SC-200 Dumps

Microsoft Security Operations Analyst

https://www.certleader.com/SC-200-dumps.html

NEW QUESTION 1
- (Exam Topic 1)
You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Internal threat:

| Add resource locks to the key vault. |
| Modify the access policy settings for the key vault. |
| Modify the role-based access control (RBAC) settings for the key vault. |

External threat:

| Implement Azure Firewall. |
| Modify the Key Vault firewall settings. |
| Modify the network security groups (NSGs). |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

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)
You plan to create a custom Azure Sentinel query that will provide a visual representation of the security alerts generated by Azure Security Center.
You need to create a query that will be used to display a bar graph. What should you include in the query?

A. extend
B. bin
C. count
D. workspace

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

NEW QUESTION 4
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Azure Defender. You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription
B. the Contributor for the subscription
C. the Contributor role for RG1
D. the Owner role for RG1

Answer: C

NEW QUESTION 5
- (Exam Topic 3)
You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Add a playbook.
B. Associate a playbook to an incident.
C. Enable Entity behavior analytics.
D. Create a workbook.
E. Enable the Fusion rule.

Answer: AB

NEW QUESTION 6
- (Exam Topic 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 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

Answer: B

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

NEW QUESTION 7
- (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 8
- (Exam Topic 3)
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

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

NEW QUESTION 9
- (Exam Topic 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 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 Entity tags, you add the accounts as Honeytoken accounts. Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 10
- (Exam Topic 3)
Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.
B. Hide the alert.
C. Create a suppression rule scoped to any device.
D. Create a suppression rule scoped to a device group.
E. Generate the alert.

Answer: BCE

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

NEW QUESTION 10
- (Exam Topic 3)
You provision Azure Sentinel for a new Azure subscription. You are configuring the Security Events connector.
While creating a new rule from a template in the connector, you decide to generate a new alert for every event. You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. user
B. resource group
C. IP address
D. computer

Answer: CD

NEW QUESTION 15
- (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

| 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

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 20
- (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 21
- (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 26
- (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

[blank]

[blank]

[blank] and

[blank]

[blank]

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 28
- (Exam Topic 3)
You have an Azure subscription that has Azure Defender enabled for all supported resource types. You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center. You need to test LA1 in Security Center.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Set the LA1 trigger to:
- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:
- Recommendations
- Workflow automation

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-whe

NEW QUESTION 32
- (Exam Topic 3)
You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to ensure that Security Center processes events from the Azure virtual machines that report to workspace1.
What should you do?

A. In workspace1, install a solution.
B. In sub1, register a provider.
C. From Security Center, create a Workflow automation.
D. In workspace1, create a workbook.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

NEW QUESTION 33
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your SC-200 Exam with Our Prep Materials Via below:

https://www.certleader.com/SC-200-dumps.html