MS-500^{Q&As}

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

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

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 have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.

Solution: You modify the privacy profile, and then create a Data Subject Request (DSR) case.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 2

DRAG DROP

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Identity. You receive the following alerts:

1.

Suspected Netlogon privilege elevation attempt

2.

Suspected Kerberos SPN exposure

3.

Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map? To answer, drag the appropriate alerts to the correct stages. Each alert may be used once, more than once, or not at all. You may need to drag the split bar between panes or

scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Stages

Compromised credentials	Lateral movements
Domain dominance	Reconnaissance

Answer Area

Suspected Netlogon privilege
elevation attempt:

Suspected Kerberos SPN exposure:

Suspected DCSync attack:

Correct Answer:

Stages

| Compromised credentials | Lateral movements |
| Domain dominance | Reconnaissance |

Answer Area

Suspected Netlogon privilege elevation attempt: Compromised credentials

Suspected Kerberos SPN exposure: Compromised credentials

Suspected DCSync attack: Domain dominance

Box 1: Compromised credential

The following security alerts help you identify and remediate Compromised credential phase suspicious activities detected by Defender for Identity in your network.

In this tutorial, you\'ll learn how to understand, classify, remediate and prevent the following types of attacks:

Suspected Netlogon privilege elevation attempt (CVE-2020-1472 exploitation) (external ID 2411)

Suspected Kerberos SPN exposure (external ID 2410)

Etc.

Box 2: Compromised credential

Box 3: Domain dominance

The following security alerts help you identify and remediate Domain dominance phase suspicious activities detected by Defender for Identity in your network. In this tutorial, learn how to understand, classify, prevent, and remediate the

following attacks:

Suspected DCSync attack (replication of directory services) (external ID 2006)

Etc.

Reference:

https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts https://docs.microsoft.com/en-us/defender-for-identity/domain-dominance-alerts

---

QUESTION 3

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create?

A. ATP anti-phishing

B. DKIM

C. Anti-spam

D. Anti-malware

Correct Answer: C

"The default value is 15 days in the default anti-spam policy and in new anti-spam policies that you create in PowerShell. The default value is 30 days in new anti-spam policies that you create in the Microsoft 365 Defender portal.A valid value is from 1 to 30 days."

References: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spam-policies-configure?view=o365-worldwide

---

QUESTION 4

Which user passwords will User2 be prevented from resetting?

A. User6 and User7

B. User4 and User6

C. User4 only

D. User7 and User8

E. User8 only

Correct Answer: E

Assign the Password admin role to a user who needs to reset passwords for non-administrators and Password Administrators.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

QUESTION 5

HOTSPOT

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

Name	Role
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure Active Directory (Azure AD) Identity Protection.

You need to identify which users can perform the following actions:

Configure a user risk policy.

View the risky users report.

Which users should you identify? To answer, select the appropriate options in the answer area.
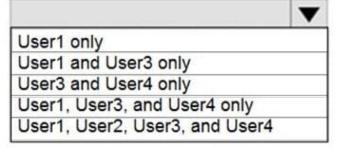
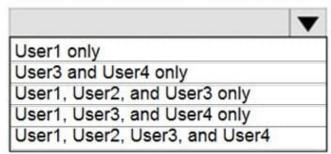NOTE: Each correct selection is worth one point.

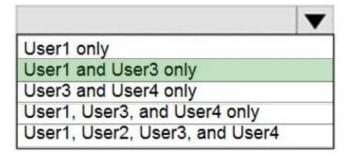Hot Area:

Answer Area
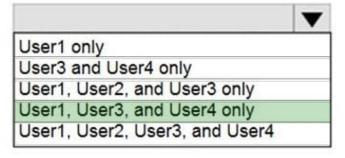
Configure a user risk policy:

▼
User1 only
User1 and User3 only
User3 and User4 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

▼
User1 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4

Correct Answer:

Answer Area

Configure a user risk policy:

▼
User1 only
User1 and User3 only
User3 and User4 only
User1, User3, and User4 only
User1, User2, User3, and User4

View the risky users report:

▼
User1 only
User3 and User4 only
User1, User2, and User3 only
User1, User3, and User4 only
User1, User2, User3, and User4