SC-200 Dumps

Microsoft Security Operations Analyst

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

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.

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 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 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 5
- (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 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: You add the accounts to an Active Directory group and add the group as a Sensitive group. 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 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

Answer: A

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

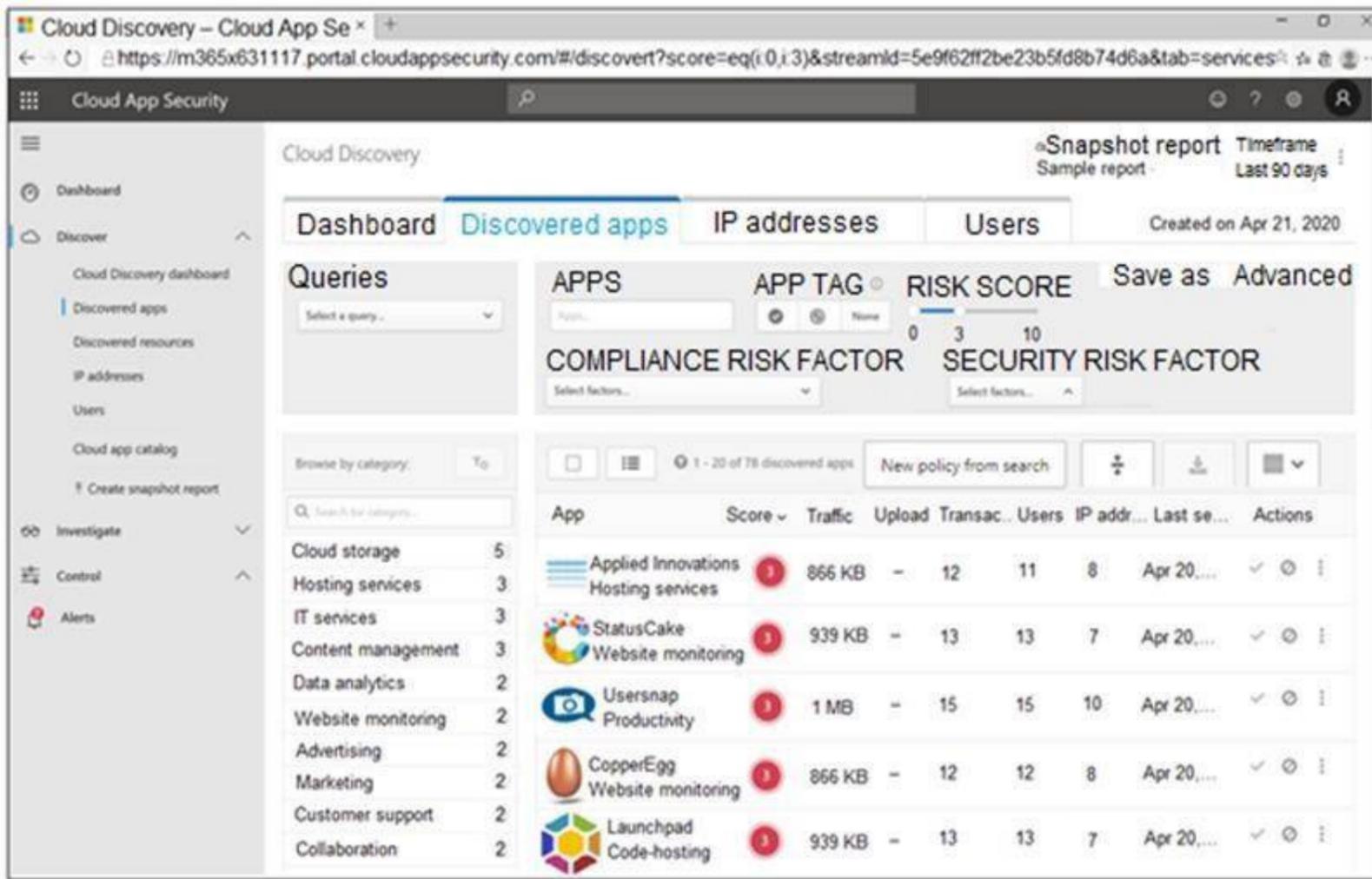**NEW QUESTION 8**
- (Exam Topic 3)
You open the Cloud App Security portal as shown in the following exhibit.

You need to remediate the risk for the Launchpad app.

Which four 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:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

NEW QUESTION 9
- (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 10
- (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.

Actions

From Azure Sentinel, select **Hunting.**

Select **Run All Queries.**

Select **New Query.**

Filter by tactics.

From Azure Sentinel, select **Notebooks.**
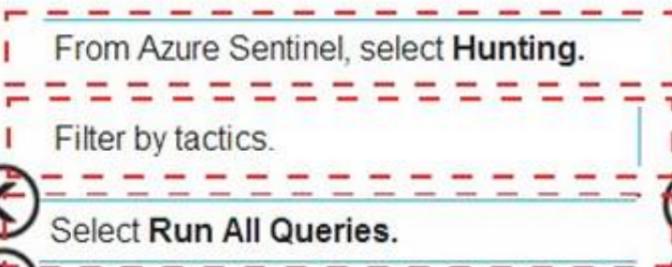
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

From Azure Sentinel, select **Hunting.**

Select **Run All Queries.**

Select **New Query.**

Filter by tactics.

From Azure Sentinel, select **Notebooks.**

Answer Area

From Azure Sentinel, select **Hunting.**

Filter by tactics.

Select **Run All Queries.**

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 12
- (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 13
- (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 14
- (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 18
- (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.

Actions

Change the alert severity threshold for emails to **Medium**.

Copy an executable file on a virtual machine and rename the file as ASC_AlertTest_662jfi039N.exe.

Enable Azure Defender for the subscription.

Change the alert severity threshold for emails to **Low**.

Run the executable file and specify the appropriate arguments.

Rename the executable file as AlertTest.exe.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 23
- (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 27
......

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