SC-200$^{Q\&As}$

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

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

QUESTION 1

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

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

What should you use?

A. the 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

Track changes to sensitive groups with Advanced Hunting in Microsoft 365 Defender.

In my role working with Defender for Identity (MDI) customers, I\\'m often asked if MDI can help them answer questions about activities taking place within the environment. MDI does have a lot of information around the activities taking place in

Active Directory and now combined with the power of Advanced Hunting in Microsoft 365 Defender, we can help customers answer some these questions with ease and efficiency.

1.

MDI tracks the changes made to Active Directory group memberships. These changes are recorded by MDI as an activity and are available in the Microsoft 365 Defender Advanced Hunting, IdentityDirectoryEvents. MDI records these changes from two different sources:

2.

Tracking changes made to an entity by the Active Directory Update Sequence Number (USN). In the case of a group, MDI can see who has been added or removed from a group, but we don\\'t see the actor who made the change or which

domain controller the change was made on.

Tracking changes to a group, including who performed the action. MDI requires specific Windows events to be recorded on the domain controller.

Reference: https://techcommunity.microsoft.com/t5/security-compliance-and-identity/track-changes-to-sensitive-groups-with-advanced-hunting-in/ba-p/3275198

QUESTION 2

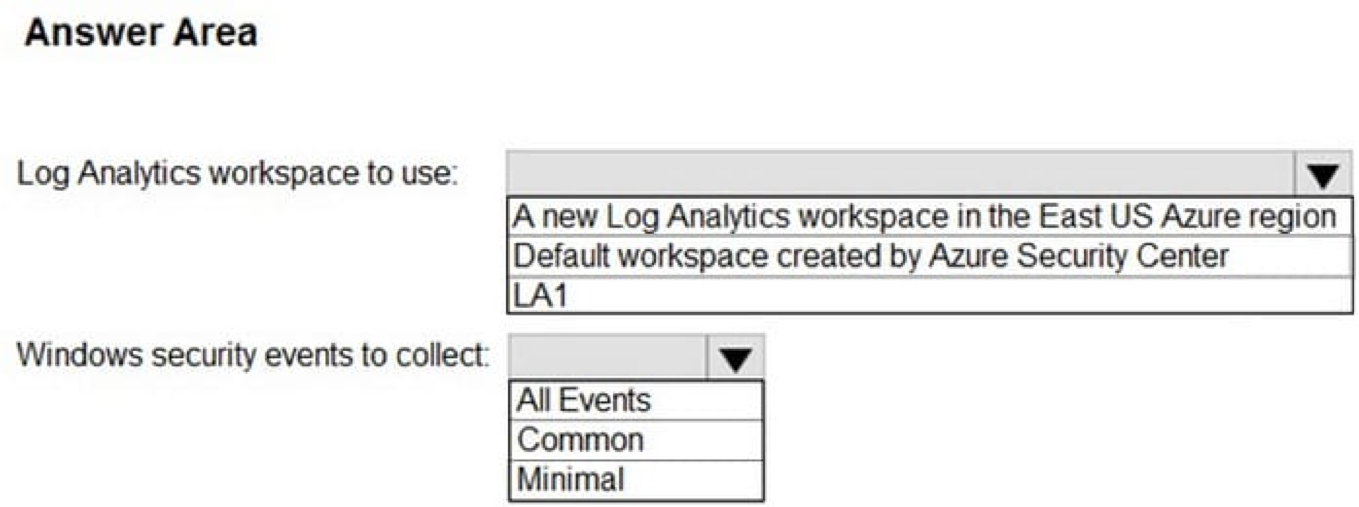
HOTSPOT

You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

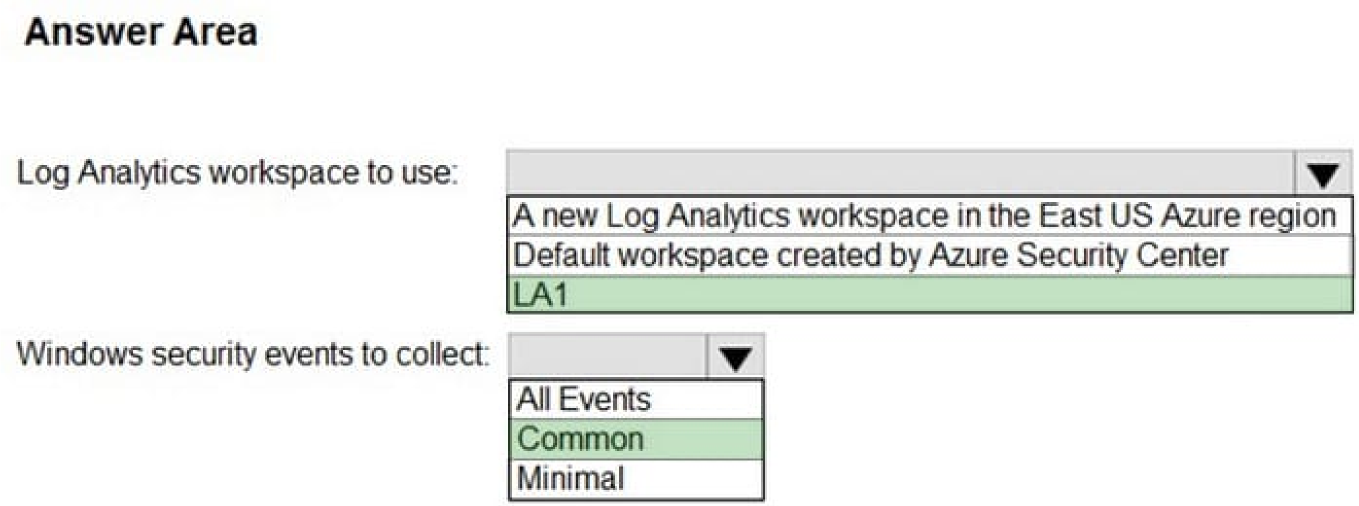
Log Analytics workspace to use: ▼

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

Windows security events to collect: ▼

- All Events
- Common
- Minimal

Correct Answer:



