Exam Questions MS-500

Microsoft 365 Security Administrator

https://www.2passeasy.com/dumps/MS-500/

NEW QUESTION 1
You need to recommend a solution for the user administrators that meets the security requirements for auditing.
Which blade should you recommend using from the Azure Active Directory admin center?

A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods
D. Access review

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

NEW QUESTION 2
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 3
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 4
Which IP address space should you include in the MFA configuration?

A. 131.107.83.0/28
B. 192.168.16.0/20
C. 172.16.0.0/24
D. 192.168.0.0/20

Answer: B

NEW QUESTION 5
HOTSPOT
Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

ADGroup1:

None
User1 and User2 only
User2 and User4 only
User3 and User4 only
User1, User2, User3, and User4

ADGroup2:

None
User1 and User2 only
User2 and User4 only
User3 and User4 only
User1, User2, User3, and User4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

NEW QUESTION 6
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

Answer: C

NEW QUESTION 7
HOTSPOT
You are evaluating which devices are compliant in Intune.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
Device2 is compliant.	○	○
Device5 is compliant.	○	○
Device6 is compliant.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device2 is compliant.	◉	○
Device5 is compliant.	○	◉
Device6 is compliant.	◉	○

NEW QUESTION 8

HOTSPOT

Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

DevicePolicy1:
| None |
| Device1 only |
| Device3 only |
| Device2 and Device3 only |
| Device1 and Device3 only |
| Device1, Device2, and Device3 |

DevicePolicy2:
| None |
| Device4 only |
| Device2 and Device4 only |
| Device2, Device3, and Device 4 only |

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

DevicePolicy1:
| None |
| Device1 only |
| Device3 only |
| **Device2 and Device3 only** |
| Device1 and Device3 only |
| Device1, Device2, and Device3 |

DevicePolicy2:
| None |
| **Device4 only** |
| Device2 and Device4 only |
| Device2, Device3, and Device 4 only |

NEW QUESTION 9

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 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:
•Source Anchor: objectGUID
•Password Hash Synchronization: Disabled
•Password writeback: Disabled
•Directory extension attribute sync: Disabled
•Azure AD app and attribute filtering: Disabled
•Exchange hybrid deployment: Disabled
•User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.
Does that meet the goal?

A. Yes
B. No
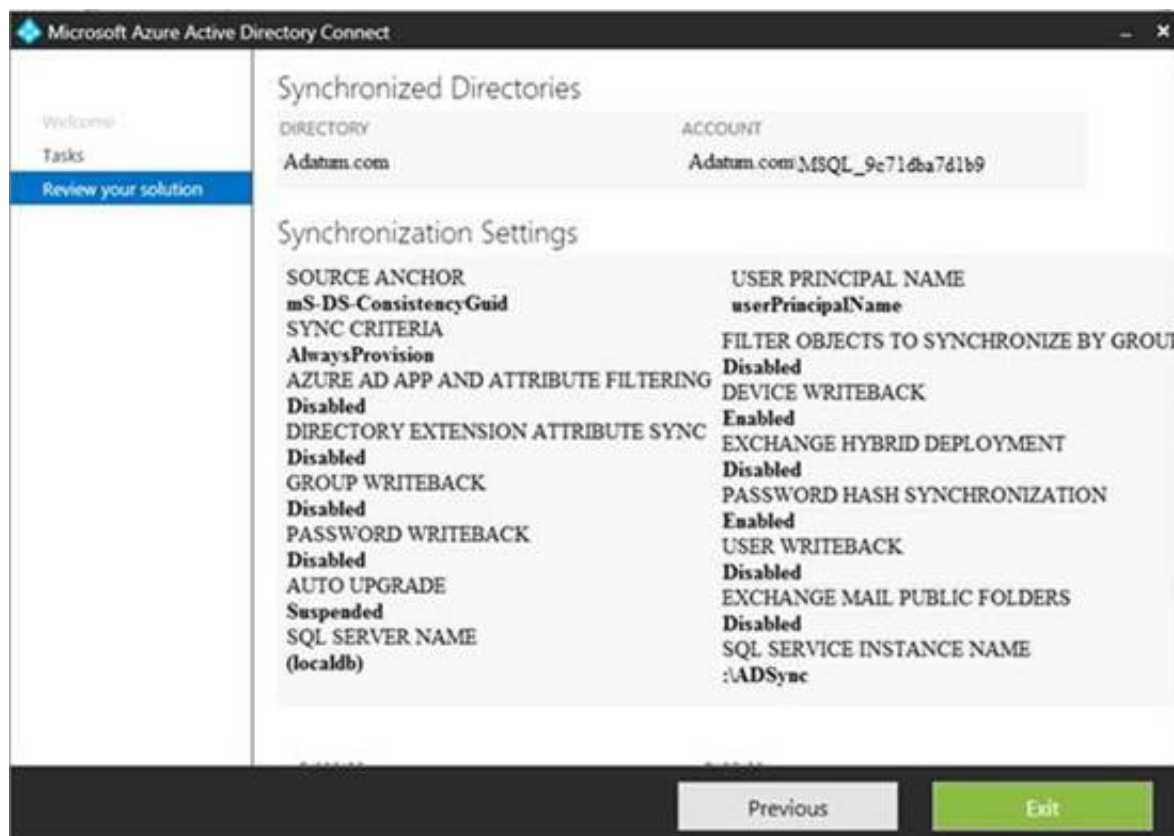
Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

NEW QUESTION 10
HOTSPOT
You configure Microsoft Azure Active Directory (Azure AD) Connect 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 you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback

NEW QUESTION 10
You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.
You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network.
What should you do first?

A. From the Azure Active Directory admin center, create a new certificate
B. Enable Application Proxy in Azure AD
C. From Active Directory Administrative Center, create a Dynamic Access Control policy
D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10

NEW QUESTION 13
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user.
You need to see the permissions of the Reports reader role. Which admin center should you use?

A. Azure Active Directory
B. Cloud App Security
C. Security & Compliance

D. Microsoft 365

Answer: A

NEW QUESTION 18
You have a Microsoft 365 subscription.
You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.
What should you use to achieve the goal?

A. Security & Compliance permissions
B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
C. Microsoft Azure AD group management
D. Microsoft Office 365 user management

Answer: B

NEW QUESTION 21
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 24
HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.
You are deploying Azure Advanced Threat Protection (ATP)
You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.
You need to integrate the VPN and Azure ATP.
What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On VPN1:

Configure an authentication provider.	∨
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	∨
1723	
1813	
8080	
8531	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

NEW QUESTION 27
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.
You create an app protection policy named ProtectionPolicy1 that has the following settings:
• Protected apps: App1
• Exempt apps: App2
• Windows Information Protection mode: Block
You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. 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   Yes   No

From Device1, User1 can copy data from App1 to App3.   ○   ○
From Device2, User1 can copy data from App1 to App2.   ○   ○
From Device2, User1 can copy data from App1 to App3.   ○   ○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area   Yes   No

From Device1, User1 can copy data from App1 to App3.   ○   ○
From Device2, User1 can copy data from App1 to App2.   ○   ○
From Device2, User1 can copy data from App1 to App3.   ○   ○

NEW QUESTION 32
HOTSPOT
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

NEW QUESTION 35

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 encryption settings of the label.

Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 38
HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.
To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12,Group13,and Group14 only	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/prepare

