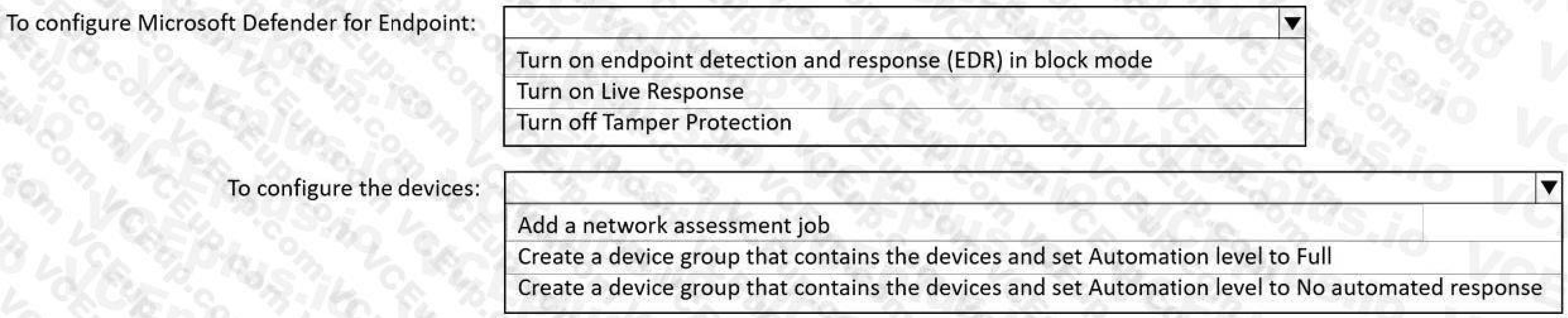
User2: Contributor

Section:
Explanation:
Box 1: Owner
Only the Owner can assign initiatives.
Box 2: Contributor
Only the Contributor or the Owner can apply security recommendations.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

QUESTION 19

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

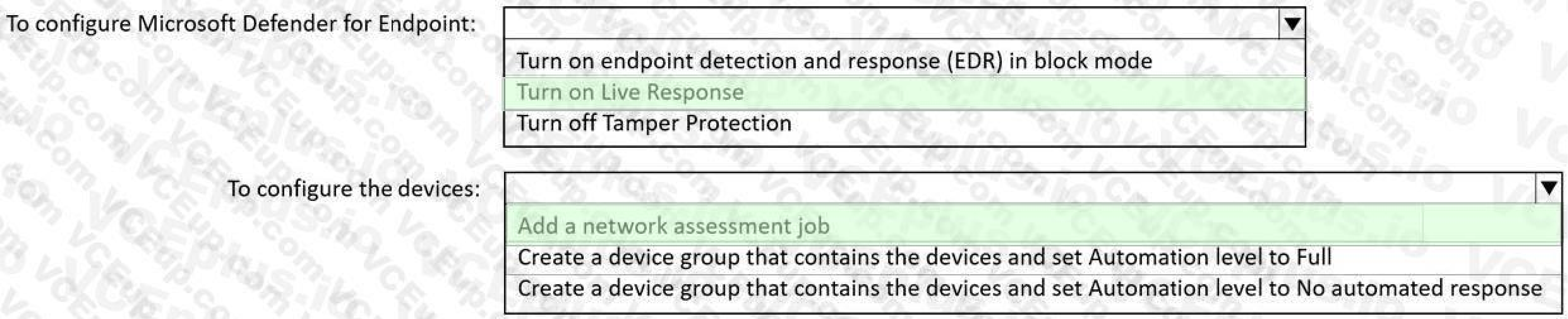
Hot Area:



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

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

Answer Area:



To configure Microsoft Defender for Endpoint: ▼

Turn on endpoint detection and response (EDR) in block mode
[✓ Turn on Live Response]
Turn off Tamper Protection

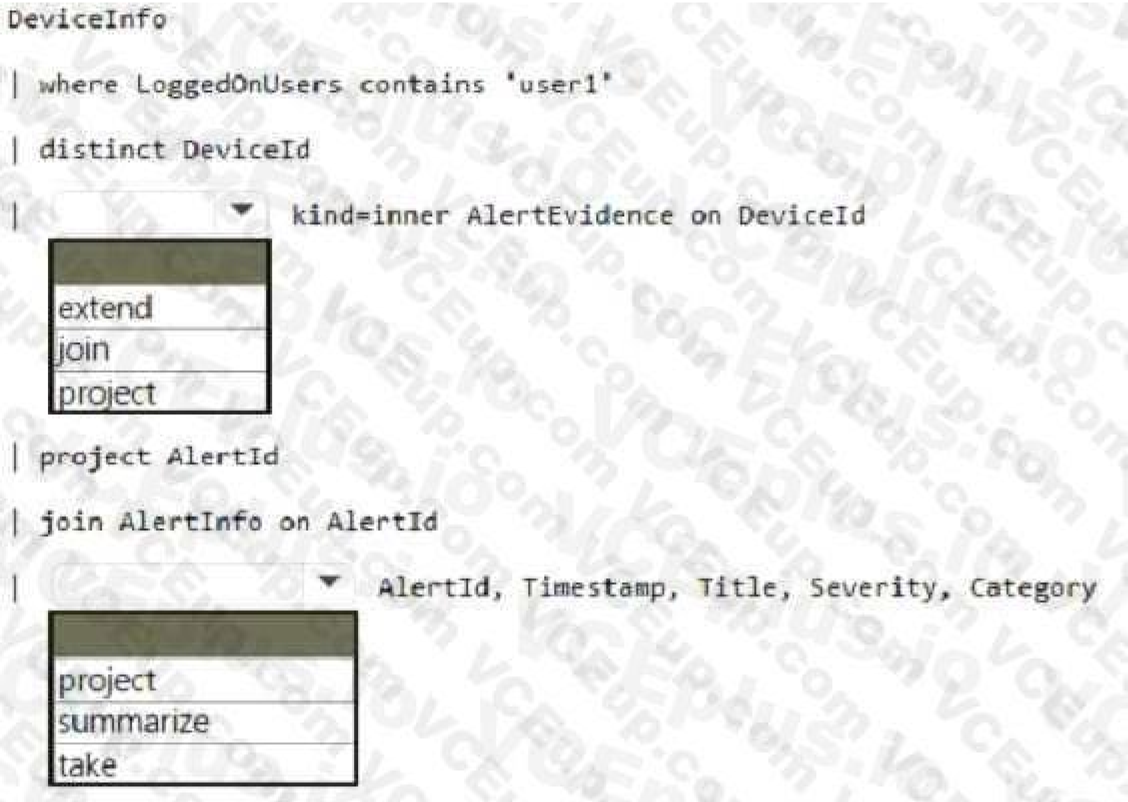
To configure the devices: ▼

[✓ Add a network assessment job]
Create a device group that contains the devices and set Automation level to Full
Create a device group that contains the devices and set Automation level to No automated response

Section:
Explanation:
Box 1: Turn on Live Response Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.
Box: 2 : Add a network assessment job
Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machinealerts?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/networkdevices?view=o365-worldwide

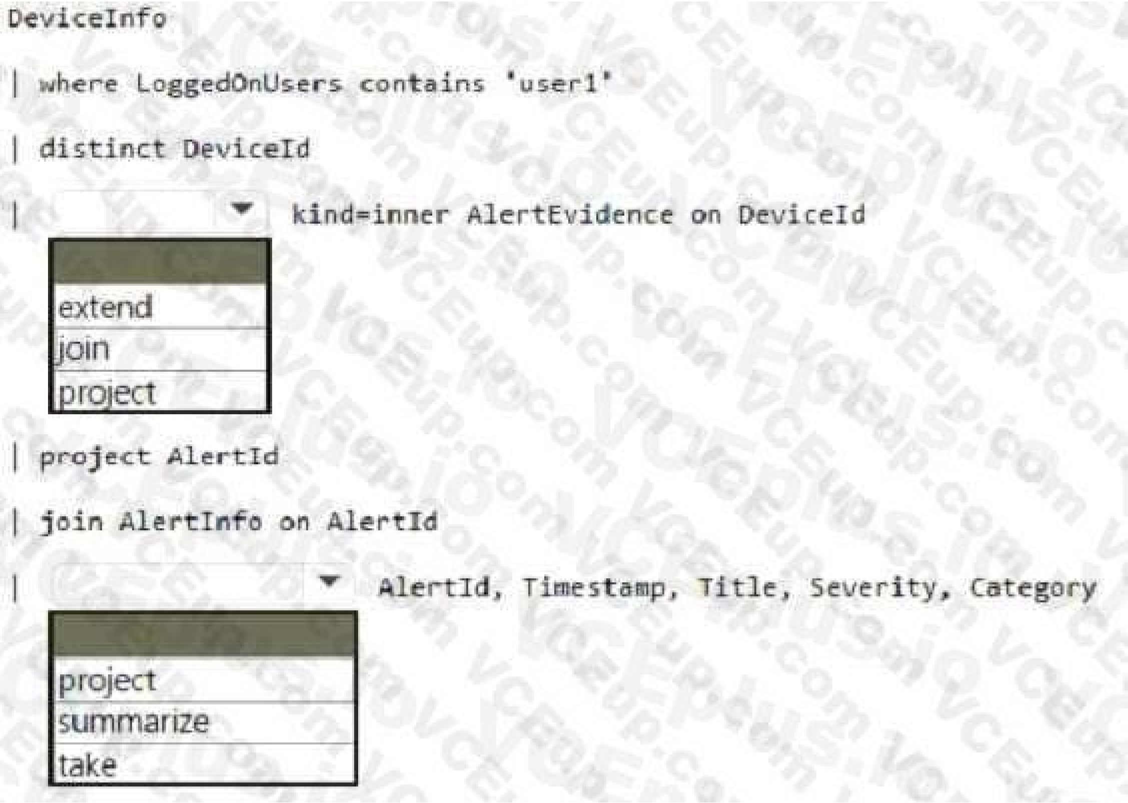
QUESTION 20
HOTSPOT
You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.
You are notified that the account of User1 is compromised.
You need to review the alerts triggered on the devices to which User1 signed in.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



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

Answer Area:



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

Section:

Explanation:

Box 1: join

An inner join.

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

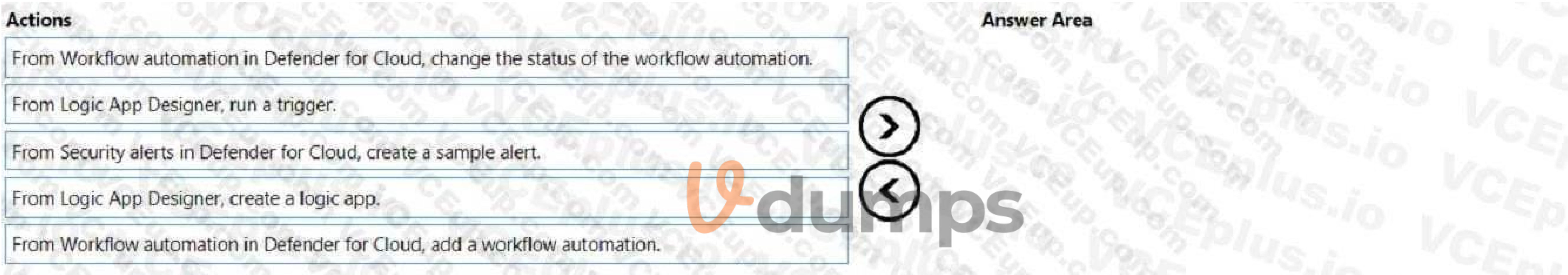
This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

DeviceInfo

//Query for devices that the potentially compromised account has logged onto | where LoggedOnUsers contains '<account-name>' | distinct DeviceId
//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables | join kind=inner AlertEvidence on DeviceId | project AlertId
//List all alerts on devices that user has logged on to
| join AlertInfo on AlertId
| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"
Box 2: project
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-huntingquery-emails-devices?view=o365-worldwide

QUESTION 21
DRAG DROP
You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

From Workflow automation in Defender for Cloud, change the status of the workflow automation.

From Logic App Designer, run a trigger.

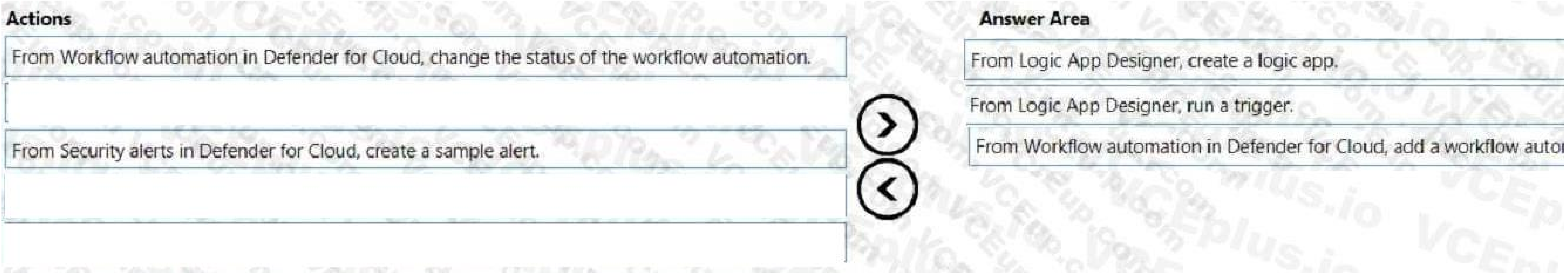
From Security alerts in Defender for Cloud, create a sample alert.

From Logic App Designer, create a logic app.

From Workflow automation in Defender for Cloud, add a workflow automation.

Answer Area

Correct Answer:



Actions

From Workflow automation in Defender for Cloud, change the status of the workflow automation.

From Security alerts in Defender for Cloud, create a sample alert.

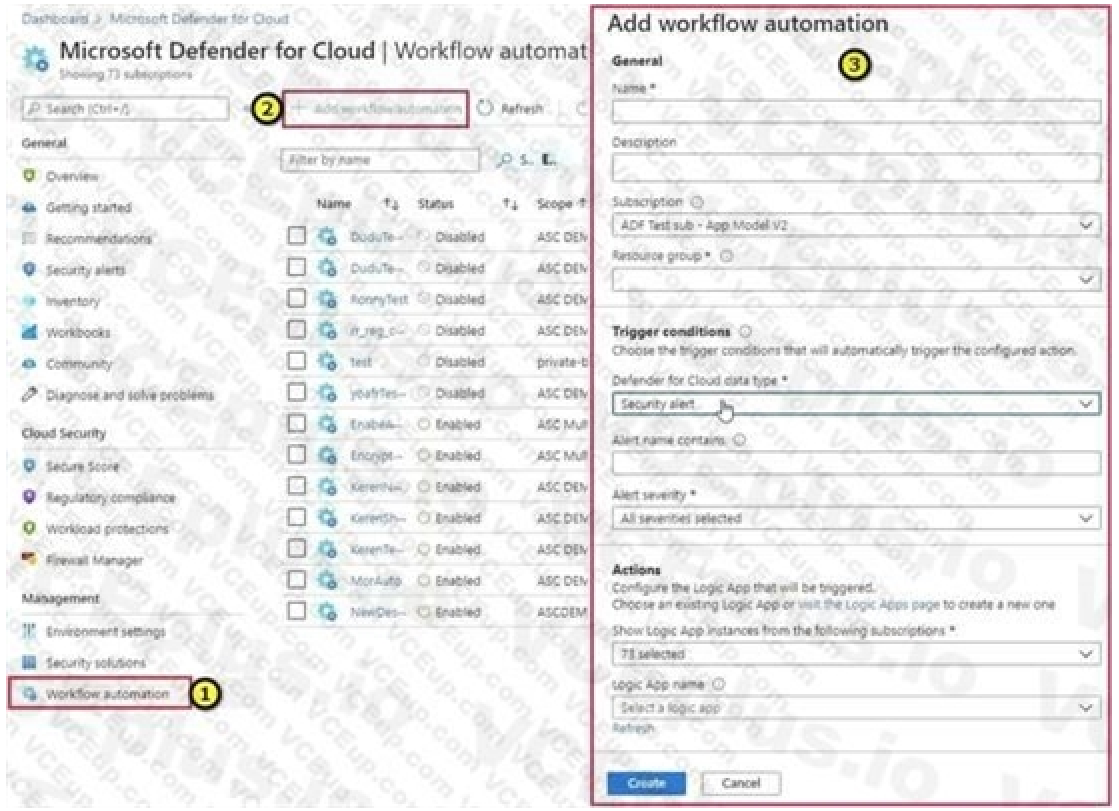
Answer Area

From Logic App Designer, create a logic app.

From Logic App Designer, run a trigger.

From Workflow automation in Defender for Cloud, add a workflow auto

Section:
Explanation:
Step 1: From Logic App Designer, create a logic app.
Create a logic app and define when it should automatically run
1. From Defender for Cloud's sidebar, select Workflow automation.
2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



	Name	Status	Scope
□	DuduTe...	Disabled	ASC DEM
□	DuduTe...	Disabled	ASC DEM
□	RonnyTest	Disabled	ASC DEM
□	rr_reg_c...	Disabled	ASC DEM
□	test	Disabled	private-b
□	yoafrTes...	Disabled	ASC DEM
□	Enable...	Enabled	ASC Mul
□	Encrypt...	Enabled	ASC Mul
□	KerenN...	Enabled	ASC DEM
□	KerenSh...	Enabled	ASC DEM
□	KerenTe...	Enabled	ASC DEM
□	MorAuto	Enabled	ASC DEM
□	NewDes...	Enabled	ASCDEM

Add workflow automation

General

Name *

Description

Subscription: ADF Test sub - App Model V2

Resource group *

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Defender for Cloud data type *: Security alert

Alert name contains

Alert severity *: All severities selected

Actions

Configure the Logic App that will be triggered.

Choose an existing Logic App or visit the Logic Apps page to create a new one

Show Logic App instances from the following subscriptions *: 73 selected

Logic App name: Select a logic app

Refresh

Create Cancel

Here you can enter:

A name and description for the automation.

