Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
HOTSPOT
You need to recommend an email malware solution that meets the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy to create:

ATP safe attachments	V
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	V
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

NEW QUESTION 2
You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

A. Synchronization Service Manager
B. Azure AD Connect wizard
C. Synchronization Rules Editor
D. IdFix

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization
Case Study: 2 Litware, Inc Overview
Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.
Existing Environment
Internal Network Infrastructure
The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active Directory.
The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).
The following operating systems are used on the network:
•Windows Server 2016
•Windows 10 Enterprise

•Windows 8.1 Enterprise
The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.
Cloud Infrastructure
Litware recently purchased Microsoft 365 subscription licenses for all users.
Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.
You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes
Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management
Security Requirements
Litware identities the following security requirements:
•Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
•Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
•Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
•Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
•Implement a permanent eligible assignment of the Compliance administrator role for User1
•Integrate Windows Defender and Windows Defender ATP on domain-joined servers
•Prevent access to Azure resources for the guest user accounts by default
•Ensure that all domain-joined computers are registered to Azure AD
Multi-factor authentication (MFA) Requirements
Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA.
Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.
If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized
General Requirements
Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

NEW QUESTION 3
You need to create Group2.
What are two possible ways to create the group?

A. an Office 365 group in the Microsoft 365 admin center
B. a mail-enabled security group in the Microsoft 365 admin center
C. a security group in the Microsoft 365 admin center
D. a distribution list in the Microsoft 365 admin center
E. a security group in the Azure AD admin center

Answer: CE

NEW QUESTION 4
You need to implement Windows Defender ATP to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the ForceDefenderPassiveMode registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run WindowsDefenderATPOnboardingScript.cmd

Answer: C

Explanation:
Case Study: 3 Contoso, Ltd Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.
The company has the offices shown in the following table.

Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.
Existing Environment Infrastructure
The network contains an Active Directory domain named contoso.com that is synced to a Microsoft

Azure Active Directory (Azure AD) tenant. Password writeback is enabled.
The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.
Each client computer has a single volume.
Each office connects to the Internet by using a NAT device. The offices have the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

Named locations are defined in Azure AD as shown in the following table.

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.
Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department. The tenant contains the users shown in the following table.

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

The tenant contains the groups shown in the following table.

Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains "SEA"
ADGroup2	Office 365	User.city-match "Sea"

Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration
The devices enrolled in Intune are configured as shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.

Name	Include	Exclude
DevicePolicy1	GroupC	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

The Mark devices with no compliance policy assigned as setting is set to Compliant.
Requirements
Technical Requirements
Contoso identifies the following technical requirements:
•Use the principle of least privilege
•Enable User1 to assign the Reports reader role to users
•Ensure that User6 approves Customer Lockbox requests as quickly as possible
•Ensure that User9 can implement Azure AD Privileged Identity Management

NEW QUESTION 5
Which role should you assign to User1?

A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim

NEW QUESTION 6
What should User6 use to meet the technical requirements?

A. Supervision in the Security & Compliance admin center
B. Service requests in the Microsoft 365 admin center
C. Security & privacy in the Microsoft 365 admin center
D. Data subject requests in the Security & Compliance admin center

Answer: B

NEW QUESTION 7
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 have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend modifying the licenses assigned to User5. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
Case Study: 4 Mix Questions

NEW QUESTION 8
Your company has a Microsoft 365 subscription.
The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.
The users must be prevented from backing up the app's data to iCloud. What should you create?

A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
B. an app protection policy in Microsoft Intune
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 9
You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports in the Threat management dashboard. Which role provides User1with the required role permissions?

A. Security reader
B. Message center reader
C. Compliance administrator
D. Information Protection administrator

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded-to-view-the-atp-reports

NEW QUESTION 10
You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.
What is a prerequisite for running Attack simulator?

A. Enable multi-factor authentication (MFA)
B. Configure Advanced Threat Protection (ATP)
C. Create a Conditional Access App Control policy for accessing Office 365
D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

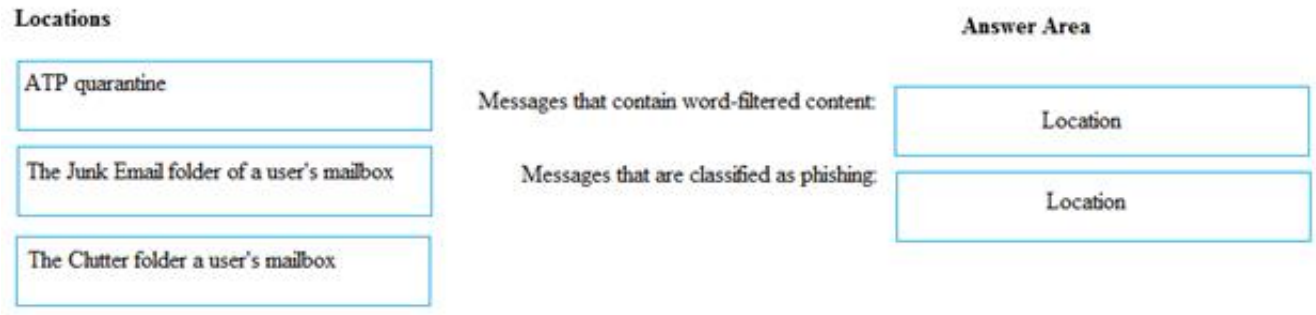
NEW QUESTION 10
You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.
The email address that you intend to spoof belongs to the Executive group members. What should you do first?

A. From Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
C. Enable MFA for the Research group members
D. Migrate the Executive group members to Exchange Online

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

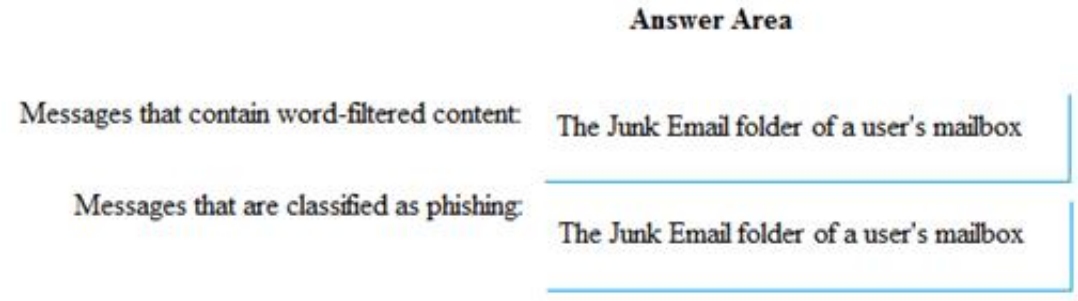
NEW QUESTION 11
DRAG DROP
You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.
Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location 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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 12
You have a Microsoft 365 subscription.
You create an Advanced Threat Protection (ATP) safe attachments policy to quarantine malware. You need to configure the retention duration for the attachments in quarantine.
Which type of threat management policy should you create from the Security&Compliance admin center?

A. ATP anti-phishing
B. DKIM
C. Anti-spam
D. Anti-malware

Answer: D

NEW QUESTION 16
Note: This question is part of 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 have a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the content expiration settings of the label.
Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 18
HOTSPOT
You have the Microsoft conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

A. Mastered
B. Not Mastered

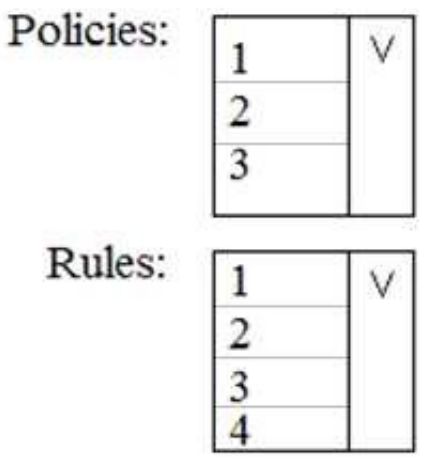
Answer: A

Explanation:

Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

NEW QUESTION 19
HOTSPOT
You have a Microsoft 365 subscription.
You identify the following data loss prevention (DLP) requirements:
•Send notifications to users if they attempt to send attachments that contain EU social security numbers
•Prevent any email messages that contain credit card numbers from being sent outside your organization
•Block the external sharing of Microsoft OneDrive content that contains EU passport numbers

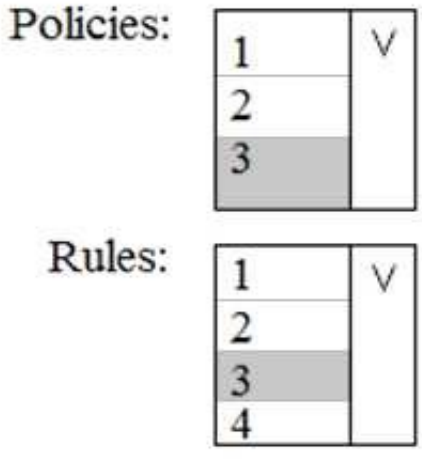
•Send administrators email alerts if any rule matches occur.
What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



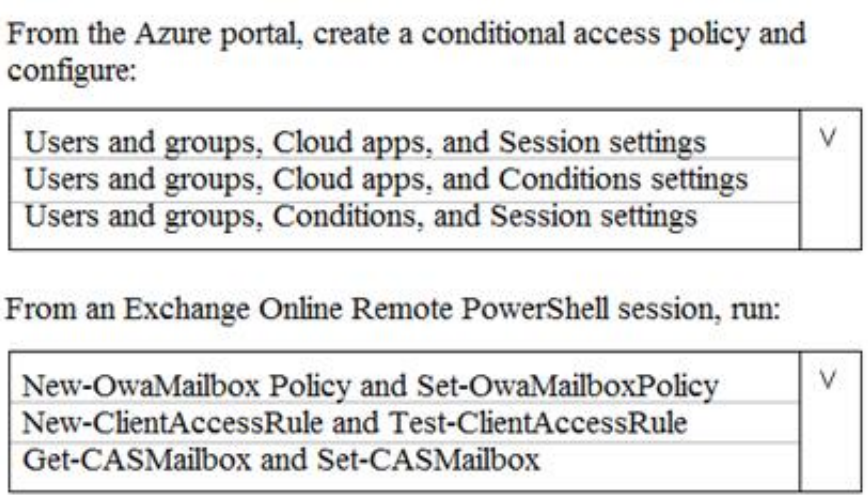
A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 21
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.
You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings
Users and groups, Cloud apps, and Conditions settings
Users and groups, Conditions, and Session settings

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy
New-ClientAccessRule and Test-ClientAccessRule
Get-CASMailbox and Set-CASMailbox

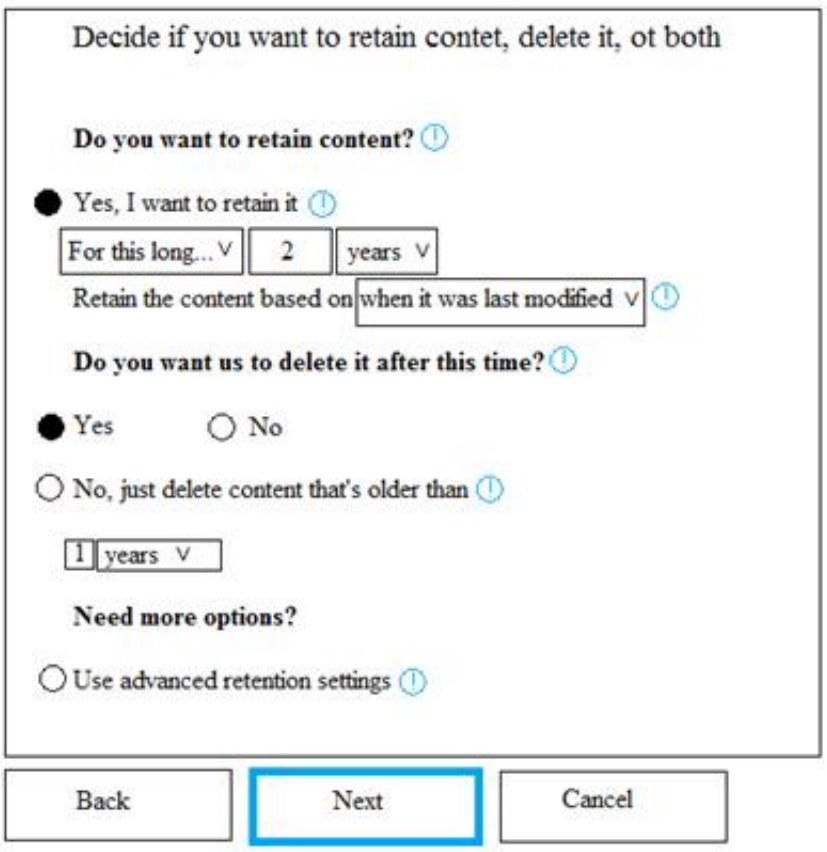
NEW QUESTION 22
You have a Microsoft 365 subscription.
A user reports that changes were made to several files in Microsoft OneDrive.
You need to identify which files were modified by which users in the user's OneDrive. What should you do?

A. From the Azure Active Directory admin center, open the audit log
B. From the OneDrive admin center, select Device access
C. From Security & Compliance, perform an eDiscovery search
D. From Microsoft Cloud App Security, open the activity log

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/activity-filters

NEW QUESTION 26
HOTSPOT
You have a Microsoft 365 subscription.
You are creating a retention policy named Retention1 as shown in the following exhibit.



You apply Retention1 to SharePoint sites and OneDrive accounts.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

If a user creates a file in a Microsoft SharePoint library on January 1,2019, and modifies the file every six months, the file will be **[answer choice]**.

retained
deleted on Jauary 1,2021
deleted on July 1,2021

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice]**.

cannot recover the file
can recover the file until Jauary 1,2020
can recover the file until March 1,2020
can recover the file until May 1,2020

A. Mastered
B. Not Mastered

Answer: A

Explanation:

If a user creates a file in a Microsoft SharePoint library on January 1,2019, and modifies the file every six months, the file will be **[answer choice]**.

retained
deleted on Jauary 1,2021
deleted on July 1,2021

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user **[answer choice].**

cannot recover the file
can recover the file until Jauary 1,2020
can recover the file until March 1,2020
can recover the file until May 1,2020

NEW QUESTION 29
You have a Microsoft 365 subscription.
The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.
You need to ensure that Admin1 can view the results of Case1. What should you do first?

A. From the Azure Active Directory admin center, assign a role group to Admin1.
B. From the Microsoft 365 admin center, assign a role to Admin1.
C. From Security & Compliance admin center, assign a role group to Admin1.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

NEW QUESTION 31
You have a Microsoft 365 subscription.
You need to enable auditing for all Microsoft Exchange Online users. What should you do?

A. From the Exchange admin center, create a journal rule
B. Run the Set-MailboxDatabase cmdlet
C. Run the Set-Mailbox cmdlet
D. From the Exchange admin center, create a mail flow message trace rule.

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

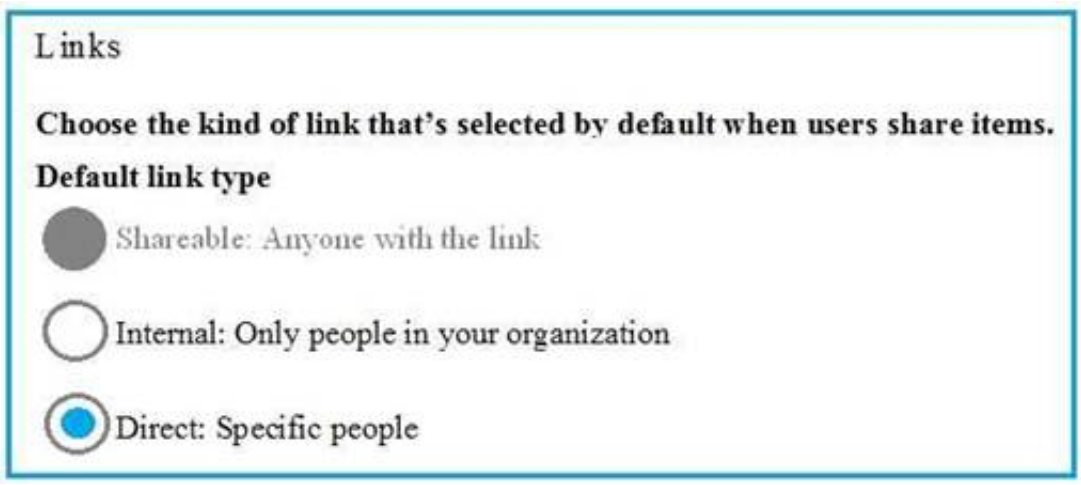
NEW QUESTION 36
You have a Microsoft 365 subscription.
All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data.
You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

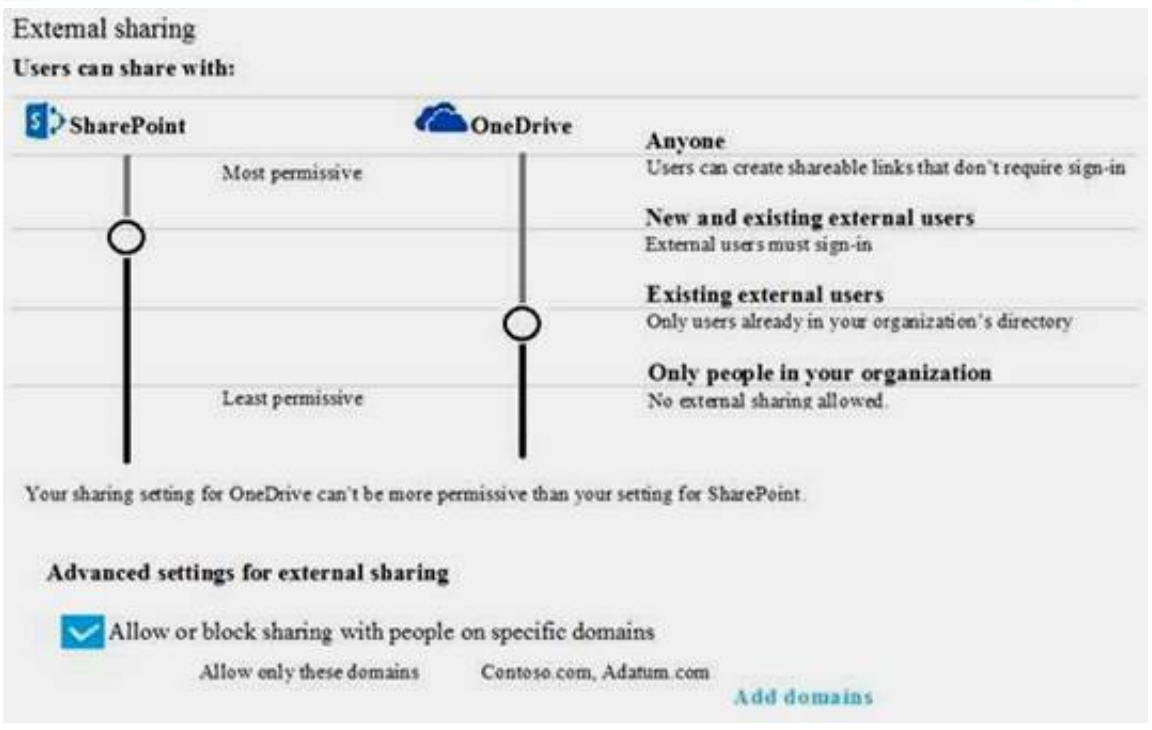
A. a device configuration profile that has device restrictions configured
B. a device configuration profile that has the Endpoint Protection settings configured
C. a device configuration policy that has the System Security settings configured
D. a device compliance policy that has the Device Health settings configured

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry

NEW QUESTION 37
HOTSPOT
You have a Microsoft 365 subscription that uses a default name of litwareinc.com.
You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.





Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

A user who has an email address of user1@fabrikam.com [answer choice].

- cannot access OneDrive content
- can access OneDrive content after a link is created
- must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

- the user cannot access OneDrive content
- the user can access OneDrive content after a link is created
- must be added to a group before the user can access shared files

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/onedrive/manage-sharing

NEW QUESTION 41
You have a Microsoft 365 subscription that includes a user named User1.
You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.
You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.
Which type of Cloud App Security policy should you create?

A. an app permission policy
B. an activity policy
C. a Cloud Discovery anomaly detection policy
D. a session policy

Answer: D

NEW QUESTION 45

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 questions 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 have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

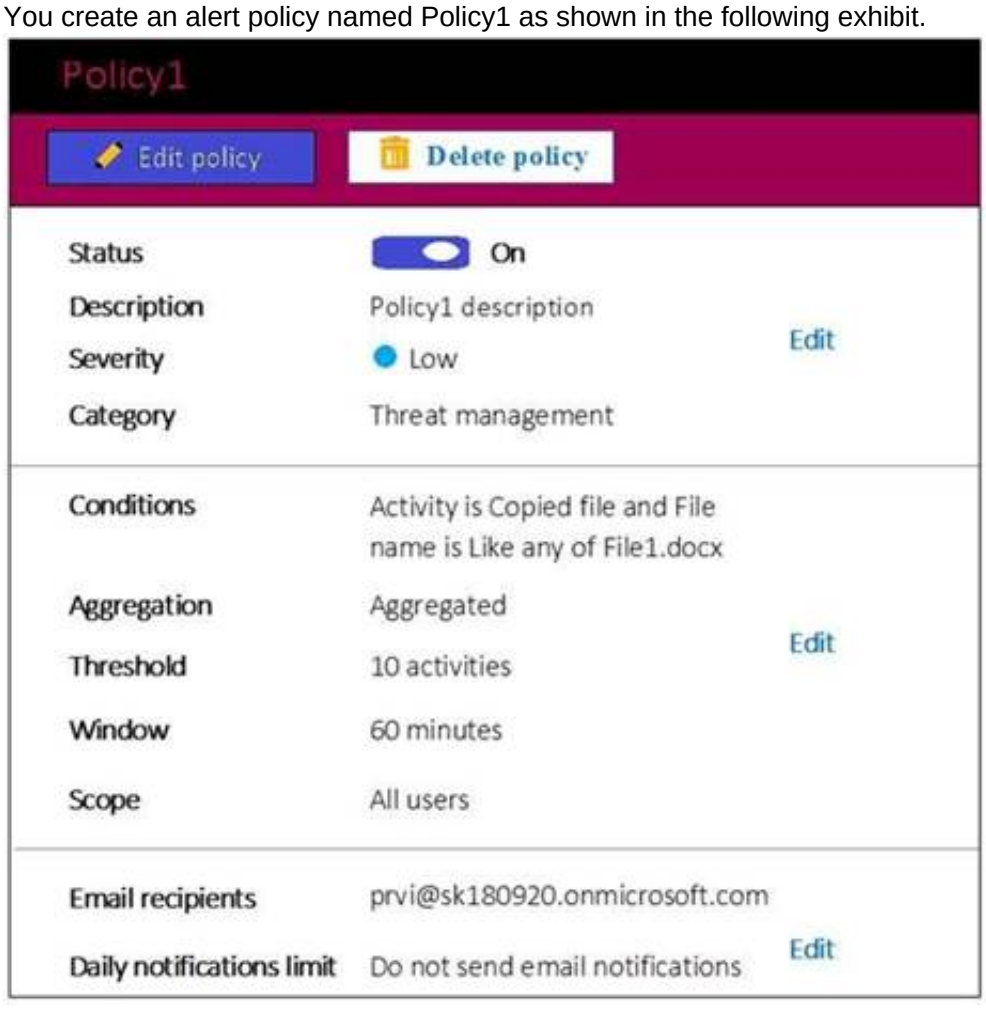
NEW QUESTION 49
You have a Microsoft 365 subscription.
You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

A. From Search & investigation, create a guided search.
B. From Events, create an event.
C. From Alerts, create an alert policy.
D. From Search & Investigation, create an eDiscovery case.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION 50
HOTSPOT
You have a Microsoft 365 subscription that include three users named User1, User2, and User3.
A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.
You create an alert policy named Policy1 as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered after 45 minutes
- Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

- Policy1 will not be triggered
- Policy1 will be triggered within 20 minutes
- Policy1 will be triggered within 45 minutes
- Policy1 will be triggered after 60 minutes

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

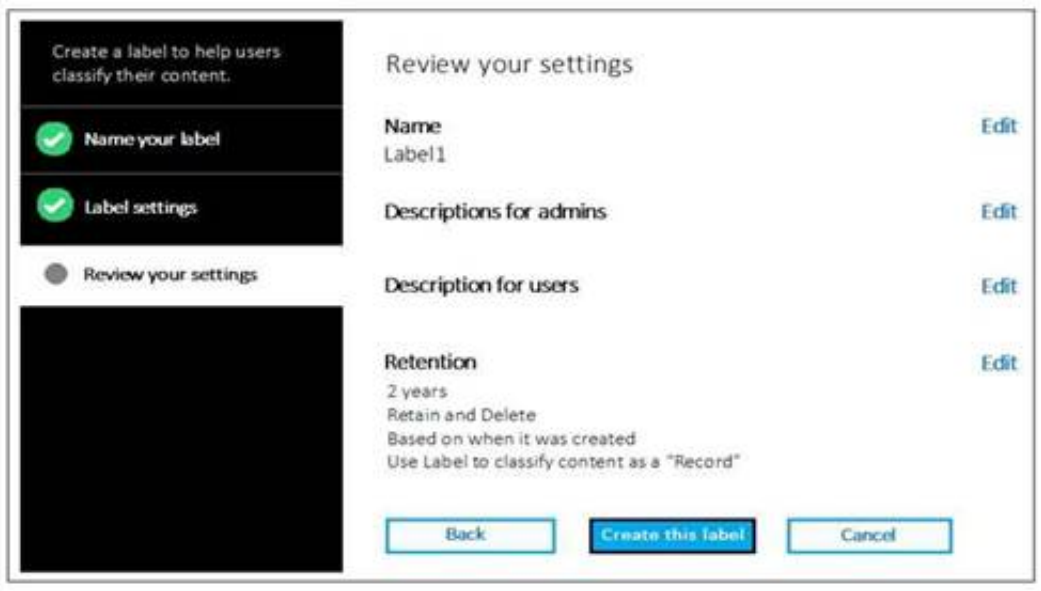
NEW QUESTION 55
You have a Microsoft 365 subscription.
All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

A. 30 days
B. 90 days
C. 365 days
D. 5 years

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance

NEW QUESTION 59
HOTSPOT
You have a Microsoft 365 subscription.
You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

If you create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

- never delete the file.
- delete the file before January 1, 2021.
- delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

- always remain in the library.
- remain in the library until you delete the file.
- be deleted automatically on March 15, 2021.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

NEW QUESTION 63
HOTSPOT
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:
•Rulel:
•Conditions: Label 1, Detect content that's shared with people outside my organization
•Actions: Restrict access to the content for external users
•User notifications: Notify the user who last modified the content
•User overrides: On
•Priority: 0
•Rule2:
•Conditions: Label 1 or Label2
•Actions: Restrict access to the content
•Priority: 1
•Rule3:
•Conditions: Label2, Detect content that's shared with people outside my organization
•Actions: Restrict access to the content for external users
•User notifications: Notify the user who last modified the content
•User overrides: On
•Priority: 2
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
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
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

NEW QUESTION 65
Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. the Exchange admin center
B. the Azure ATP admin center
C. Microsoft Azure Security Center

D. the Security & Compliance admin center
E. Outlook on the web

Answer: AD

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages- and-files

NEW QUESTION 66
You have a Microsoft 365 subscription. You enable auditing for the subscription.
You plan to provide a user named Auditor with the ability to review audit logs. You add Auditor to the Global administrator role group.
Several days later, you discover that Auditor disabled auditing.
You remove Auditor from the Global administrator role group and enable auditing.

A. Security operator
B. Security reader
C. Security administrator
D. Compliance administrator

Answer: D

NEW QUESTION 70
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. Anti-malware
B. DKIM
C. Anti-spam
D. ATP anti-phishing

Answer: A

NEW QUESTION 71
Your network contains an on-premises Active Directory domain. The domain contains servers that
run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Configure Event Forwarding on the domain controllers
B. Configure auditing in the Office 365 Security & Compliance center.
C. Turn on Delayed updates for the Azure ATP sensors.
D. Enable the Audit account management Group Policy setting for the servers.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION 74
.....

Relate Links

100% Pass Your MS-500 Exam with Exambible Prep Materials

https://www.exambible.com/MS-500-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/