Exam Questions SC-200

Microsoft Security Operations Analyst

https://www.2passeasy.com/dumps/SC-200/

NEW QUESTION 1
- (Exam Topic 1)
You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access
B. Azure Defender
C. Azure Firewall
D. Azure Application Gateway

Answer: B

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

NEW QUESTION 2
- (Exam Topic 3)
You use Azure Sentinel.
You need to receive an immediate alert whenever Azure Storage account keys are enumerated. 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 livestream
B. Add a data connector
C. Create an analytics rule
D. Create a hunting query.
E. Create a bookmark.

Answer: BD

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

NEW QUESTION 3
- (Exam Topic 3)
Your company stores the data for every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant. Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.
B. Create a query that uses the workspace expression and the union operator.
C. Use the alias statement.
D. Create a query that uses the resource expression and the alias operator.
E. Add the Azure Sentinel solution to each workspace.

Answer: BE

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

NEW QUESTION 4
- (Exam Topic 3)
You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.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.

Answer: AE

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

NEW QUESTION 5
- (Exam Topic 3)
You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel. What should you do first?

A. And a new scheduled query rule.
B. Add a data connector to Azure Sentinel.
C. Configure a custom Threat Intelligence connector in Azure Sentinel.
D. Modify the trigger in the logic app.

Answer: B

NEW QUESTION 6
- (Exam Topic 3)
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

Answer: AD

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

NEW QUESTION 7
- (Exam Topic 3)
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.

Actions	Answer Area
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**.	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps

NEW QUESTION 8
- (Exam Topic 3)
Your company uses Azure Security Center and Azure Defender.
The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

A. Security solutions
B. Security policy
C. Pricing & settings
D. Security alerts
E. Azure Defender

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

NEW QUESTION 9
- (Exam Topic 3)
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.

Answer: BDE

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

NEW QUESTION 10
- (Exam Topic 3)
You are investigating an incident by using Microsoft 365 Defender.
You need to create an advanced hunting query to detect failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.
How should you complete the query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Values

| project LogonFailures=count()

| summarize LogonFailures=count() by DeviceName, LogonType

| where ActionType == FailureReason

| where DeviceName in ("CFOLaptop, "CEOLaptop", "COOLaptop")

ActionType == "LogonFailed"

Answer Area

and

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Values

| project LogonFailures=count()

| summarize LogonFailures=count()
by DeviceName, LogonType

| where ActionType ==
FailureReason

| where DeviceName in ("CFOLaptop,
"CEOLaptop", "COOLaptop")

ActionType == "LogonFailed"

Answer Area

| summarize LogonFailures=count()
by DeviceName, LogonType

| where DeviceName in ("CFOLaptop,
"CEOLaptop", "COOLaptop")

| where ActionType ==
FailureReason   and

ActionType == "LogonFailed"

| project LogonFailures=count()

NEW QUESTION 10
- (Exam Topic 3)
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.

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
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36

NEW QUESTION 15
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-200 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-200 Product From:

https://www.2passeasy.com/dumps/SC-200/

Money Back Guarantee

SC-200 Practice Exam Features:

* SC-200 Questions and Answers Updated Frequently

* SC-200 Practice Questions Verified by Expert Senior Certified Staff

* SC-200 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SC-200 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year