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

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

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

4. Etc.

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

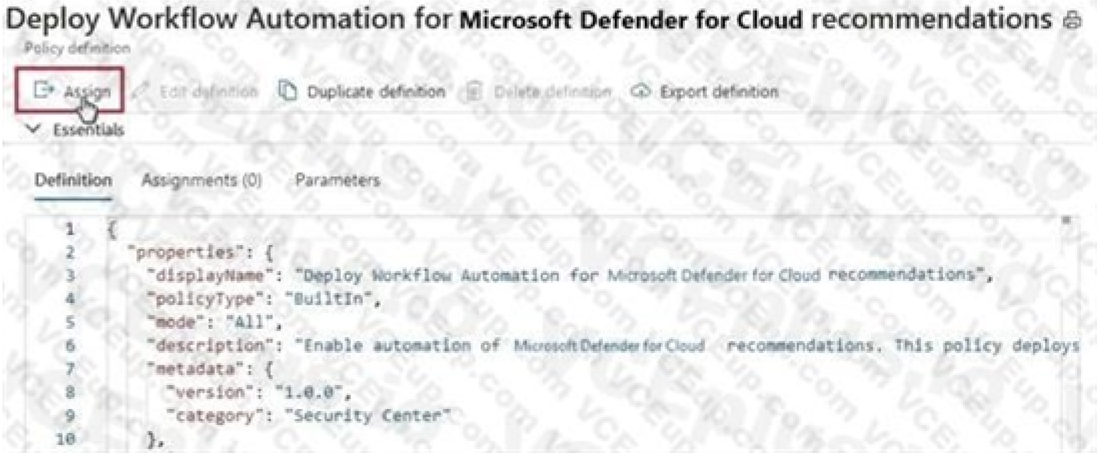
Manually trigger a Logic App

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

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

Configure workflow automation at scale using the supplied policies

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



```
{
  "properties": {
    "displayName": "Deploy Workflow Automation for Microsoft Defender for Cloud recommendations",
    "policyType": "BuiltIn",
    "mode": "All",
    "description": "Enable automation of Microsoft Defender for Cloud  recommendations. This policy deploys
    "metadata": {
      "version": "1.0.0",
      "category": "Security Center"
    },
```

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

QUESTION 22

HOTSPOT

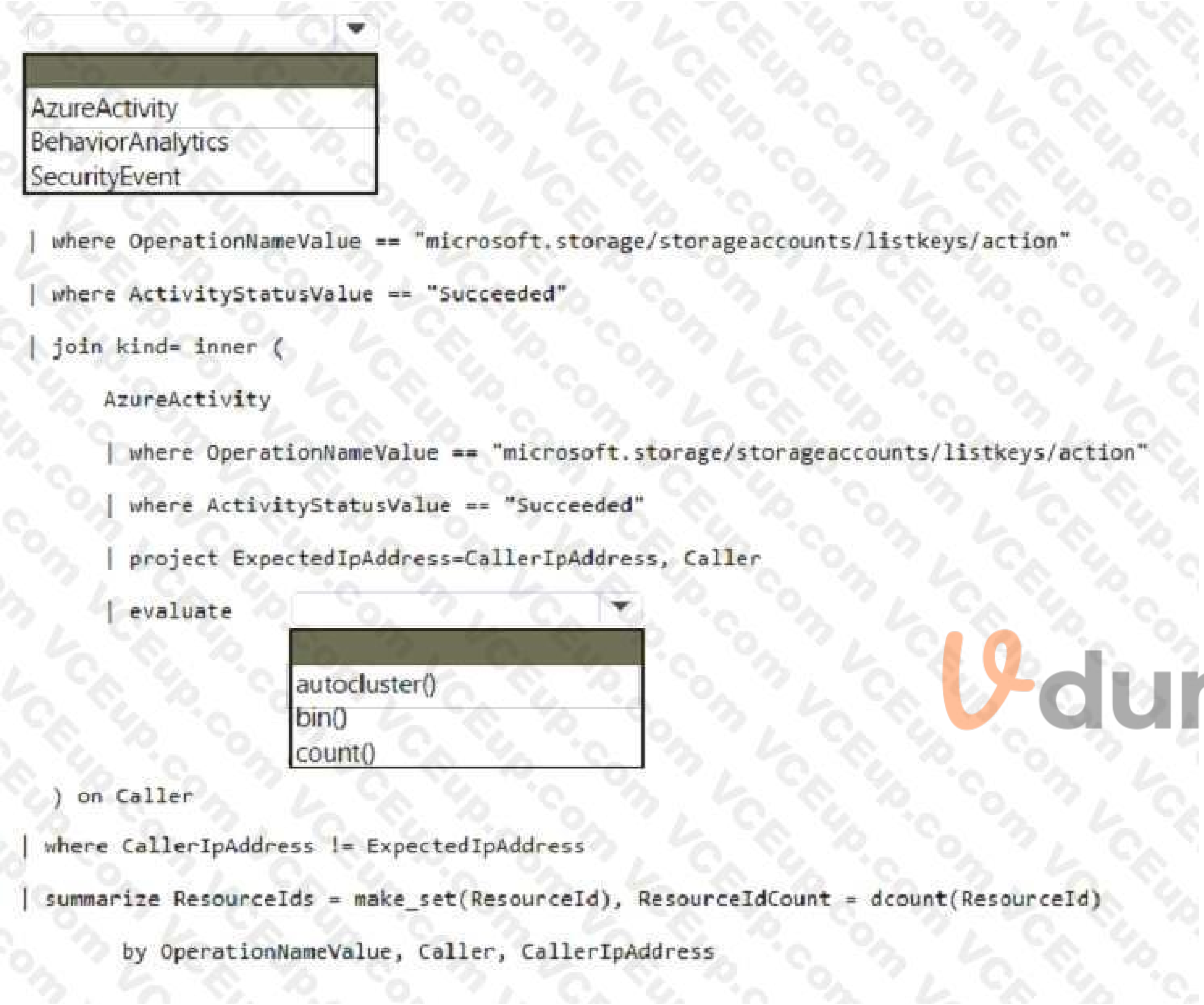
You have a Microsoft Sentinel workspace named sws1.

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

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

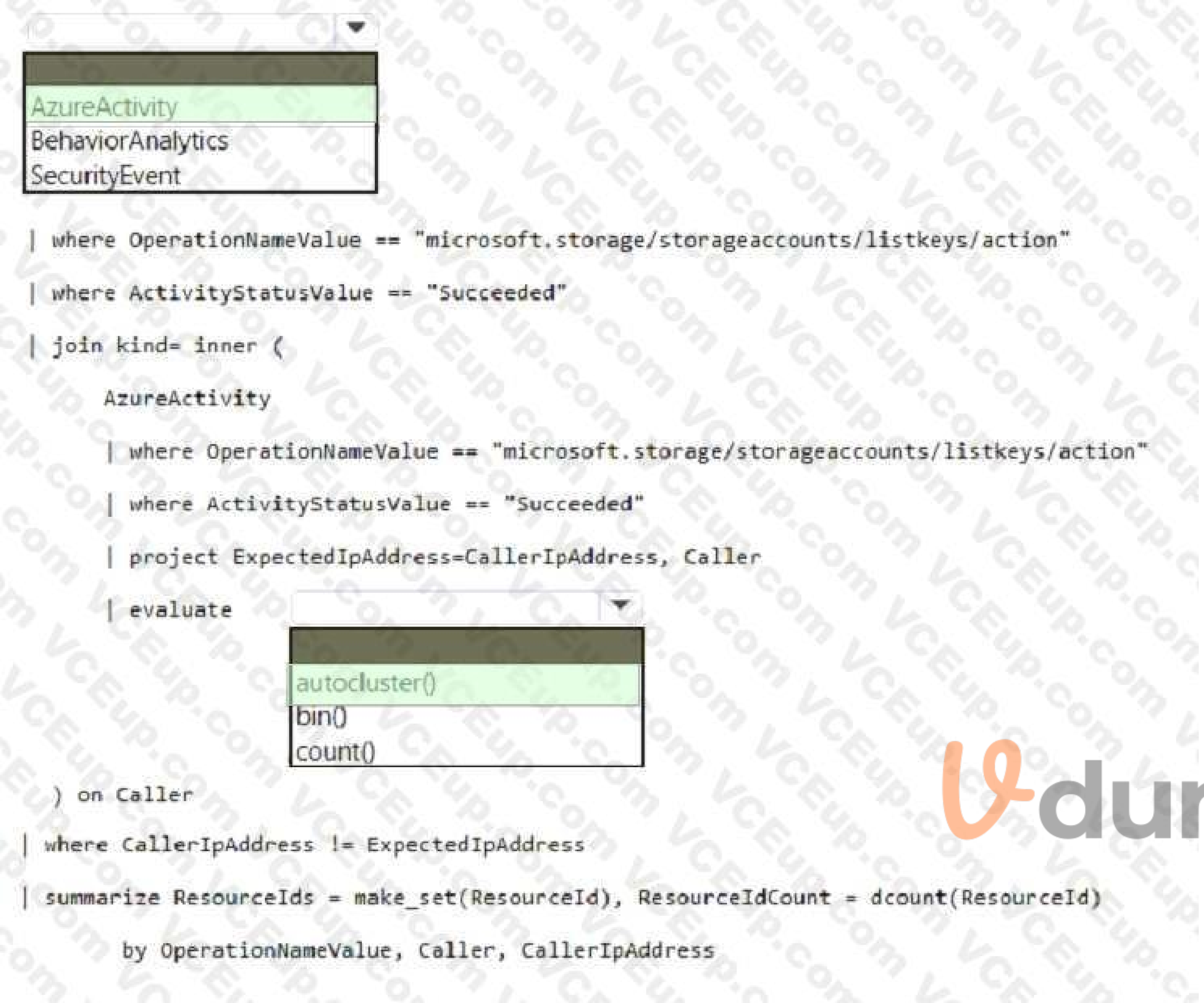
NOTE: Each correct selection is worth one point.

Hot Area:



```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
      | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
      | where ActivityStatusValue == "Succeeded"
      | project ExpectedIpAddress=CallerIpAddress, Caller
      | evaluate
 ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
      by OperationNameValue, Caller, CallerIpAddress
```

Answer Area:



```
[            ▼]
 AzureActivity
 BehaviorAnalytics
 SecurityEvent

| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
    AzureActivity
     | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
     | where ActivityStatusValue == "Succeeded"
     | project ExpectedIpAddress=CallerIpAddress, Caller
     | evaluate [            ▼]
                 autocluster()
                 bin()
                 count()
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
      by OperationNameValue, Caller, CallerIpAddress
```

Section:

Explanation:

Box 1: AzureActivity The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:

Box 2: autocluster()

Example: description: | 'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.

The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.

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

```
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds =
make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller,
CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress
```

Reference: https://github.com/Azure/Azure-Sentinel/blob/master/Hunting%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.yaml

QUESTION 23

DRAG DROP

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

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

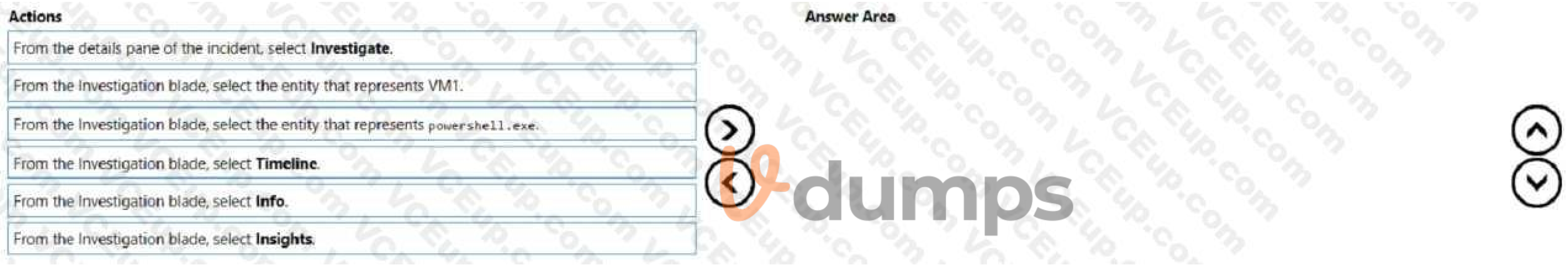
You need to investigate the incident, identify which event triggered the alert, and identify whether the following actions occurred on VM1 after the alert:

The modification of local group memberships

The purging of event logs

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

Select and Place:



Actions

From the details pane of the incident, select **Investigate**.

From the Investigation blade, select the entity that represents VM1.

From the Investigation blade, select the entity that represents `powershell.exe`.

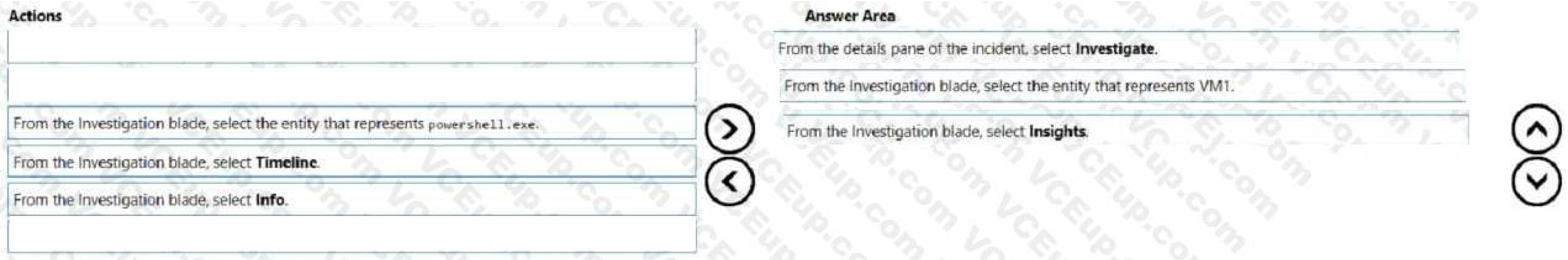
From the Investigation blade, select **Timeline**.

From the Investigation blade, select **Info**.

From the Investigation blade, select **Insights**.

Answer Area

Correct Answer:



Actions

From the Investigation blade, select the entity that represents `powershell.exe`.

From the Investigation blade, select **Timeline**.

From the Investigation blade, select **Info**.

Answer Area

From the details pane of the incident, select **Investigate**.

From the Investigation blade, select the entity that represents VM1.

From the Investigation blade, select **Insights**.

Section:

Explanation:

Step 1: From the Investigation blade, select Insights

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

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

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

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

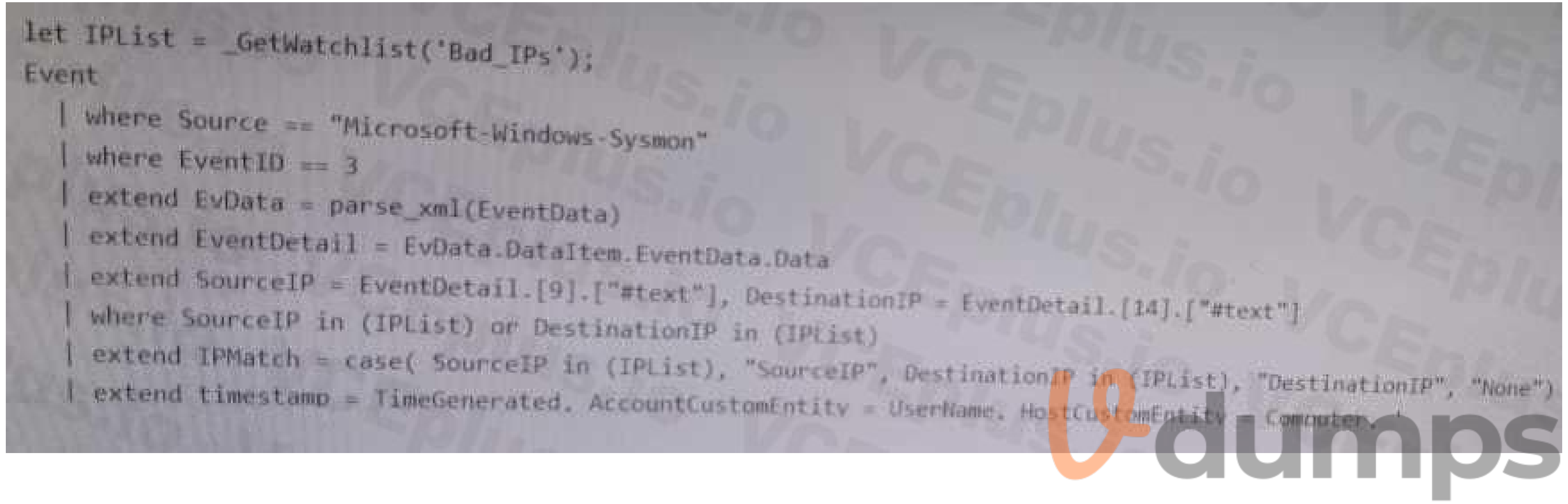
Entity Insights The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

IP Address
Account
Host
URL
Step 3: From the details pane of the incident, select Investigate.
Choose a single incident and click View full details or Investigate.
Reference:
https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

QUESTION 24

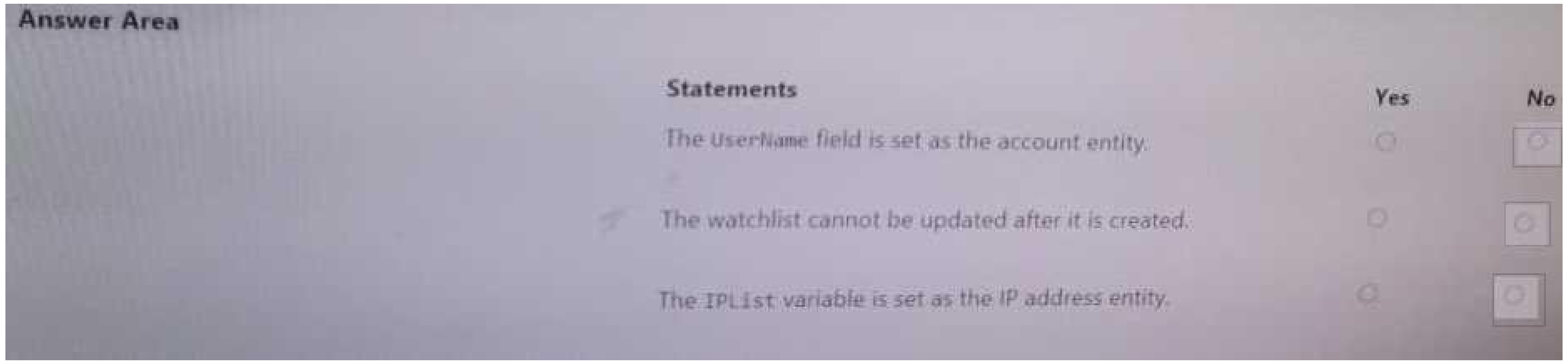
HOTSPOT

You have the following SQL query.



```
let IPList = _GetWatchlist('Bad_IPs');
Event
  | where Source == "Microsoft-Windows-Sysmon"
  | where EventID == 3
  | extend EvData = parse_xml(EventData)
  | extend EventDetail = EvData.DataItem.EventData.Data
  | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
  | where SourceIP in (IPList) or DestinationIP in (IPList)
  | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
  | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer
```

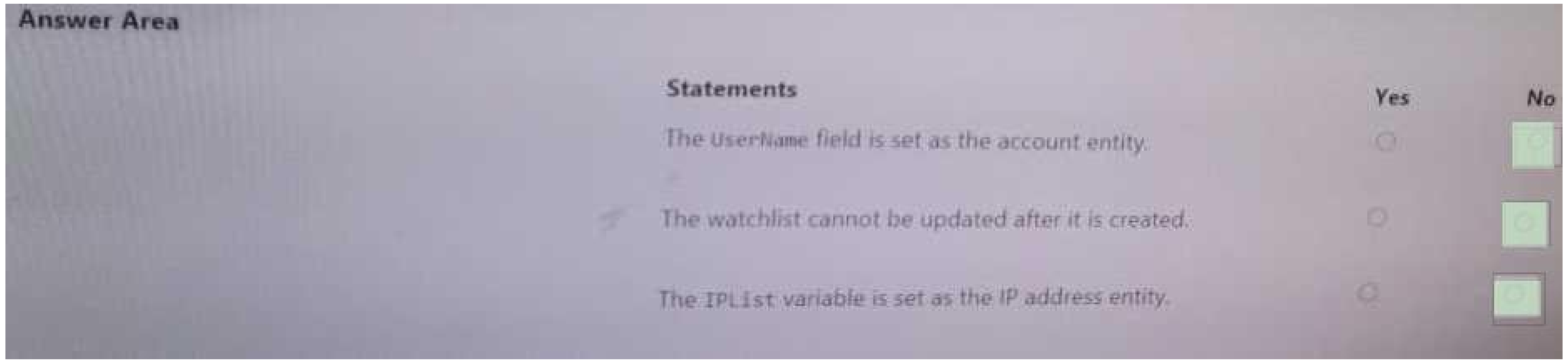
Hot Area:



Answer Area

Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

Answer Area:



Answer Area

Statements	Yes	No
The UserName field is set as the account entity.	○	[✓ ○]
The watchlist cannot be updated after it is created.	○	[✓ ○]
The IPList variable is set as the IP address entity.	○	[✓ ○]

Section:
Explanation:

QUESTION 25
You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.
You need to identify all the changes made to Domain Admins group during the past 30 days.
What should you use?

A. the Azure Active Directory Provisioning Analysis workbook
B. the Overview settings of Insider risk management
C. the Modifications of sensitive groups report in Microsoft Defender for Identity
D. the identity security posture assessment in Microsoft Defender for Cloud Apps

Correct Answer: C
Section:

QUESTION 26
You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.
You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort
Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting
B. Threat analytics
C. Incidents & alerts
D. Learning hub

Correct Answer: B
Section:
Explanation:
To review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription, you should use the Threat Analytics blade in the Microsoft 365 Defender portal. The Threat Analytics blade provides insights into attack techniques, configuration vulnerabilities, and suspicious activities, and it can help you identify risks and prioritize threats in your environment.
Reference:Ă, https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defenderthreat-analytics

QUESTION 27
You have a Microsoft 365 subscription that uses Microsoft 365 Defender A remediation action for an automated investigation quarantines a file across multiple devices. You need to mark the file as safe and remove the file from quarantine on the devices. What should you use m the Microsoft 365 Defender portal?

A. From Threat tracker, review the queries.
B. From the History tab in the Action center, revert the actions.
C. From the investigation page, review the AIR processes.
D. From Quarantine from the Review page, modify the rules.

Correct Answer: B
Section:

QUESTION 28
You have a Microsoft Sentinel workspace named Workspaces
You need to exclude a built-in. source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser.
What should you create in Workspace1?

A. a workbook
B. a hunting query
C. a watchlist
D. an analytic rule

Correct Answer: D
Section:
Explanation:
To exclude a built-in, source-specific Advanced Security Information Model (ASIM) parser from a built-in unified ASIM parser, you should create an analytic rule in the Microsoft Sentinel workspace.
An analytic rule allows you to customize the behavior of the unified ASIM parser and exclude specific source-specific parsers from being used. Reference:Ă, https://docs.microsoft.com/en-us/azure/sentinel/analytics-create-analytic-rule

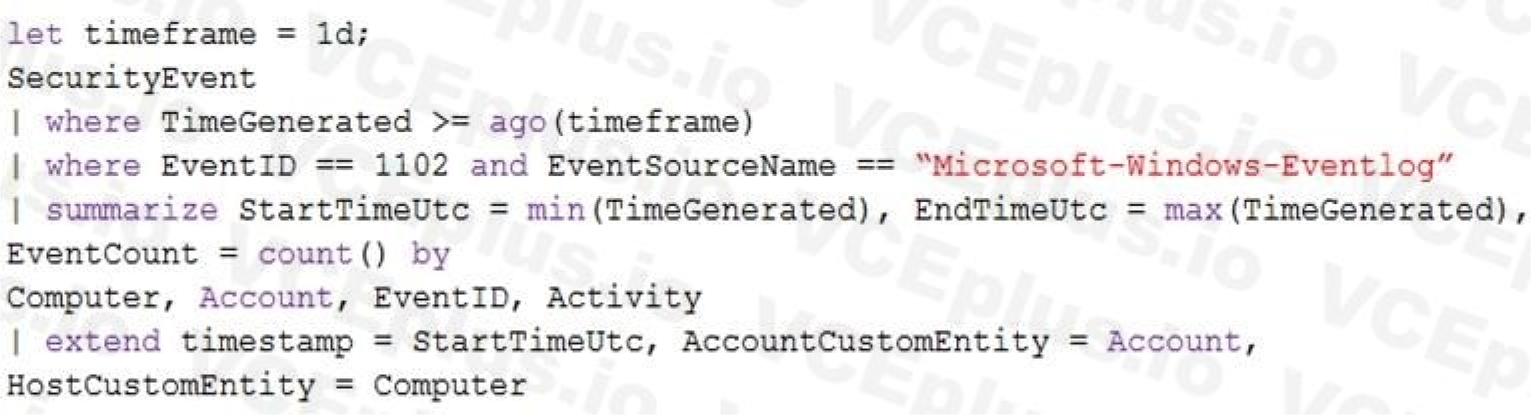
QUESTION 29
Your company uses Microsoft Sentinel
A new security analyst reports that she cannot assign and resolve incidents in Microsoft Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

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

Correct Answer: A
Section:
Explanation:
The Microsoft Sentinel Responder role allows users to investigate, triage, and resolve security incidents, which includes the ability to assign incidents to other users. This role is designed to provide the necessary permissions for incident management and response while still adhering to the principle of least privilege. Other roles such as Logic App Contributor and Microsoft Sentinel Contributor would have more permissions than necessary and may not be suitable for the analyst's needs. Microsoft Sentinel Reader role is not sufficient as it doesn't have permission to assign and resolve incidents.
Reference:Ă, https://docs.microsoft.com/en-us/azure/sentinel/role-based-access-control-rbac

QUESTION 30
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. a workbook
B. a hunting query
C. a notebook
D. a playbook

Correct Answer: A
Section:
Explanation:
A workbook is a data-driven interactive report in Microsoft Sentinel. You can use workbooks to create custom reports based on data from your Azure subscription. Reference:
https://docs.microsoft.com/en-us/azure/sentinel/workbooks-overview

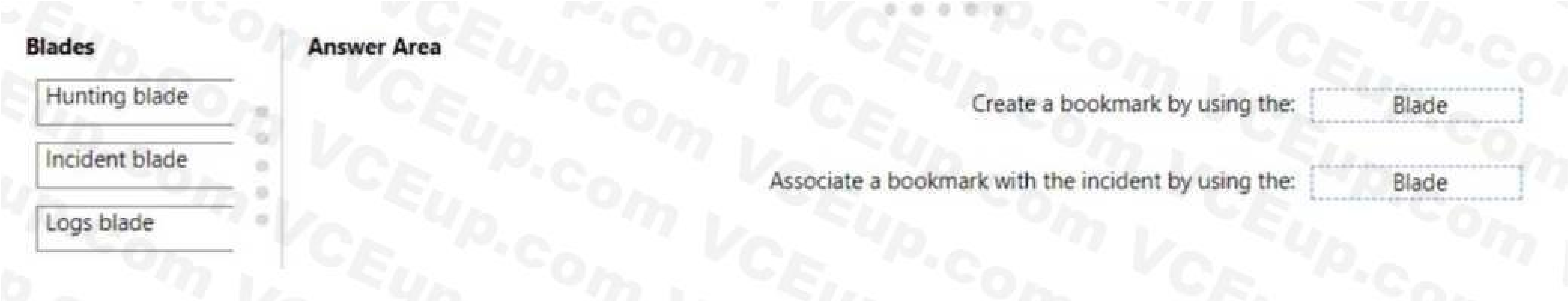
QUESTION 31
You create an Azure subscription.
You enable Microsoft Defender for Cloud for the subscription.
You need to use Defender for Cloud to protect on-premises computers.
What should you do on the on-premises computers?

A. Configure the Hybrid Runbook Worker role.
B. Install the Connected Machine agent.
C. Install the Log Analytics agent
D. Install the Dependency agent.

Correct Answer: C
Section:
Explanation:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboardmachines?pivots=azure-arc

QUESTION 32
DRAG DROP
You have a Microsoft Sentinel workspace that contains an Azure AD data connector.
You need to associate a bookmark with an Azure AD-related incident.
What should you do? To answer, drag the appropriate blades to the correct tasks. Each blade 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:



Blades

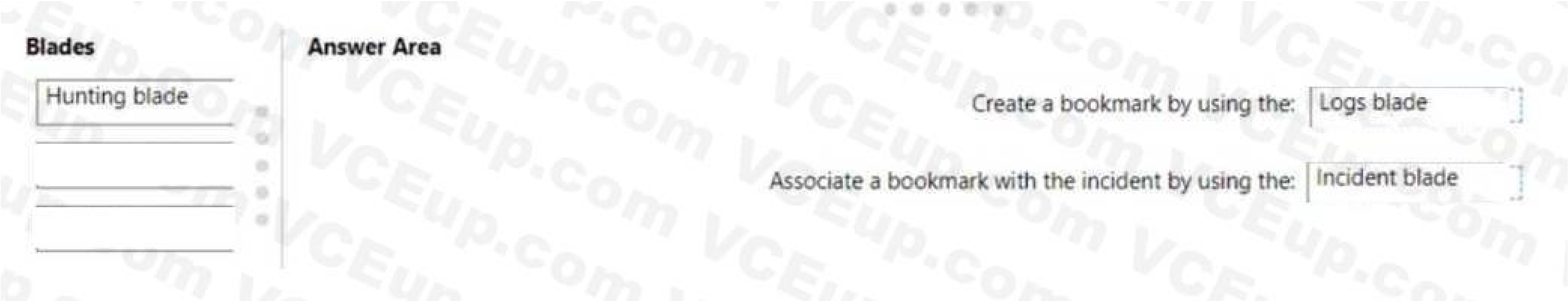
- Hunting blade
- Incident blade
- Logs blade

Answer Area

Create a bookmark by using the: Blade

Associate a bookmark with the incident by using the: Blade

Correct Answer:



Blades

- Hunting blade

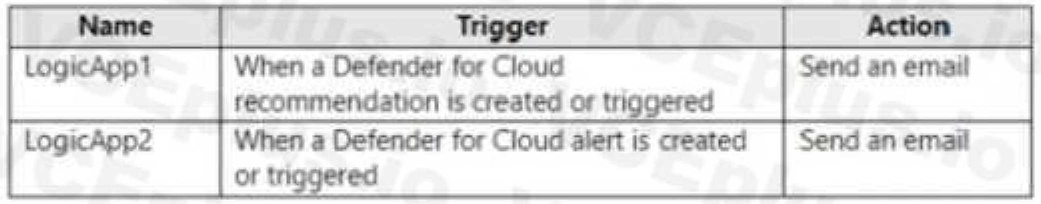
Answer Area

Create a bookmark by using the: Logs blade

Associate a bookmark with the incident by using the: Incident blade

Section:
Explanation:

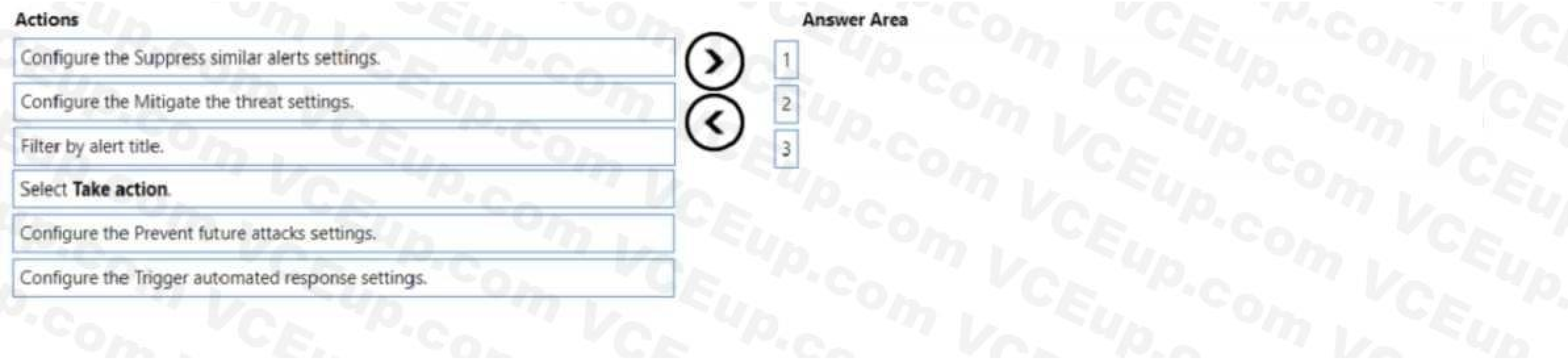
QUESTION 33
DRAG DROP
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled You configure the Azure logic apps shown in the following table.



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

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

Filter by alert title.

Select **Take action**.

Configure the Prevent future attacks settings.

Configure the Trigger automated response settings.

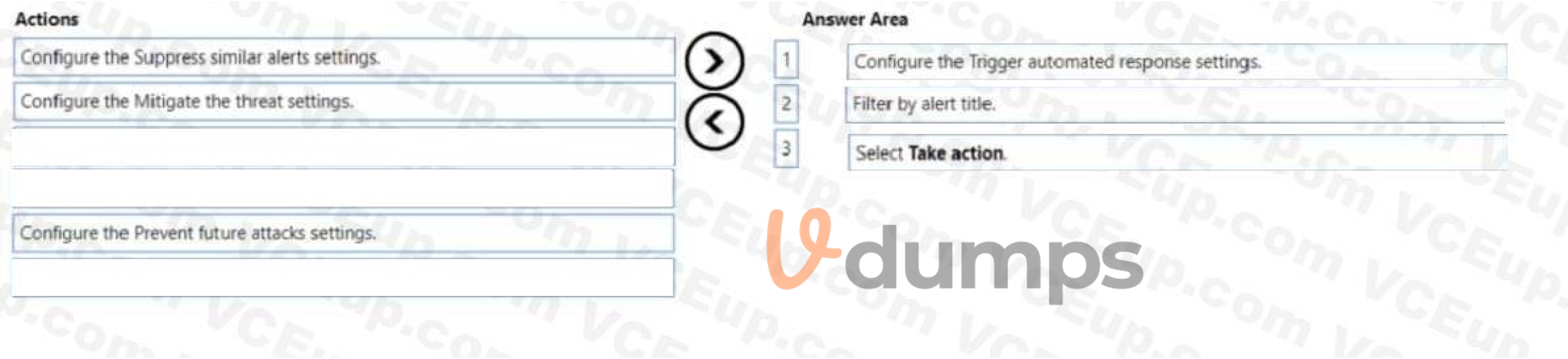
Answer Area

1

2

3

Correct Answer:



Actions

Configure the Suppress similar alerts settings.

Configure the Mitigate the threat settings.

Configure the Prevent future attacks settings.

Answer Area

1 Configure the Trigger automated response settings.

2 Filter by alert title.

3 Select **Take action**.

Section:
Explanation:

QUESTION 34

DRAG DROP

You have 50 on-premises servers.

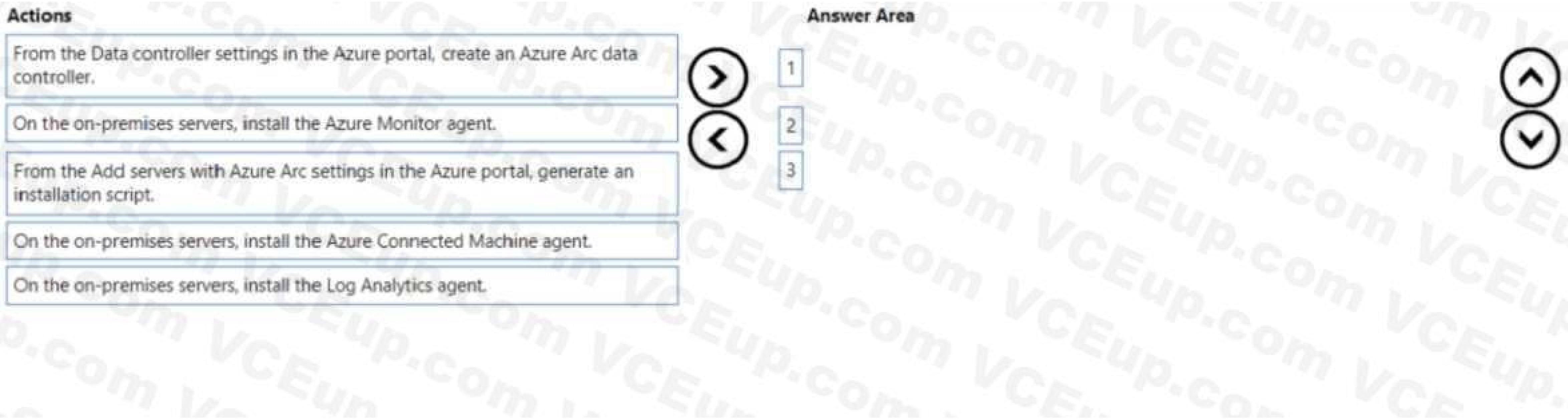
You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

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

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

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

Select and Place:



Actions

From the Data controller settings in the Azure portal, create an Azure Arc data controller.

On the on-premises servers, install the Azure Monitor agent.

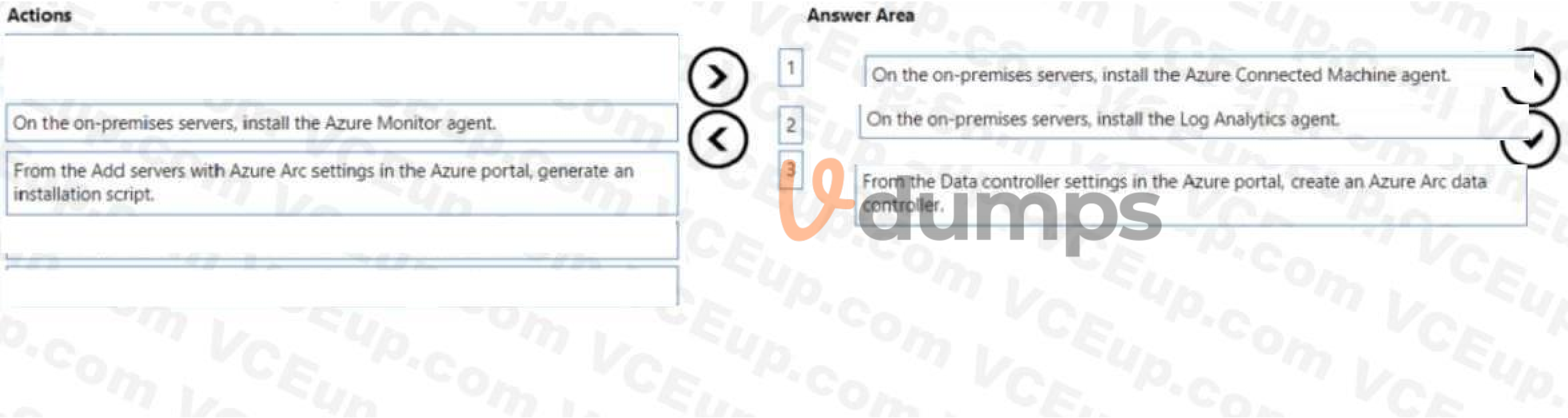
From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

On the on-premises servers, install the Azure Connected Machine agent.

On the on-premises servers, install the Log Analytics agent.

Answer Area

Correct Answer:



Actions

On the on-premises servers, install the Azure Monitor agent.

From the Add servers with Azure Arc settings in the Azure portal, generate an installation script.

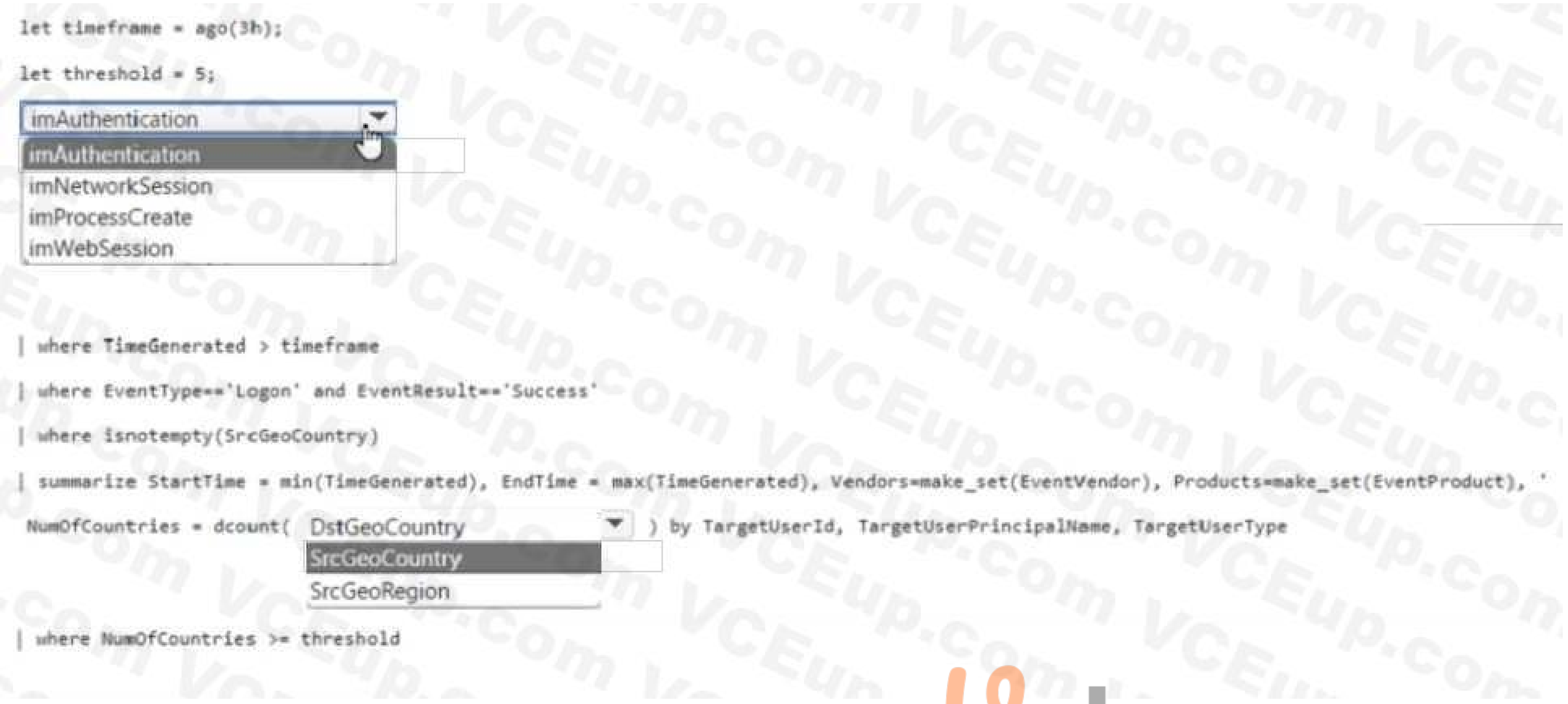
Answer Area

1. On the on-premises servers, install the Azure Connected Machine agent.
2. On the on-premises servers, install the Log Analytics agent.
3. From the Data controller settings in the Azure portal, create an Azure Arc data controller.

Section:
Explanation:
To configure Defender for Cloud to support the on-premises servers, you should perform the following three actions in sequence:
On the on-premises servers, install the Azure Connected Machine agent.
On the on-premises servers, install the Log Analytics agent.
From the Data controller settings in the Azure portal, create an Azure Arc data controller.
Once these steps are completed, the on-premises servers will be able to communicate with the
Azure Defender for Cloud deployment and will be able to support threat and vulnerability management as well as data collection rules. Reference: https://docs.microsoft.com/enus/azure/security-center/deploy-azure-security-center#on-premises-deployment

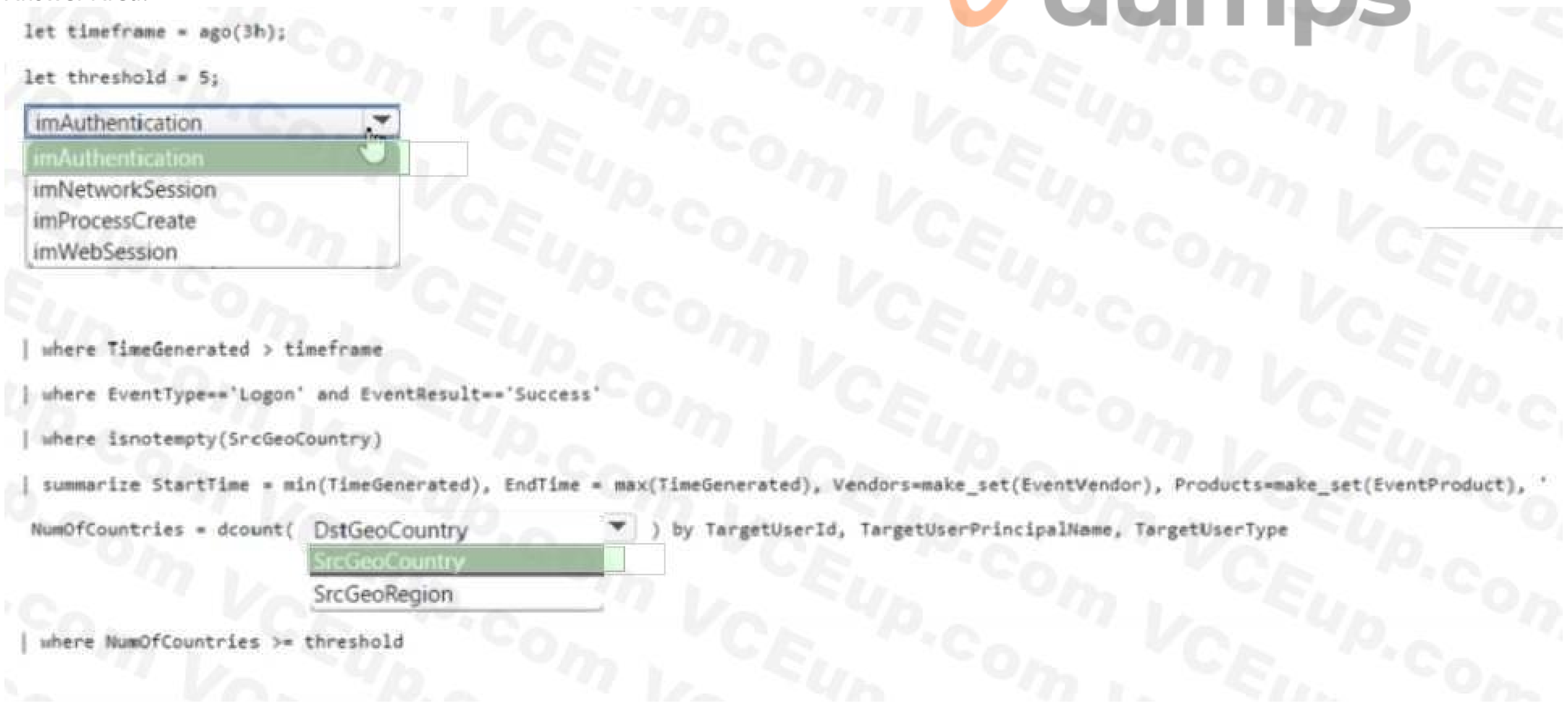
QUESTION 35
HOTSPOT
You have a Microsoft Sentinel workspace.
You need to create a KQL query that will identify successful sign-ins from multiple countries during the last three hours.
How should you complete the query? To answer, select the appropriate options in the answer area.
NOTE Each correct selection is worth one point

Hot Area:



```
let timeframe = ago(3h);

let threshold = 5;

imAuthentication ▼

| where TimeGenerated > timeframe

| where EventType=='Logon' and EventResult=='Success'

| where isnotempty(SrcGeoCountry)

| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '

NumOfCountries = dcount( DstGeoCountry ▼ ) by TargetUserId, TargetUserPrincipalName, TargetUserType

| where NumOfCountries >= threshold
```

Answer Area:



```
let timeframe = ago(3h);

let threshold = 5;

imAuthentication ▼

| where TimeGenerated > timeframe

| where EventType=='Logon' and EventResult=='Success'

| where isnotempty(SrcGeoCountry)

| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), Vendors=make_set(EventVendor), Products=make_set(EventProduct), '

NumOfCountries = dcount( DstGeoCountry ▼ ) by TargetUserId, TargetUserPrincipalName, TargetUserType

| where NumOfCountries >= threshold
```

Section:

Explanation:

QUESTION 36

HOTSPOT

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

You create an Azure logic app named LA1.

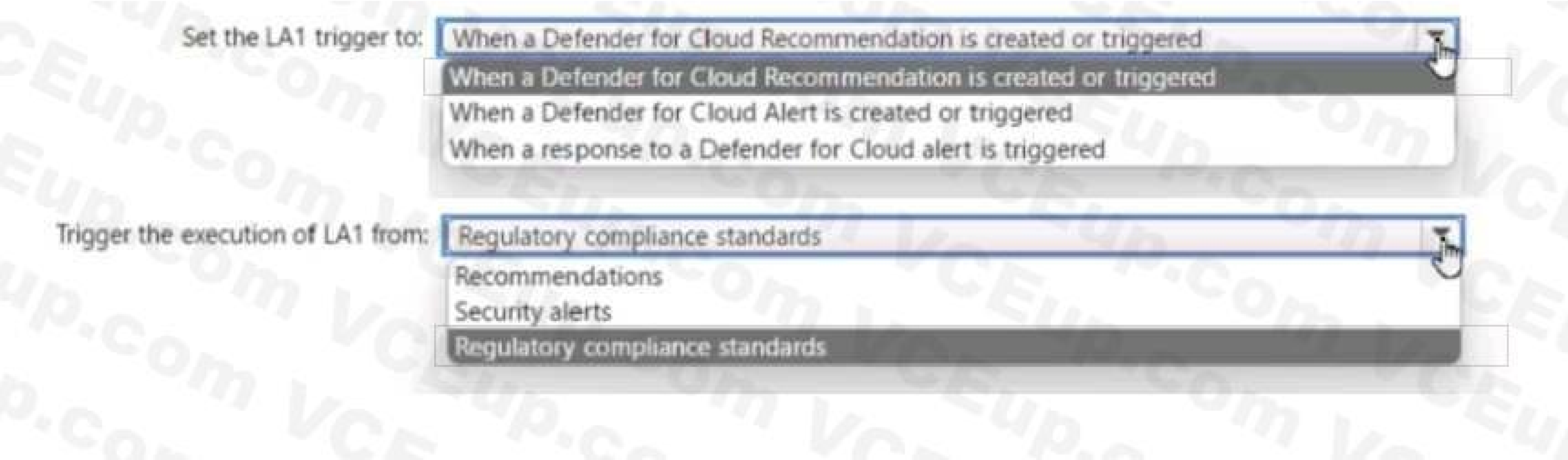
You plan to use LA1 to automatically remediate security risks detected in Defenders for Cloud.

You need to test LA1 in Defender for Cloud.

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

NOTE: Each correct selection is worth one point.

Hot Area:



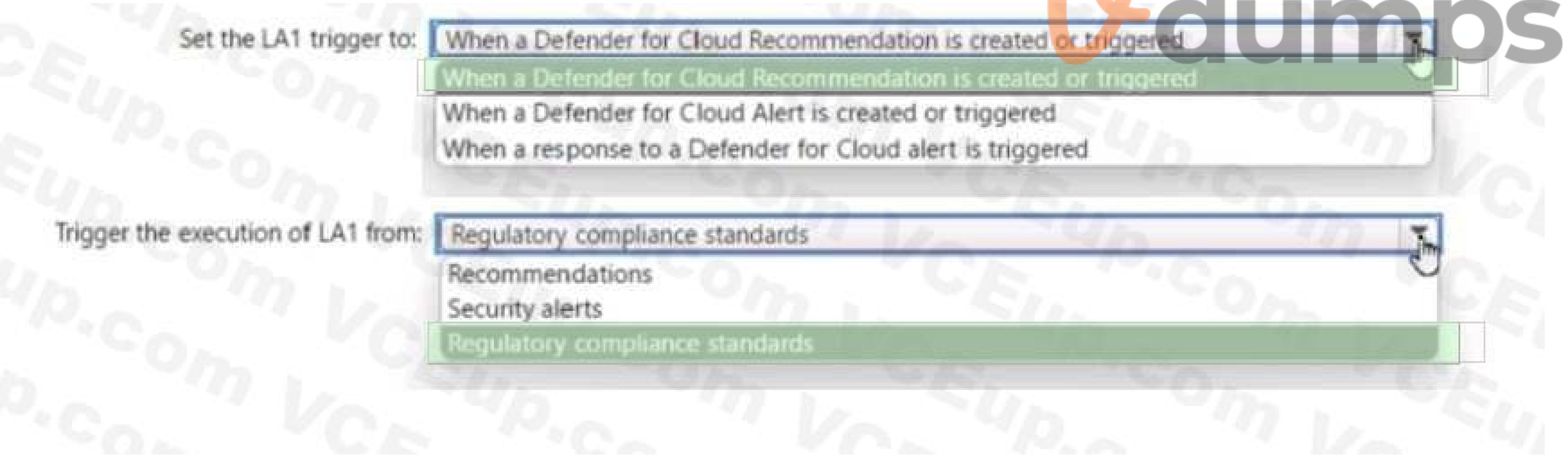
Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered

- When a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards

- Recommendations
- Security alerts
- Regulatory compliance standards

Answer Area:



Set the LA1 trigger to: When a Defender for Cloud Recommendation is created or triggered

- [✓ When a Defender for Cloud Recommendation is created or triggered]
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from: Regulatory compliance standards

- Recommendations
- Security alerts
- [✓ Regulatory compliance standards]

Section:

Explanation:

QUESTION 37

DRAG DROP

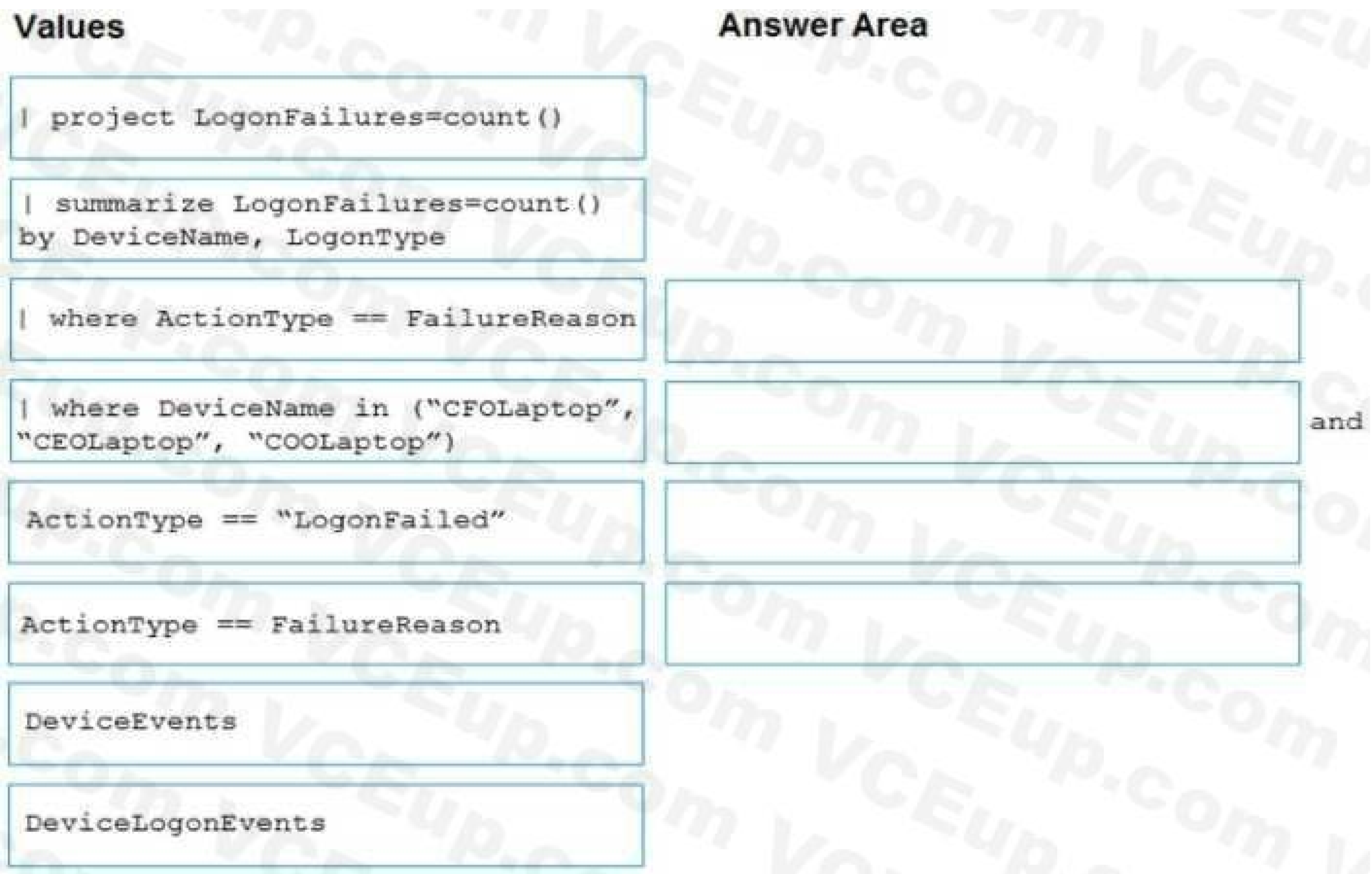
You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop. CEOLaptop, and COOLaptop.

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

NOTE Each correct selection is worth one point

Select and Place:



Values

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

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

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

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

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

```
ActionType == FailureReason
```

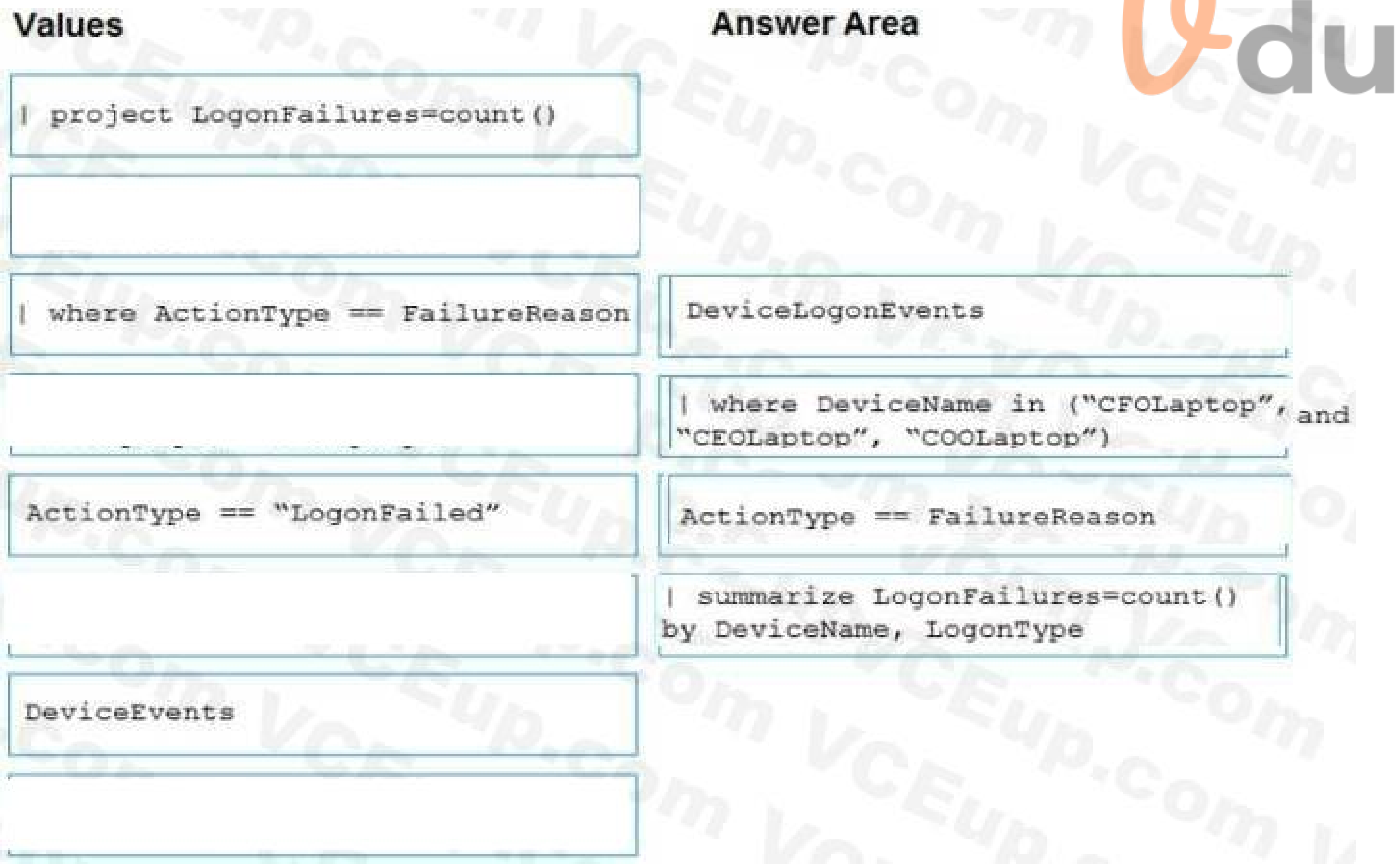
```
DeviceEvents
```

```
DeviceLogonEvents
```

Answer Area

and

Correct Answer:



Values

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

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

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

```
DeviceEvents
```

Answer Area

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

and

Section:

Explanation:

QUESTION 38

HOTSPOT

You have an Azure subscription.

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

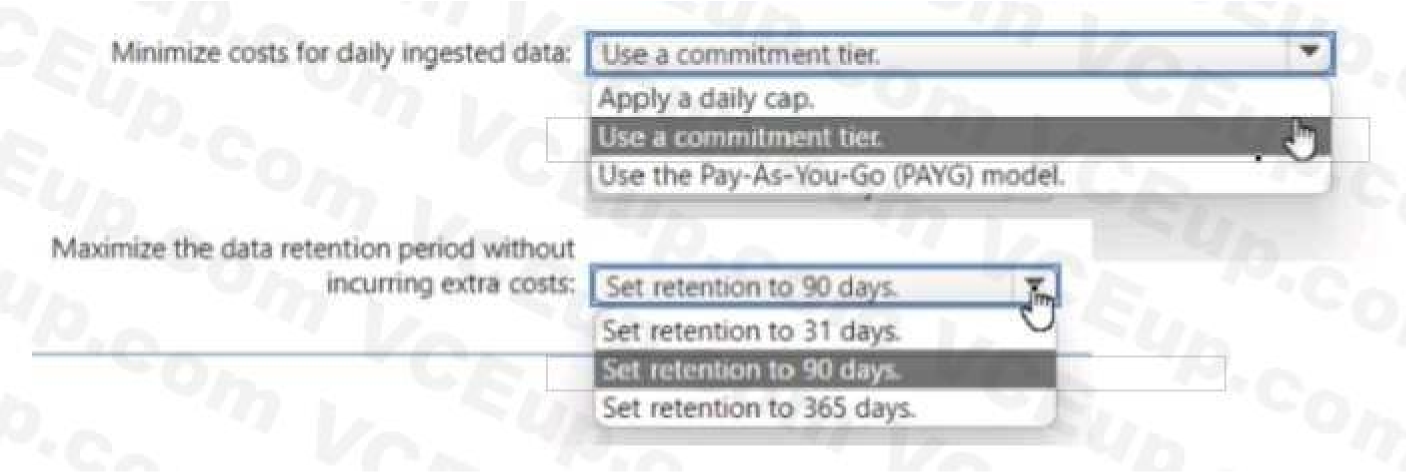
You need to configure storage for the workspace. The solution must meet the following requirements:

• Minimize costs for daily ingested data.

• Maximize the data retention period without incurring extra costs.

What should you do for each requirement? To answer, select the appropriate options in the answer are a. NOTE Each correct selection is worth one point.

Hot Area:



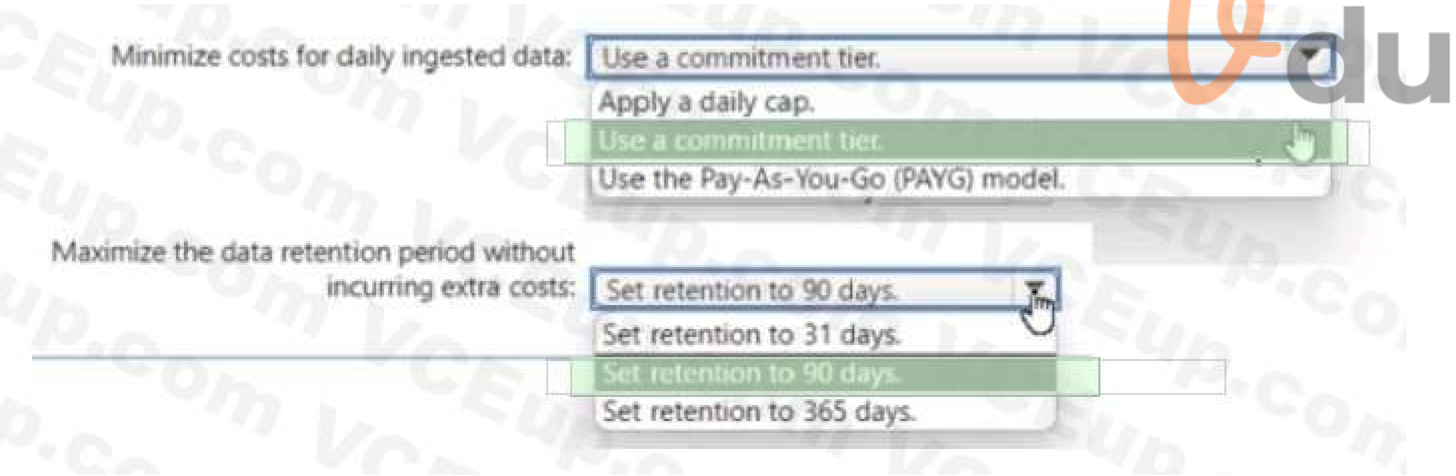
Minimize costs for daily ingested data: Use a commitment tier.

Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.

Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

Answer Area:



Minimize costs for daily ingested data: Use a commitment tier.

Apply a daily cap.
Use a commitment tier.
Use the Pay-As-You-Go (PAYG) model.

Maximize the data retention period without incurring extra costs: Set retention to 90 days.

Set retention to 31 days.
Set retention to 90 days.
Set retention to 365 days.

Section:

Explanation:

QUESTION 39

HOTSPOT

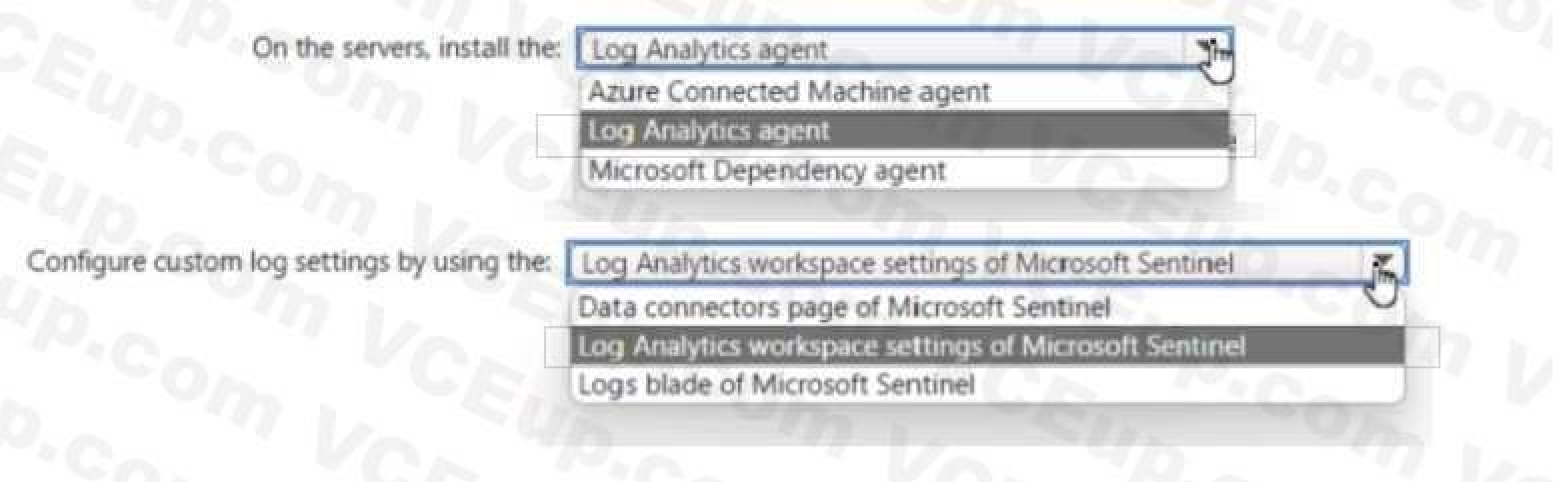
Your on-premises network contains 100 servers that run Windows Server.

You have an Azure subscription that uses Microsoft Sentinel.

You need to upload custom logs from the on-premises servers to Microsoft Sentinel.

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

Hot Area:



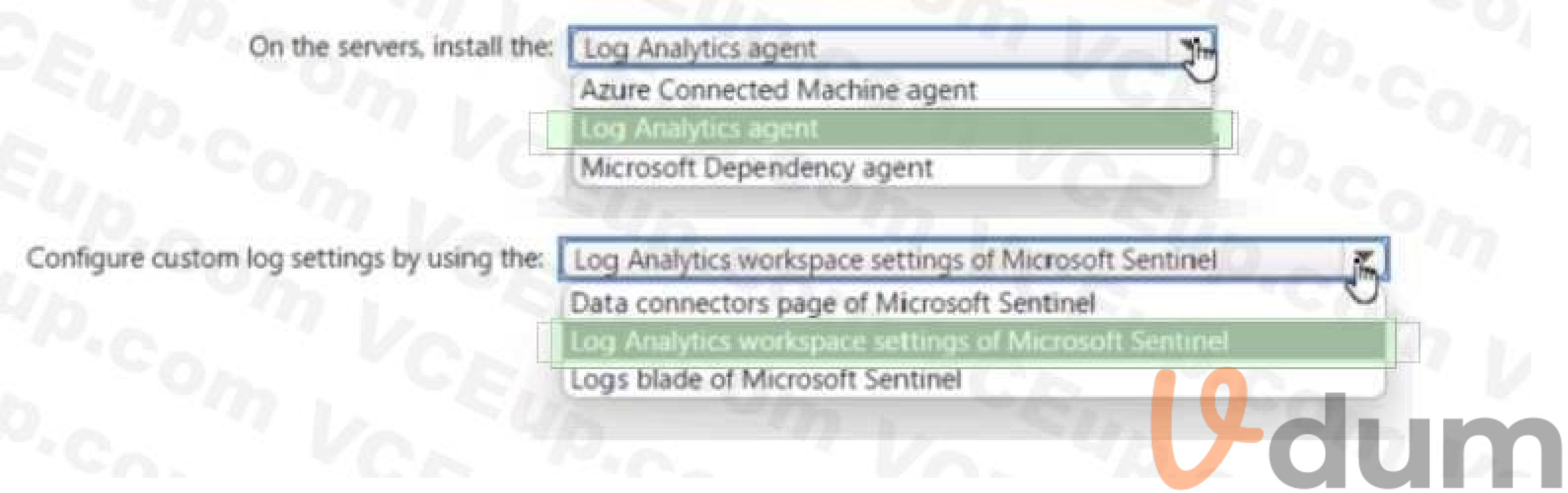
On the servers, install the: Log Analytics agent

- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

Answer Area:



On the servers, install the: Log Analytics agent

- Azure Connected Machine agent
- Log Analytics agent
- Microsoft Dependency agent

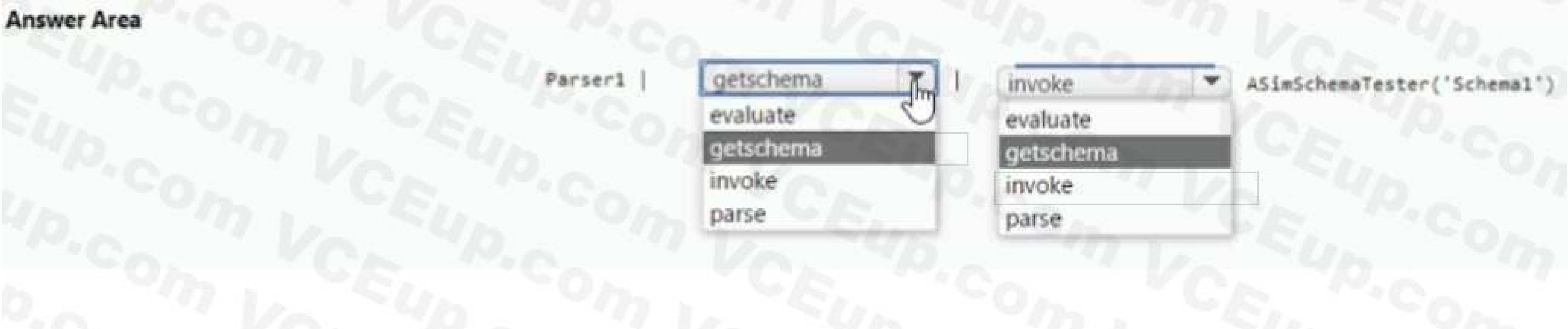
Configure custom log settings by using the: Log Analytics workspace settings of Microsoft Sentinel

- Data connectors page of Microsoft Sentinel
- Log Analytics workspace settings of Microsoft Sentinel
- Logs blade of Microsoft Sentinel

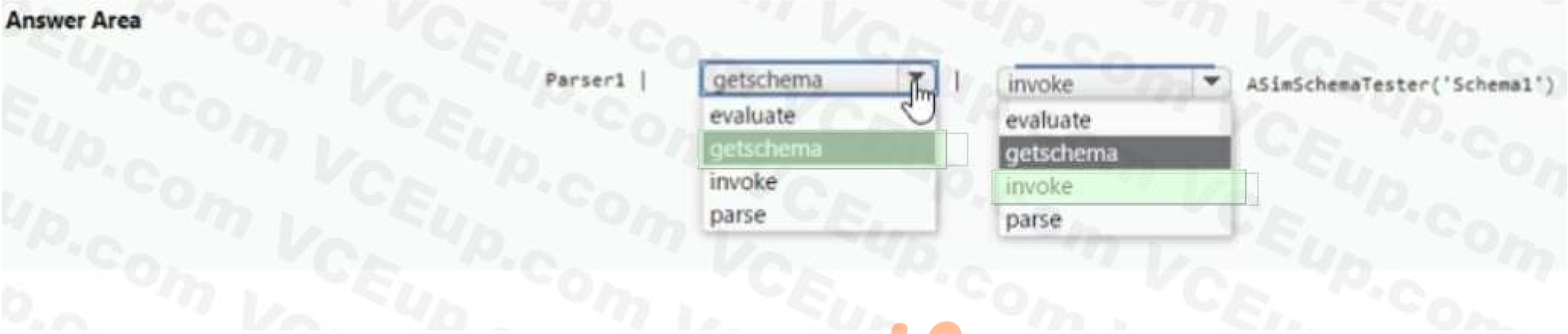
Section:
Explanation:
To upload custom logs from the on-premises servers to Microsoft Sentinel, you should install the Log
Analytics agent on each of the 100 servers. The Log Analytics agent is a lightweight agent that runs on the server and allows it to connect to the cloud-based Microsoft Defender Security Center. Once installed, the agent will allow the Microsoft Sentinel service to collect and analyze the custom log data from the servers.

QUESTION 40
HOTSPOT
You have a Microsoft Sentinel workspace
You develop a custom Advanced Security information Model (ASIM) parser named Parser1 that produces a schema named Schema1.
You need to validate Schema1.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

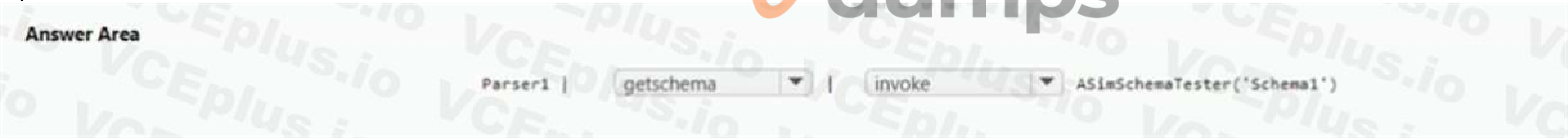
Hot Area:



Answer Area:



Section:
Explanation:



```
Parser1 | getschema | invoke ASimSchemaTester('Schema1')
```

QUESTION 41

HOTSPOT

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

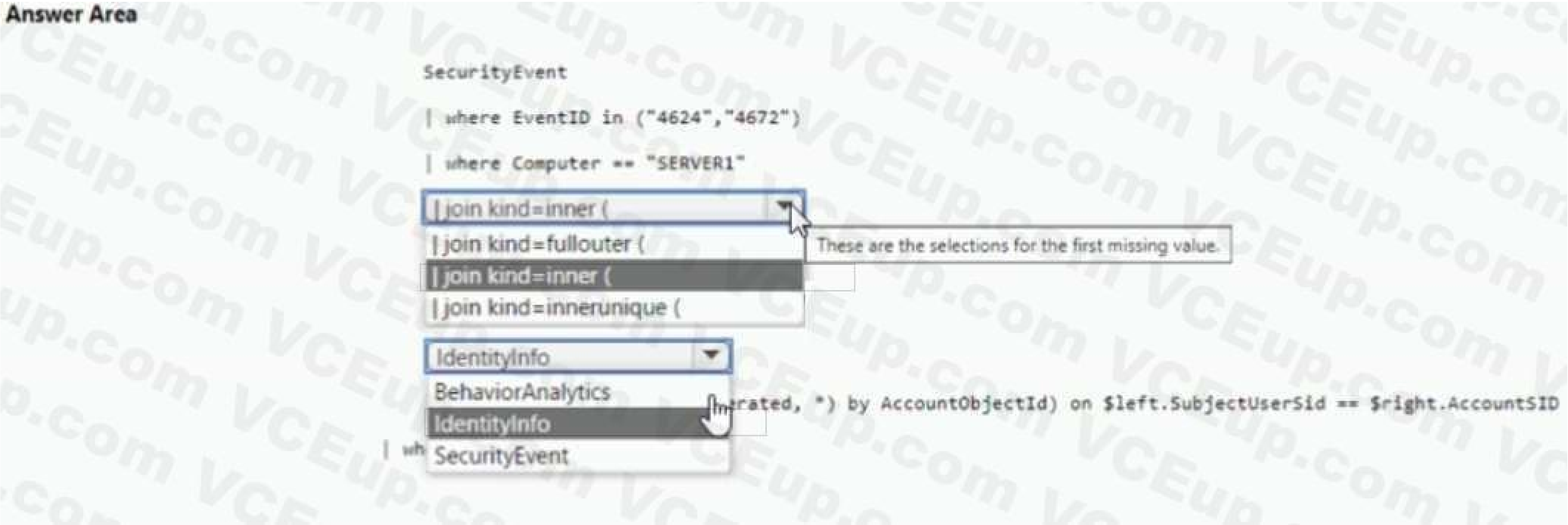
You need to identify all the log entries that relate to security-sensitive user actions performed on a server named Server1. The solution must meet the following requirements:

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

• Minimize the number of false positives.

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

Hot Area:

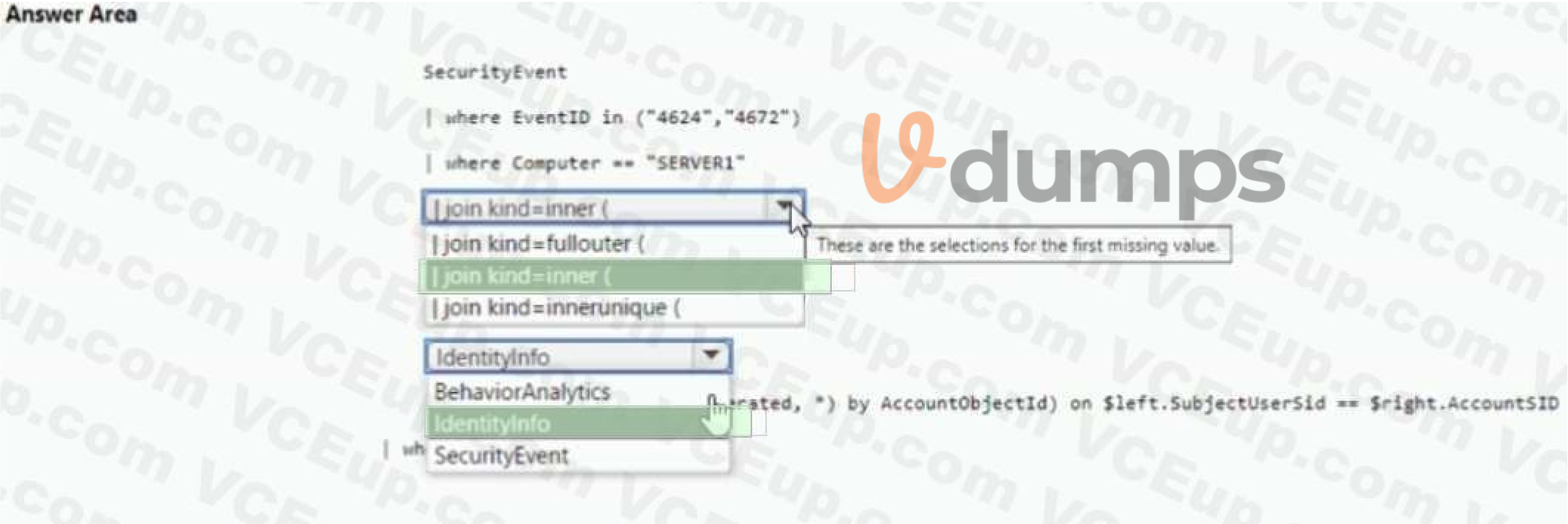


Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
```

```
erated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| wh
```

Answer Area:



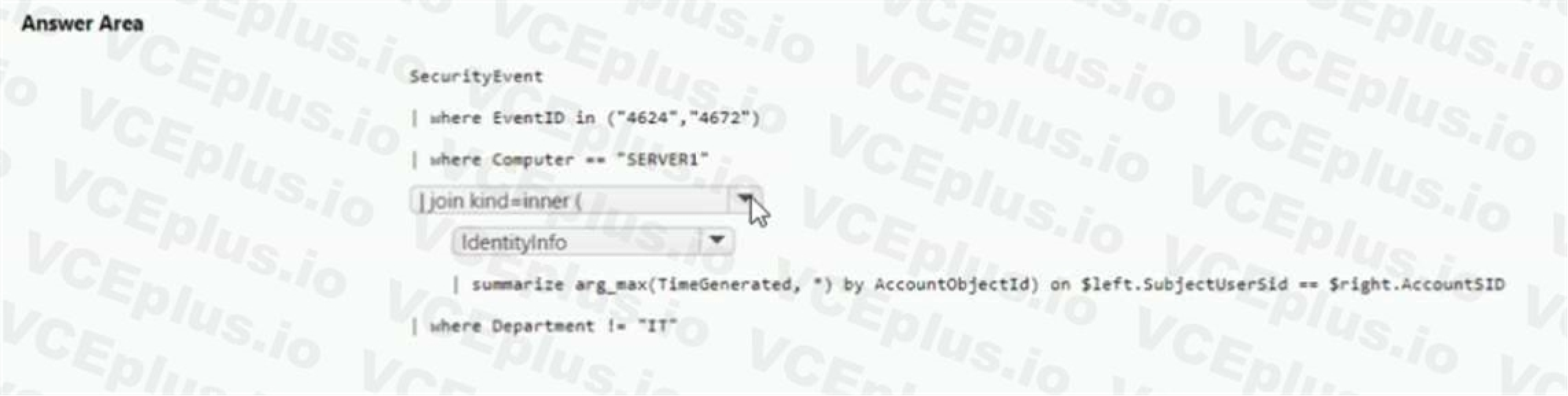
Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
```

```
erated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| wh
```

Section:

Explanation:



Answer Area

```
SecurityEvent
| where EventID in ("4624","4672")
| where Computer == "SERVER1"
| join kind=inner (
    IdentityInfo
    | summarize arg_max(TimeGenerated, *) by AccountObjectId) on $left.SubjectUserSid == $right.AccountSID
| where Department != "IT"
```

QUESTION 42
You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.
You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common
B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.
C. From the Azure portal, create an Azure Event Grid subscription.
D. From the workspace created by Defender for Cloud, set the data collection level to All Events
E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Correct Answer: D, E
Section:

QUESTION 43
You have an Azure subscription that use Microsoft Defender for Ctoud and contains a user named User1.
You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Security operator
B. Security Admin
C. Owner
D. Contributor

Correct Answer: B
Section:

QUESTION 44
You have an Azure subscription that uses Microsoft Defender fof Ctoud.
You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.
You need to onboard EC2-1 to Defender for Cloud.
What should you install on EC2-1?

A. the Log Analytics agent
B. the Azure Connected Machine agent
C. the unified Microsoft Defender for Endpoint solution package
D. Microsoft Monitoring Agent

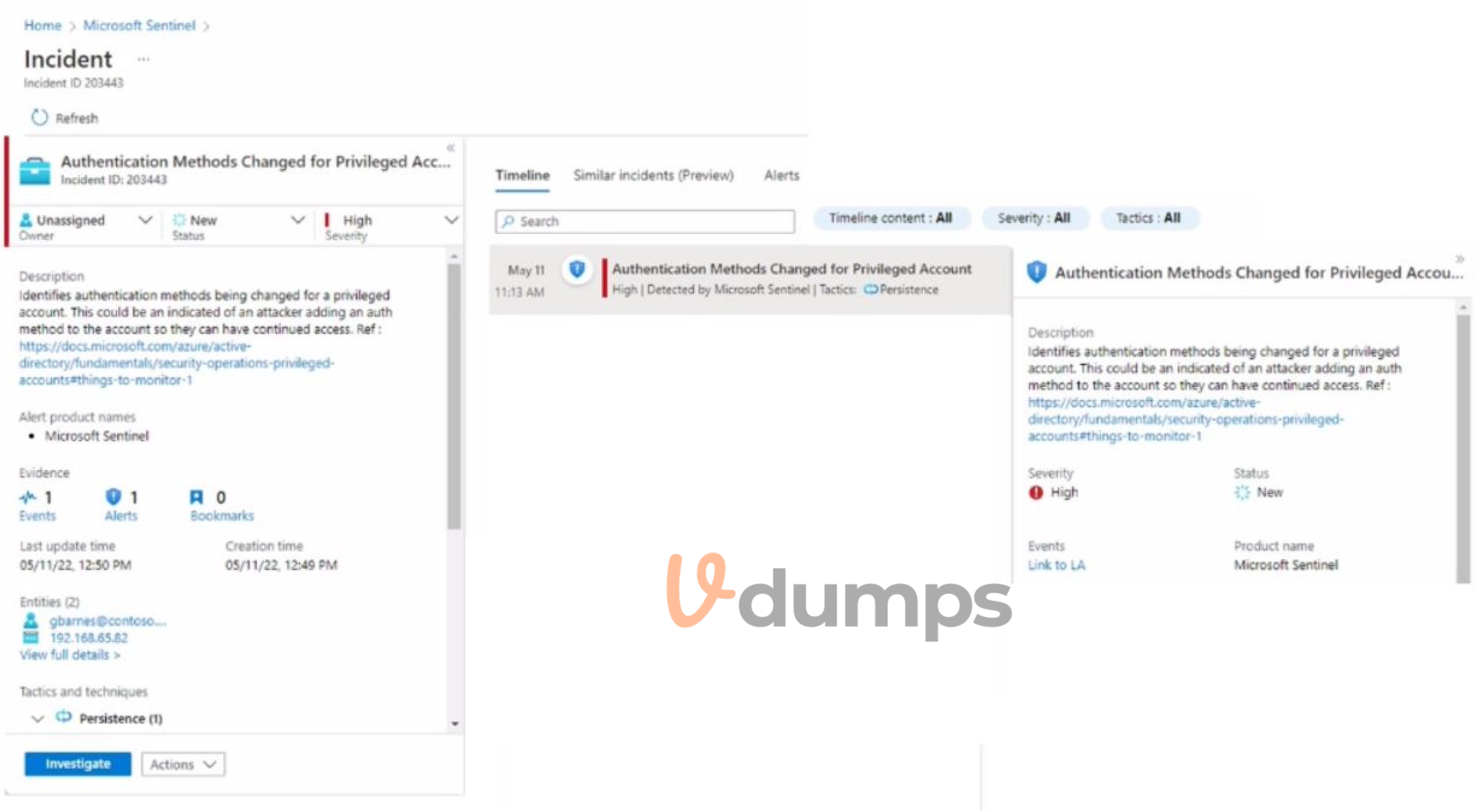
Correct Answer: A
Section:

QUESTION 45
You have a Microsoft Sentinel workspace named Workspace1 and 200 custom Advanced Security Information Model (ASIM) parsers based on the DNS schema. You need to make the 200 parsers available in Workspace1. The solution must minimize administrative effort. What should you do first?

A. Copy the parsers to the Azure Monitor Logs page.
B. Create a JSON file based on the DNS template.
C. Create an XML file based on the DNS template.
D. Create a YAML file based on the DNS template.

Correct Answer: A
Section:
Explanation:

QUESTION 46
HOTSPOT
You have a Microsoft Sentinel workspace.
A Microsoft Sentinel incident is generated as shewn in the following exhibit.



Home > Microsoft Sentinel >

Incident ...

Incident ID 203443

Refresh

Authentication Methods Changed for Privileged Acc...

Incident ID: 203443

Unassigned
Owner

New
Status

High
Severity

Description

Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

Alert product names

- Microsoft Sentinel

Evidence

1 Events | 1 Alerts | 0 Bookmarks

Last update time 05/11/22, 12:50 PM

Creation time 05/11/22, 12:49 PM

Entities (2)

gbarnes@contoso....

192.168.65.82

View full details >

Tactics and techniques

Persistence (1)

Investigate | Actions

Timeline | Similar incidents (Preview) | Alerts

Search | Timeline content : All | Severity : All | Tactics : All

May 11 11:13 AM — Authentication Methods Changed for Privileged Account
High | Detected by Microsoft Sentinel | Tactics: Persistence

Authentication Methods Changed for Privileged Accou...

Description

Identifies authentication methods being changed for a privileged account. This could be an indicated of an attacker adding an auth method to the account so they can have continued access. Ref : https://docs.microsoft.com/azure/active-directory/fundamentals/security-operations-privileged-accounts#things-to-monitor-1

Severity: High

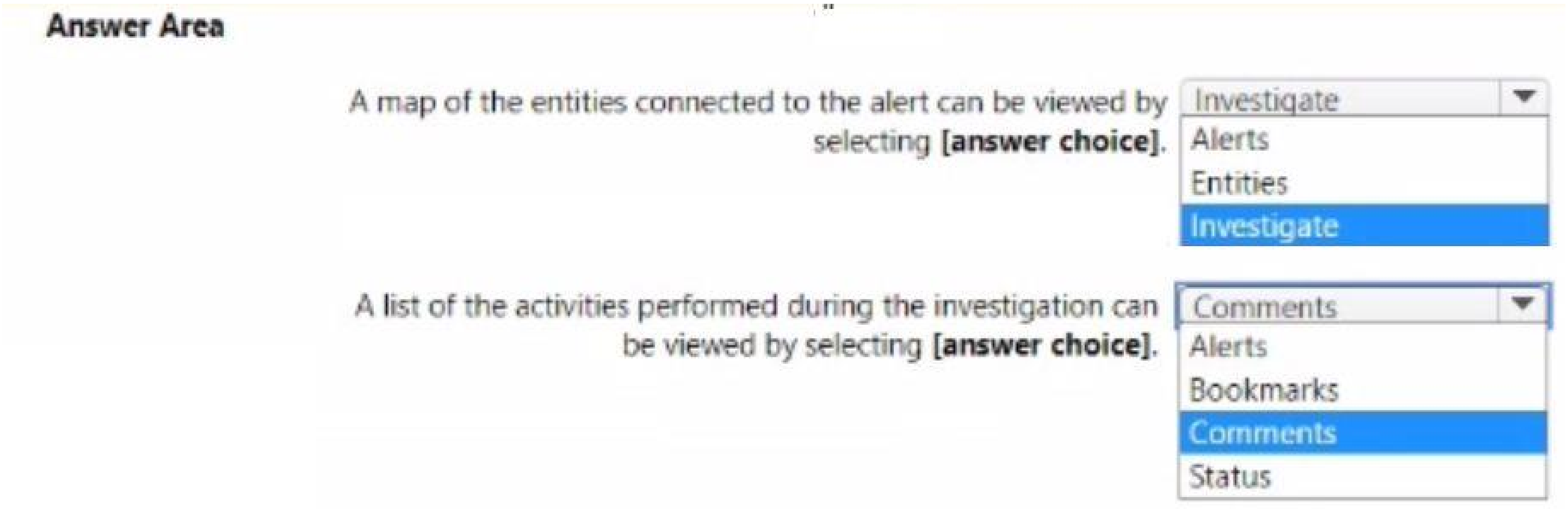
Status: New

Events: Link to LA

Product name: Microsoft Sentinel

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:

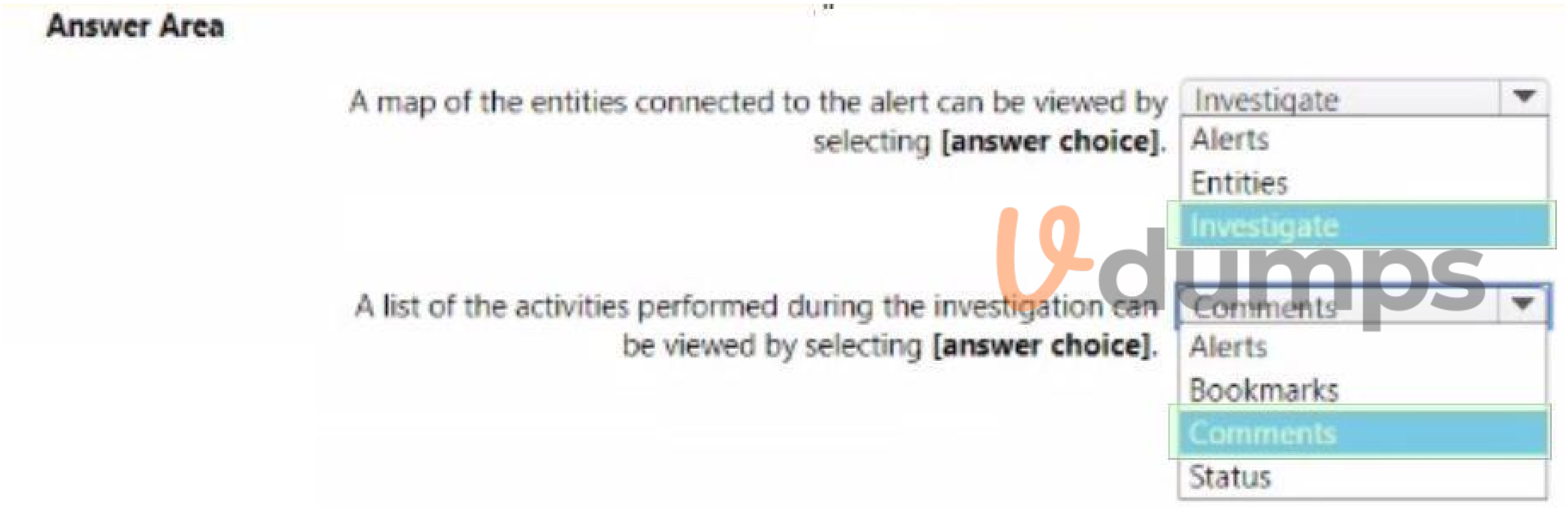


Answer Area

A map of the entities connected to the alert can be viewed by selecting **[answer choice]**.

A list of the activities performed during the investigation can be viewed by selecting **[answer choice]**.

Answer Area:



Answer Area

A map of the entities connected to the alert can be viewed by selecting **[answer choice]**.

[✓ Investigate]

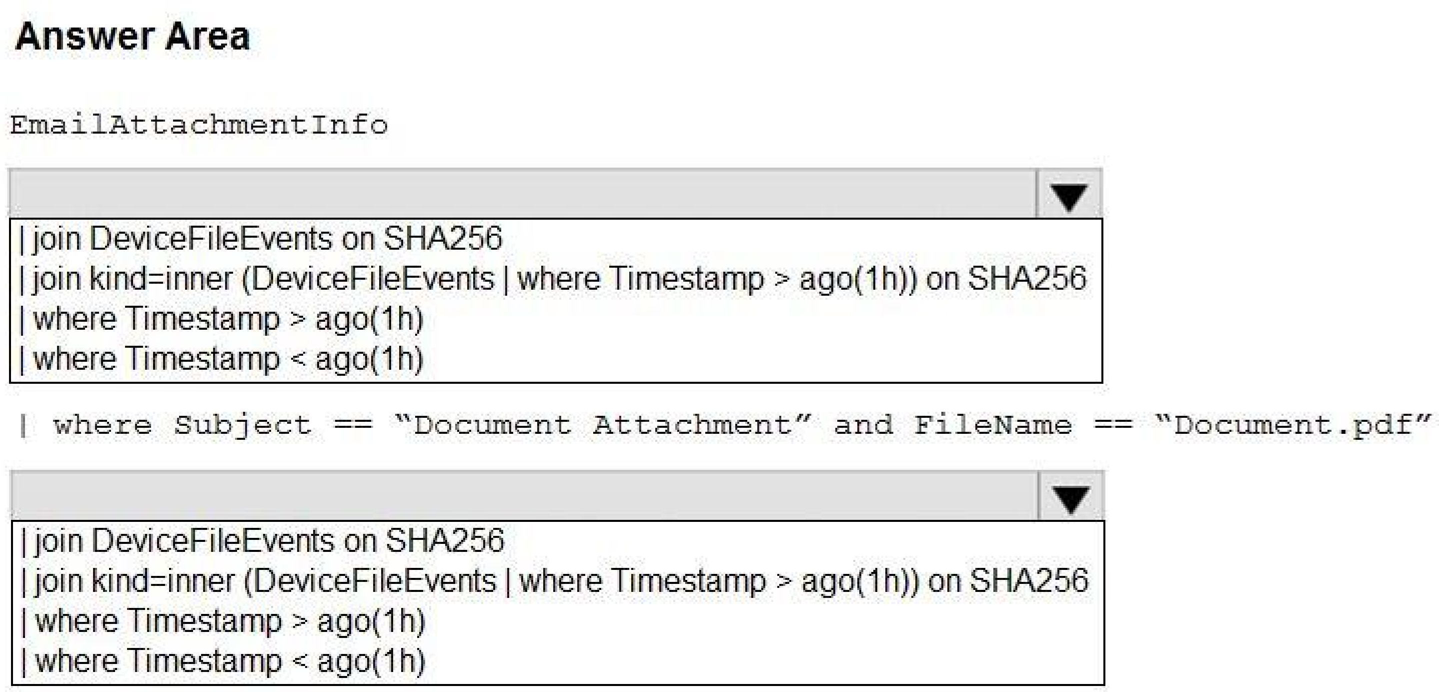
A list of the activities performed during the investigation can be viewed by selecting **[answer choice]**.

[✓ Comments]

Section:
Explanation:

QUESTION 47
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:
* Only show emails sent during the last hour.
* Optimize query performance.
How should you complete the query? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

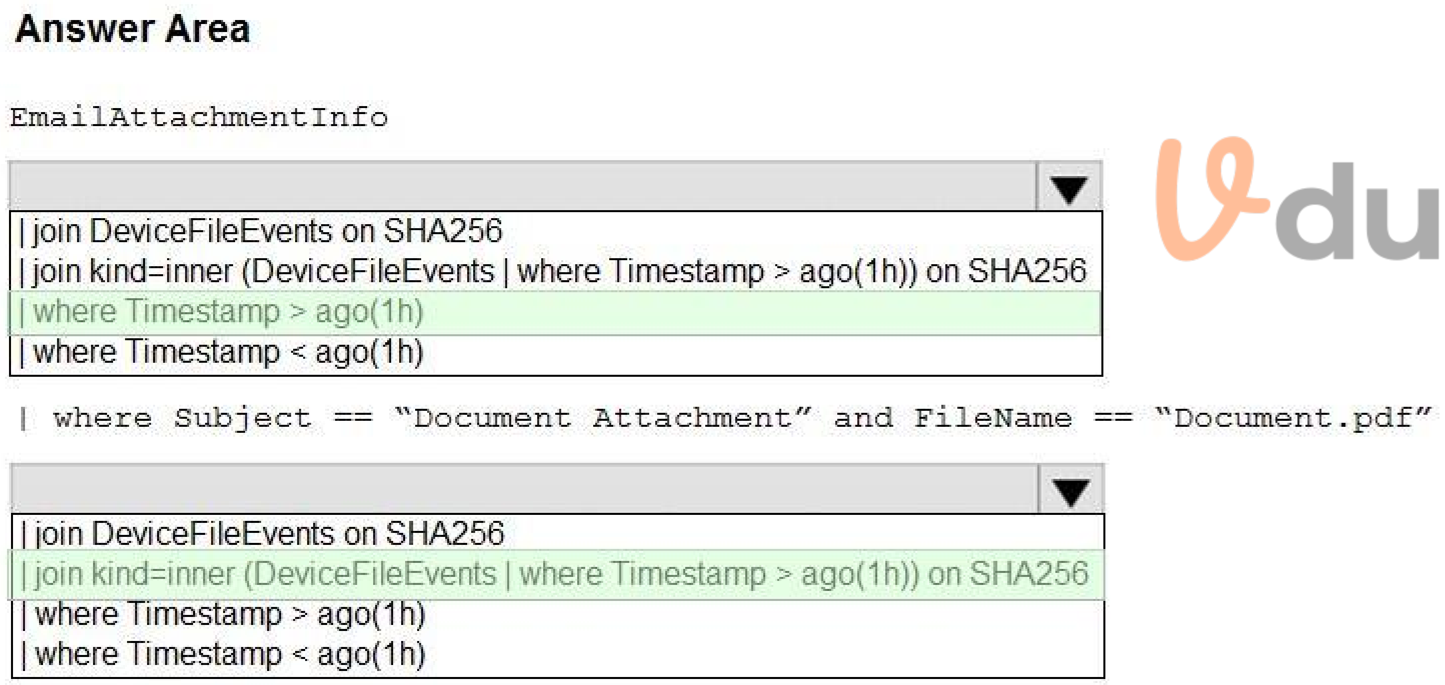
EmailAttachmentInfo

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

| where Subject == "Document Attachment" and FileName == "Document.pdf"

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

Answer Area:



Answer Area

EmailAttachmentInfo

| join DeviceFileEvents on SHA256
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
[✓ | where Timestamp > ago(1h)]
| where Timestamp < ago(1h)

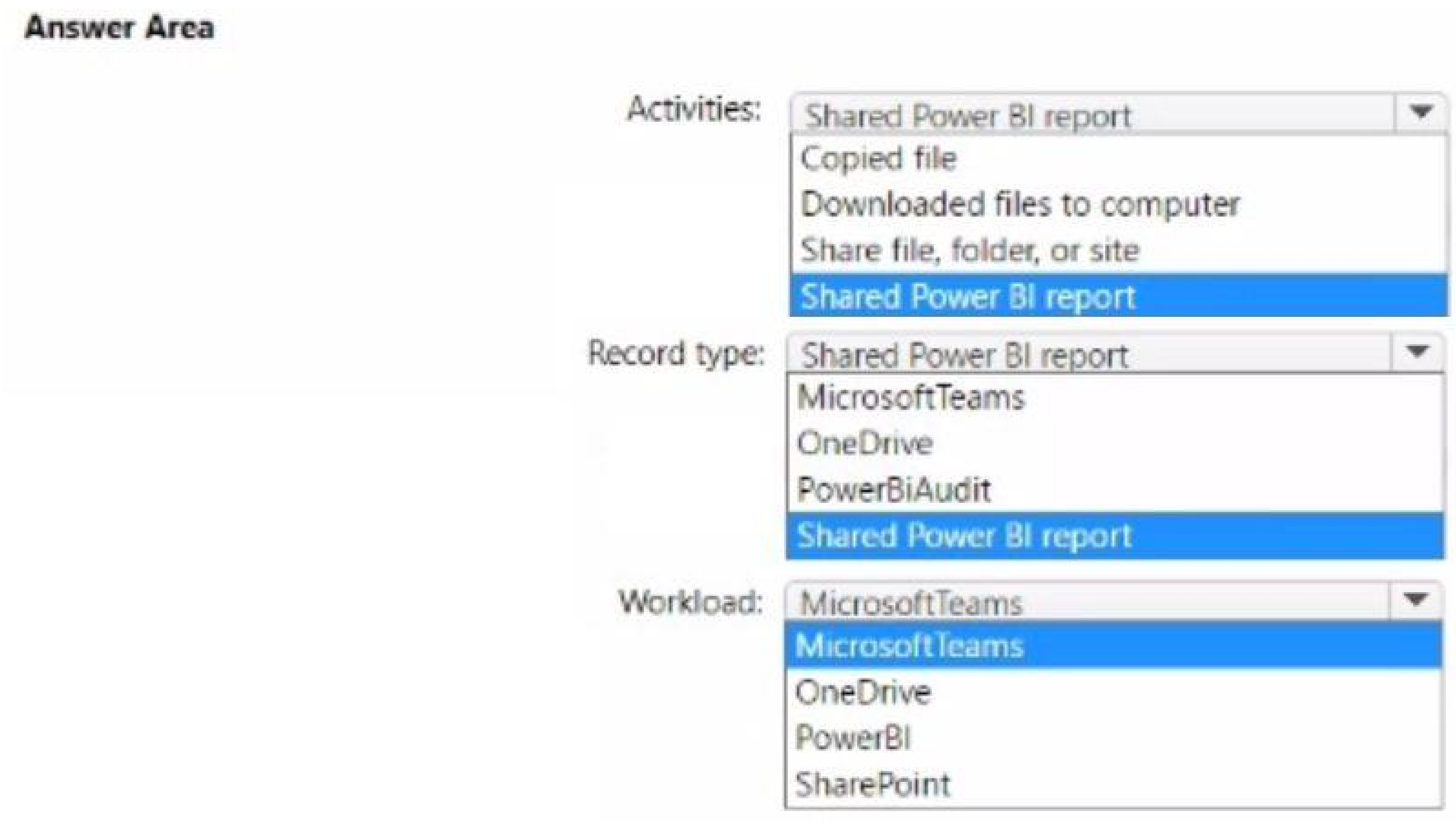
| where Subject == "Document Attachment" and FileName == "Document.pdf"

| join DeviceFileEvents on SHA256
[✓ | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256]
| where Timestamp > ago(1h)
| where Timestamp < ago(1h)

Section:
Explanation:

QUESTION 48
HOTSPOT
You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.
User1 shares a Microsoft Power Bi report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.
You need to identity which Power BI report file was shared.
How should you configure the search? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

Activities: Shared Power BI report

- Copied file
- Downloaded files to computer
- Share file, folder, or site
- Shared Power BI report

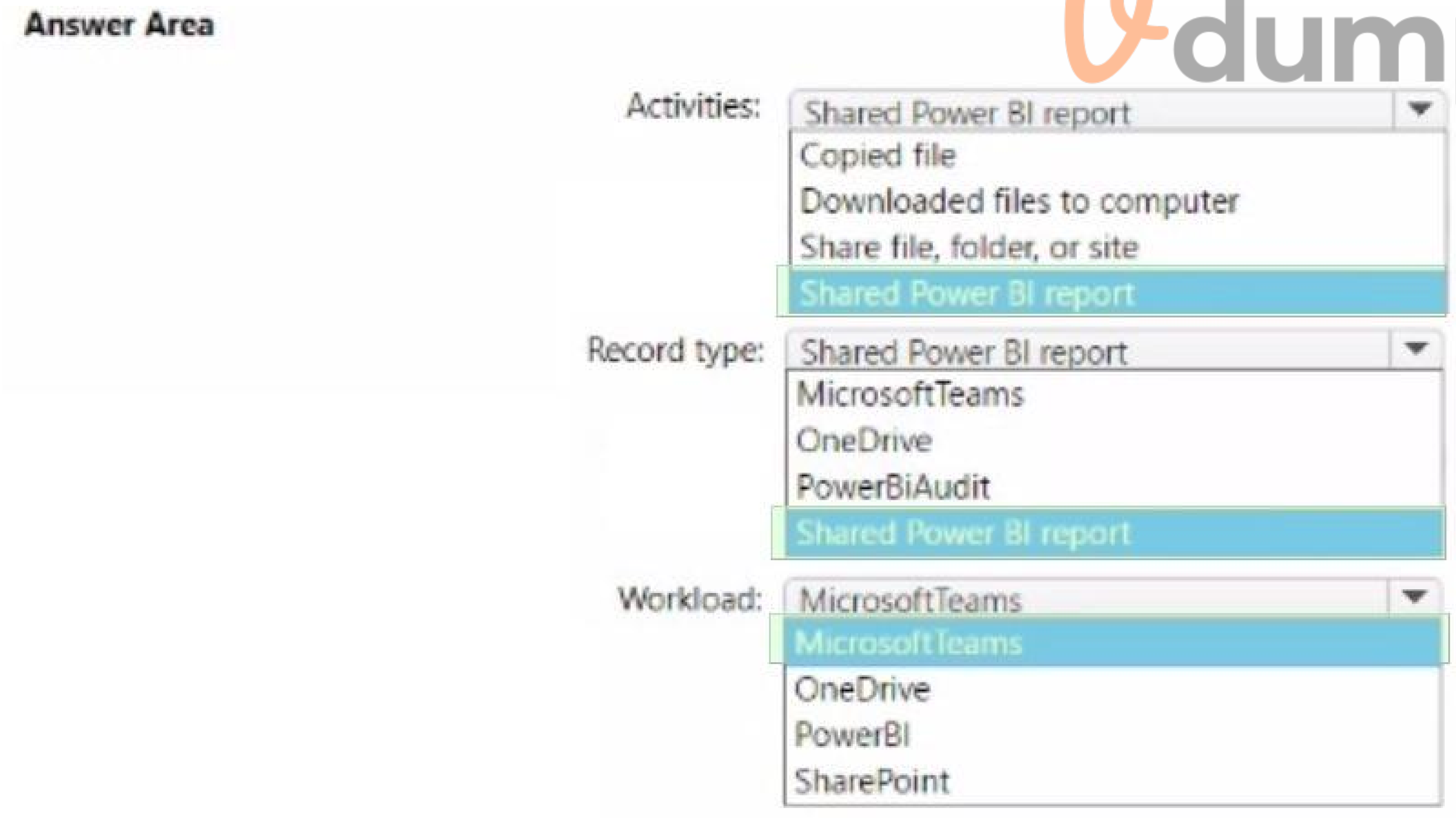
Record type: Shared Power BI report

- MicrosoftTeams
- OneDrive
- PowerBiAudit
- Shared Power BI report

Workload: MicrosoftTeams

- MicrosoftTeams
- OneDrive
- PowerBI
- SharePoint

Answer Area:



Answer Area

Activities: Shared Power BI report

- Copied file
- Downloaded files to computer
- Share file, folder, or site
- [✓ Shared Power BI report]

Record type: Shared Power BI report

- MicrosoftTeams
- OneDrive
- PowerBiAudit
- [✓ Shared Power BI report]

Workload: MicrosoftTeams

- [✓ MicrosoftTeams]
- OneDrive
- PowerBI
- SharePoint

Section:

Explanation:

QUESTION 49

DRAG DROP

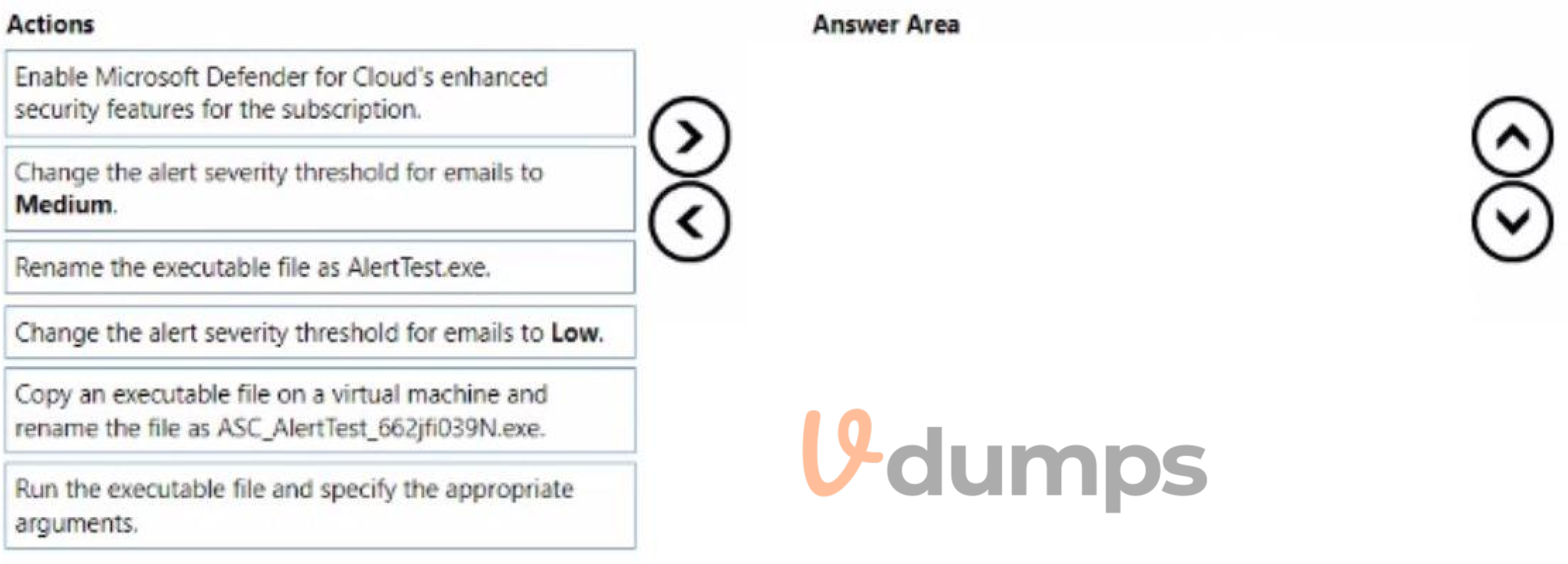
You create a new Azure subscription and start collecting logs for Azure Monitor.

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

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

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

Select and Place:

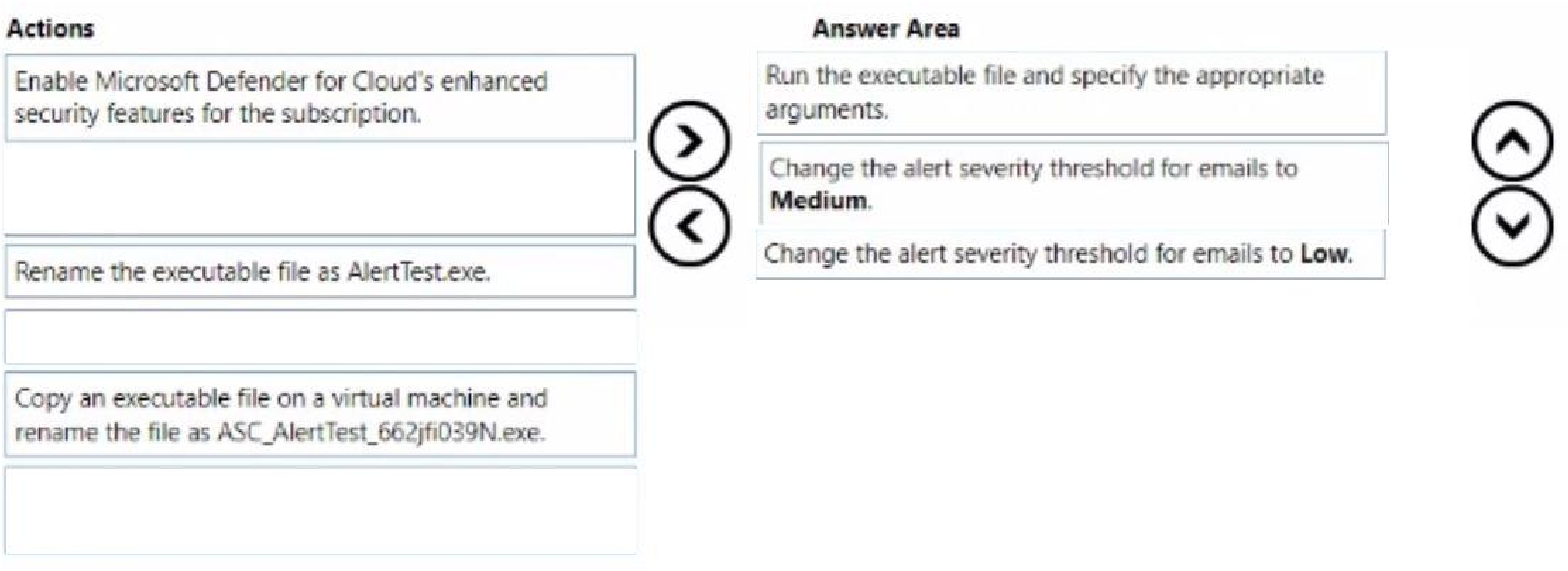


Actions

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

Answer Area

Correct Answer:



Actions

Enable Microsoft Defender for Cloud's enhanced security features for the subscription.

Rename the executable file as AlertTest.exe.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.

Answer Area

Run the executable file and specify the appropriate arguments.

Change the alert severity threshold for emails to **Medium**.

Change the alert severity threshold for emails to **Low**.

Section:
Explanation:

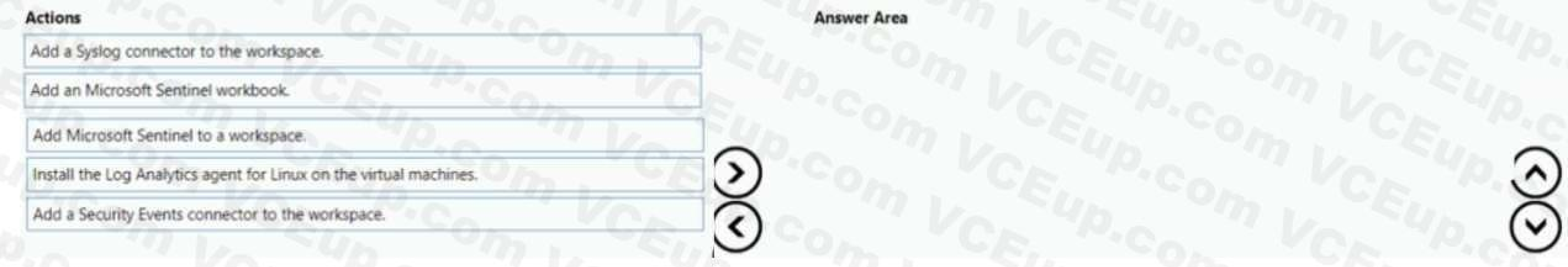
QUESTION 50
You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.
You need to enable Microsoft Defender for Servers on the virtual machines.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct answer is worth one point.

A. From Defender for Cloud, enable agentless scanning.
B. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.
C. Onboard the virtual machines to Microsoft Defender for Endpoint.
D. From Defender for Cloud, configure auto-provisioning.
E. From Defender for Cloud, configure the AWS connector.

Correct Answer: B, C
Section:

QUESTION 51
DRAG DROP
You have an Azure subscription that contains 100 Linux virtual machines.
You need to configure Microsoft Sentinel to collect event logs from the virtual machines.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

Add a Syslog connector to the workspace.

Add an Microsoft Sentinel workbook.

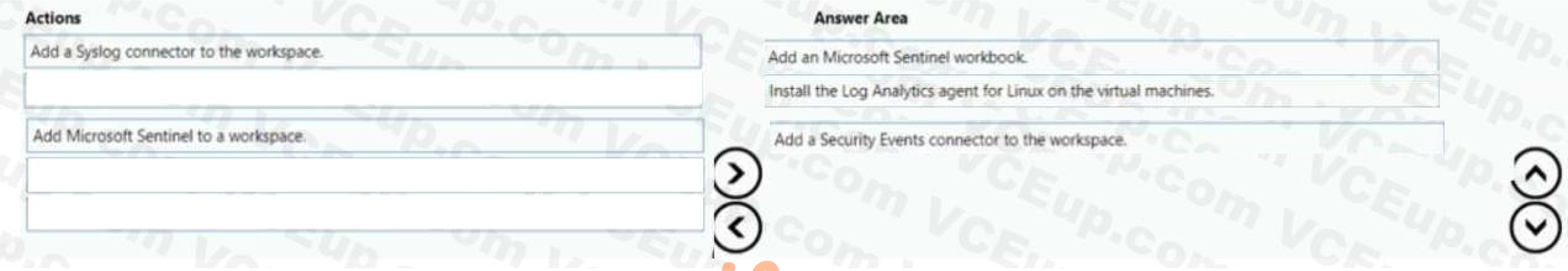
Add Microsoft Sentinel to a workspace.

Install the Log Analytics agent for Linux on the virtual machines.

Add a Security Events connector to the workspace.

Answer Area

Correct Answer:



Actions

Add a Syslog connector to the workspace.

Add Microsoft Sentinel to a workspace.

Answer Area

Add an Microsoft Sentinel workbook.

Install the Log Analytics agent for Linux on the virtual machines.

Add a Security Events connector to the workspace.

Section:
Explanation:

QUESTION 52
You have an Azure subscription that contains an Azure logic app named app1 and a Microsoft Sentinel workspace that has an Azure AD connector. You need to ensure that app1 launches when Microsoft Sentinel detects an Azure AD- generated alert. What should you create first?

A. a repository connection
B. a watchlist
C. an analytics rule
D. an automation rule

Correct Answer: D
Section:

QUESTION 53
You have an Azure subscription that contains a user named User1.
User1 is assigned an Azure Active Directory Premium Plan 2 license
You need to identify whether the identity of User1 was compromised during the last 90 days.
What should you use?

A. the risk detections report
B. the risky users report
C. Identity Secure Score recommendations
D. the risky sign-ins report

Correct Answer: B
Section:

QUESTION 54
You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

A. Run antivirus scan
B. Initiate Automated Investigation
C. Collect investigation package
D. Initiate Live Response Session

Correct Answer: D
Section:

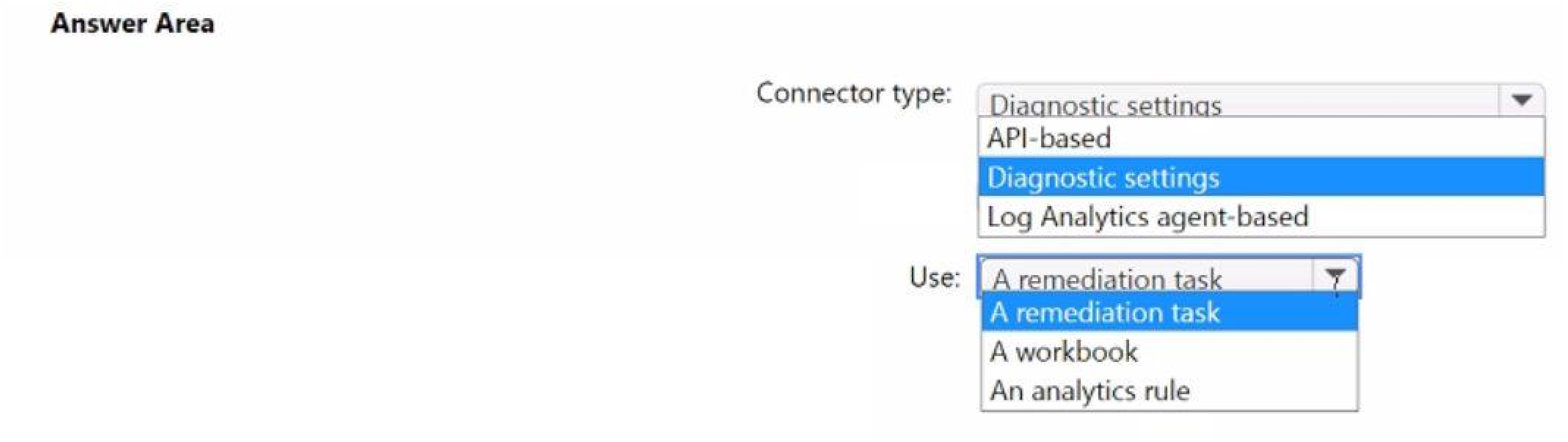
QUESTION 55
You have a Microsoft Sentinel workspace that uses the Microsoft 365 Defender data connector.
From Microsoft Sentinel, you investigate a Microsoft 365 incident.
You need to update the incident to include an alert generated by Microsoft Defender for Cloud Apps.
What should you use?

A. the entity side panel of the Timeline card in Microsoft Sentinel
B. the investigation graph on the Incidents page of Microsoft Sentinel
C. the Timeline tab on the Incidents page of Microsoft Sentinel
D. the Alerts page in the Microsoft 365 Defender portal

Correct Answer: A
Section:

QUESTION 56
OTSPOT
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.
You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

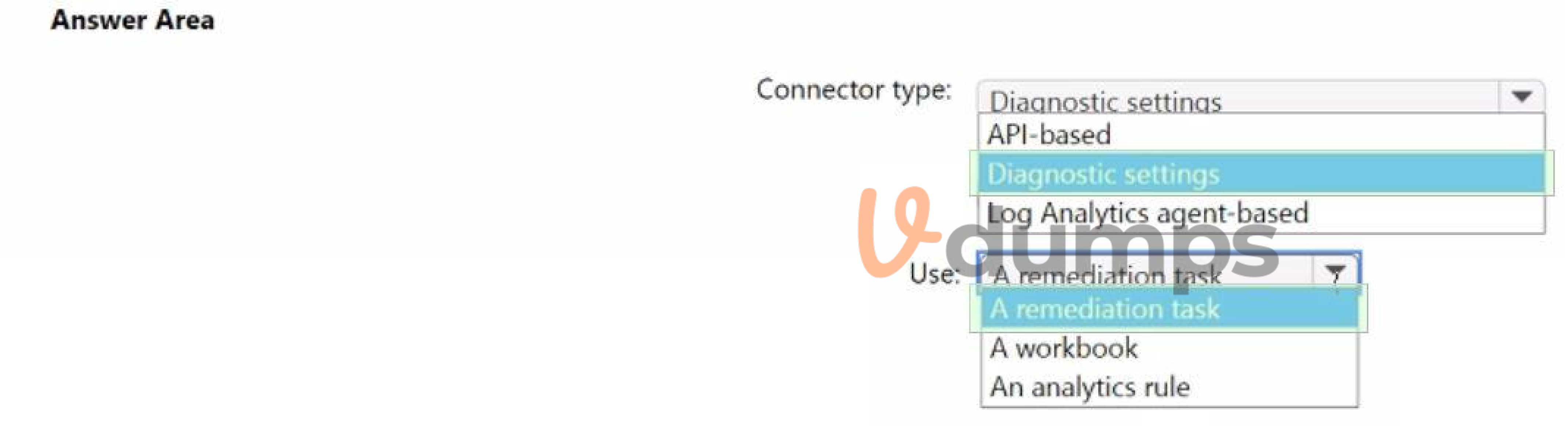
Connector type: Diagnostic settings

- API-based
- Diagnostic settings
- Log Analytics agent-based

Use: A remediation task

- A remediation task
- A workbook
- An analytics rule

Answer Area:



Answer Area

Connector type: Diagnostic settings

- API-based
- Diagnostic settings
- Log Analytics agent-based

Use: A remediation task

- A remediation task
- A workbook
- An analytics rule

Section:
Explanation:

QUESTION 57
You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.
You need to create a new near-real-time (NRT) analytics rule that will use the playbook.
What should you configure for the rule?

A. the Incident automation settings
B. entity mapping
C. the query rule
D. the Alert automation settings

Correct Answer: B
Section:

QUESTION 58

HOTSPOT

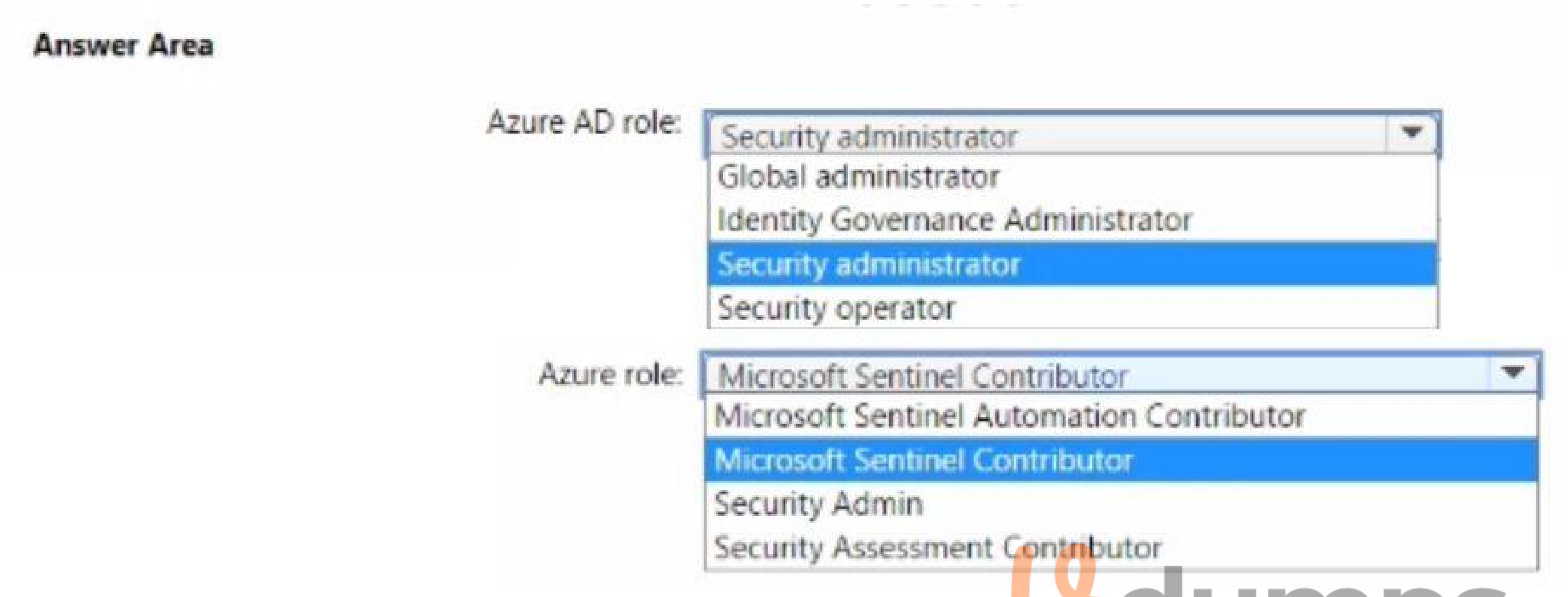
You have an Azure subscription that uses Microsoft Sentinel and contains a user named User1.

You need to ensure that User1 can enable User and Entity Behavior Analytics (UEBA) for entity behavior in Azure AD The solution must use The principle of least privilege.

Which roles should you assign to Used? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

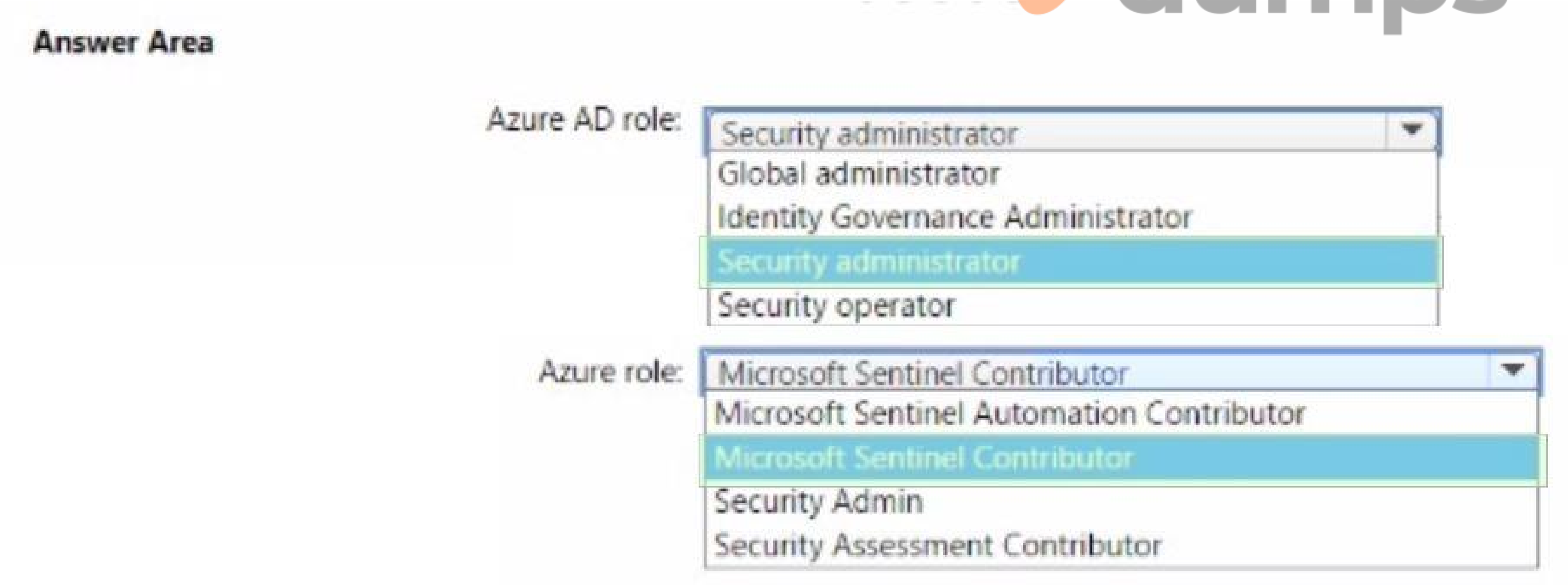
Azure AD role: Security administrator ▾

- Global administrator
- Identity Governance Administrator
- Security administrator
- Security operator

Azure role: Microsoft Sentinel Contributor ▾

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor
- Security Admin
- Security Assessment Contributor

Answer Area:



Answer Area

Azure AD role: Security administrator ▾

- Global administrator
- Identity Governance Administrator
- Security administrator
- Security operator

Azure role: Microsoft Sentinel Contributor ▾

- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor
- Security Admin
- Security Assessment Contributor

Section:

Explanation: