



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

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



**QUESTION 1****DRAG DROP**

You have the resources shown in the following table.

Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

You need to prevent duplicate events from occurring in SW1.

What should you use for each action? To answer, drag the appropriate resources to the correct actions. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view

content.

NOTE: Each correct selection is worth one point.

Select and Place:

Resources**Answer Area**

SW1

CEF1

Server1

Server2

From the Syslog configuration, remove the facilities that send CEF messages.

From the Log Analytics agent, disable Syslog synchronization.

Correct Answer:



Resources

Answer Area

SW1

CEF1

Server1

Server2

From the Syslog configuration, remove the facilities that send CEF messages.

Server1

From the Log Analytics agent, disable Syslog synchronization.

Server1

Using the same machine to forward both plain Syslog and CEF messages

If you plan to use this log forwarder machine to forward Syslog messages as well as CEF, then in order to avoid the duplication of events to the Syslog and CommonSecurityLog tables:

On each source machine that sends logs to the forwarder in CEF format, you must edit the Syslog configuration file to remove the facilities that are being used to send CEF messages. This way, the facilities that are sent in CEF won't also be

sent in Syslog. See Configure Syslog on Linux agent for detailed instructions on how to do this.

You must run the following command on those machines to disable the synchronization of the agent with the Syslog configuration in Microsoft Sentinel. This ensures that the configuration change you made in the previous step does not get

overwritten.

```
sudo su omsagent -c '\python /opt/microsoft/omsconfig/Scripts/OMS_MetaConfigHelper.py --disable\'
```

QUESTION 2

HOTSPOT

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

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

You need to identify all the interactive authentication attempts by the users in the finance department of your company.

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:



Answer Area

	▼
BehaviorAnalytics	
IdentityInfo	
IdentityQueryEvents	

```
| where Department == 'Finance'  
| project-rename objid = AccountObjectId  
| join
```

	▼
AuditLogs	
IdentityLogonEvents	
SigninLogs	

```
on $left.objid == $right.AccountObjectId
```

Correct Answer:

Answer Area

	▼
BehaviorAnalytics	
IdentityInfo	
IdentityQueryEvents	

```
| where Department == 'Finance'  
| project-rename objid = AccountObjectId  
| join
```

	▼
AuditLogs	
IdentityLogonEvents	
SigninLogs	

```
on $left.objid == $right.AccountObjectId
```

Box 1: IdentityInfo Example: IdentityInfo | where JobTitle == "CONSULTANT" | join hint.shufflekey = AccountObjectId (IdentityDirectoryEvents

| where Application == "Active Directory" | where ActionType == "Private data retrieval") on AccountObjectId

Note: The IdentityInfo table in the advanced hunting schema contains information about user accounts obtained from various services, including Azure Active Directory. Use this reference to construct queries that return information from this table.

AccountObjectId Unique identifier for the account in Azure AD

Department Name of the department that the account user belongs to

Box 2: IdentityLogonEvents The IdentityLogonEvents table in the advanced hunting schema contains information about authentication activities made through your on-premises Active Directory captured by Microsoft Defender for Identity and authentication activities related to Microsoft online services captured by Microsoft Defender for Cloud Apps.



Column names include:

AccountObjectId Unique identifier for the account in Azure AD

Etc.

Incorrect:

Audit Logs (User and group management activity)

SignInLogs (Authentication Activity)

Reference: <https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identityinfo-table>

<https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitylogonevents-table>

QUESTION 3

HOTSPOT

You need to implement the ASIM query for DNS requests. The solution must meet the Microsoft Sentinel requirements. How should you configure the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

ASIM parser:

	▼
_Im_Dns	
_Im_Dns_InfobloxNIOs	
imDns	

Filter:

	▼
A filtering parameter	
A pack parameter	
The WHERE clause	

Correct Answer:



Answer Area

ASIM parser:

	▼
_Im_Dns	
_Im_Dns_InfobloxNIOs	
imDns	

Filter:

	▼
A filtering parameter	
A pack parameter	
The WHERE clause	

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription.

You need to identify all the security principals that submitted requests to change or delete groups.

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:



Answer Area

MicrosoftGraphActivityLogs

| where contains '/group'

RequestUri

Scopes

Type

| where RequestMethod !=

"GET"

"POST"

"PUT"

| project AppId, UserId, ServicePrincipalId

Correct Answer:

Answer Area

MicrosoftGraphActivityLogs

| where contains '/group'

RequestUri

Scopes

Type

| where RequestMethod !=

"GET"

"POST"

"PUT"

| project AppId, UserId, ServicePrincipalId

QUESTION 5

HOTSPOT



You have a Microsoft Sentinel workspace named Workspace1.

You configure Workspace1 to collect DNS events and deploy the Advanced Security Information Model (ASIM) unifying parser for the DNS schema.

You need to query the ASIM DNS schema to list all the DNS events from the last 24 hours that have a response code of 'NXDOMAIN'

Correct Answer:

Answer Area

	▼
_Im_Dns	
Dns	
imDns	

	▼
(starttime=ago(1d).responsecodename= 'NXDOMAIN'	
where TimeGenerated > ago(1d) where ResponseCodeName =~ "NXDOMAIN"	
where ResponseCodeName = "NXDOMAIN" where TimeGenerated > ago(1d)	
summarize count() by SrcIpAddr, bin(TimeGenerated,15m)	

Box 1: _Im_Dns

Example:

If your data source supports full DNS logging and you've chosen to log multiple segments, adjust your queries to prevent data duplication in Microsoft Sentinel.

For example, you might modify your query with the following normalization:

KQL

_Im_Dns | where SrcIpAddr != "127.0.0.1" and EventSubType == "response"

Box 2: | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN" Example without filtering parameters would look like this:

Kusto

_Im_Dns | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN" | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)

Incorrect:

(starttime=ago(1d), responsecodename='NXDOMAIN')



Closing parantheses missing.

Correct would be: (starttime=ago(1d), responsecodename=\\'NXDOMAIN\\') as in the following code:

```
_Im_Dns(starttime=ago(1d), responsecodename=\\'NXDOMAIN\\') | summarize count() by SrcIpAddr, bin(TimeGenerated,15m)
```

Reference: <https://learn.microsoft.com/en-us/azure/sentinel/normalization-schema-dns>

[Latest SC-200 Dumps](#)

[SC-200 Practice Test](#)

[SC-200 Exam Questions](#)