Answer Area

Log Analytics workspace to use: ▼

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

Windows security events to collect: ▼

- All Events
- [✓ Common]
- Minimal

QUESTION 3

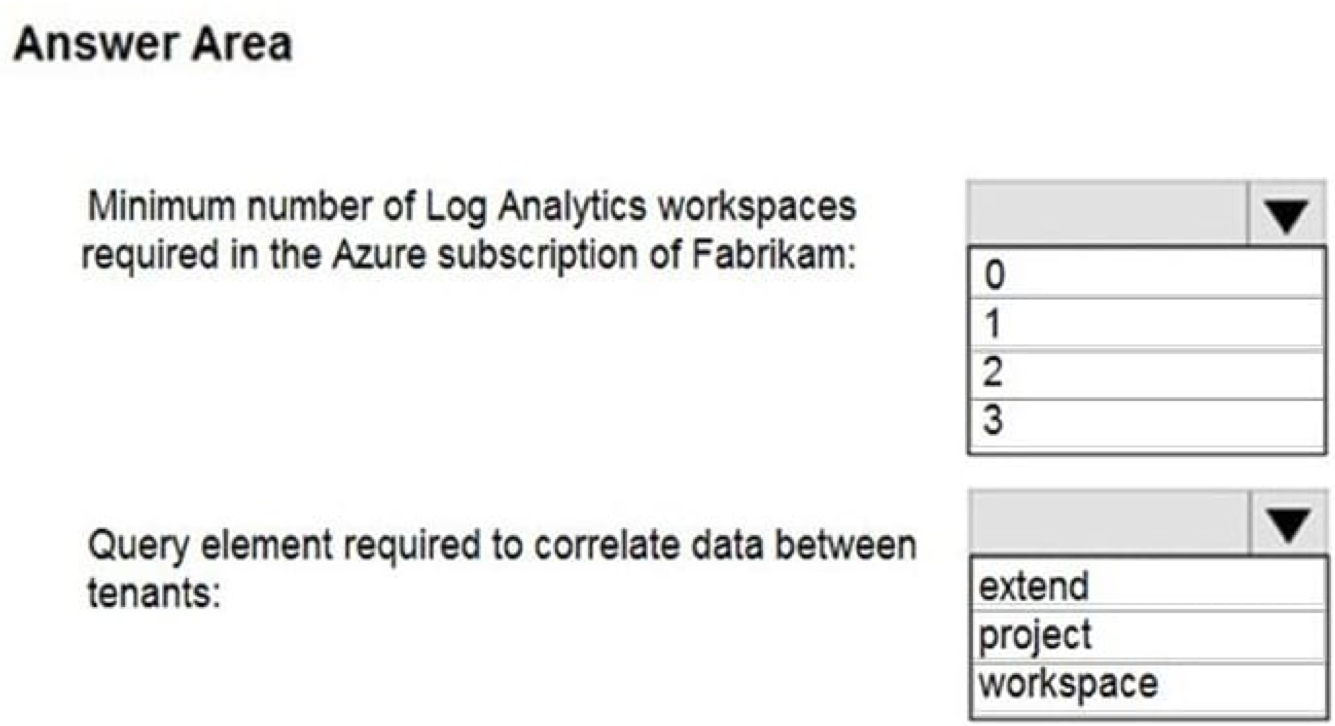
HOTSPOT

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

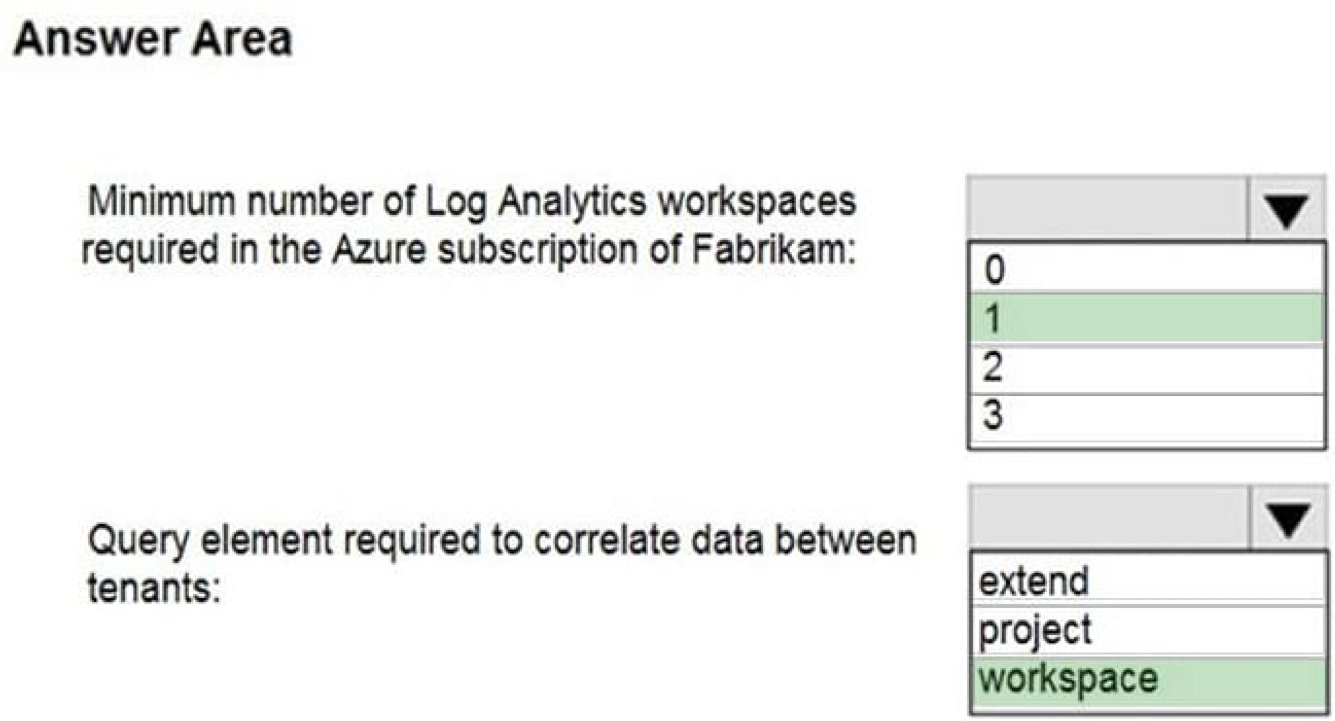
Minimum number of Log Analytics workspaces required in the Azure subscription of Fabrikam:

- 0
- 1
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- workspace

Correct Answer:



Answer Area

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

- 0
- [✓ 1]
- 2
- 3

Query element required to correlate data between tenants:

- extend
- project
- [✓ workspace]

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

QUESTION 4

A company uses Azure Security Center and Azure Defender. However, the security operator of the company doesn\\'t receive any email notifications for security alerts. What should be configured in Security Center to enable the email notifications?

A. Pricing and settings

B. Security solutions

C. Security policy

D. Azure Defender

Correct Answer: A

QUESTION 5

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 individual IP addresses in the range. Select Import and import the file.

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

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

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

Correct Answer: A

Import a list of IoCs

You can choose to upload a CSV file that defines the attributes of indicators, the action to be taken, and other details.

1.

Download the sample CSV to know the supported column attributes.

2.

In the navigation pane, select Settings > Endpoints > Indicators (under Rules).

3.

Select the tab of the entity type you\\'d like to import indicators for.

4.

Select Import > Choose file.

5.

Select Import. Do this for all the files you\\'d like to import.

6.

Select Done.

Note: You can create an indicator for:

Files

IP addresses

URLs/domains

Certificates

Incorrect:

Not B: Classless Inter-Domain Routing (CIDR) notation for IP addresses is not supported.

Not C: Only single IP addresses are supported (no CIDR blocks or IP ranges) in custom indicators.

Not D: Classless Inter-Domain Routing (CIDR) notation for IP addresses is not supported.

Note 2: Create an indicator for IPs, URLs, or domains from the settings page

1.

In the navigation pane, select Settings > Endpoints > Indicators (under Rules).

2.

Select the IP addresses or URLs/Domains tab.

Only single IP addresses are supported (no CIDR blocks or IP ranges) in custom indicators

3.

Select Add item.

4.

Specify the following details:

Indicator - Specify the entity details and define the expiration of the indicator.

Action - Specify the action to be taken and provide a description.

Scope - Define the scope of the machine group.

5.

Review the details in the Summary tab, then select Save.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-manage
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-indicators
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain