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.geekcert.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

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

The security team at your company detects command and control (C2) agent traffic on the network. Agents communicate once every 50 hours.

You need to create a Microsoft Defender XDR custom detection rule that will identify compromised devices and establish a pattern of communication. The solution must meet the following requirements:

1.

Identify all the devices that have communicated during the past 14 days.

2.

Minimize how long it takes to identify the devices. To what should you set the detection frequency for the rule?

A. Every 12 hours

B. Every 24 hours

C. Every three hours

D. Every hour

Correct Answer: B

QUESTION 2

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addresses and URLs.

What should you enable first in the advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. endpoint detection and response (EDR) in block mode

B. custom network indicators

C. web content filtering

D. Live response for servers

Correct Answer: B

Custom network indicators Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of

the location you have selected for your Microsoft Defender for Endpoint data.

QUESTION 3

You have a Microsoft Sentinel workspace.

You investigate an incident that has the following entities:

1.

A user account named User1

2.

An IP address of 192.168.10.200

3.

An Azure virtual machine named VM1

4.

An on-premises server named Server1

You need to label an entity as an indicator of compromise (IoC) directly by using the incidents page.

Which entity can you label?

A. 192.168.10.200

B. VM1

C. Server1

D. User1

Correct Answer: A

Add entities to threat intelligence in Microsoft Sentinel When investigating an incident, you examine entities and their context as an important part of understanding the scope and nature of the incident. In the course of the investigation, you may discover a domain name, URL, file, or IP address in the incident that should be labeled and tracked as an indicator of compromise (IOC), a threat indicator.

For example, you may discover an IP address performing port scans across your network, or functioning as a command and control node, sending and/or receiving transmissions from large numbers of nodes in your network.

Microsoft Sentinel allows you to flag these types of entities as malicious, right from within your incident investigation, and add it to your threat indicator lists. You\\'ll then be able to view the added indicators both in Logs and in the Threat Intelligence blade, and use them across your Microsoft Sentinel workspace.

Reference: https://learn.microsoft.com/en-us/azure/sentinel/add-entity-to-threat-intelligence

QUESTION 4

HOTSPOT

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

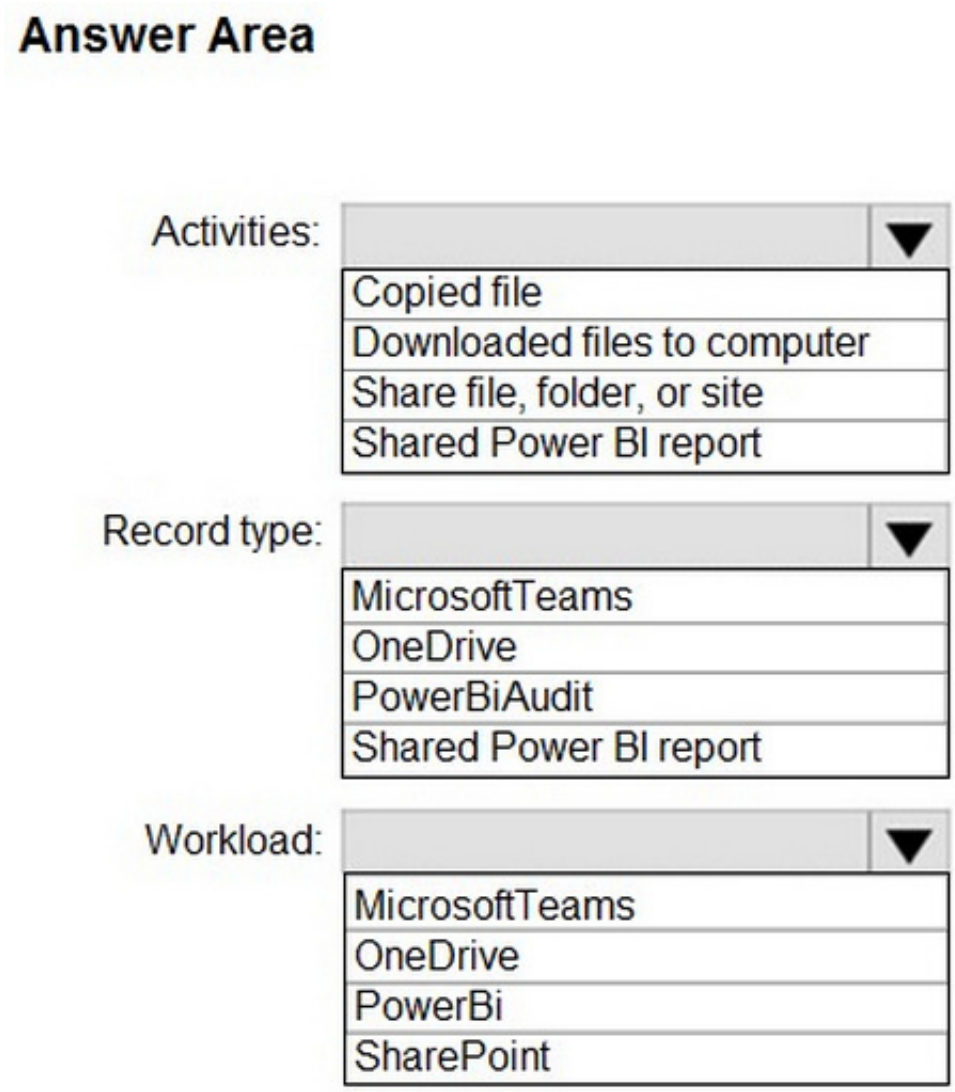
User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

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.

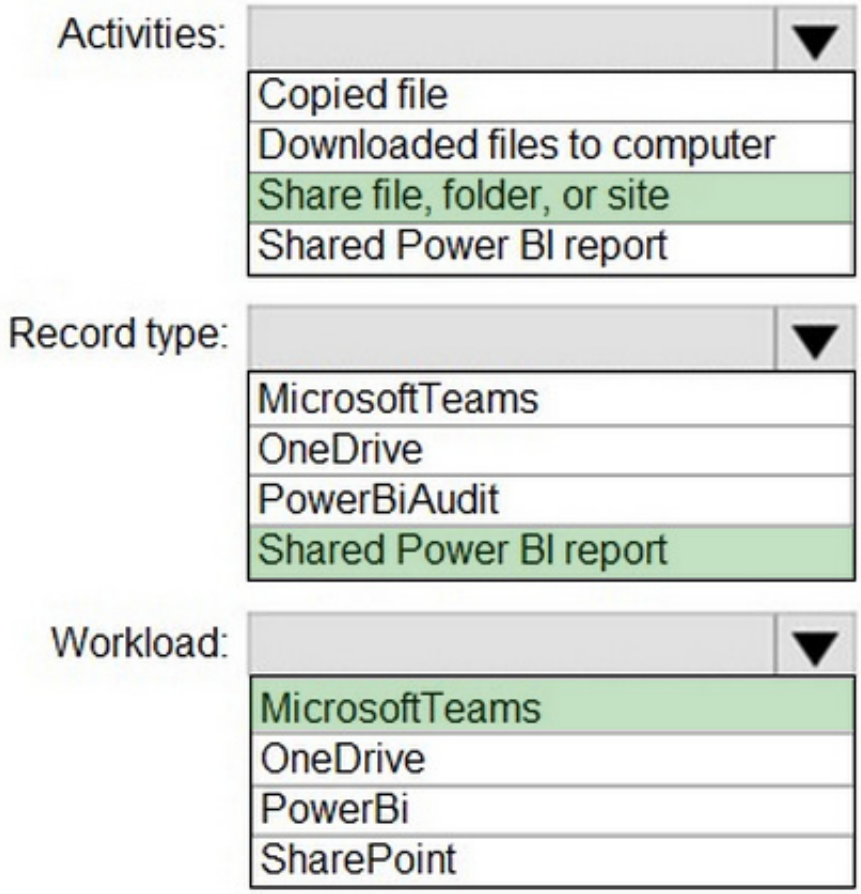
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



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 5

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 parses 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: D

Deploy parsers

Deploy parsers manually by copying them to the Azure Monitor Log page and saving the query as a function. This method is useful for testing.

To deploy a large number of parsers, we recommend using parser ARM templates, as follows:

Create a YAML file based on the relevant template for each schema and include your query in it. Start with the YAML template relevant for your schema and parser type, filtering or parameter-less.

Use the ASIM Yaml to ARM template converter to convert your YAML file to an ARM template.

If deploying an update, delete older versions of the functions using the portal or the function delete PowerShell tool.

Deploy your template using the Azure portal or PowerShell.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/normalization-develop-parsers

Latest SC-200 Dumps SC-200 Study Guide SC-200 Braindumps