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.geekcert.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

HOTSPOT

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

Name	Type	Member of
User1	Member	Group1
User2	Member	Group2
User3	Guest	Group1

You assign an enterprise application named App1 to Group1 and User2.

You configure an Azure AD access review of App1. The review has the following settings:

Review name: Review1 Start date: 01–15–2020 Frequency: One time End date: 02–14–2020 Users to review: Assigned to an application Scope: Everyone Applications: App1 Reviewers: Members (self) Auto apply results to resource: Enable Should reviewer not respond: Take recommendations

On February 15, 2020, you review the access review report and see the entries shown in the following table:

Name	User requires access to App1	Last sign in
User1	Yes	February 14, 2020
User2	No response	February 1, 2020
User3	No response	January 3, 2020

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
On February 20, 2020, User1 can access App1.	○	○
On February 20, 2020, User2 can access App1.	○	○
On February 20, 2020, User3 can access App1.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
On February 20, 2020, User1 can access App1.	○	○
On February 20, 2020, User2 can access App1.	○	○
On February 20, 2020, User3 can access App1.	○	○

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/perform-access-review

QUESTION 2

HOTSPOT

You have a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) deployment that has the custom network indicators turned on. Microsoft Defender ATP protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP has the machine groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	*None*

From Microsoft Defender Security Center, you create the URLs/Domains indicators shown in the following table.

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

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
From a web browser on Computer1, you can open http://www.contoso.com.	O	O
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	O	O
From a web browser on Computer2, you can open http://www.litwareinc.com.	O	O

Correct Answer:

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	O	●
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	●	O
From a web browser on Computer2, you can open http://www.litwareinc.com.	O	●

QUESTION 3

Your company has a Microsoft 365 E5 subscription that uses Microsoft Defender for identity.

You plan to create a detection exclusion in Microsoft Defender for Identity.

What should you use to create the detection exclusion?

A. Microsoft Defender for Identity portal

B. Microsoft 365 Compliance center

C. Microsoft Defender for Cloud Apps portal

D. Microsoft 365 Defender portal

Correct Answer: D

https://learn.microsoft.com/en-us/defender-for-identity/exclusions

QUESTION 4

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the data loss prevention (DIP) policies in following table.

Name	Priority	Rule
DLP1	0	Rule1
DLP2	1	Rule2
DLP3	2	Rule3
DLP4	3	Rule4

The DLP rules are configured as shown in the following table.

Rule	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	On	Tip 1	Enabled
Rule2	On	Tip 2	Disabled
Rule3	On	Tip 3	Enabled
Rule4	On	Tip 4	Disabled

All the policies are assigned to Site1.

You need to ensure that if a user uploads a document to Site1 that matches all the rules, the user will be shown the Tip 2 policy tip.

What should you do?

A. Enable additional processing Of the policies if is a match for Rule1.

B. Change the priority Of DLP2 to 3.

C. Change the priority of DLP2 to 0

D. Prevent additional processing of the policies if there is a match for Rule2.

Correct Answer: C

The rule with priority 0 is processed first.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference

QUESTION 5

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

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.

Edit role setting - Security Operator ...
Privileged Identity Management | Azure AD roles

Activation   Assignment   Notification

Activation maximum duration (hours)

━━●━━━━━━━━━━━━━━━━━━━━━━━━ | 3 |

On activation, require ◯ None
                        ◉ Azure MFA

You add assignments to the Security Operator role as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

A. User2 only

B. User3 only

C. User1 and User2 only

D. User2 and User3 only

E. User1, User2, and User3

Correct Answer: D