MS-500$^{Q\&As}$

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2, and User3 can use self-service password reset (SSPR). The solution must not affect User4.

Solution: You enable SSPR for Group3.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3. User4 would thus be affected if we enable it on Group3.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

---

QUESTION 2

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

A. Endpoint protection

B. Device restrictions

C. Identity protection

D. Windows Defender ATP

Correct Answer: A

References: https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

QUESTION 3

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) connector and a Microsoft Office 365 connector. You need to assign built-in role-based access control (RBAC) roles to achieve the following tasks:

1.

Create and run playbooks.

2.

Manage incidents.

The solution must use the principle of least privilege.

Which two roles should you assign? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Automation Operator

B. Azure Sentinel responder

C. Automation Runbook Operator

D. Azure Sentinel contributor

E. Logic App contributor

Correct Answer: DE

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

Refer to the table

Microsoft Sentinel Contributor + Logic App Contributor

Create and run playbooks

Manage incidents (dismiss, assign, etc.)

Microsoft Sentinel roles and allowed actions

The following table summarizes the Microsoft Sentinel roles and their allowed actions in Microsoft Sentinel.

QUESTION 4

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You register devices in contoso.com as shown in the following table.

Name	Platform	Member of	Microsoft Intune managed
Device1	Windows 10	GroupA	Yes
Device2	iOS	GroupB	No

You create app protection policies in Intune as shown in the following table.

Name	Platform	Management state	Assigned to
Policy1	Windows 10	With enrollment	Group1
Policy2	Windows 10	With enrollment	Group2
Policy3	iOS	Apps on Intune managed devices	GroupA
Policy4	iOS	Apps on Intune managed devices	GroupB

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	○	○
When User2 uses Device1, Policy2 applies.	○	○
When User2 uses Device2, Policy4 applies.	○	○

Correct Answer:

Statements	Yes	No
When User1 uses Device1, Policy3 applies.	○	●
When User2 uses Device1, Policy2 applies.	●	○
When User2 uses Device2, Policy4 applies.	○	●

Since Policy3 applies to iOS and Device1 is a Windows 10 device Policy3 does not apply.

Since User2 is a member of Group2 and Policy2 apply to Windows 10 devices, Policy2 applies to User2 on Device1.

User2 isn\'t a member of Group2 and since you need to have users as part of the protected group Policy4 does not apply to Device2 / User2.

References:

https://docs.microsoft.com/en-us/intune/apps/app-protection-policy

QUESTION 5

You have a hybrid Microsoft 365 environment.

All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.

You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.

What should you do?

A. On Server1, run readinessreportcreator.exe

B. Configure a registry entry on Server1

C. Configure a registry entry on the computers

D. On the computers, run tdadm.exe

Correct Answer: C

"To allow yourself and other administrators to identify the owners of Office files that have compatibility issues without revealing file names or specific locations, you can enable file obfuscation, which disguises Office file names, titles, and file paths. This setting is configured on the agent, which performs the obfuscation task before uploading data to the shared folder. The data that is stored on the local computer is not obfuscated."
https://docs.microsoft.com/enus/deployoffice/compat/manage-the-privacy-of-data-monitored-by-telemetry-in-office

[Latest MS-500 Dumps](#)   [MS-500 VCE Dumps](#)   [MS-500 Practice Test](#)