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 subscription.

You have a Data Subject Request (DSR) case named Case1. You need to ensure that Case1 includes all the email posted by the data subject to the Microsoft Exchange Online public folders.

Which additional property should you include in the Content Search query?

A. kind:externaldata

B. itemclass:ipm.externaldata

C. itemclass:ipm.post

D. kind:email

Correct Answer: C

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the- dsrcase-tool?view=o365-worldwide

QUESTION 2

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Azure Advanced Threat Protection (ATP) for the domain.

You install an Azure ATP standalone sensor on Server1.

You need to monitor the domain by using Azure ATP.

What should you do?

A. Configure port mirroring for Server1.

B. Install the Microsoft Monitoring Agent on DC1.

C. Install the Microsoft Monitoring Agent on Server1.

D. Configure port mirroring for DC1.

Correct Answer: D

Taken from: https://learn.microsoft.com/en-us/defender-for-identity/prerequisites

"The Defender for Identity standalone sensor is installed on a dedicated server and requires port mirroring to be configured on the domain controller to receive network traffic."

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring

---

QUESTION 3

You have a Microsoft 365 tenant that has modern authentication enabled.

You have Windows 10, MacOS. Android, and iOS devices that are managed by using Microsoft Endpoint Manager. Some users have older email client applications that use Basic authentication to connect to Microsoft Exchange Online. You need to implement a solution to meet the following security requirements:

1.

Allow users to connect to Exchange Online only by using email client applications that support modern authentication protocols based on OAuth 2.0.

2.

Block connections to Exchange Online by any email client applications that do NOT support modern authentication.

What should you implement?

A. a conditional access policy in Azure Active Directory (Azure AD)

B. an OAuth app policy m Microsoft Defender for Cloud Apps

C. a compliance policy in Microsoft Endpoint Manager

D. an application control profile in Microsoft Endpoint Manager

Correct Answer: A

Block clients that don\\'t support multi-factor with a Conditional Access policy.

Note: Clients that do not use modern authentication can bypass Conditional Access policies, so it\\'s important to block these.

Incorrect:

Not D: OAuth app policies enable you to investigate which permissions each app requested and which users authorized them for Office 365, Google Workspace, and Salesforce. You\\'re also able to mark these permissions as approved or

banned.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/identity-access-policies

---

QUESTION 4

HOTSPOT

You have a Microsoft 365 subscription.

You configure Microsoft Defender for Endpoint as shown in the following table.

Device group	Automation level
Group1	Full – remediate threats automatically
Group2	Semi – require approval for core folders
Group3	Semi – require approval for all folders

You onboard devices to Microsoft Defender for Endpoint as shown in the following table.

Name	In device group
Device1	Group1
Device2	Group2
Device3	Group3

Microsoft Defender for Endpoint contains the incidents shown in the following table.

Name	Device	File evidence	File verdict
Case1	Device1	C:\Temp\File1.exe	Suspicious
Case2	Device2	C:\Temp\File2.exe	Malicious
Case3	Device3	C:\Temp\File3.exe	Malicious

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:

Answer Area

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
C:\Temp\File1.exe will be remediated automatically.	○	○
C:\Temp\File2.exe will be remediated automatically.	○	○
C:\Temp\File3.exe will be remediated automatically.	○	○

Box 1: No

File1.exe on Device1 is suspicious. Device1 is in Group1. Group1 has automation level Full - remediate threats automatically.

Note: Full automation (recommended) means remediation actions are taken automatically on artifacts determined to be malicious.

Box 2: Yes

File2 on Device2 is malicious. Device2 is in Group2. Group2 has automation level Semi - require approval for core folders.

Note: Semi-automation means some remediation actions are taken automatically, but other remediation actions await approval before being taken.

Semi - require approval for core folders remediation:

With this level of semi-automation, approval is required for any remediation actions needed on files or executables that are in core folders. Core folders include operating system directories, such as the Windows (\windows*).

Remediation actions can be taken automatically on files or executables that are in other (non-core) folders.

Box 3: No

File3 on Device3 is malicious. Device3 is in Group3. Group3 has automation level Semi - require approval for all folders.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels

QUESTION 5

You have a Microsoft 365 subscription and a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) subscription. You have devices enrolled in Microsoft Endpoint Manager as shown in the following table:

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You integrate Microsoft Defender ATP and Endpoint Manager. You plan to evaluate the Microsoft Defender ATP risk level for the devices. You need to identify which devices can be evaluated. Which devices should you identify?

A. Device1 and Device2 only

B. Device1 only

C. Device1 and Device3 only

D. Device2 and Device3 only

Correct Answer: B

Microsoft Defender ATP supports Windows 10, Windows Server, macOSX, and Linux

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/evaluation-lab
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/ minimumrequirements