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 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)
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.
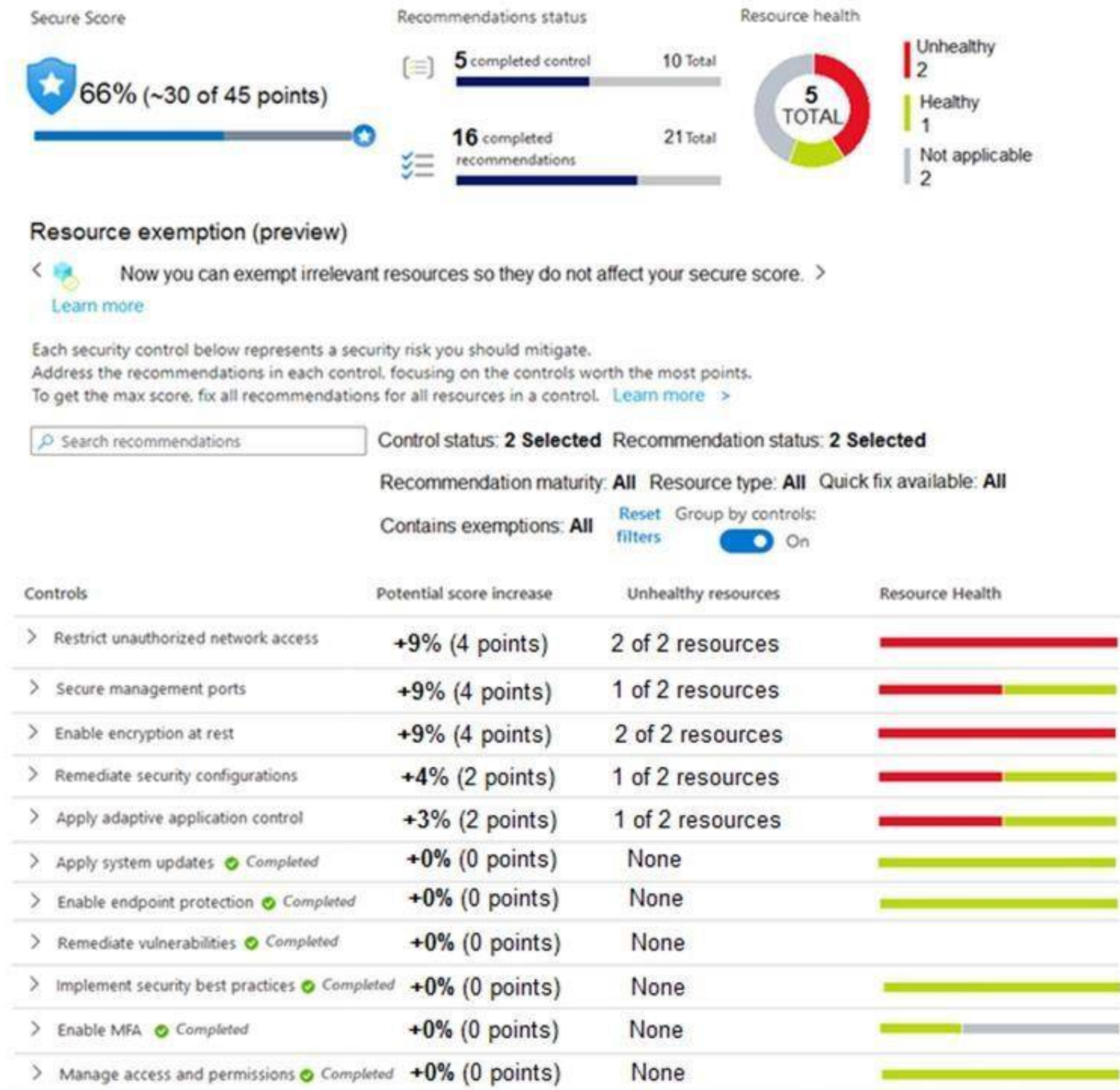
Answer: BE

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants
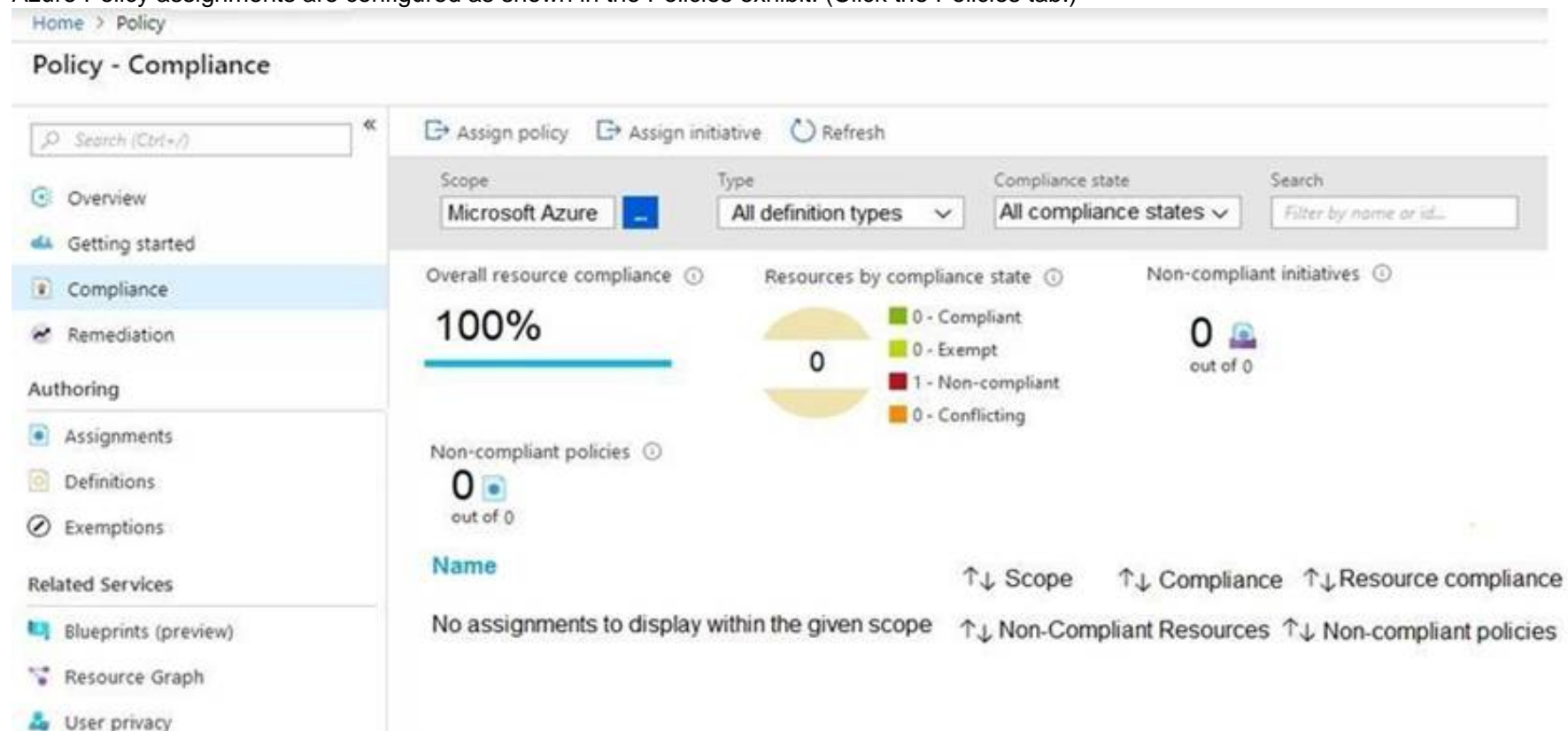
NEW QUESTION 3
- (Exam Topic 3)
You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.
The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)

Secure Score

66% (~30 of 45 points)

Recommendations status

[≡] **5** completed control — 10 Total

✓ **16** completed recommendations — 21 Total

Resource health

5 TOTAL

Unhealthy	2
Healthy	1
Not applicable	2

Resource exemption (preview)

< Now you can exempt irrelevant resources so they do not affect your secure score. >

Learn more

Each security control below represents a security risk you should mitigate.
Address the recommendations in each control, focusing on the controls worth the most points.
To get the max score, fix all recommendations for all resources in a control. Learn more >

🔍 Search recommendations

Control status: **2 Selected**   Recommendation status: **2 Selected**

Recommendation maturity: **All**   Resource type: **All**   Quick fix available: **All**

Contains exemptions: **All**   Reset filters   Group by controls: ● On

Controls	Potential score increase	Unhealthy resources	Resource Health
> Restrict unauthorized network access	**+9% (4 points)**	2 of 2 resources	
> Secure management ports	**+9% (4 points)**	1 of 2 resources	
> Enable encryption at rest	**+9% (4 points)**	2 of 2 resources	
> Remediate security configurations	**+4% (2 points)**	1 of 2 resources	
> Apply adaptive application control	**+3% (2 points)**	1 of 2 resources	
> Apply system updates ✓ Completed	**+0% (0 points)**	None	
> Enable endpoint protection ✓ Completed	**+0% (0 points)**	None	
> Remediate vulnerabilities ✓ Completed	**+0% (0 points)**	None	
> Implement security best practices ✓ Completed	**+0% (0 points)**	None	
> Enable MFA ✓ Completed	**+0% (0 points)**	None	
> Manage access and permissions ✓ Completed	**+0% (0 points)**	None	

Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)

Home > Policy

Policy - Compliance

🔍 Search (Ctrl+/)

⊡ Assign policy   ⊡ Assign initiative   ↻ Refresh

⊙ Overview

📖 Getting started

▣ Compliance

⚲ Remediation

Authoring

⊙ Assignments

⊡ Definitions

⊘ Exemptions

Related Services

📘 Blueprints (preview)

🔹 Resource Graph

👤 User privacy

Scope: Microsoft Azure ▢

Type: All definition types ▾

Compliance state: All compliance states ▾

Search: Filter by name or id...

Overall resource compliance ⓘ
100%

Resources by compliance state ⓘ
0
- ▣ 0 - Compliant
- ▣ 0 - Exempt
- ▣ 1 - Non-compliant
- ▣ 0 - Conflicting

Non-compliant initiatives ⓘ
0 🔒
out of 0

Non-compliant policies ⓘ
0 ▢
out of 0

Name   ↑↓ Scope   ↑↓ Compliance   ↑↓ Resource compliance

No assignments to display within the given scope   ↑↓ Non-Compliant Resources   ↑↓ Non-compliant policies

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Both virtual machines have inbound rules that allow access from either Any or Internet ranges.	○	○
Both virtual machines have management ports exposed directly to the internet.	○	○
If you enable just-in-time network access controls on all virtual machines, you will increase the secure score by four point.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-ac https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1

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)
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 6
- (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 7
- (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 8
- (Exam Topic 3)
You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.
You need to deploy the log forwarder.
Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

| Deploy an OMS Gateway on the network. |
| Set the syslog daemon to forward the events directly to Azure Sentinel. |
| Configure the syslog daemon. Restart the syslog daemon and the Log Analytics agent. |
| Download and install the Log Analytics agent. |
| Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel. |

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

NEW QUESTION 9
- (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 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 10
- (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. `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

Answer: BC

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

NEW QUESTION 12
- (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 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 17
- (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 21
......

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