



# SC-200<sup>Q&As</sup>

Microsoft Security Operations Analyst

**Pass Microsoft SC-200 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.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 Sentinel workspace named Workspaces

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\\' and were aggregated by the source IP address in 15-minute intervals. The solution must maximize query performance.

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:

Dropdown menu with options: **\_Im\_Dns**, Dns, imDns

Query input field with options: (starttime=ago(1d), responsecodename='NXDOMAIN'), | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN", **| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)**

Correct Answer:

Dropdown menu with options: **\_Im\_Dns**, Dns, imDns

Query input field with options: (starttime=ago(1d), responsecodename='NXDOMAIN'), | where TimeGenerated > ago(1d) | where ResponseCodeName =~ "NXDOMAIN", **| where ResponseCodeName == "NXDOMAIN" | where TimeGenerated > ago(1d)**

### 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 are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a scheduled query rule for a data connector.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

---

### QUESTION 3

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

You need to identify all the entities affected by an incident.

Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations

B. Devices

C. Evidence and Response

D. Alerts

Correct Answer: C

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents>

---

### QUESTION 4

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 are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a hunting bookmark.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center>

---

#### QUESTION 5

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

You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.

You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?

A. the Log Analytics agent

B. the Azure Connected Machine agent

C. the unified Microsoft Defender for Endpoint solution package

D. Microsoft Monitoring Agent

Correct Answer: A

Defender for Cloud can monitor the security posture of your non-Azure computers, but first you need to connect them to Azure.

You can connect your non-Azure computers in any of the following ways:

Using Azure Arc-enabled servers (recommended)

From Defender for Cloud's pages in the Azure portal (Getting started and Inventory)

Add non-Azure machines with Azure Arc

The preferred way of adding your non-Azure machines to Microsoft Defender for Cloud is with Azure Arc-enabled servers.



A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines>

[SC-200 PDF Dumps](#)

[SC-200 VCE Dumps](#)

[SC-200 Study Guide](#)