SC-200 Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

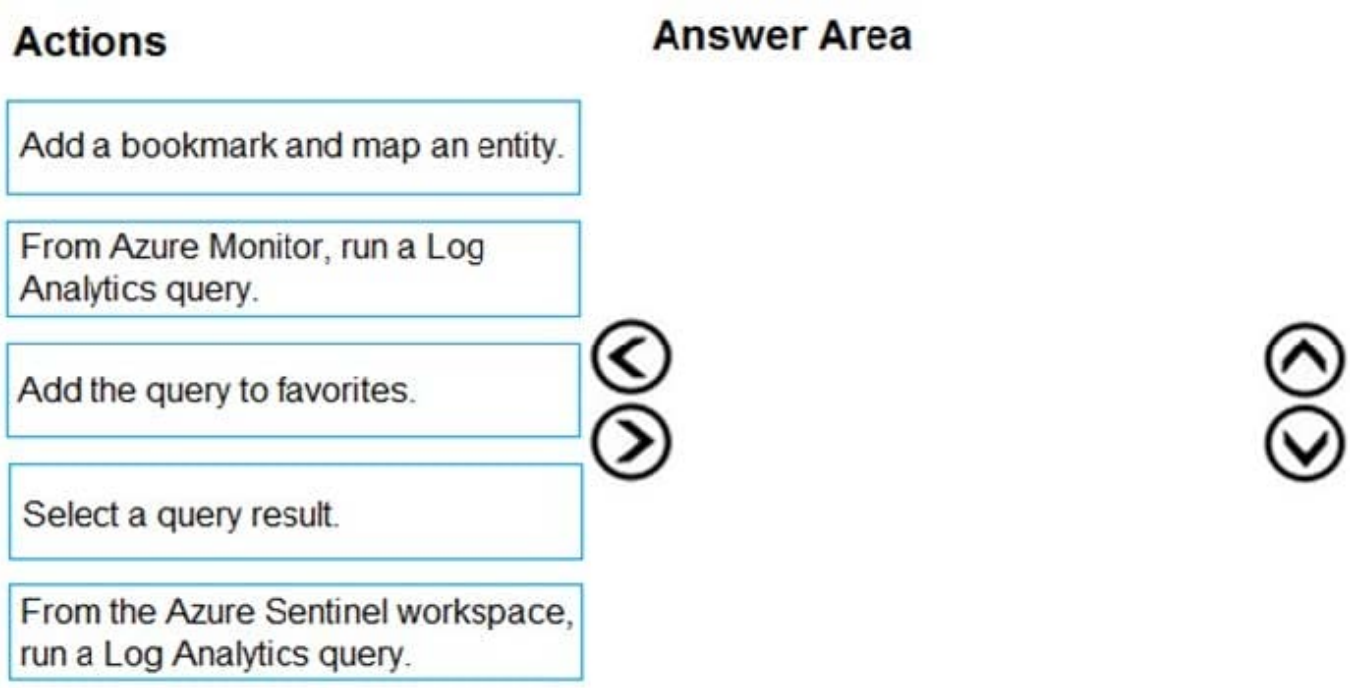
QUESTION 1

DRAG DROP

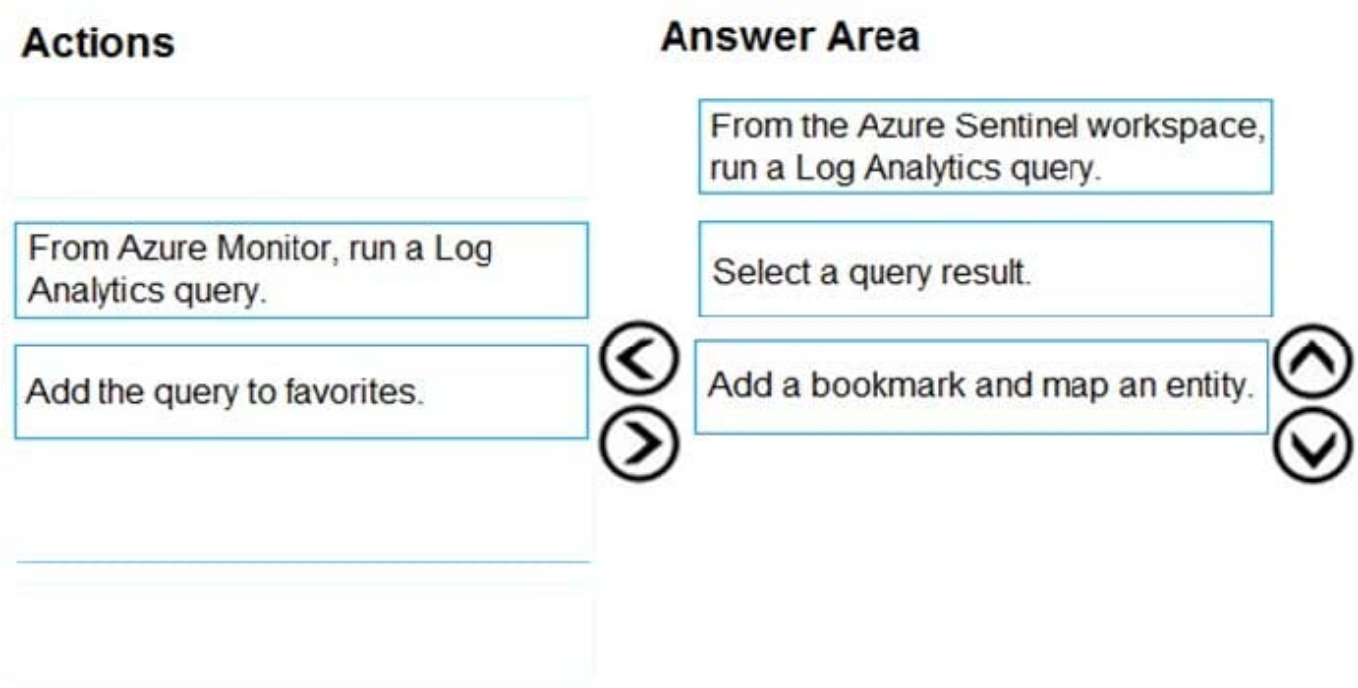
You need to add notes to the events to meet the Azure Sentinel requirements.

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

Select and Place:



Correct Answer:



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

QUESTION 2

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1. You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

A. the Azure Storage Analytics logs

B. the activity logs of storage1

C. the alert details

D. the related entities of the alert

Correct Answer: A

Configure Microsoft Defender for Storage Security alerts are triggered when anomalies in activity occur. These security alerts are integrated with Microsoft Defender for Cloud, and are also sent via email to subscription administrators, with details of suspicious activity and recommendations on how to investigate and remediate threats.

The service ingests resource logs of read, write, and delete requests to Blob storage and to Azure Files for threat detection. To investigate alerts from Microsoft Defender for Cloud, you can view related storage activity using Storage Analytics Logging.

Reference: https://learn.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure

QUESTION 3

You use Azure Sentinel.

You need to receive an immediate alert whenever Azure Storage account keys are enumerated.

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

NOTE: Each correct selection is worth one point.

A. Create a livestream

B. Add a data connector

C. Create an analytics rule

D. Create a hunting query.

E. Create a bookmark.

Correct Answer: BD

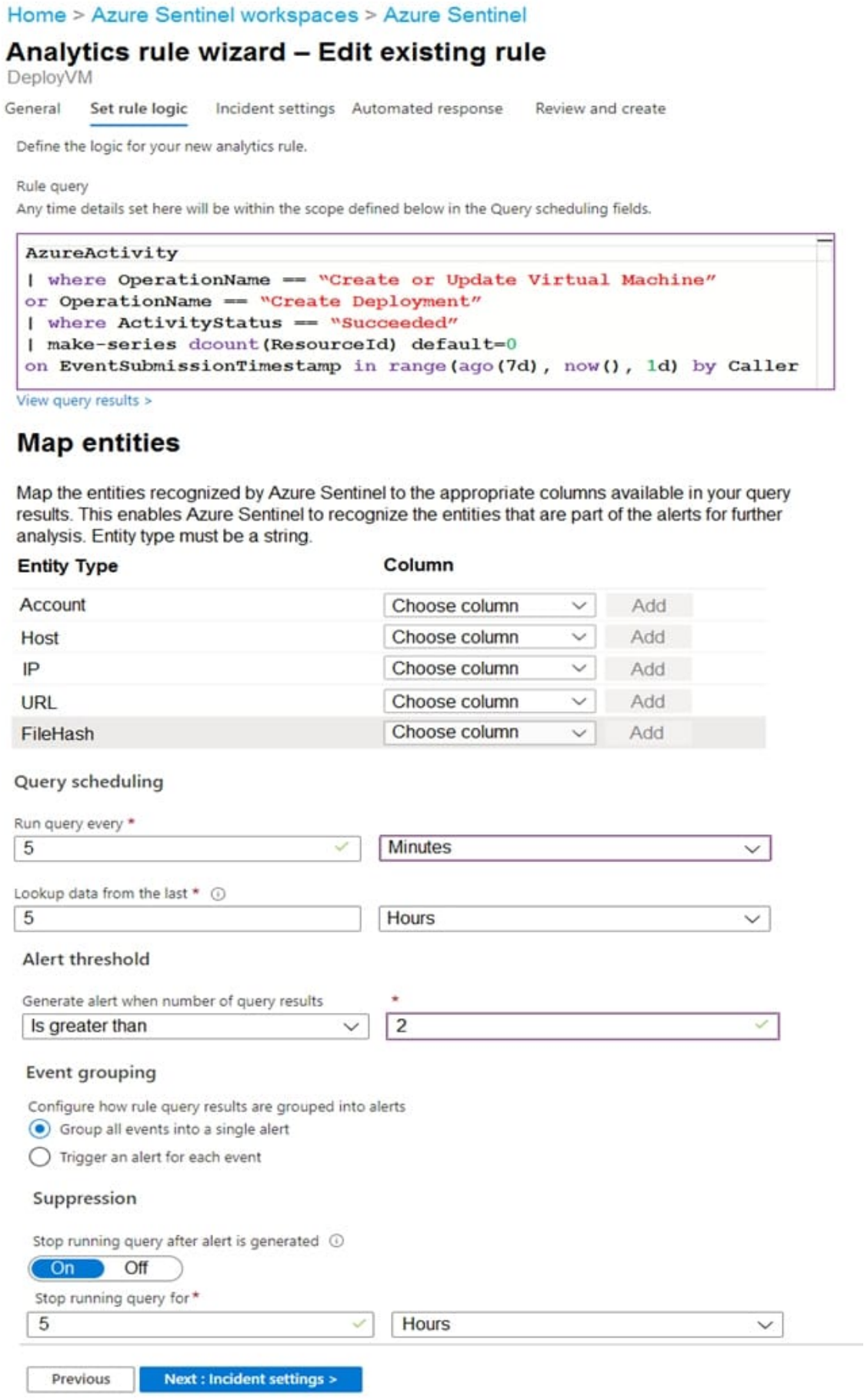
Reference: https://docs.microsoft.com/en-us/azure/sentinel/livestream

QUESTION 4

HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.

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

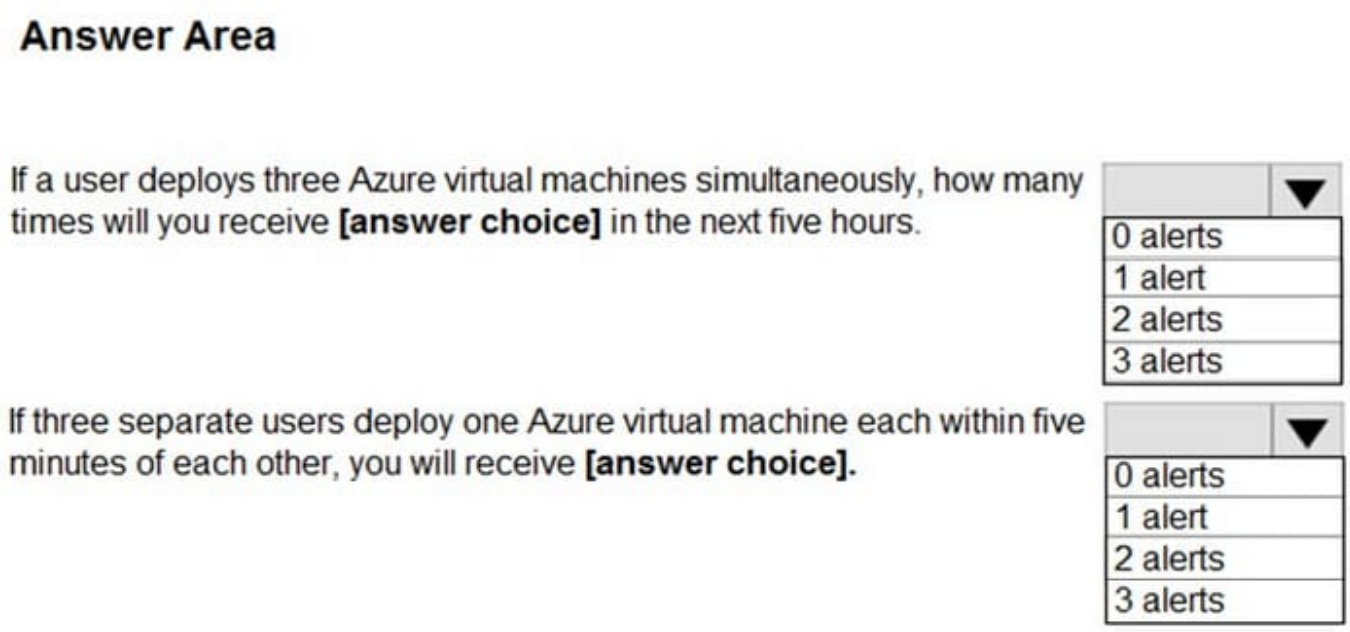

Home > Azure Sentinel workspaces > Azure Sentinel
Analytics rule wizard – Edit existing rule
DeployVM
General
Set rule logic
Incident settings
Automated response
Review and create
Define the logic for your new analytics rule.
Rule query
Any time details set here will be within the scope defined below in the Query scheduling fields.
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
View query results >
Map entities
Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.
Entity Type
Column
Account
Choose column
Add
Host
Choose column
Add
IP
Choose column
Add
URL
Choose column
Add
FileHash
Choose column
Add
Query scheduling
Run query every *
5
Minutes
Lookup data from the last *
5
Hours
Alert threshold
Generate alert when number of query results *
Is greater than
2
Event grouping
Configure how rule query results are grouped into alerts
Group all events into a single alert
Trigger an alert for each event
Suppression
Stop running query after alert is generated
On
Off
Stop running query for *
5
Hours
Previous
Next : Incident settings >

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

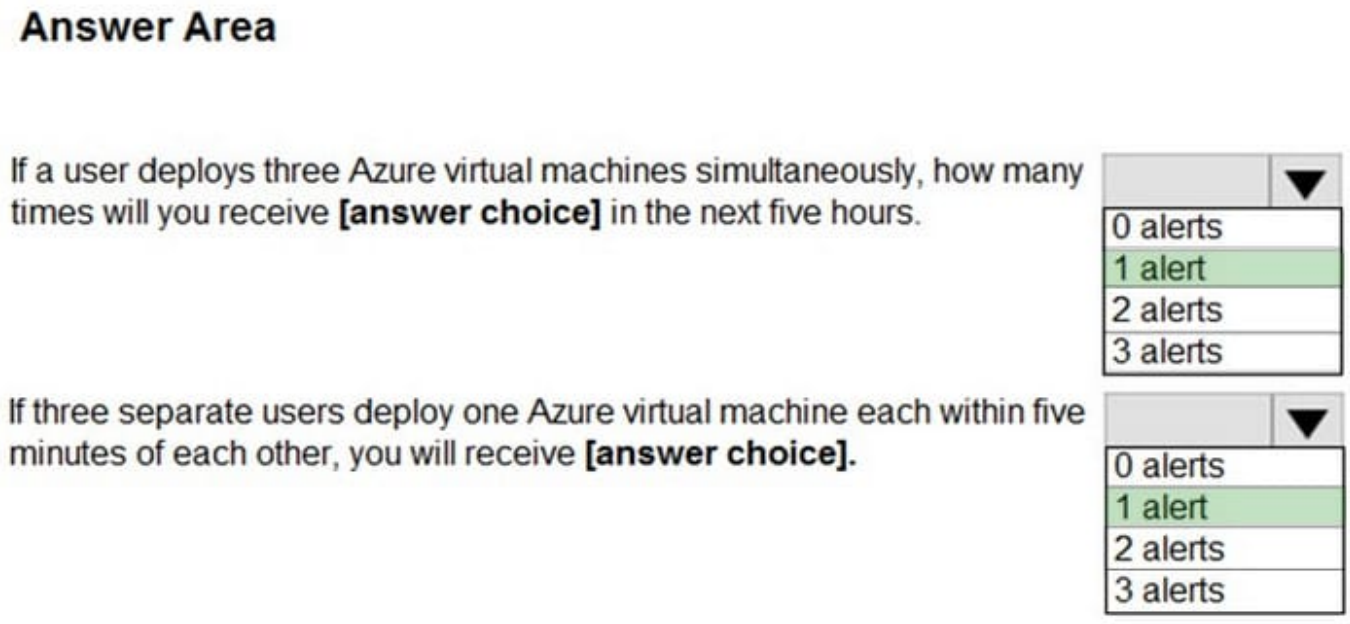
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



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

QUESTION 5

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

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

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

QUESTION 6

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

You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.

You need to create a data loss prevention (DLP) policy to protect the sensitive documents.

What should you use to detect which documents are sensitive?

A. SharePoint search

B. a hunting query in Microsoft 365 Defender

C. Azure Information Protection

D. RegEx pattern matching

Correct Answer: C

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

QUESTION 7

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: AD

QUESTION 8

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

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

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

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

NOTE: Each correct selection is worth one point.

A. Add a tag to the device group.

B. Add the device users to the admin role.

C. Add a tag to the machines.

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

E. Create a new admin role.

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

Correct Answer: ACD

Reference: https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/

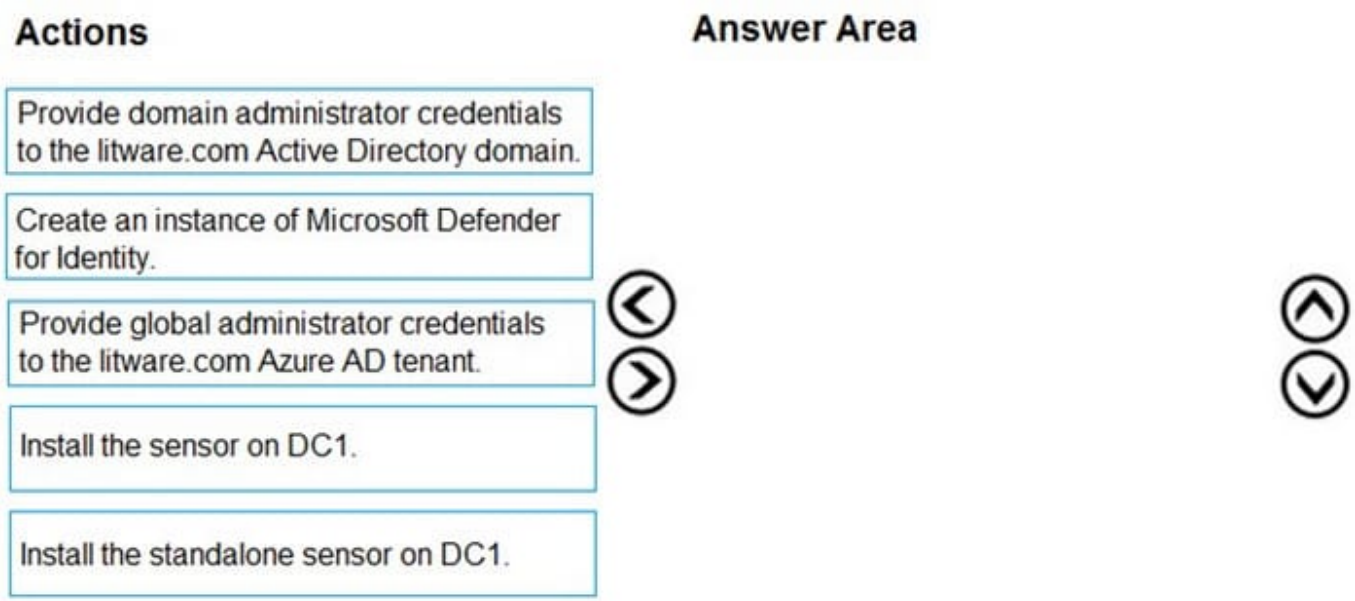
QUESTION 9

DRAG DROP

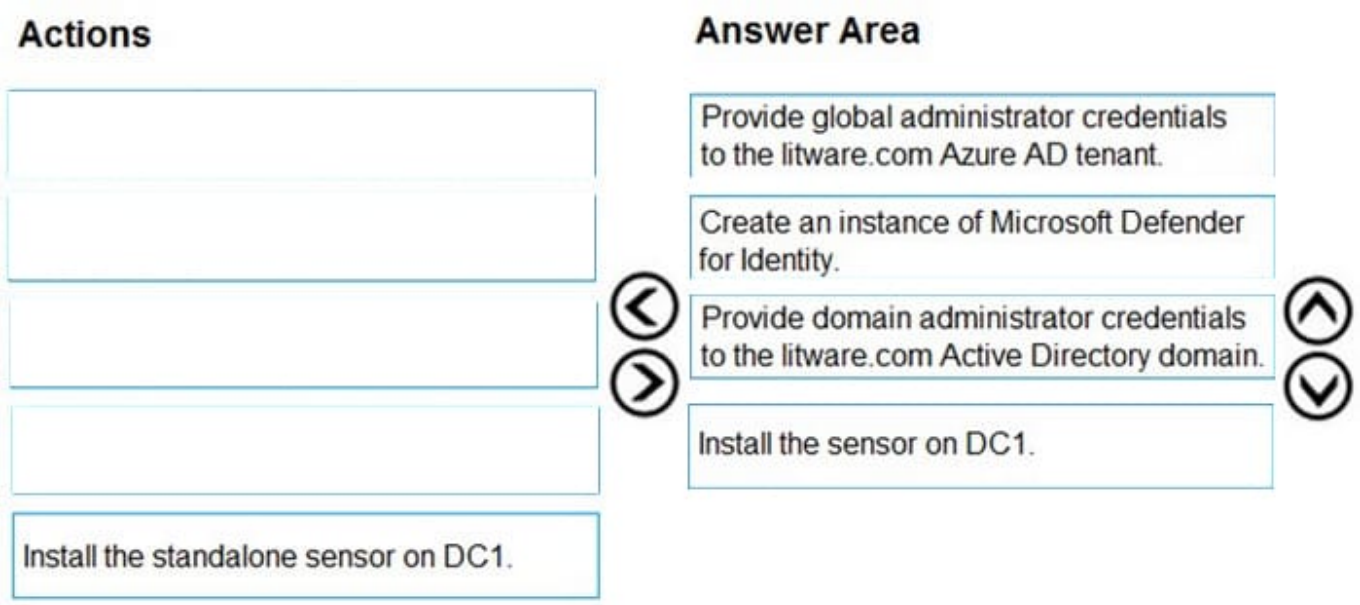
You need to configure DC1 to meet the business requirements.

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

Select and Place:



Correct Answer:



Step 1: log in to https://portal.atp.azure.com as a global admin Step 2: Create the instance Step 3. Connect the instance to Active Directory Step 4. Download and install the sensor.

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

QUESTION 10

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1

D. the Owner role for RG1

Correct Answer: C

QUESTION 11

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

A. executive

B. sales

C. marketing

Correct Answer: B

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

QUESTION 12

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

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

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

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

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

QUESTION 13

HOTSPOT

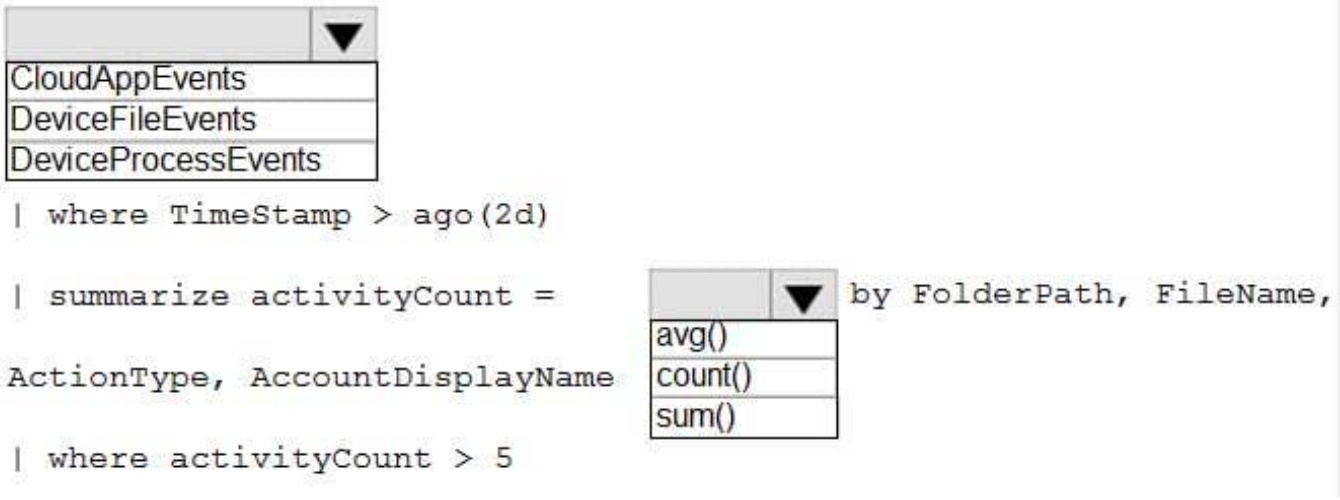
You need to create an advanced hunting query to investigate the executive team issue.

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

NOTE: Each correct selection is worth one point.

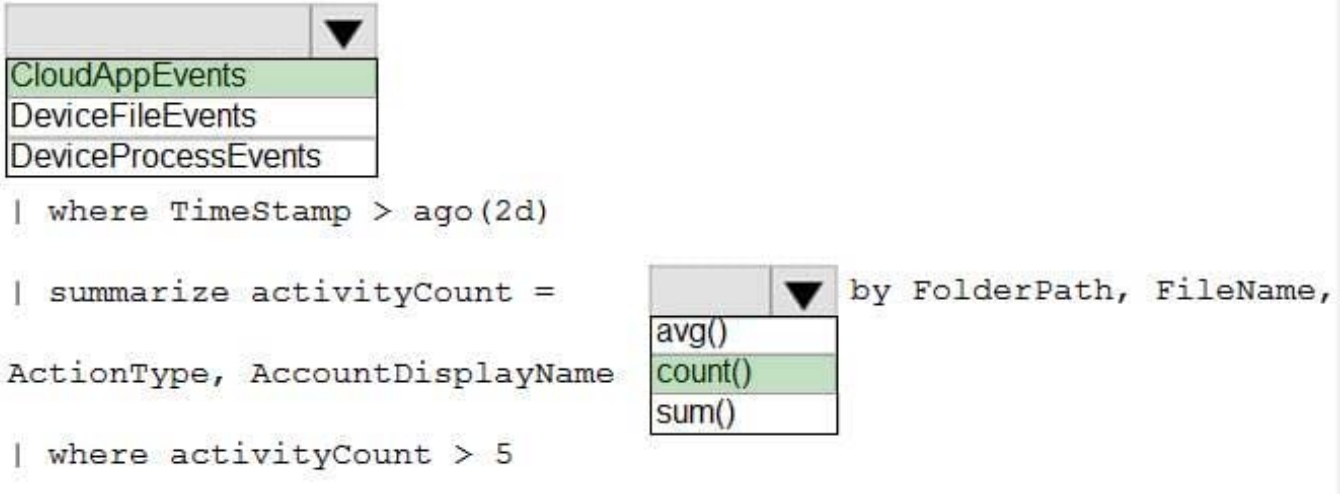
Hot Area:

Answer Area



Correct Answer:

Answer Area



QUESTION 14

You need to deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements. What should you do in Account1 first?

A. Create an AWS user for Defender for Cloud.

B. Configure AWS Security Hub.

C. Deploy the AWS Systems Manager (SSM) agent.

D. Create an Access control (IAM) role for Defender for Cloud.

Correct Answer: A

Dynamic scaled onboarding of AWS EC2 instances to Azure Arc using Ansible

Create an AWS identity

In order for Terraform to create resources in AWS, we will need to create a new AWS IAM role with appropriate permissions and configure Terraform to use it.

Scenario: Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and

does NOT have any agents installed.

Reference:

https://github.com/microsoft/azure_arc/blob/main/docs/azure_arc_jumpstart/azure_arc_servers/scaled_deployment/aws_scaled_ansible/_index.md

QUESTION 15

HOTSPOT

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

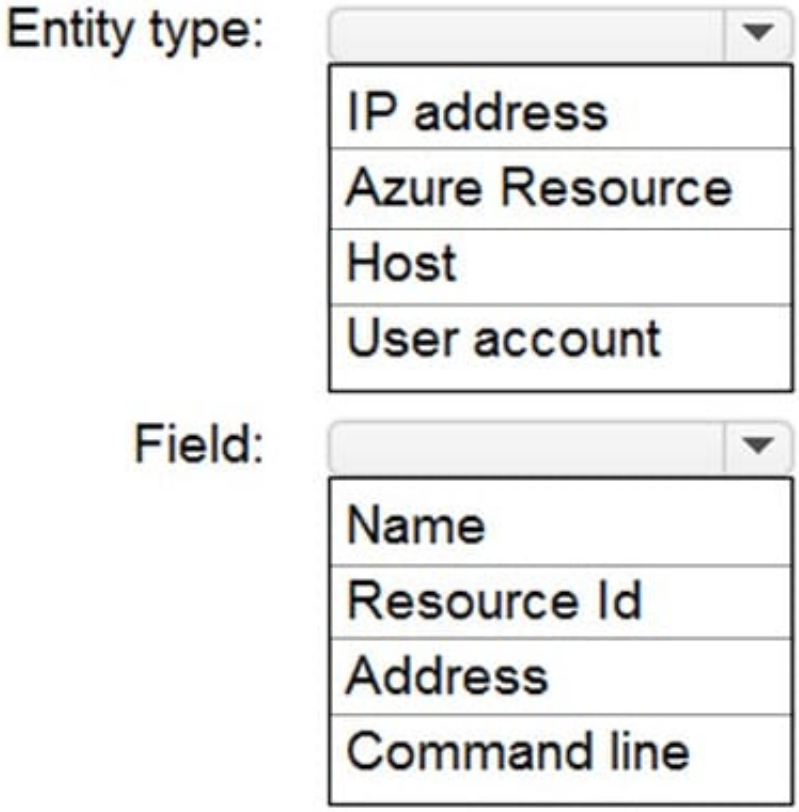
You need to hide Azure Defender alerts for the storage account.

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.

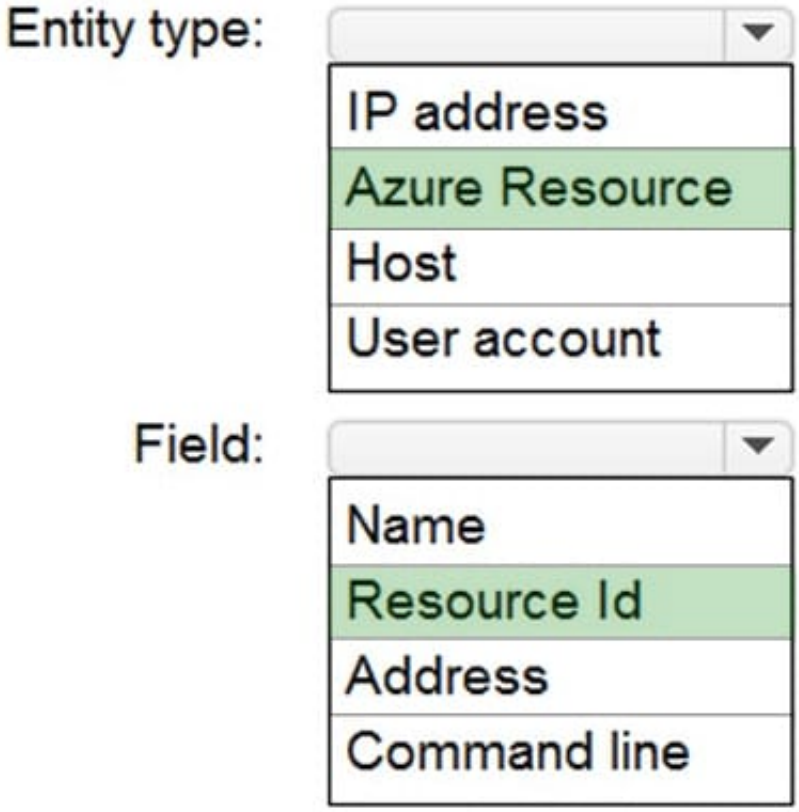
Hot Area:

Answer Area



Correct Answer:

Answer Area



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