

Microsoft

SC-200

Microsoft Security Operations Analyst
QUESTION & ANSWERS

QUESTION 1

The issue for which team can be resolved by using Microsoft Defender for Endpoint?

- A. executive
- B. sales
- C. marketing

Correct Answer: B

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defenderatp-ios>

QUESTION 2

You are investigating a potential attack that deploys a new ransomware strain.

You plan to perform automated actions on a group of highly valuable machines that contain sensitive information.

You have three custom device groups.

You need to be able to temporarily group the machines to perform actions on the devices.

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

NOTE: Each correct selection is worth one point.

- A. Add a tag to the device group
- B. Add the device users to the admin role.
- C. Add a tag to the machines.
- D. Create a new device group that has a rank of 1.
- E. Create a new admin role
- F. Create a new device group that has a rank of 4.

Correct Answer: B,D,E

Explanation/Reference:

Reference:

<https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/>

QUESTION 3

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 Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat

section.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Explanation/Reference:

Reference:

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

QUESTION 4

You need to receive a security alert when a user attempts to sign in from a location that was never used by the

other users in your organization to sign in. Which anomaly detection policy should you use?

- A. Impossible travel
- B. Activity from anonymous IP addresses
- C. Activity from infrequent country
- D. Malware detection

Correct Answer: C

Explanation/Reference:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy>

QUESTION 5

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

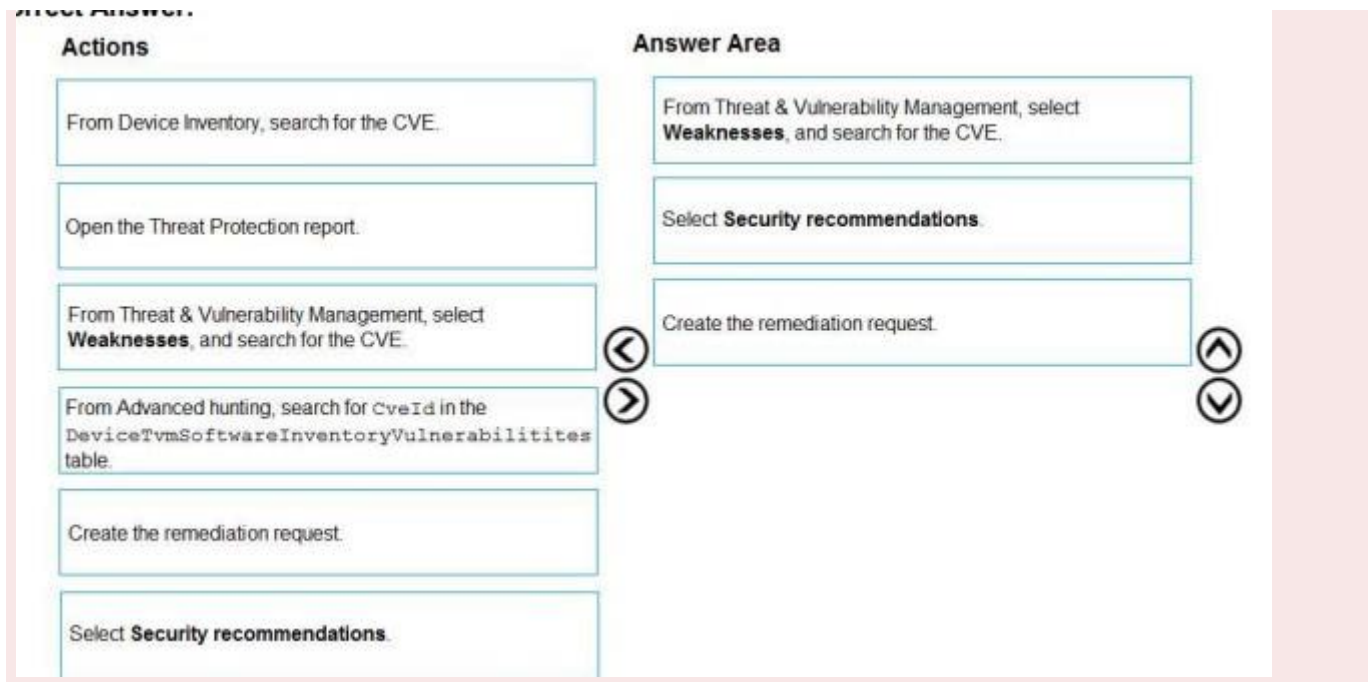
Create the remediation request.

Select **Security recommendations**.

Answer Area



Correct Answer:



Explanation/Reference:

Reference:

<https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediateapps-using-mem/ba-p/1599271>