# 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**

HOTSPOT

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

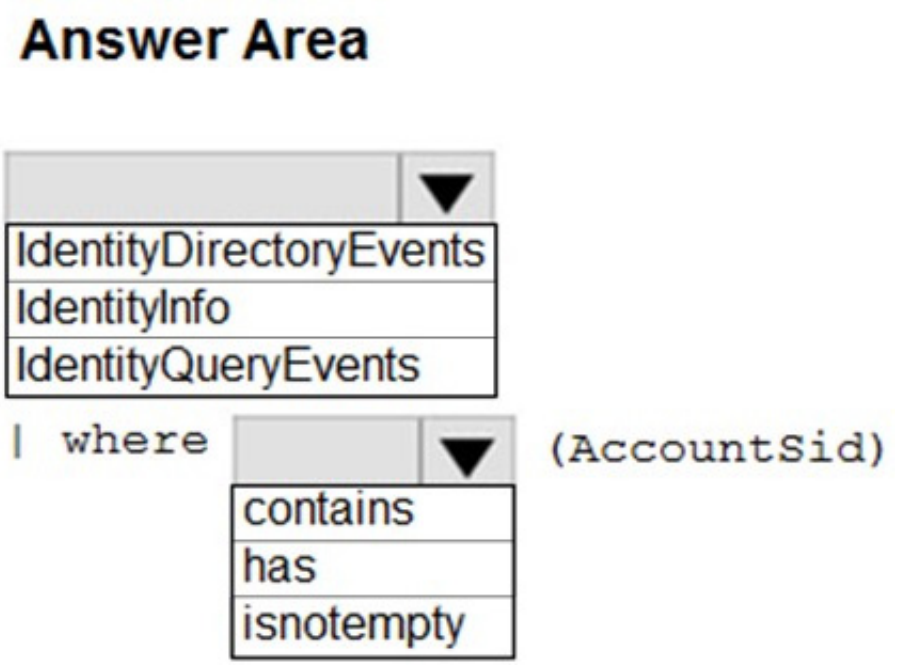
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify LDAP requests by AD DS users to enumerate AD DS objects.

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

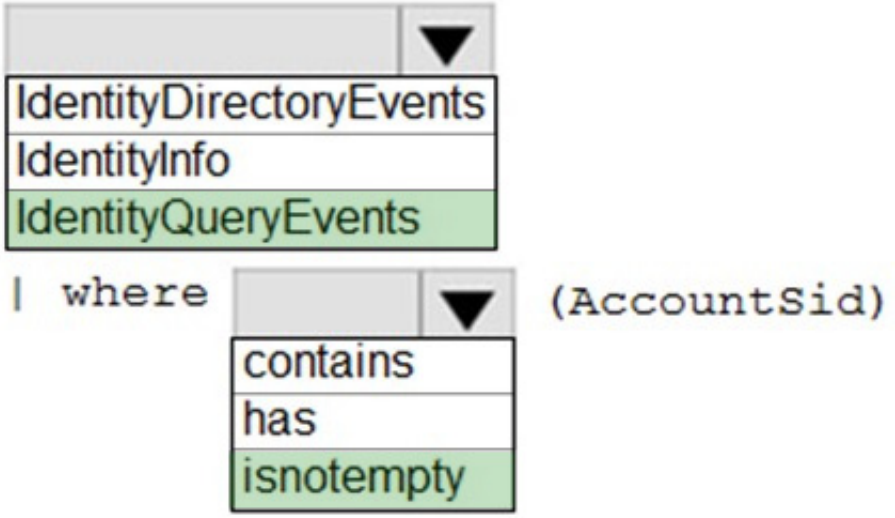
NOTE: Each correct selection is worth one point.

Hot Area:




Correct Answer:

## Answer Area




Box 1: IdentityQueryEvents

The IdentityQueryEvents table in the advanced hunting schema contains information about queries performed against Active Directory objects, such as users, groups, devices, and domains.

Box 2: isnotempty

Example:

IdentityQueryEvents

| where isnotempty(AccountSid)

| take 100

// IdentityQueryEvents

// - contains query activities performed against Active Directory objects, such as users, groups, devices, and domains monitored by Azure ATP

// - Includes SAMR, DNS and LDAP requests

// ----------

Incorrect:

IdentityInfo

The IdentityInfo table in the advanced hunting schema contains information about user accounts obtained from various services, including Azure Active Directory.

IdentityDirectoryEvents

IdentityDirectoryEvents

The IdentityDirectoryEvents table in the advanced hunting schema contains events involving an on-premises domain controller running Active Directory (AD). This table captures various identity-related events, like password changes,

password expiration, and user principal name (UPN) changes. It also captures system events on the domain controller, like scheduling of tasks and PowerShell activity.

Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identityqueryevents-table https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitydirectoryevents-table https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Webcasts/TrackingTheAdversary/Episode%201%20-%20KQL%20Fundamentals.txt

**QUESTION 2**

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 an Azure subscription that uses Microsoft Defender XDR.

From the Microsoft Defender portal, you perform an audit search and export the results as a file named File1.csv that contains 10,000 rows.

You use Microsoft Excel to perform Get and Transform Data operations to parse the AuditData column from File1.csv. The operations fail to generate columns for specific JSON properties.

You need to ensure that Excel generates columns for the specific JSON properties in the audit search results.

Solution: From Excel, you apply filters to the existing columns in File1.csv to reduce the number of rows, and then you perform the Get and Transform Data operations to parse the AuditData column.

Does this meet the requirement?

A. Yes

B. No

Correct Answer: B

**QUESTION 3**

HOTSPOT

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the

following requirements:

1.

Minimize administrative effort.

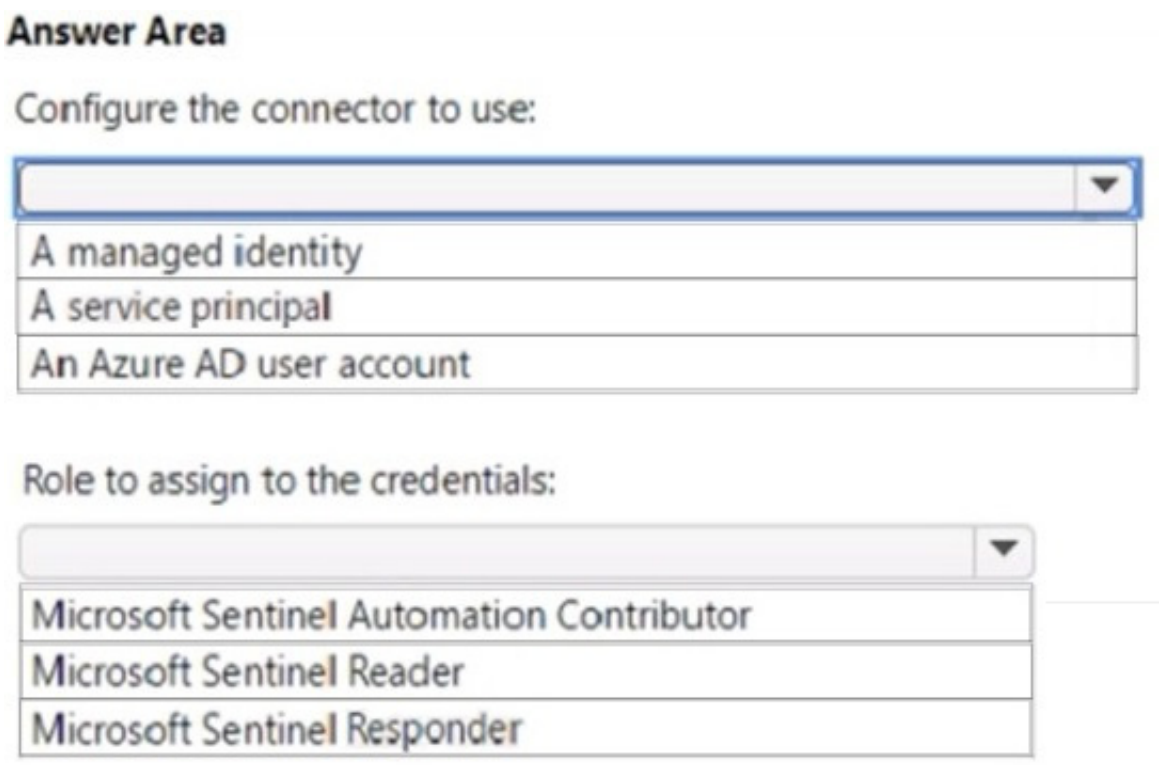
2.

Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

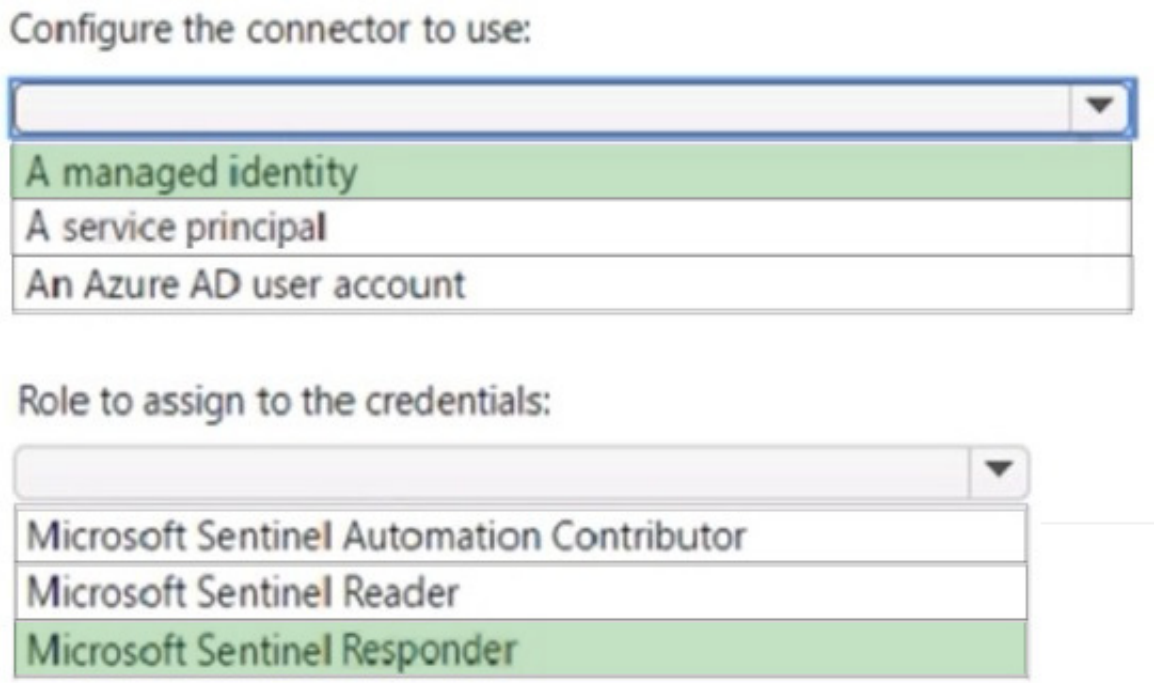
NOTE: Each correct selection is worth one point.

Hot Area:




Correct Answer:

**Answer Area**




Box 1: A managed identity Managed Identity for Azure Sentinel Logic Apps connector With the availability of Managed Identity for the Azure Sentinel connector, you can give permissions directly to the playbook (Logic App workflow resource), so Sentinel connector actions will operate on its behalf, as if it were an independent object which has permissions on Azure Sentinel. This lowers the number of identities you have to manage and gives the power to give access directly to the resource that operates.

Incorrect:

The service principal connection type allows us to create a registered application and use it as the identity behind the connector. You can define what this app can do, who can access it and what resources can this app access. It\\'s easy to delete it or replace its credentials if it\\'s suspected to have been compromised. For these reasons it\\'s great from a security perspective, but it still requires managing as another identity in the cloud that has credentials and permissions which potentially others can use.

Many would prefer not to authenticate with a user to a tool that generates automated actions. It is harder to audit (for example, using the incident table) which actions have been taken on behalf of a user and which are made by the playbook. It also makes less sense to see, for example, new comments that were generated by a playbook, but appear as if a user is their author. Also, if a user leaves the organization, you need to update all the connections that use its identity.

Box 2: Azure Sentinel Responder role

Reference: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-managed-identity-for-azure-sentinel-logic-apps/ba-p/2068204

**QUESTION 4**

You have an Azure subscription that uses Microsoft Defender for Cloud. You need to filter the security alerts view to show the following alerts:

1.

Unusual user accessed a key vault

2.

Log on from an unusual location

3.

Impossible travel activity Which severity should you use?

A. Informational

B. Low

C. Medium

D. High

Correct Answer: C

Medium This is probably a suspicious activity might indicate that a resource is compromised. Defender for Cloud\\'s confidence in the analytic or finding is medium and the confidence of the malicious intent is medium to high. These would usually be machine learning or anomaly-based detections, for example a sign-in attempt from an unusual location.

Incorrect:

*

High There is a high probability that your resource is compromised. You should look into it right away. Defender for Cloud has high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert that detects the execution of a known malicious tool such as Mimikatz, a common tool used for credential theft.

*

Low This might be a benign positive or a blocked attack. Defender for Cloud isn\\'t confident enough that the intent is malicious and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins. Defender for Cloud doesn\\'t usually tell you when attacks were blocked, unless it\\'s an interesting case that we suggest you look into.

*

Low This might be a benign positive or a blocked attack. Defender for Cloud isn\\'t confident enough that the intent is malicious and the activity might be innocent. For example, log clear is an action that might happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins. Defender for Cloud doesn\\'t usually tell you when attacks were blocked, unless it\\'s an interesting case that we suggest you look into.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview

**QUESTION 5**

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

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

NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common.

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C. From the Azure portal, create an Azure Event Grid subscription.

D. From the workspace created by Defender for Cloud, set the data collection level to All Events.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Correct Answer: AE

A (not D): What event types are stored for "Common" and "Minimal"?

The Common and Minimal event sets were designed to address typical scenarios based on customer and industry standards for the unfiltered frequency of each event and their usage.

*

Common - A set of events that satisfies most customers and provides a full audit trail.

This set is intended to provide a full user audit trail, including events with low volume. For example, this set contains both user logon events (event ID 4624) and user logoff events (event ID 4634). We include auditing actions like security

group changes, key domain controller Kerberos operations, and other events that are recommended by industry organizations.

*

Minimal

*

All events