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

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

A. executive

B. sales

C. marketing

Correct Answer: B

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

QUESTION 2

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

A. notebooks in Azure Sentinel

B. Microsoft Cloud App Security

C. Azure Monitor

D. hunting queries in Azure Sentinel

Correct Answer: A

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

QUESTION 3

You need to create the test rule to meet the Azure Sentinel requirements. What should you do when you create the rule?

A. From Set rule logic, turn off suppression.

B. From Analytics rule details, configure the tactics.

C. From Set rule logic, map the entities.

D. From Analytics rule details, configure the severity.

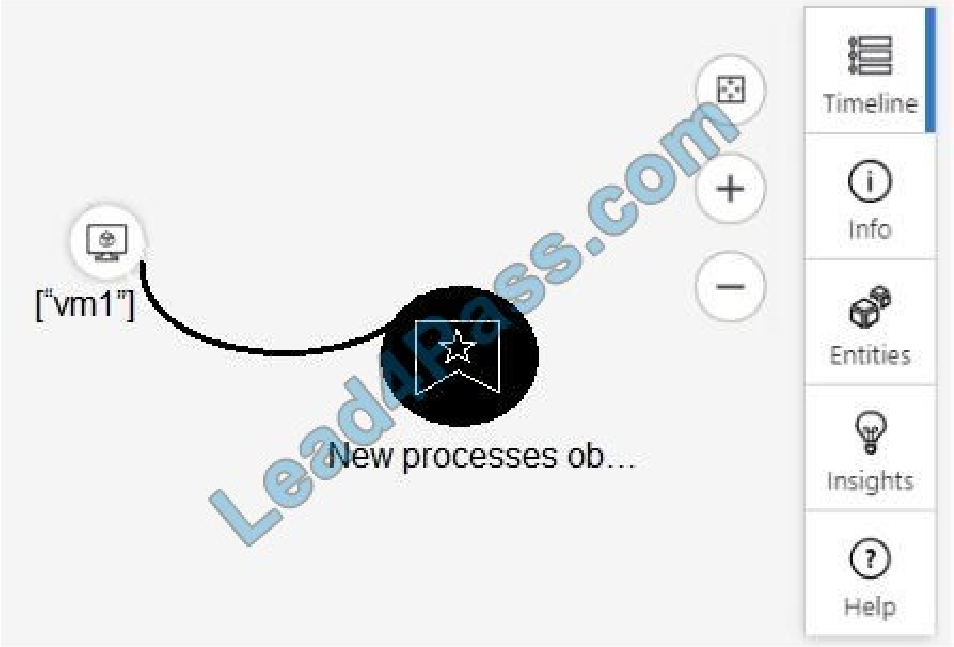
Correct Answer: C

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 4

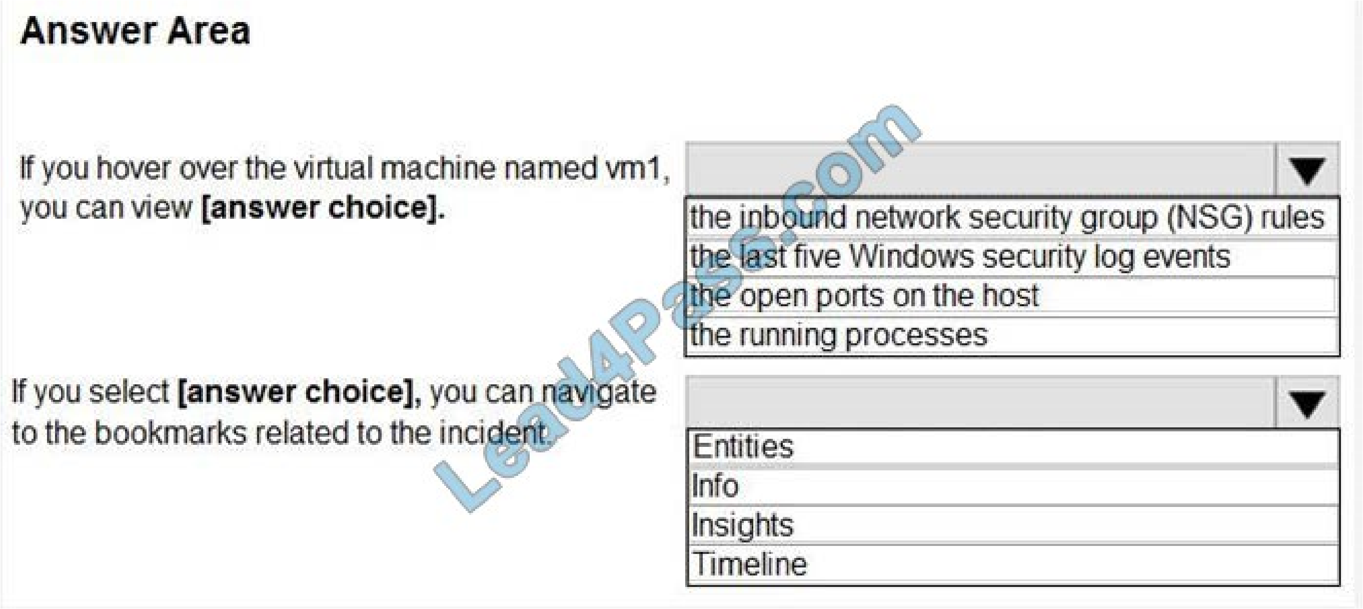
HOTSPOT

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

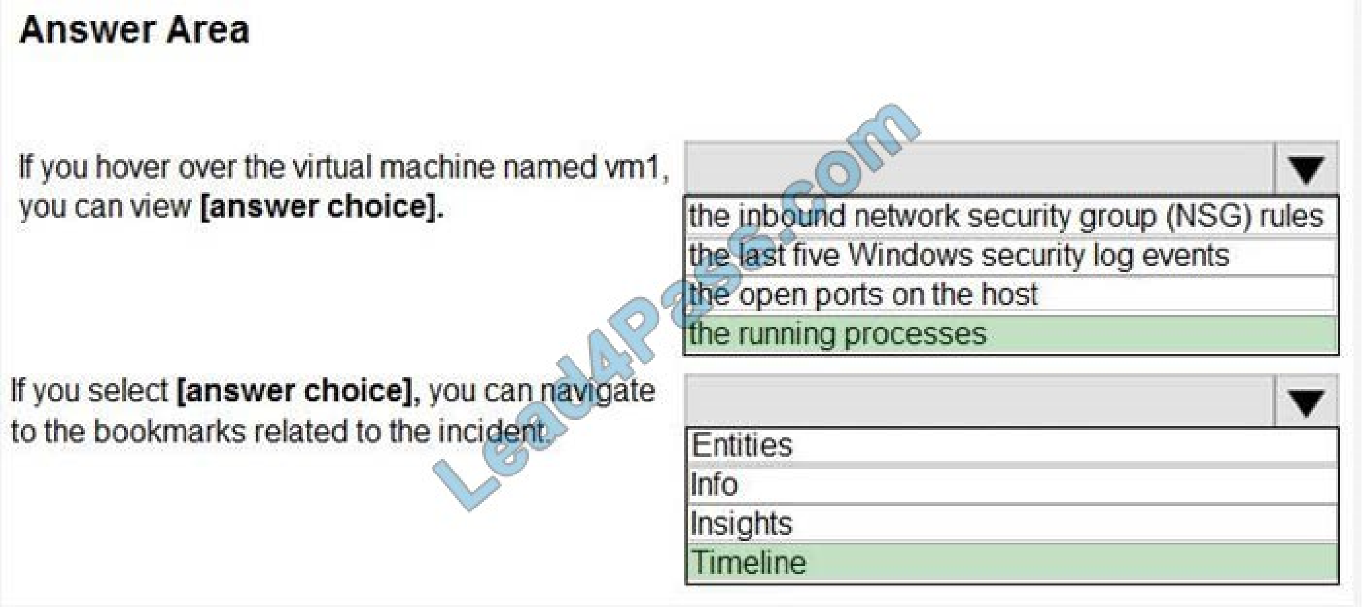
If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

Correct Answer:



Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- [✓ the running processes]

If you select **[answer choice]**, you can navigate to the bookmarks related to the incident.

- Entities
- Info
- Insights
- [✓ Timeline]

QUESTION 5

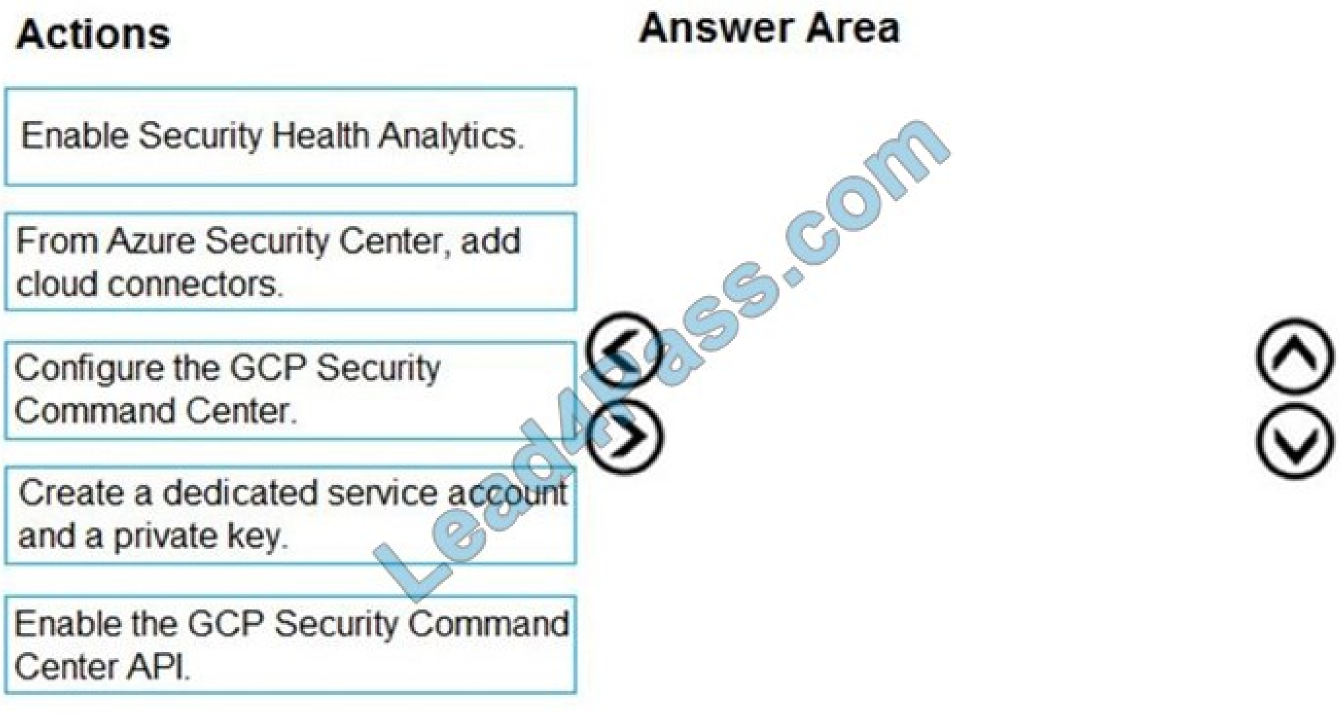
DRAG DROP

You have resources in Azure and Google cloud.

You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

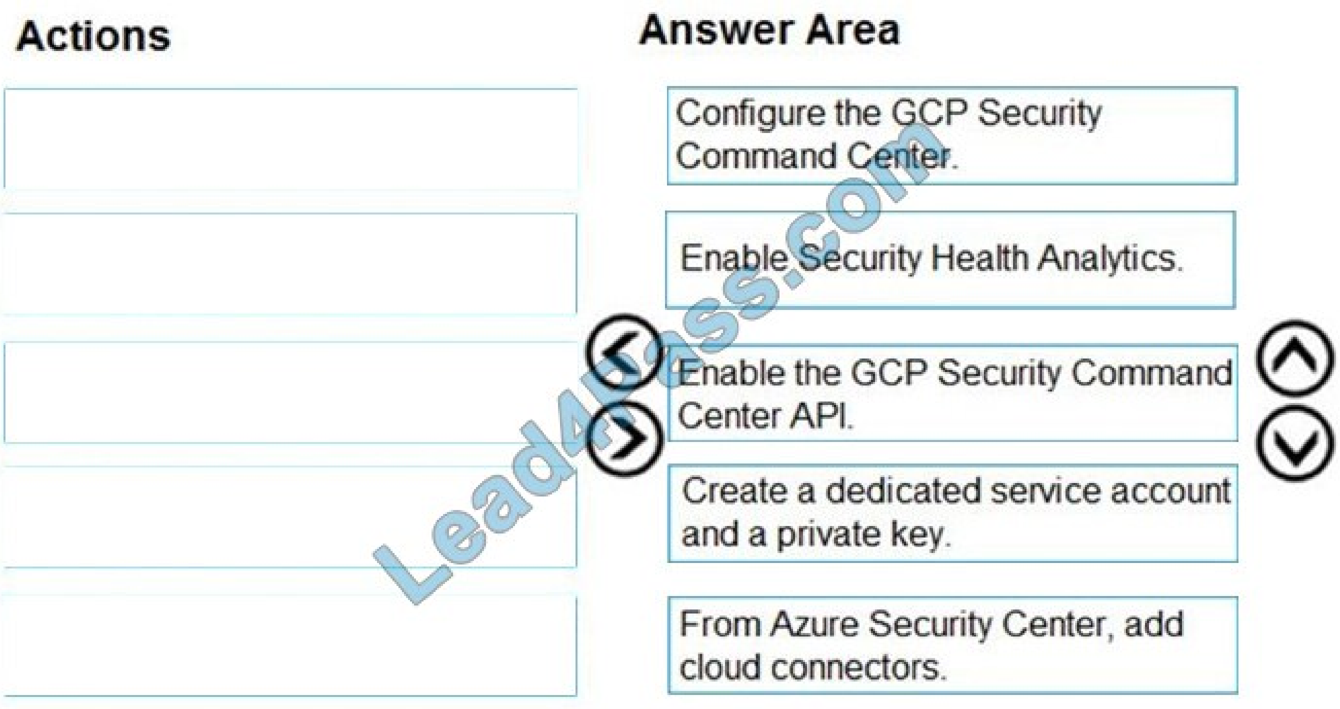


Actions

- Enable Security Health Analytics.
- From Azure Security Center, add cloud connectors.
- Configure the GCP Security Command Center.
- Create a dedicated service account and a private key.
- Enable the GCP Security Command Center API.

Answer Area

Correct Answer:



Actions

Answer Area

1. Configure the GCP Security Command Center.
2. Enable Security Health Analytics.
3. Enable the GCP Security Command Center API.
4. Create a dedicated service account and a private key.
5. From Azure Security Center, add cloud connectors.

QUESTION 6

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 7

You need to assign a role-based access control (RBAC) role to admin1 to meet the Azure Sentinel requirements and the business requirements. Which role should you assign?

A. Automation Operator

B. Automation Runbook Operator

C. Azure Sentinel Contributor

D. Logic App Contributor

Correct Answer: C

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

QUESTION 8

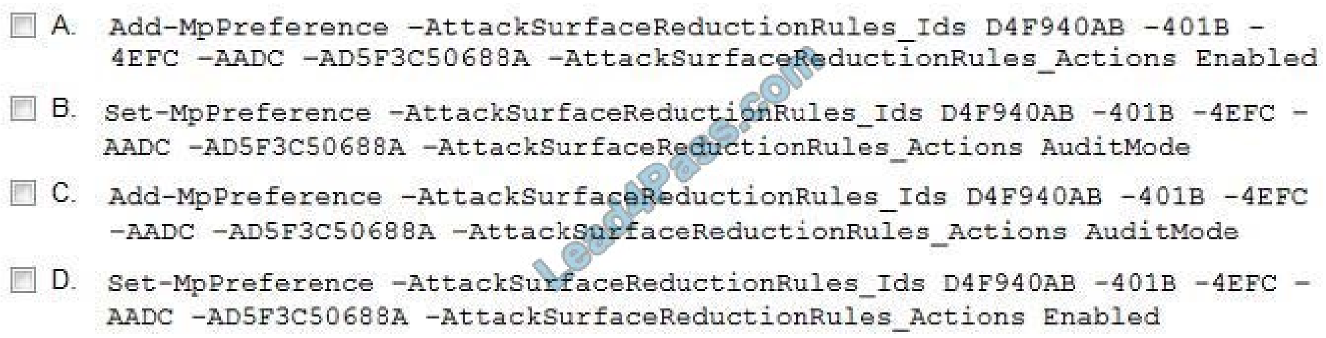
Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You plan to enable protection against downloading and running additional payloads from the Office VBA macros as additional child processes.

You need to identify which Office VBA macros might be affected.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.



```
☐ A.  Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
      4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
☐ B.  Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
      AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
☐ C.  Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC
      -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
☐ D.  Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
      AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: BC

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

QUESTION 9

You provision a Linux virtual machine in a new Azure subscription.

You enable Azure Defender and onboard the virtual machine to Azure Defender.

You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.

Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n

B. ./alerttest testing eicar pipe

C. cp /bin/echo ./alerttest

D. ./asc_alerttest_662jfi039n testing eicar pipe

Correct Answer: AD

Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-

QUESTION 10

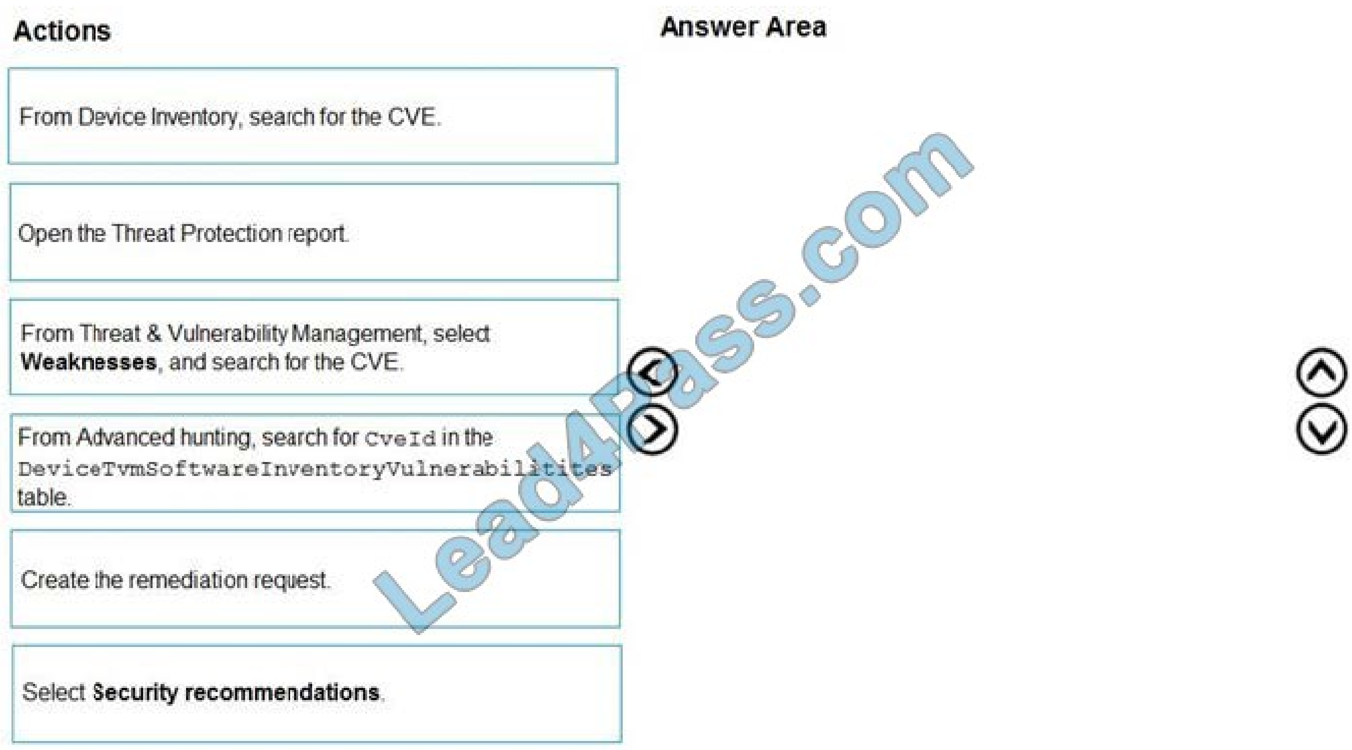
DRAG DROP

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.

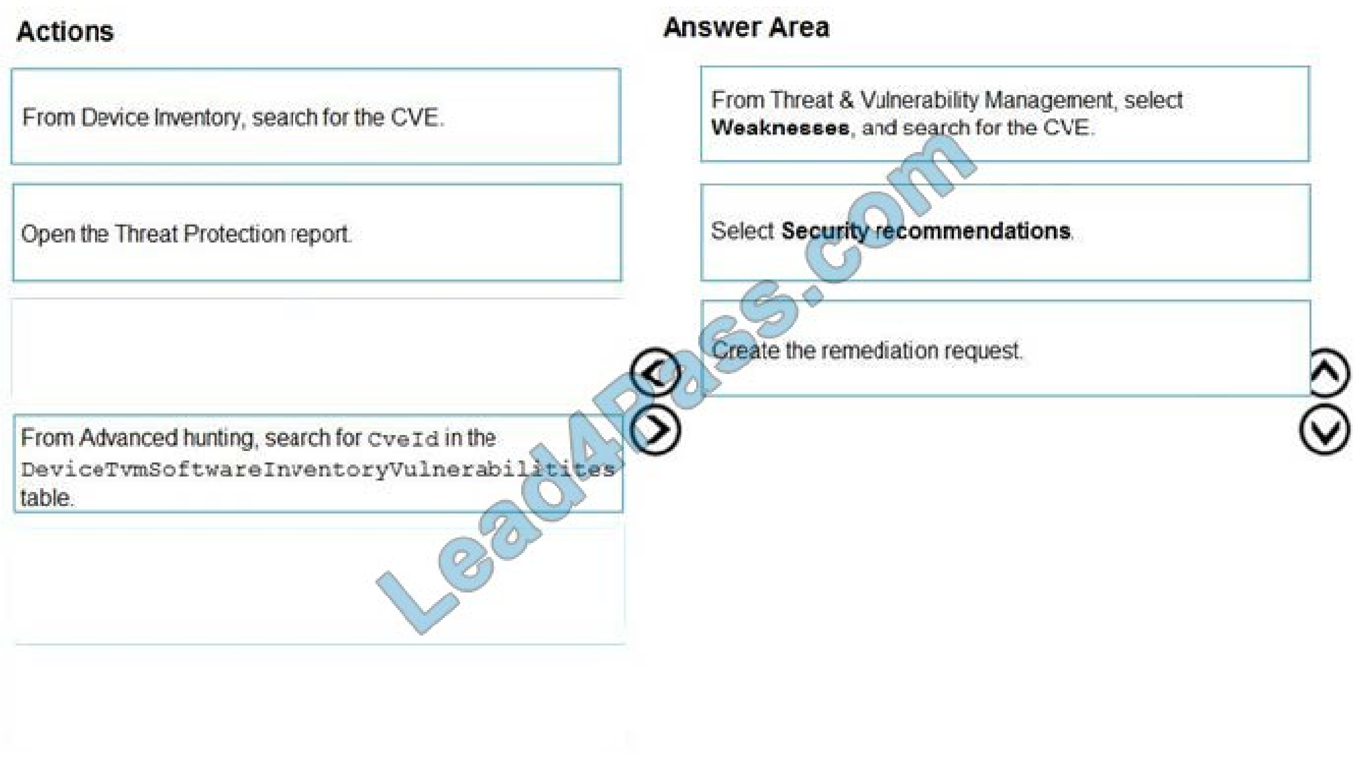
From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

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

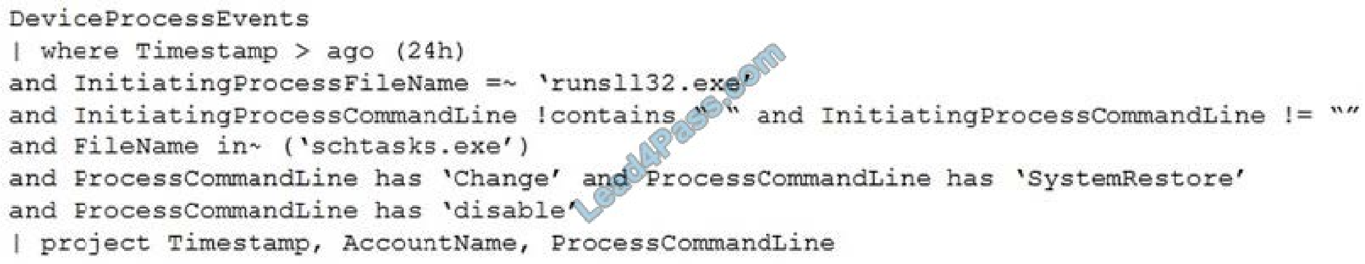
From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

Select **Security recommendations**.

Create the remediation request.

QUESTION 11

You have the following advanced hunting query in Microsoft 365 Defender.



```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsl132.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

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

NOTE: Each correct selection is worth one point.

A. Create a detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Replace DeviceProcessEvents with DeviceNetworkEvents.

E. Add DeviceId and ReportId to the output of the query.

Correct Answer: AE

Reference: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

QUESTION 12

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

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

QUESTION 13

You need to modify the anomaly detection policy settings to meet the Cloud App Security requirements. Which policy should you modify?

A. Activity from suspicious IP addresses

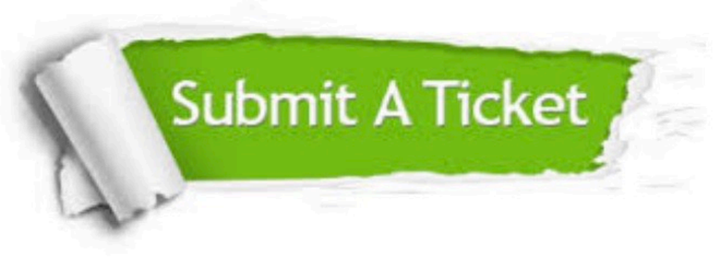
B. Activity from anonymous IP addresses

C. Impossible travel

D. Risky sign-in

Correct Answer: C

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


Submit A Ticket