Microsoft

Exam Questions SC-200

Microsoft Security Operations Analyst

NEW QUESTION 1
- (Exam Topic 1)
The issue for which team can be resolved by using Microsoft Defender for Endpoint?

A. executive
B. sales
C. marketing

Answer: B

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

NEW QUESTION 2
- (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.

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 3
- (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 4
- (Exam Topic 2)
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

Answer: C

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

NEW QUESTION 5
- (Exam Topic 2)
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

Answer: C

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

NEW QUESTION 6
- (Exam Topic 2)
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.

Answer: C

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

NEW QUESTION 7
- (Exam Topic 3)
You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

A. Modify the access control settings for the key vault.
B. Enable the Key Vault firewall.
C. Create an application security group.
D. Modify the access policy for the key vault.

Answer: B

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

NEW QUESTION 8
- (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 9
- (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 10
- (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 10
- (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 13
- (Exam Topic 3)
You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents. What should you use to detect which documents are sensitive?

A. SharePoint search
B. a hunting query in Microsoft 365 Defender
C. Azure Information Protection
D. RegEx pattern matching

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

NEW QUESTION 14
- (Exam Topic 3)
You have the following advanced hunting query in Microsoft 365 Defender.

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 19
- (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 20
- (Exam Topic 3)
You have an Azure Sentinel deployment.
You need to query for all suspicious credential access activities.
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 22
- (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 27
- (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 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

Answer: A

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

NEW QUESTION 29
- (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 31
- (Exam Topic 3)
You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

A. Add a parameter and modify the trigger.
B. Add a custom data connector and modify the trigger.
C. Add a condition and modify the action.
D. Add a parameter and modify the action.

Answer: D

Explanation:
Reference:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

NEW QUESTION 36
- (Exam Topic 3)
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. Option A
B. Option B
C. Option C
D. Option D

Answer: BC

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

NEW QUESTION 40
- (Exam Topic 3)
Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.

A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

A. built-in queries
B. livestream
C. notebooks
D. bookmarks

Answer: C

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

NEW QUESTION 44
- (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 48
- (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 52
- (Exam Topic 3)
You create a new Azure subscription and start collecting logs for Azure Monitor.
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.
Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 53
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
Order The SC-200 Practice Test Here