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 Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements:

1.

Ensure that failed sign-in alerts are generated for other accounts.

2.

Minimize administrative effort What should do?

A. Create an automation rule.

B. Create a watchlist.

C. Modify the analytics rule.

D. Add an activity template to the entity behavior.

Correct Answer: A

There are two methods for avoiding false positives:

Automation rules create exceptions without modifying analytics rules.

Scheduled analytics rules modifications permit more detailed and permanent exceptions.

Automation rules

Can apply to several analytics rules.

Keep an audit trail. Exceptions prevent incident creation, but alerts are still recorded for audit purposes.

Are often generated by analysts.

Allow applying exceptions for a limited time. For example, maintenance work might trigger false positives that outside the maintenance timeframe would be true incidents.

Incorrect:

Not A: Analytics rules modifications

Allow advanced boolean expressions and subnet-based exceptions.

Let you use watchlists to centralize exception management.

Typically require implementation by Security Operations Center (SOC) engineers.

Are the most flexible and complete false positive solution, but are more complex

Reference:

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

QUESTION 2

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal. From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

D. Incidents

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

QUESTION 3

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

You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.

What should you configure first?

A. the User enrichment settings

B. the Azure connector

C. the Office 365 connector

D. the Automatic log upload settings

Correct Answer: C

How to connect Microsoft 365 to Defender for Cloud Apps

1.

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Under Connected apps, select App Connectors.

2.

In the App connectors page, select +Connect an app, and then select Microsoft 365.

3.

In the Select Microsoft 365 components page, select the options you require, and then select Connect.

4.

On the Follow the link page, select Connect Microsoft 365.

5.

After Microsoft 365 is displayed as successfully connected, select Done.

6.

In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Under Connected apps, select App Connectors. Make sure the status of the connected App Connector is Connected.

Reference: https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365

QUESTION 4

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365. You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal. Which response action should you use?

A. Run antivirus scan

B. Initiate Automated Investigation

C. Collect investigation package

D. Initiate Live Response Session

Correct Answer: D

QUESTION 5

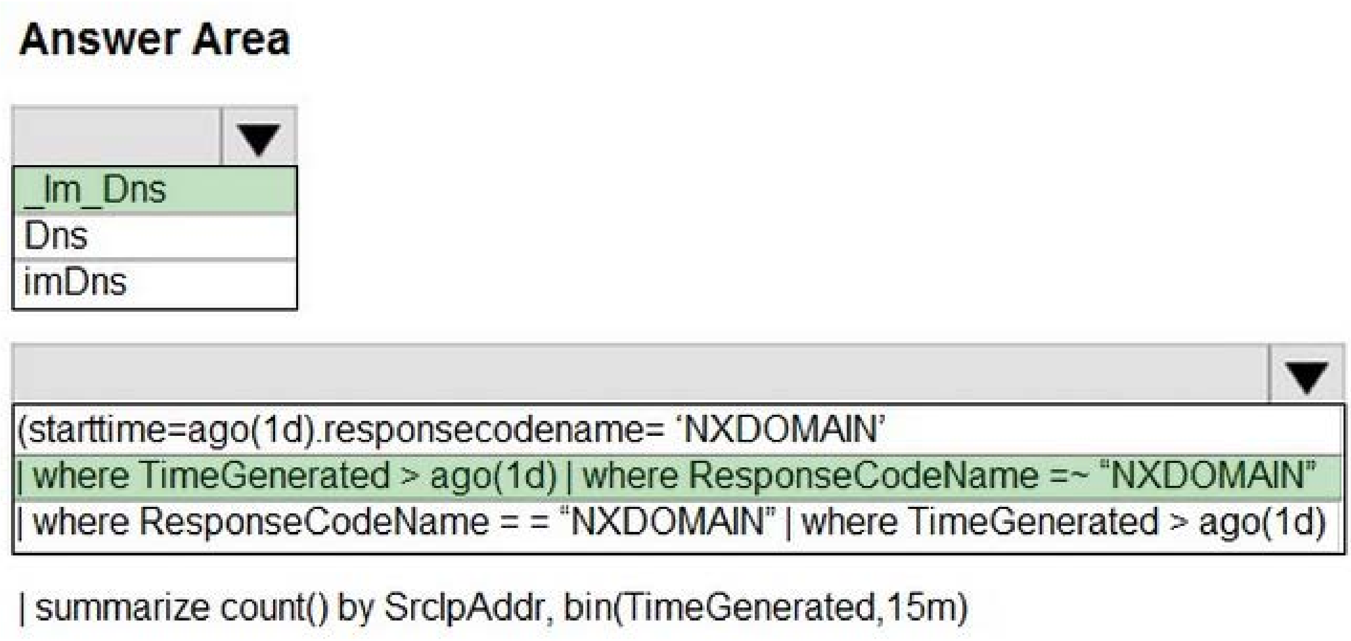
HOTSPOT

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

QUESTION 6

You have two Azure subscriptions that use Microsoft Defender for Cloud.

You need to ensure that specific Defender for Cloud security alerts are suppressed at the root management group level. The solution must minimize administrative effort.

What should you do in the Azure portal?

A. Create an Azure Policy assignment.

B. Modify the Workload protections settings in Defender for Cloud.

C. Create an alert rule in Azure Monitor.

D. Modify the alert settings in Defender for Cloud.

Correct Answer: A

You can use alerts suppression rules to suppress false positives or other unwanted security alerts from Defender for Cloud. Note: To create a rule directly in the Azure portal:

1.

From Defender for Cloud\\'s security alerts page:

Select the specific alert you don\\'t want to see anymore, and from the details pane, select Take action.

Or, select the suppression rules link at the top of the page, and from the suppression rules page select Create new suppression rule:

2.

In the new suppression rule pane, enter the details of your new rule. Your rule can dismiss the alert on all resources so you don\\'t get any alerts like this one in the future. Your rule can dismiss the alert on specific criteria - when it relates to

a specific IP address, process name, user account, Azure resource, or location.

3.

Enter details of the rule.

4.

Save the rule.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules

QUESTION 7

DRAG DROP

You have an Azure subscription.

You need to delegate permissions to meet the following requirements:

1.

Enable and disable Azure Defender.

2.

Apply security recommendations to resource.

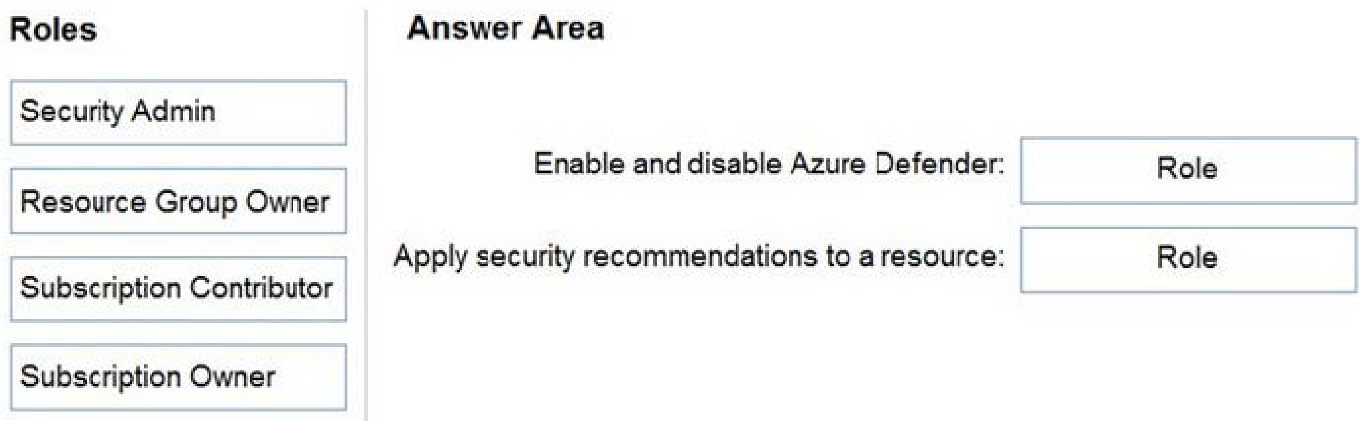
The solution must use the principle of least privilege.

Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements. Each role 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:



Roles

Security Admin

Resource Group Owner

Subscription Contributor

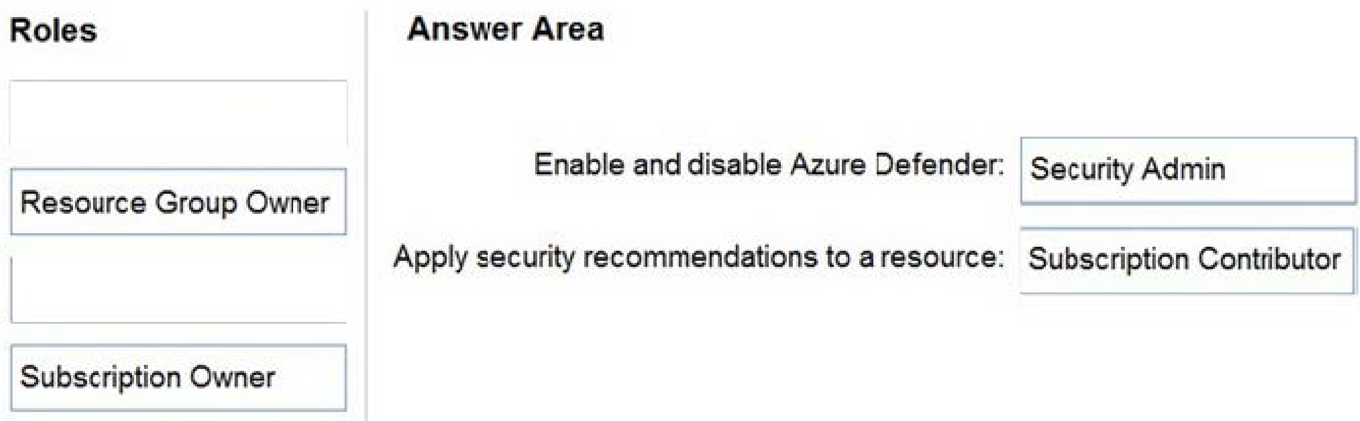
Subscription Owner

Answer Area

Enable and disable Azure Defender: Role

Apply security recommendations to a resource: Role

Correct Answer:



Roles

Resource Group Owner

Subscription Owner

Answer Area

Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Subscription Contributor

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

QUESTION 8

You have a Microsoft Sentinel playbook that is triggered by using the Azure Activity connector.

You need to create a new near-real-time (NRT) analytics rule that will use the playbook.

What should you configure for the rule?

A. the incident automation settings

B. the query rule

C. entity mapping

D. the Alert automation settings

Correct Answer: C

Entity mapping is an integral part of the configuration of scheduled query analytics rules. It enriches the rules\\' output (alerts and incidents) with essential information that serves as the building blocks of any investigative processes and remedial actions that follow.

Note: How to map entities

1.

From the Microsoft Sentinel navigation menu, select Analytics.

2.

Select a scheduled query rule and select Edit from the details pane. Or create a new rule by clicking Create > Scheduled query rule at the top of the screen.

3.

Select the Set rule logic tab.

4.

In the Alert enrichment section, expand Entity mapping.

5.

In the now-expanded Entity mapping section, select an entity type from the Entity type drop-down list.

Note 2: The configuration of NRT rules is in most ways the same as that of scheduled analytics rules.

You can refer to multiple tables and watchlists in your query logic.

*-> You can use all of the alert enrichment methods: entity mapping, custom details, and alert details.

You can choose how to group alerts into incidents, and to suppress a query when a particular result has been generated.

You can automate responses to both alerts and incidents.

Reference:

https://learn.microsoft.com/en-us/azure/sentinel/map-data-fields-to-entities

QUESTION 9

HOTSPOT

You have an Azure subscription that contains a Log Analytics workspace named Workspace1.

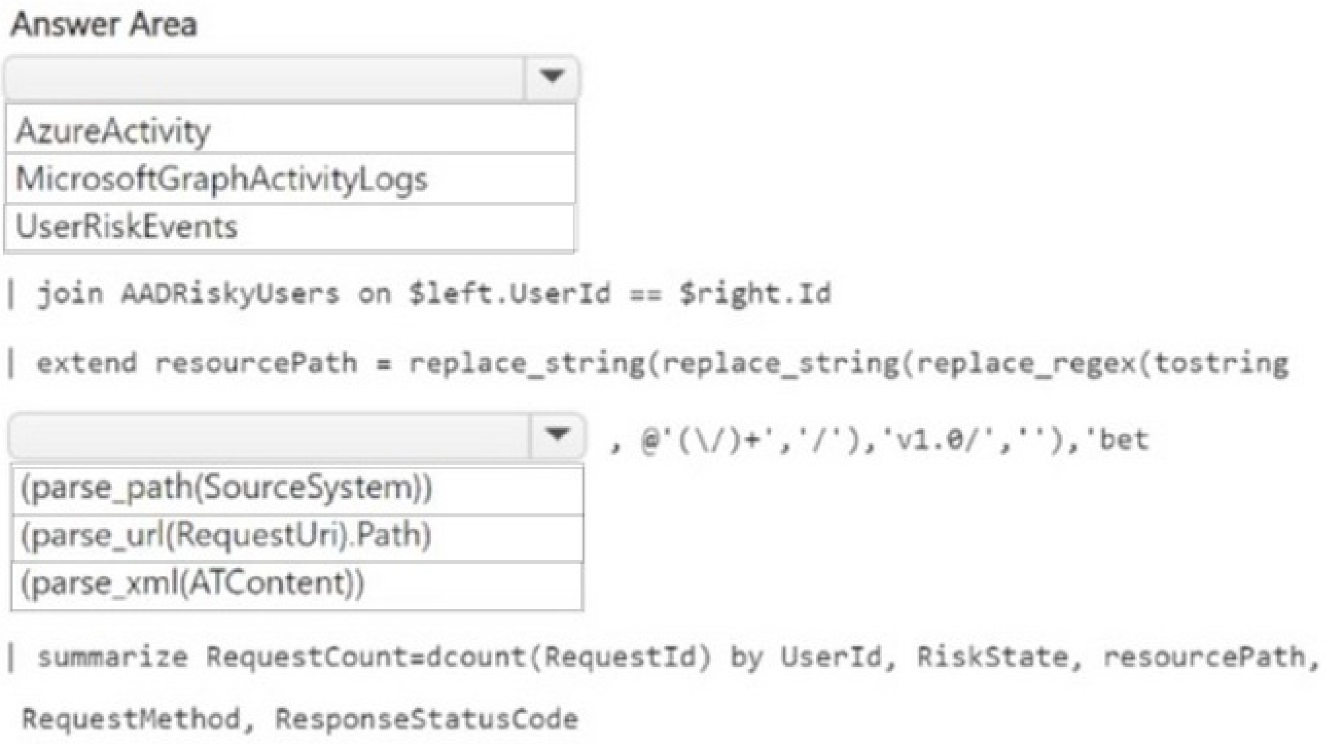
You configure Azure activity logs and Microsoft Entra ID logs to be forwarded to Workspace1.

You need to identify which Azure resources have been queried or modified by risky users.

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

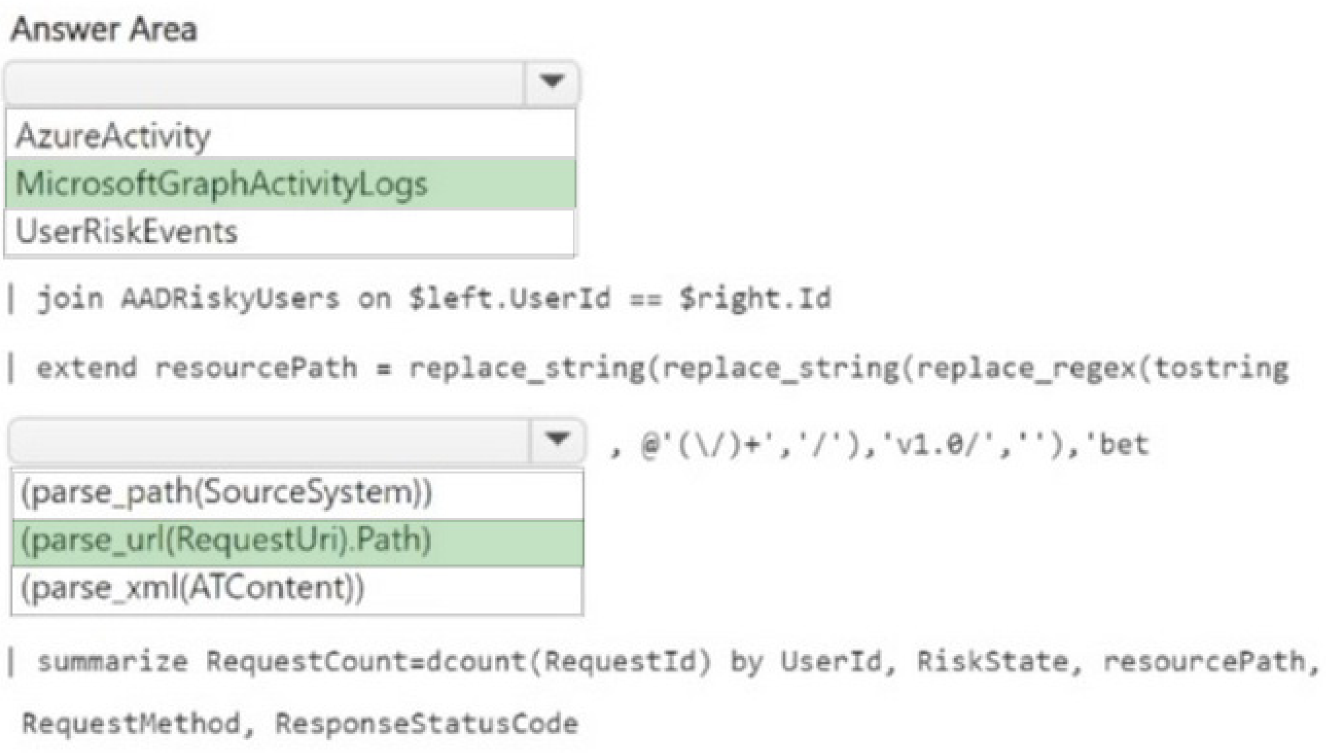
- AzureActivity
- MicrosoftGraphActivityLogs
- UserRiskEvents

```
| join AADRiskyUsers on $left.UserId == $right.Id
| extend resourcePath = replace_string(replace_string(replace_regex(tostring
```

- (parse_path(SourceSystem))
- (parse_url(RequestUri).Path)
- (parse_xml(ATContent))

```
, @'(\/)+','/'),'v1.0/',''),'bet
| summarize RequestCount=dcount(RequestId) by UserId, RiskState, resourcePath,
 RequestMethod, ResponseStatusCode
```

Correct Answer:



Answer Area

AzureActivity
[✓ MicrosoftGraphActivityLogs]
UserRiskEvents

```
| join AADRiskyUsers on $left.UserId == $right.Id
| extend resourcePath = replace_string(replace_string(replace_regex(tostring
```

(parse_path(SourceSystem))
[✓ (parse_url(RequestUri).Path)]
(parse_xml(ATContent))

```
, @'(\/)+','/'),'v1.0/',''),'bet
| summarize RequestCount=dcount(RequestId) by UserId, RiskState, resourcePath,
RequestMethod, ResponseStatusCode
```

QUESTION 10

HOTSPOT

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

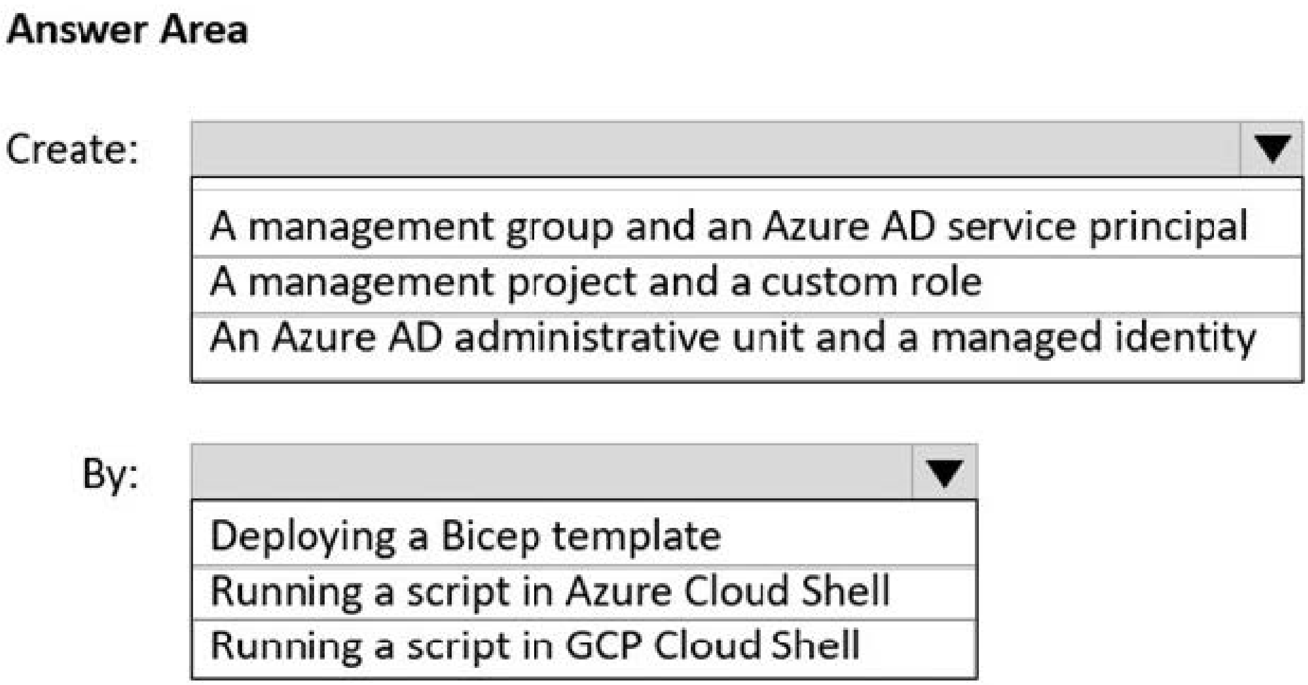
You create a Google Cloud Platform (GCP) organization named GCP1.

You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.

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

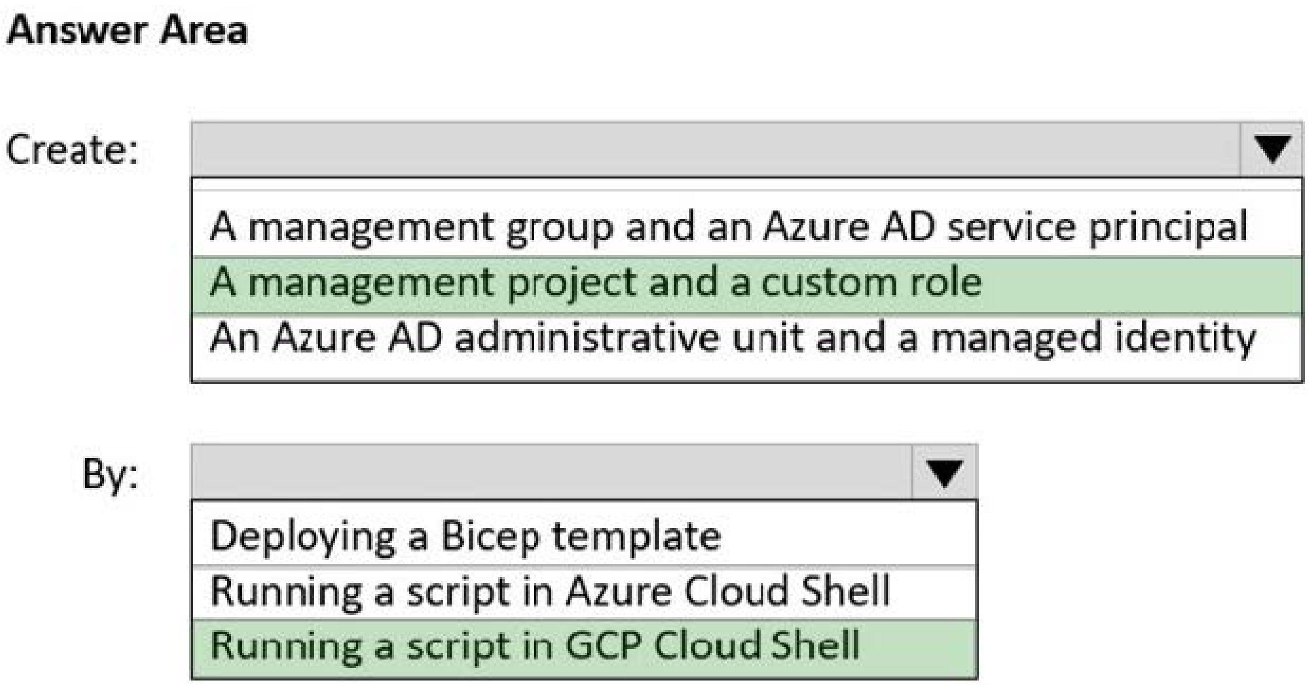
Create: ▼

- A management group and an Azure AD service principal
- A management project and a custom role
- An Azure AD administrative unit and a managed identity

By: ▼

- Deploying a Bicep template
- Running a script in Azure Cloud Shell
- Running a script in GCP Cloud Shell

Correct Answer:



Answer Area

Create: ▼

- A management group and an Azure AD service principal
- [✓ A management project and a custom role]
- An Azure AD administrative unit and a managed identity

By: ▼

- Deploying a Bicep template
- Running a script in Azure Cloud Shell
- [✓ Running a script in GCP Cloud Shell]

Box 1: A management project and a custom role (See 5. Below) (Optional) If you select Organization, a management project and an organization custom role will be created on your GCP project for the onboarding process. Auto-provisioning will be enabled for the onboarding of new projects.

Box 2: Steps below:

10.

Select the GCP Cloud Shell >.

11.

The GCP Cloud Shell will open.

12.

Paste the script into the Cloud Shell terminal and run it.

Note: To protect your GCP-based resources, you can connect a GCP project with either:

Native cloud connector (recommended) - Provides an agentless connection to your GCP account that you can extend with Defender for Cloud\\'s Defender plans to secure your GCP resources

Classic cloud connector

To connect your GCP project to Defender for Cloud with a native connector:

1.

Sign in to the Azure portal.

2.

Navigate to Defender for Cloud > Environment settings.

3.

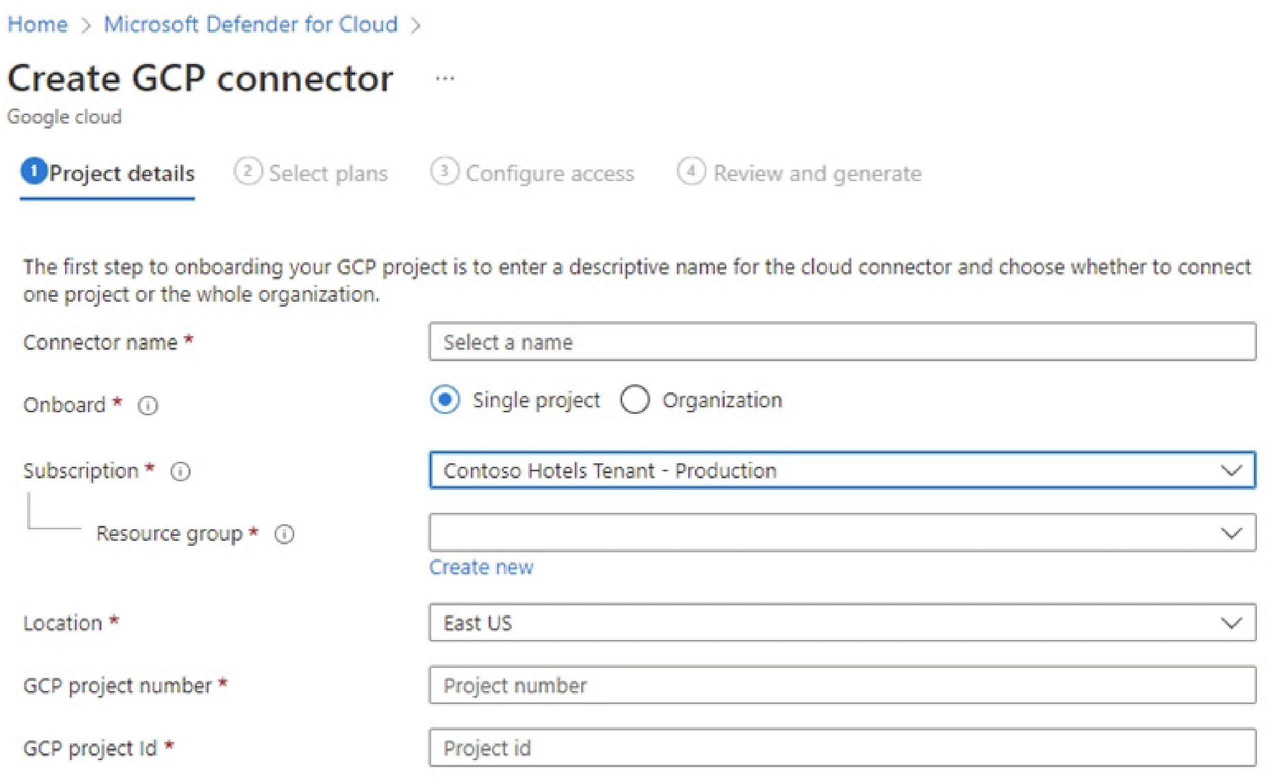
Select + Add environment.

4.

Select the Google Cloud Platform.

5.

Enter all relevant information.



Home > Microsoft Defender for Cloud >

Create GCP connector ...

Google cloud

The first step to onboarding your GCP project is to enter a descriptive name for the cloud connector and choose whether to connect one project or the whole organization.

Connector name * Select a name

Onboard * ● Single project ○ Organization

Subscription * Contoso Hotels Tenant - Production

Resource group *

Create new

Location * East US

GCP project number * Project number

GCP project Id * Project id

(Optional) If you select Organization, a management project and an organization custom role will be created on your GCP project for the onboarding process. Auto-provisioning will be enabled for the onboarding of new projects.

6\.

Select the Next: Select Plans.

7\.

Toggle the plans you want to connect to On.

8\.

Select the Next: Configure access.

9\.

Select Copy.

10\.

Select the GCP Cloud Shell >.

11\.

The GCP Cloud Shell will open.

12\.

Paste the script into the Cloud Shell terminal and run it.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp

QUESTION 11

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

You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can access the repositories in Account1.

What should you do first in the Microsoft Defender for Cloud portal?

A. Enable integrations.

B. Enable a plan.

C. Add an environment.

D. Enable security policies.

Correct Answer: C

Connect your GitHub repositories to Microsoft Defender for Cloud

Connect your GitHub account

To connect your GitHub account to Microsoft Defender for Cloud:

1.

Sign in to the Azure portal.

2.

Go to Microsoft Defender for Cloud > Environment settings.

3.

Select Add environment.

4.

Select GitHub.

5.

Enter a name (limit of 20 characters), and then select your subscription, resource group, and region.

6.

Etc.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-github

QUESTION 12

HOTSPOT

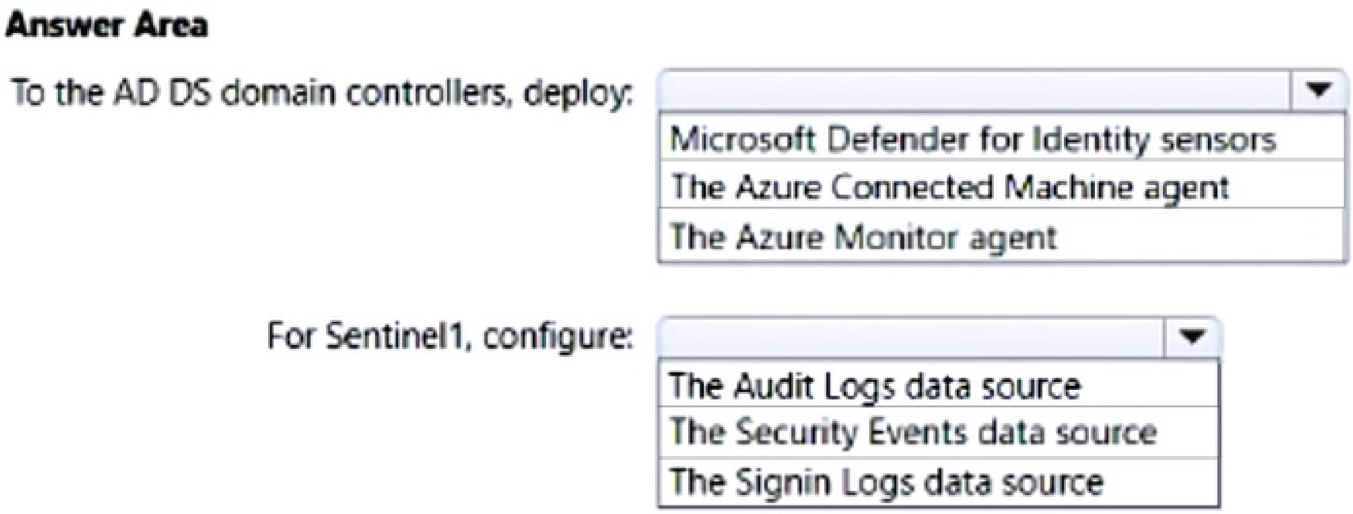
You have an Azure subscription that is linked to a hybrid Azure AD tenant and contains a Microsoft Sentinel workspace named Sentinel1.

You need to enable User and Entity Behavior Analytics (UEBA) for Sentinel and configure UEBA to use data collected from Active Directory Domain Services (AD DS).

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

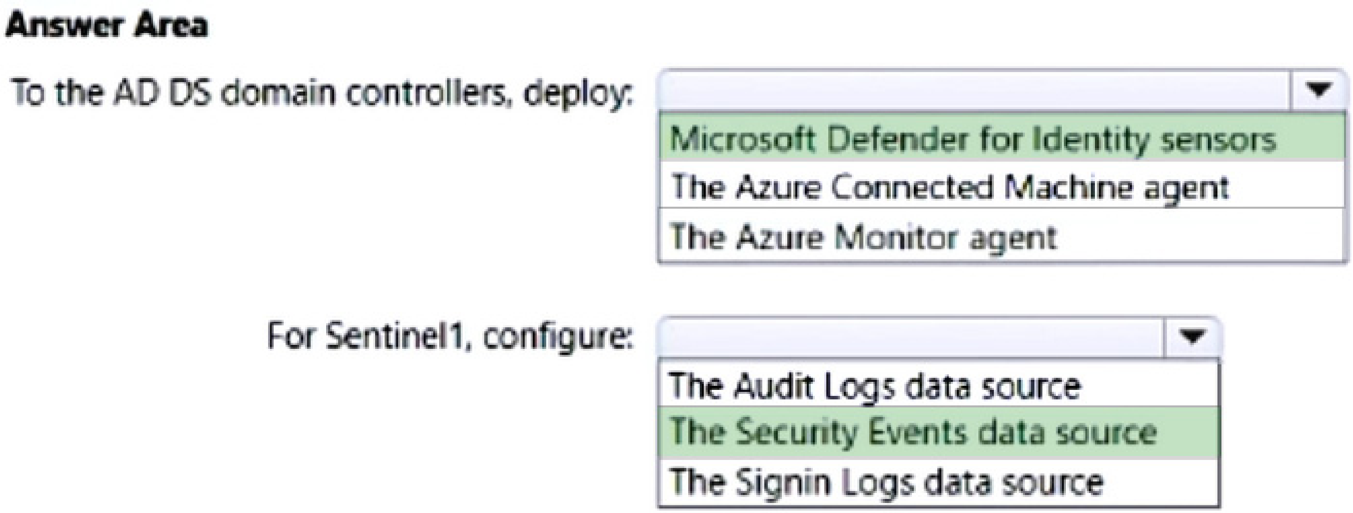
To the AD DS domain controllers, deploy:

- Microsoft Defender for Identity sensors
- The Azure Connected Machine agent
- The Azure Monitor agent

For Sentinel1, configure:

- The Audit Logs data source
- The Security Events data source
- The Signin Logs data source

Correct Answer:



Answer Area

To the AD DS domain controllers, deploy:

- [✓ Microsoft Defender for Identity sensors]
- The Azure Connected Machine agent
- The Azure Monitor agent

For Sentinel1, configure:

- The Audit Logs data source
- [✓ The Security Events data source]
- The Signin Logs data source

To sync user entities from on-premises Active Directory, your Azure tenant must be onboarded to Microsoft Defender for Identity (either standalone or as part of Microsoft 365 Defender) and you must have the MDI sensor installed on your Active Directory domain controller https://learn.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics

QUESTION 13

Your company uses Microsoft Defender for Endpoint.

The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company\\'s accounting team.

You need to hide false positive in the Alerts queue, while maintaining the existing security posture.

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

NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.

B. Hide the alert.

C. Create a suppression rule scoped to any device.

D. Create a suppression rule scoped to a device group.

E. Generate the alert.

Correct Answer: BCE

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

QUESTION 14

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 use Azure Security Center.

You receive a security alert in Security Center.

You need to view recommendations to resolve the alert in Security Center.

Solution: From Regulatory compliance, you download the report.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

QUESTION 15

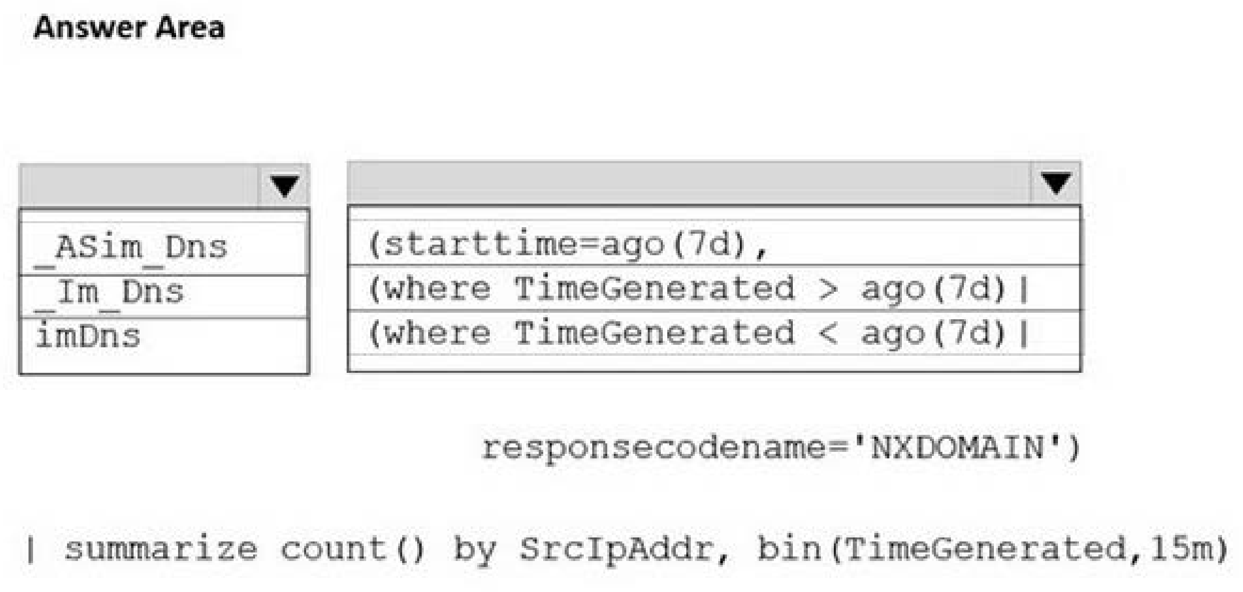
HOTSPOT

You need to create a query to investigate DNS-related activity. The solution must meet the Microsoft Sentinel requirements.

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

NOTE: Each correct selection is worth one point.

Hot Area:



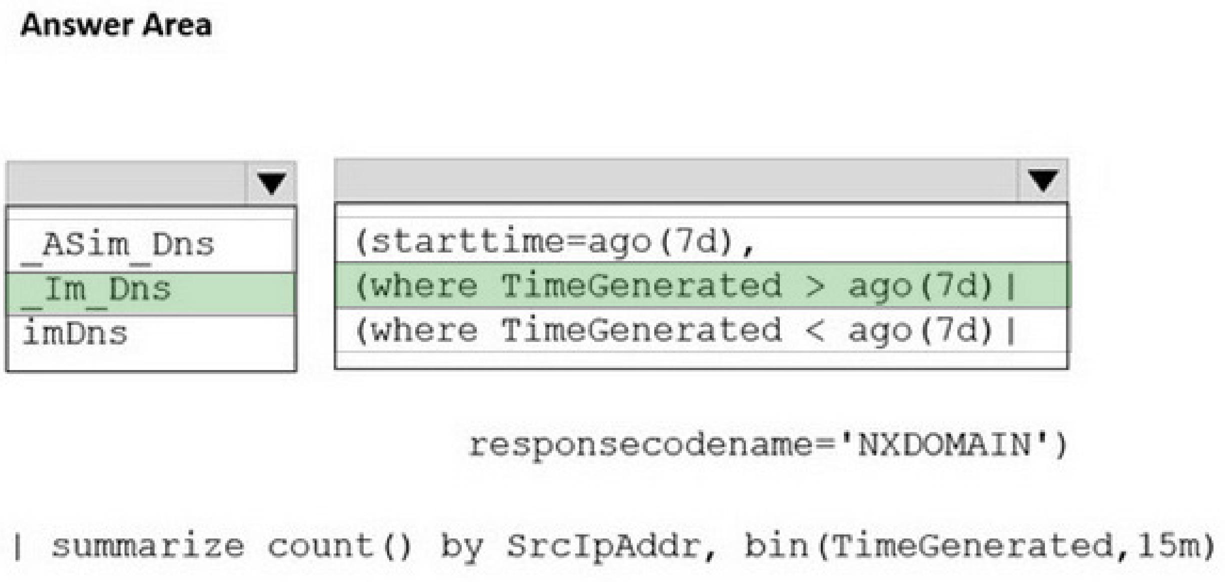
Answer Area

```
_ASim_Dns                (starttime=ago(7d),
_Im_Dns                  (where TimeGenerated > ago(7d)|
imDns                    (where TimeGenerated < ago(7d)|

                    responsecodename='NXDOMAIN')

| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)
```

Correct Answer:



Answer Area

```
_ASim_Dns
[✓ _Im_Dns]
imDns
```

```
(starttime=ago(7d),
[✓ (where TimeGenerated > ago(7d) |]
(where TimeGenerated < ago(7d) |
```

```
responsecodename='NXDOMAIN')
| summarize count() by SrcIpAddr, bin(TimeGenerated,15m)
```

Box 1: _Im_Dns

Fabrikam identifies the following Microsoft Sentinel requirements:

Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.

Unifying parsers

When using ASIM in your queries, use unifying parsers to combine all sources, normalized to the same schema, and query them using normalized fields. The unifying parser name is _Im_ for built-in parsers and im for

workspace deployed parsers, where stands for the specific schema it serves.

For example, the following query uses the built-in unifying DNS parser to query DNS events using the ResponseCodeName, SrcIpAddr, and TimeGenerated normalized fields:

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

The example uses filtering parameters, which improve ASIM performance. The same example without filtering parameters would look like this:

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

Box 2: (where TimeGenerated > ago(7d) |

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