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.pass4itsure.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You need to visualize Microsoft 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 Microsoft Sentinel

B. Microsoft Defender for Cloud Apps

C. Azure Monitor

Correct Answer: A

To visualize Azure Sentinel data and enrich it by using third-party data sources to identify indicators of compromise (IoC), you can use notebooks in Azure Sentinel.

Notebooks in Azure Sentinel are interactive documents that allow you to run queries, create visualizations, and perform data analysis on your Azure Sentinel data. They also allow you to connect to other data sources, such as third-party

threat intelligence feeds, to enrich the data and identify indicators of compromise (IoCs).

Once you have connected to the third-party data source, you can use Azure Sentinel notebook to blend the data, and create visualizations, and perform data analysis to identify the potential attack.

Reference:

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

QUESTION 2

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.

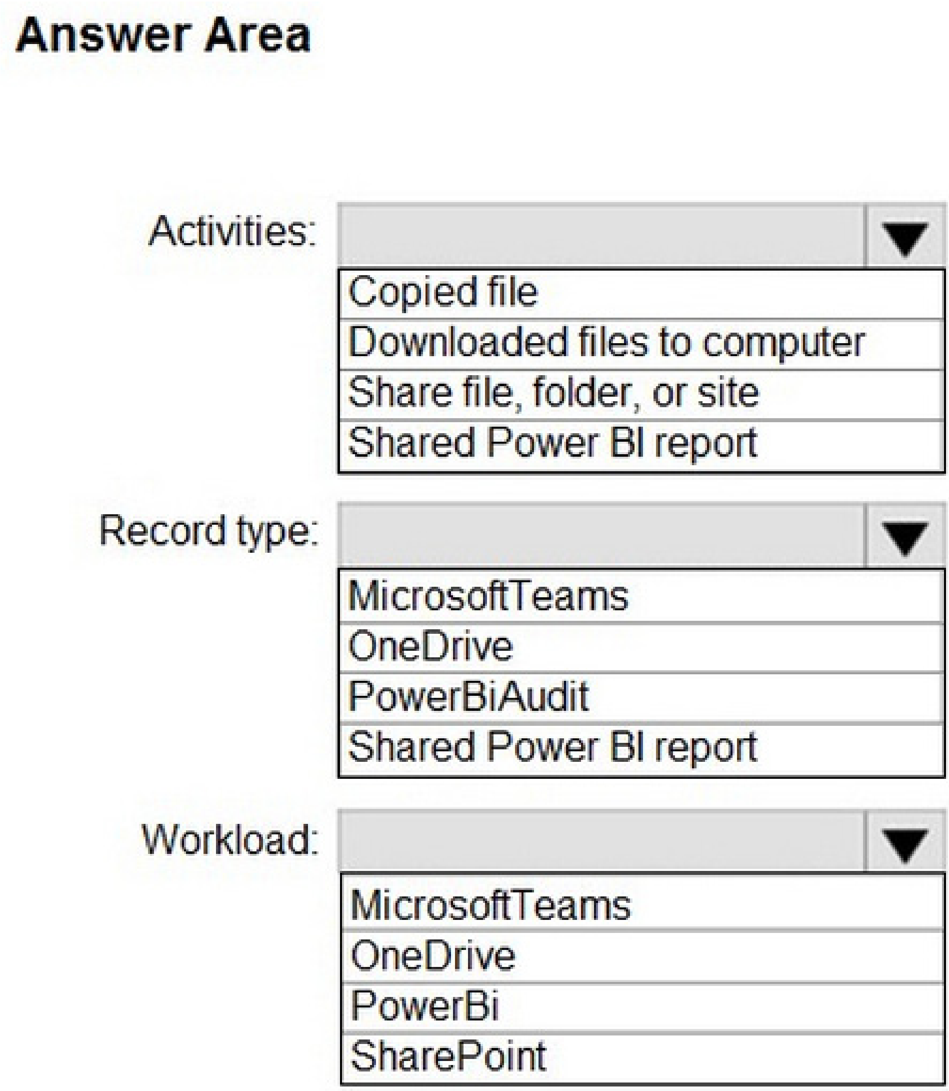
User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identify 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: ▼

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

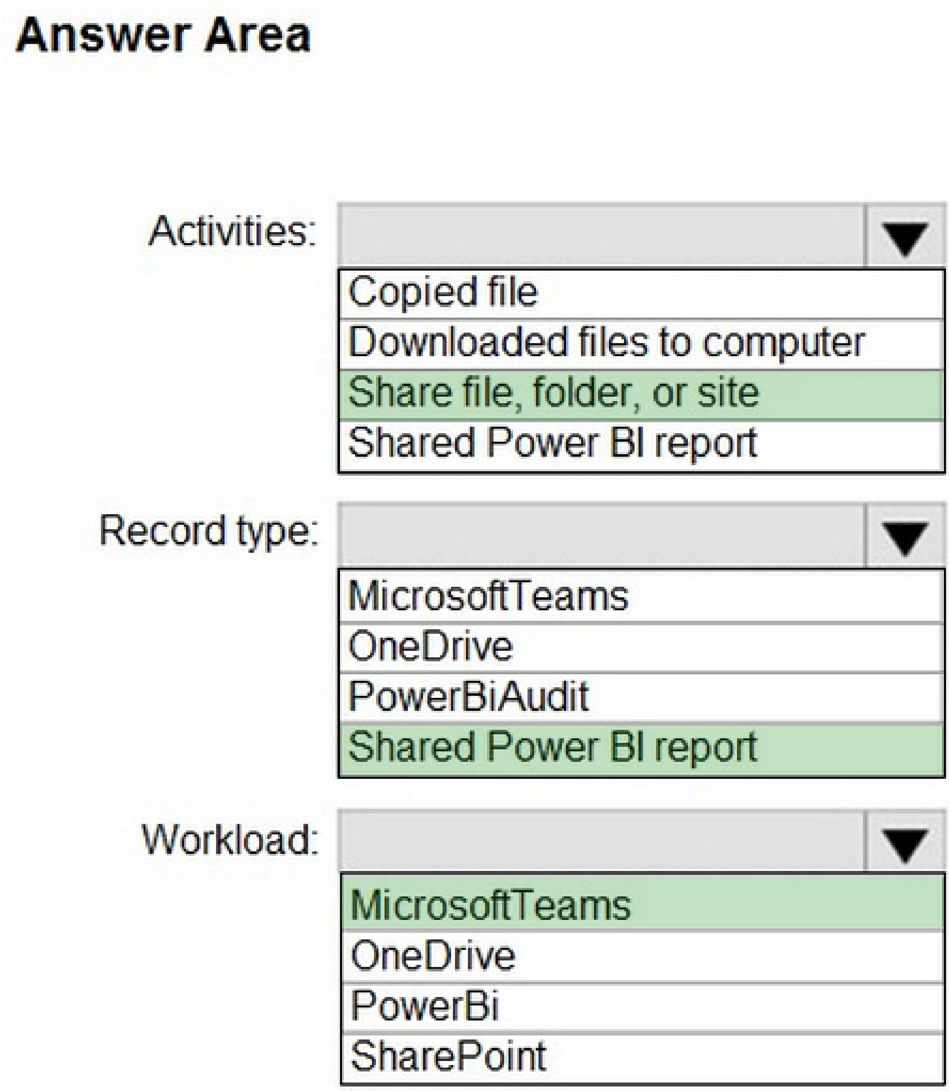
Record type: ▼

- MicrosoftTeams
- OneDrive
- PowerBiAudit
- Shared Power BI report

Workload: ▼

- MicrosoftTeams
- OneDrive
- PowerBi
- SharePoint

Correct Answer:



Answer Area

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

Record type:
- MicrosoftTeams
- OneDrive
- PowerBiAudit
- [✓ Shared Power BI report]

Workload:
- [✓ MicrosoftTeams]
- OneDrive
- PowerBi
- SharePoint

Box 1: Share file, folder, or site

Activities

Box 2: Shared Power BI report

Record type

Box 3: Microsoft teams

Workload

Note: Search-UnifiedAuditLog

Applies to:

Exchange Online, Exchange Online Protection

This cmdlet is available only in the cloud-based service.

Use the Search-UnifiedAuditLog cmdlet to search the unified audit log. This log contains events from Exchange Online, SharePoint Online, OneDrive for Business, Azure Active Directory, Microsoft Teams, Power BI, and other Microsoft 365 services. You can search for all events in a specified date range, or you can filter the results based on specific criteria, such as the user who performed the action, the action, or the target object.

Example:

Search-UnifiedAuditLog -StartDate 5/1/2018 -EndDate 5/8/2018 -RecordType SharePointFileOperation -Operations FileAccessed -SessionId "WordDocs_SharepointViews"-SessionCommand ReturnLargeSet

This example searches the unified audit log for any files accessed in SharePoint Online from May 1, 2018 to May 8, 2018. The data is returned in pages as the command is rerun sequentially while using the same SessionId value.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/security/defender/auditing

https://learn.microsoft.com/en-us/powershell/module/exchange/search-unifiedauditlog

QUESTION 3

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a user named User1.

You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege.

Which role should you assign to User1?

A. Security Administrator

B. Security Operator

C. Cloud Device Administrator

D. Desktop Analytics Administrator

Correct Answer: A

QUESTION 4

You have a Microsoft 365 E5 subscription.

Automated investigation and response (AIR) is enabled in Microsoft Defender for Office 365 and devices use full automation in Microsoft Defender for Endpoint.

You have an incident involving a user that received malware-infected email messages on a managed device.

Which action requires manual remediation of the incident?

A. soft deleting the email message

B. hard deleting the email message

C. isolating the device

D. containing the device

Correct Answer: C

QUESTION 5

You have an Azure subscription that uses Microsoft Defender for Cloud 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

Security Admin

View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.

Incorrect:

*

Security Reader

View permissions for Microsoft Defender for Cloud. Can view recommendations, alerts, a security policy, and security states, but cannot make changes.

* owner - too much permissions

*

Contributor (too much permissions)

Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Reference:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles