DUMPSQUEEN

Microsoft Security Operations Analyst

Microsoft SC-200

Version Demo

Total Demo Questions: 15

Total Premium Questions: 243

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 2, New Update	133
Topic 3, Case Study 1	2
Topic 4, Case Study 2	3
Topic 5, Case Study 3	2
Topic 6, Case Study 4	4
Topic 7, Case Study 5	6
Topic 8, Mixed Questions	93
Total	243

QUESTION NO: 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 have Linux virtual machines on Amazon Web Services (AWS).

You deploy Azure Defender and enable auto-provisioning.

You need to monitor the virtual machines by using Azure Defender.

Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Reference:

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

QUESTION NO: 2

You use Azure Defender.

You have an Azure Storage account that contains sensitive information.

You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.

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

NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

B. Create an Azure logic appthat has a manual trigger

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

D. Create an Azure logic appthat has an HTTP trigger.

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

ANSWER: A C

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center

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

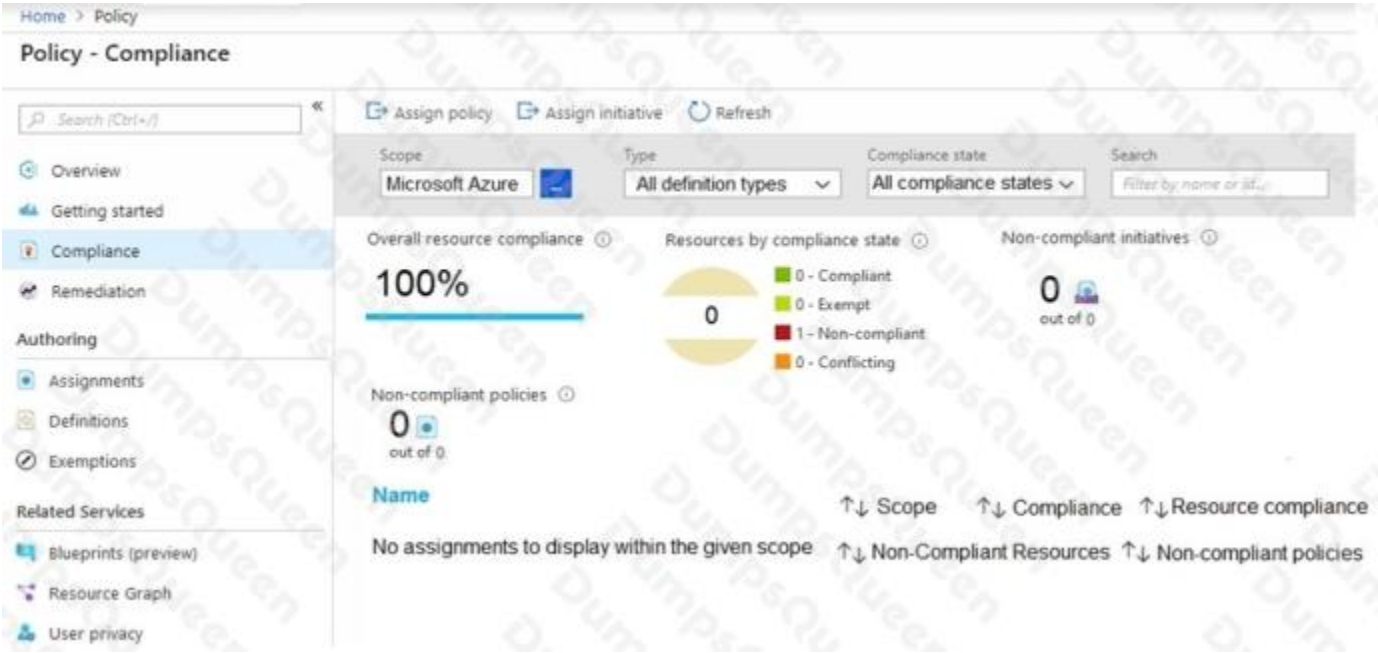
QUESTION NO: 3 - (HOTSPOT)

HOTSPOT

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

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

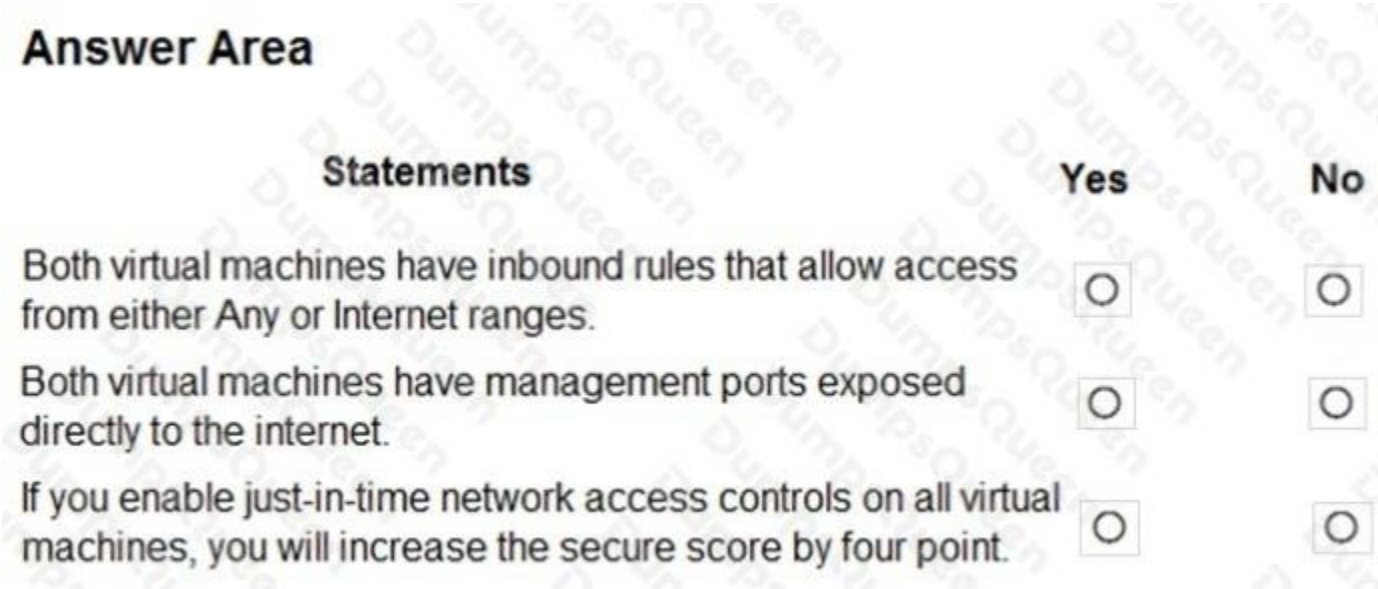
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



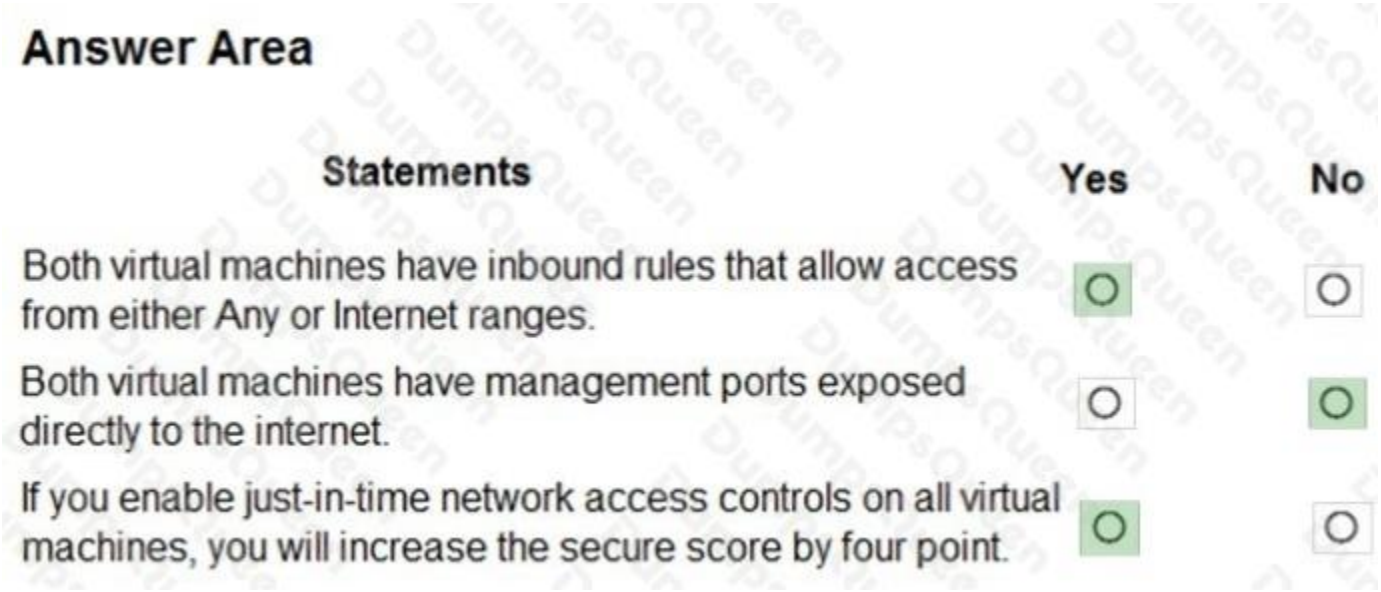
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



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 NO: 4

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.

ANSWER: A B

Explanation:

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

QUESTION NO: 5

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

ANSWER: C D

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 NO: 6

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

ANSWER: B

Explanation:

Reference:

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

QUESTION NO: 7

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

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

You are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Entity tags, you add the accounts as Honeytoken accounts.

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

Reference:

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

QUESTION NO: 8

You are investigating a potential attack that deploys a new ransomware strain.

You have three custom device groups. The groups contain devices that store highly sensitive information.

You plan to perform automated actions on all devices.

You need to be able to temporarily group the machines to perform actions on the devices.

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

NOTE: Each correct selection is worth one point.

A. Assign a tag to the device group.

B. Add the device users to the admin role.

C. Add a tag to the machines.

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

E. Create a new admin role.

F. Create a new device group that has a rank of 4.

ANSWER: A C D

Explanation:

Reference:

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

QUESTION NO: 9

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

ANSWER: B

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: https://docs.microsoft.com/en-us/microsoft-365/security/mtp/microsoft-365-defender-threat-analytics

QUESTION NO: 10 - (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.

ANSWER:

Explanation:

QUESTION NO: 11

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

You need to add threat indicators for all the IP addresses in a range of 171.23.3432-171.2334.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

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

B. Select Add indicator and set the IP address to 171.2334.32-171.23.34.63.

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

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

ANSWER: C

Explanation:

This will add all the IP addresses in the range of 171.23.34.32/27 as threat indicators. This is the simplest and most efficient way to add all the IP addresses in the range.

Reference: [1] https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/threat-intelligence-manage-indicators

QUESTION NO: 12

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

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

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

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

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

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

ANSWER: D E

Explanation:

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

QUESTION NO: 13 - (DRAG DROP)

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:

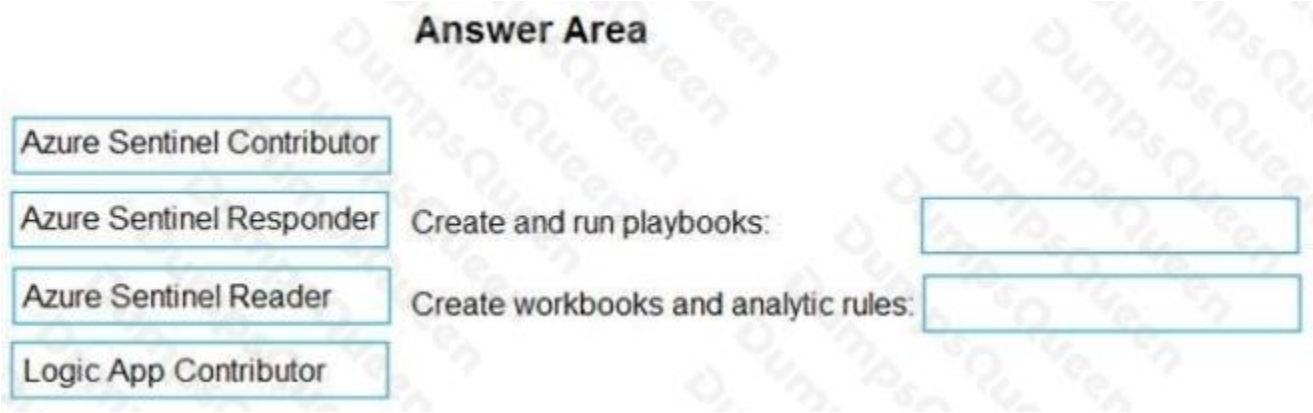
- Create and run playbooks
- Create workbooks and analytic rules.

The solution must use the principle of least privilege.

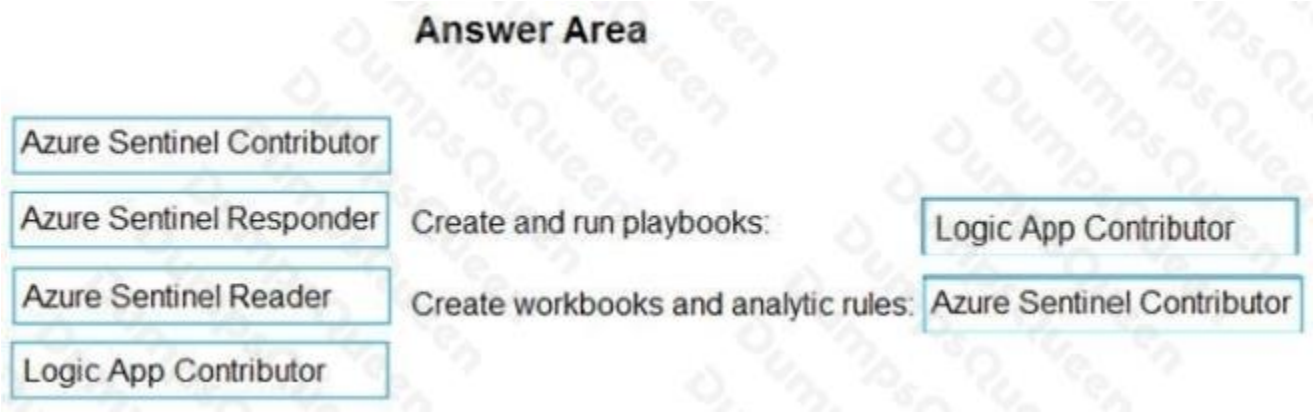
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



ANSWER:



Explanation:

Reference:

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

QUESTION NO: 14 - (HOTSPOT)

HOTSPOT

You purchase a Microsoft 365 subscription.

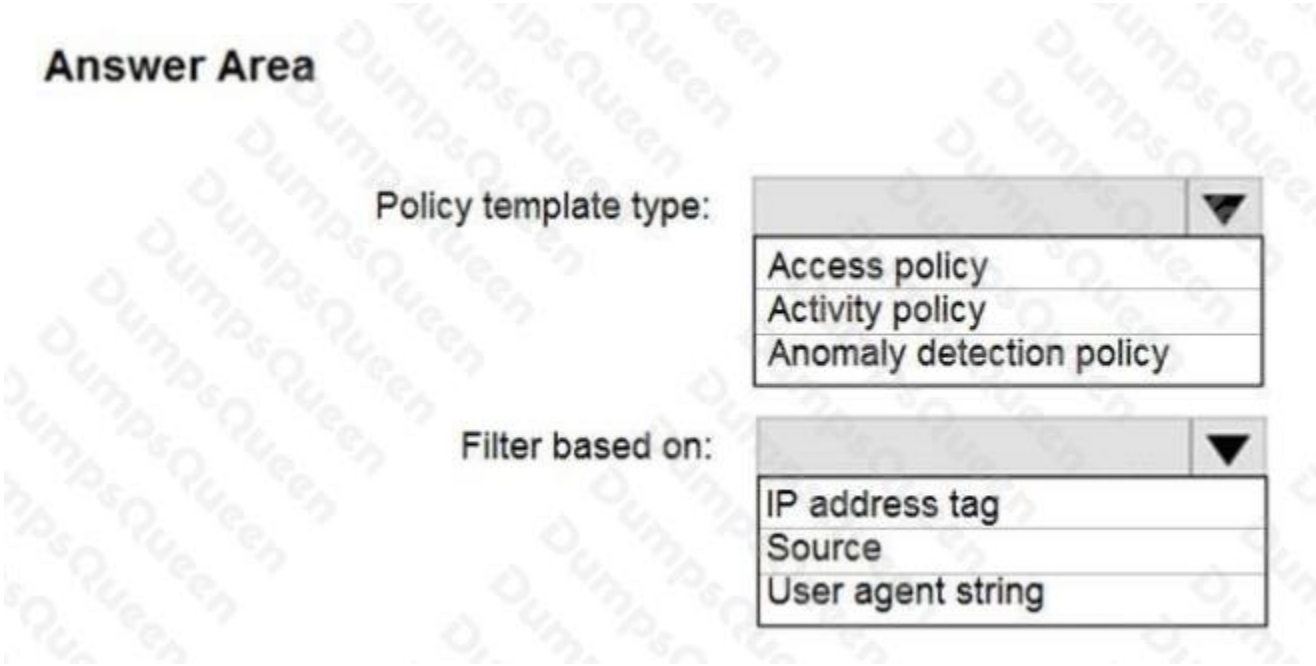
You plan to configure Microsoft Cloud App Security.

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

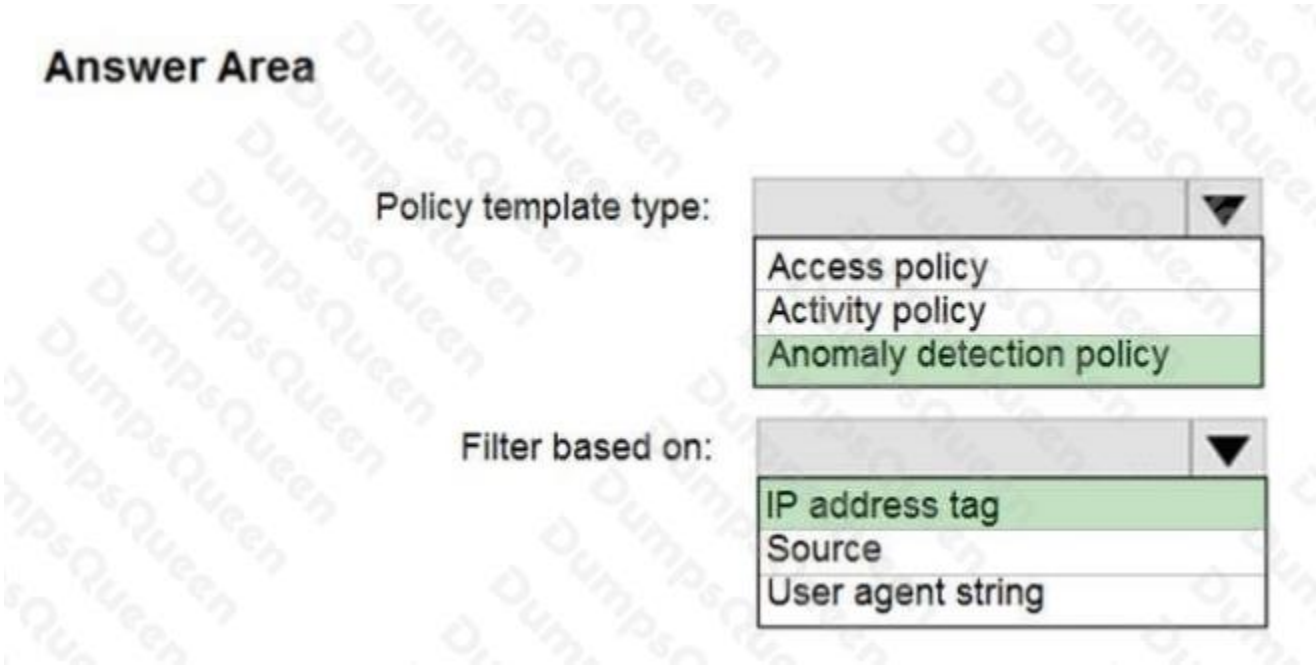
What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

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

QUESTION NO: 15

You have a custom Microsoft Sentinel workbook named Workbooks.

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

What should you do?

A. In the query editor interface, configure Settings.

B. In the query editor interface, select Advanced Editor

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

D. In the grid query, include the take operator.

ANSWER: B