SC-200$^{Q\&As}$

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

QUESTION 1

HOTSPOT

You have a Microsoft 365 E5 subscription.

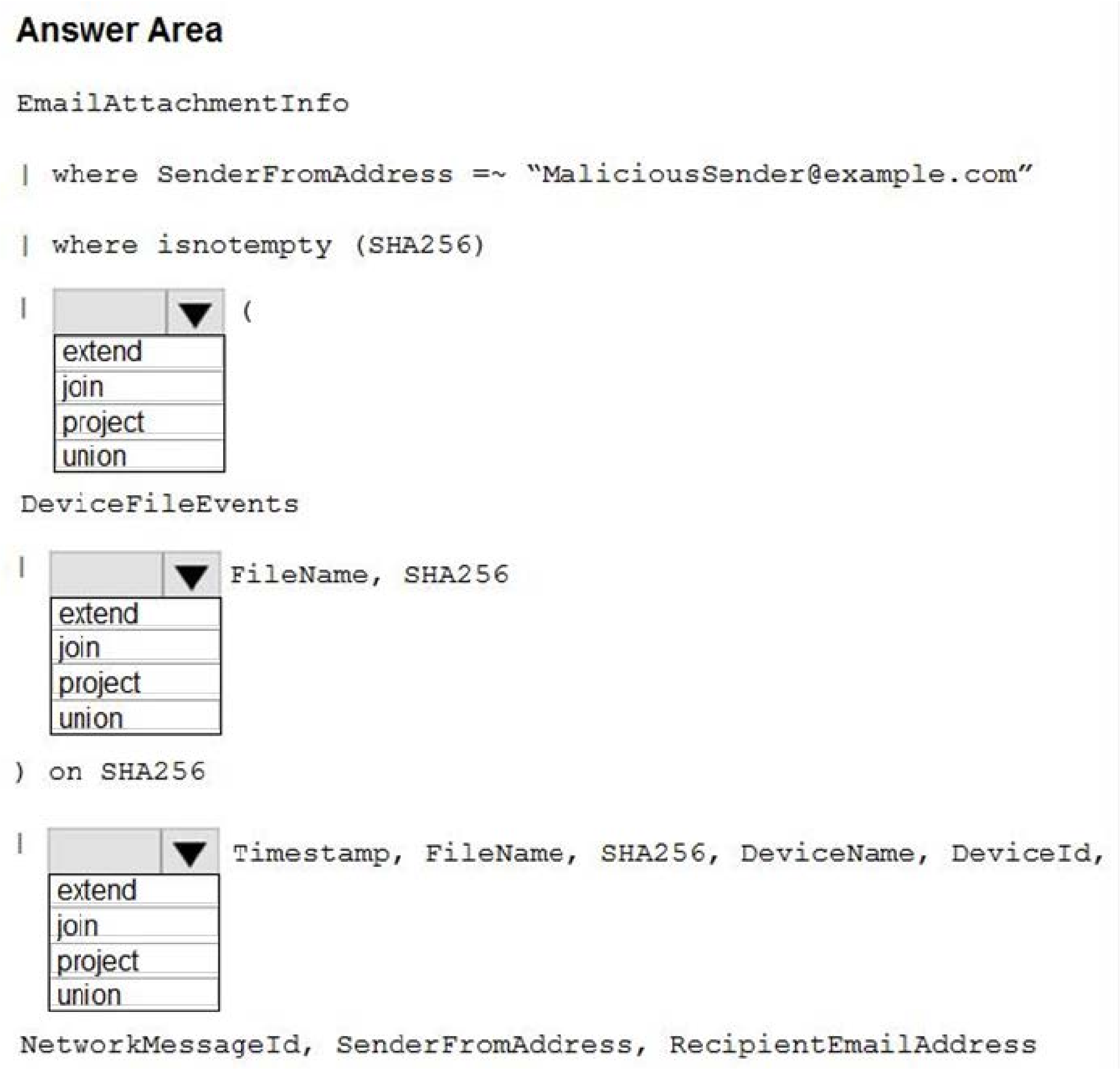
You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

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

NOTE: Each correct selection is worth one point.

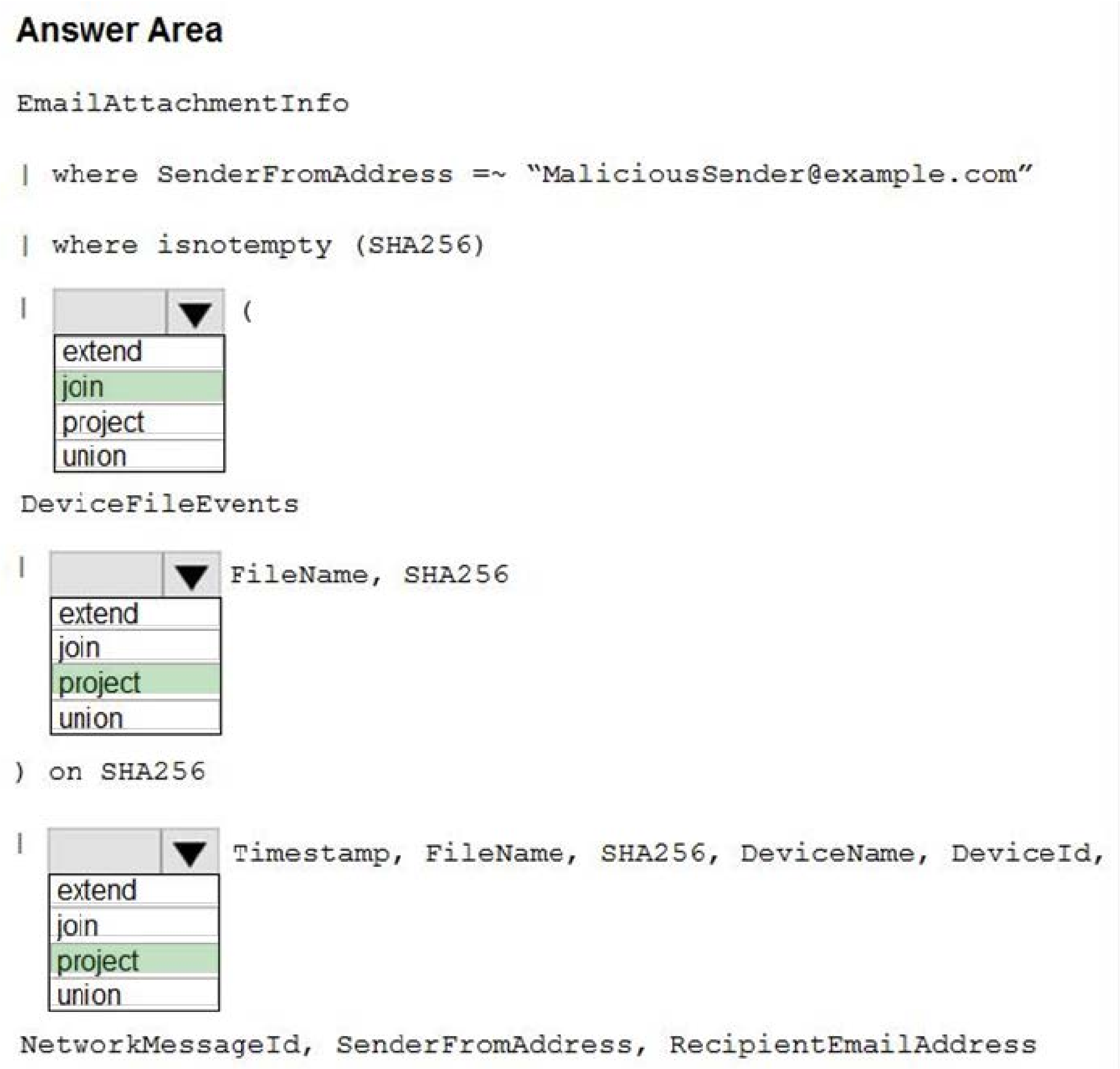
Hot Area:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [          ▼] (
  extend
  join
  project
  union
DeviceFileEvents

| [          ▼] FileName, SHA256
  extend
  join
  project
  union
) on SHA256

| [          ▼] Timestamp, FileName, SHA256, DeviceName, DeviceId,
  extend
  join
  project
  union
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Correct Answer:



Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ “MaliciousSender@example.com”

| where isnotempty (SHA256)

| [ ▼ ] (
    extend
    [✓ join]
    project
    union

DeviceFileEvents

| [ ▼ ] FileName, SHA256
    extend
    join
    [✓ project]
    union

) on SHA256

| [ ▼ ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
    extend
    join
    [✓ project]
    union

NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

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 Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

QUESTION 3

You use Azure Sentinel.

By using a built-in role, you have to provide a security analyst with the ability to edit the queries of custom Azure Sentinel workbooks.

Which role should you assign to the analyst if using the principle of least privilege ?

A. Security Administrator

B. Azure Sentinel Responder

C. Azure Sentinel Contributor

D. Logic App Contributor

Correct Answer: C

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

QUESTION 4

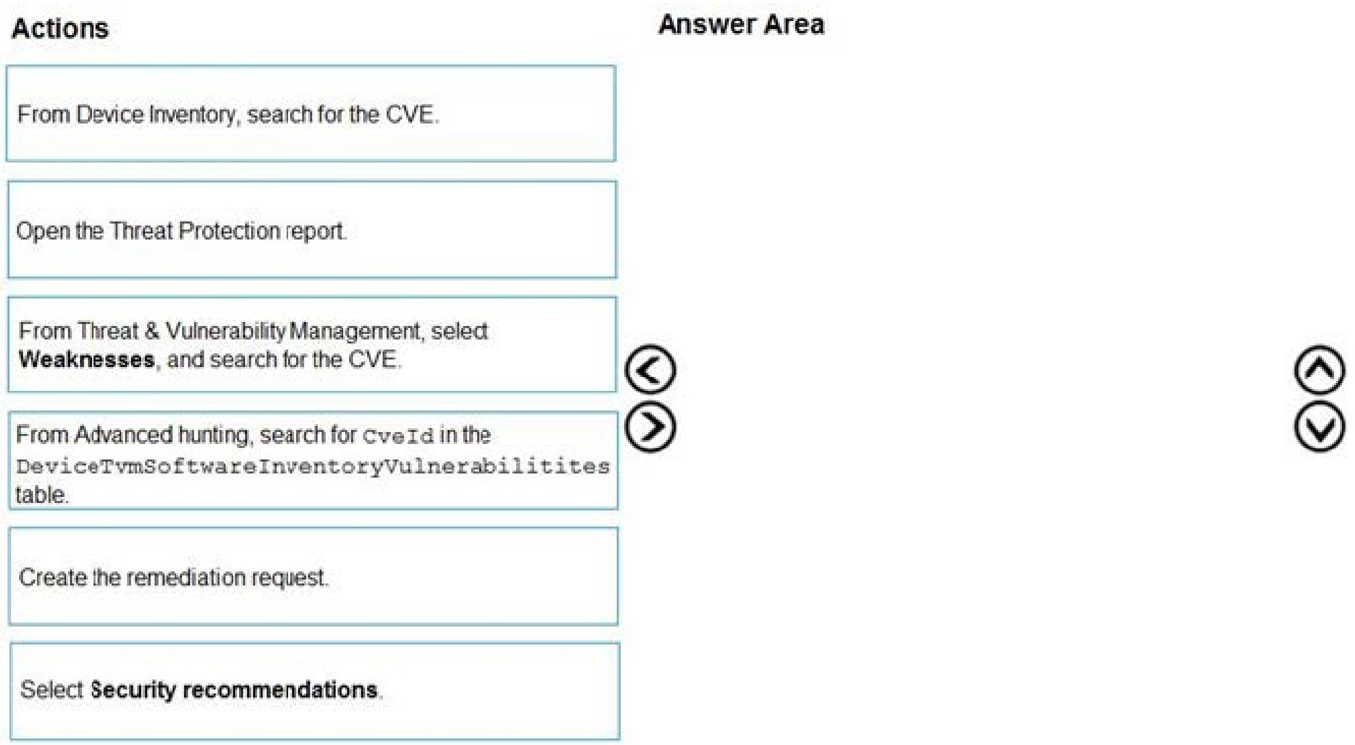
DRAG DROP

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

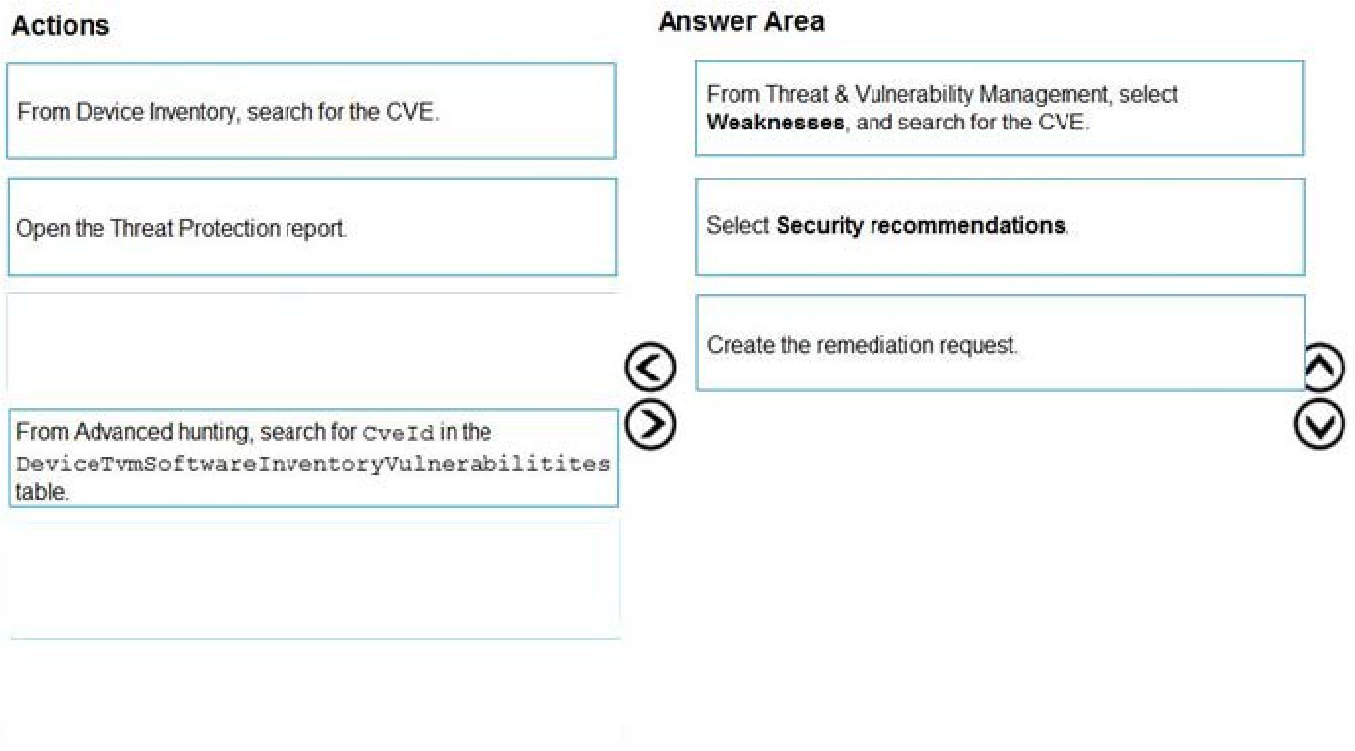
From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

Correct Answer:



Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Answer Area

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

QUESTION 5

You have an Azure subscription that contains a Microsoft Sentinel workspace. The workspace contains a Microsoft Defender for Cloud data connector.

You need to customize which details will be included when an alert is created for a specific event.

What should you do?

A. Modify the properties of the connector.

B. Create a Data Collection Rule (DCR).

C. Create a scheduled query rule.

D. Enable User and Entity Behavior Analytics (UEBA)

Correct Answer: C

https://learn.microsoft.com/en-us/azure/sentinel/customize-alert-details