NEW QUESTION 41
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 45
You create a data loss prevention (DLP) policy as shown in the following shown:
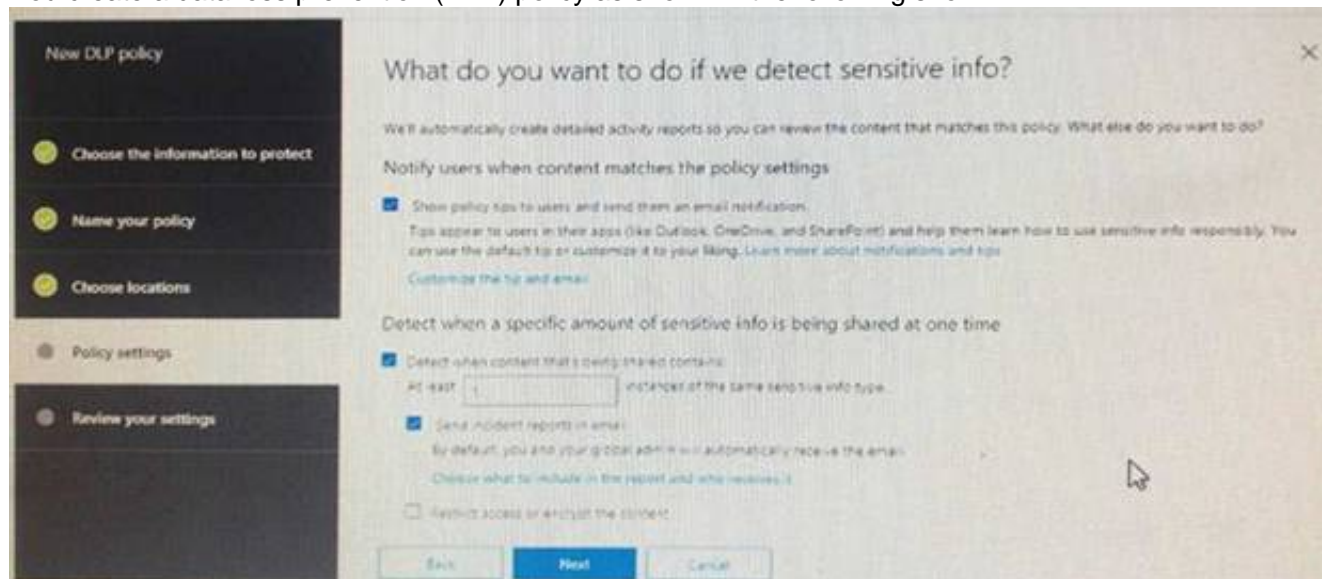
What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

A. The user receives a notification and can send the email message
B. The user receives a notification and cannot send the email message
C. The email message is sent without a notification
D. The email message is blocked silently

Answer: A

Explanation:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION 46
You have a Microsoft 365 subscription.
You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.
Which type of site collection should you create first?

A. Records Center
B. Compliance Policy Center
C. eDiscovery Center
D. Enterprise Search Center
E. Document Center

Answer: C

Explanation:
Reference:
https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb944-448d-b83d-8fec4abcc24c

NEW QUESTION 47
You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries.
Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. From the Cloud App Security admin center, create a file policy.
B. From the SharePoint admin center, modify the Site Settings.
C. From the SharePoint & Compliance admin center, create a label.
D. From the SharePoint admin center, modify the records management settings.
E. From the Security & Compliance admin center, publish a label.

Answer: CE

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp

NEW QUESTION 51
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 55
HOTSPOT
You view Compliance Manager 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.

To increase the GDPR Compliance Score for Microsoft Office 365, you must **[answer choice]**.

assign action items	V
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score **[answer choice]**.

proves that the organization is non-compliant	V
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

NEW QUESTION 56
You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.
You need to ensure that the users can use the new label to protect their email. What should you do?

A. Modify the priority order of label policies
B. Wait six hours and ask the users to try again
C. Create a label policy
D. Create a new sensitive information type

Answer: B

NEW QUESTION 59
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 on Server1

C. Configure a registry on the computers
D. On the computers, run tdadm.exe

Answer: C

NEW QUESTION 62
HOTSPOT
You have a Microsoft 365 E5 subscription.
Users and device objects are added and removed daily. Users in the sales department frequently
change their device.
You need to create three following groups:

Group		Requirement
	1	All the devices of users where the Department attributes is set to Sales
	2	All the devices where the Department attribute is set to Sales
	3	All the devices where the deviceOwnership attribute is set to Company

The solution must minimize administrative effort.
What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Groups that have assigned membership:

0
1
2
3

Groups that have dynamic membership:

0
1
2
3

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md

NEW QUESTION 64
HOTSPOT
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
•Assignments: Include Group1, Exclude Group2
•Conditions: Sign in risk of Low and above
•Access: Allow access, Require password change
You need to identify how the policy affects User1 and User2.
What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Must change their password: [dropdown]

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

Prompted for MFA: [dropdown]

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Must change their password: [dropdown]

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

Prompted for MFA: [dropdown]

User1 only
User2 only
Both User1 and User2
Neither User1 not User2

NEW QUESTION 66
You have a Microsoft 365 Enterprise E5 subscription.
You use Windows Defender Advanced Threat Protection (Windows Defender ATP).
You need to integrate Microsoft Office 365 Threat Intelligence and Windows Defender ATP. Where should you configure the integration?

A. From the Microsoft 365 admin center, select Settings, and then select Services & add-ins.
B. From the Security & Compliance admin center, select Threat management, and then select Explorer.
C. From the Microsoft 365 admin center, select Reports, and then select Security & Compliance.
D. From the Security & Compliance admin center, select Threat management and then select Threat tracker.

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp

NEW QUESTION 70
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 auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

NEW QUESTION 73

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 74
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-AdminAuditLogConfig -AdminAuditLogEnabled $true-AdminAuditLogCmdlets *Mailbox* 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/setadminauditlogconfig?view=exchange-ps

NEW QUESTION 76
You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
B. From the Cloud App Security admin center, apply a filter to the alerts.
C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Answer: D

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

NEW QUESTION 81
HOTSPOT
You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

Search   [Clear]   **Results**

Activities

	Date ∨	IP address	User	Activity	Item
Show results for all activities ∨					

× Clear all to show results for all activities

Search

User administration activities

Added user	Deleted user	Set license properties
Reset user password	Changed user password	Changed user license
Updated user	Set property that forces user to change password	

Azure AD group administration activities

Added group	Updated group	Deleted group
Added member to group	Removed member from group	

Application administration activities

Added service principal	Removed a service principal from the directory	Set delegation entry
Removed credentials from a service principal	Added delegation entity	Added credentials to a service principal

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 83
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.

Policy1

[Edit policy]   [Delete policy]

Status	On
Description	Policy1 description
Severity	● Low
Category	Threat management

Edit

Conditions	Activity is Copied file and File name is Like any of File1.docx
Aggregation	Aggregated
Threshold	10 activities
Window	60 minutes
Scope	All users

Edit

Email recipients	prvi@sk180920.onmicrosoft.com
Daily notifications limit	Do not send email notifications

Edit

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 88
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 92
HOTSPOT
You have a Microsoft 365 subscription.
You create a retention label named Label1 as shown in the following exhibit.

Create a label to help users classify their content.

✅ Name your label

✅ Label settings

⚪ Review your settings

Review your settings

Name	Edit
Label1	

Descriptions for admins	Edit

| Description for users | Edit |

Retention	Edit
2 years	
Retain and Delete	
Based on when it was created	
Use Label to classify content as a "Record"	

Back | Create this label | Cancel

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 96
You have a Microsoft 365 subscription.
You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.
You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.
Which cmdlet should you use?

A. Get-UnifiedGroup
B. Get-MailUser
C. Get-TeanMessagingSettings
D. Get-TeamChannel

Answer: A

NEW QUESTION 99
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 101
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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.
You use the Directory Service event log on Server1. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 102
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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.
You use the System event log on Server1. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION 105
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-MailboxFolderPermission –Identity "User1"
-User User1@contoso.com –AccessRights Owner command. Does that meet the goal?

A. Yes
B. No

Answer: B

Explanation:
References:
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set- mailbox?view=exchange-ps

NEW QUESTION 106
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-500 Product From:

https://www.2passeasy.com/dumps/MS-500/

Money Back Guarantee

MS-500 Practice Exam Features:

* MS-500 Questions and Answers Updated Frequently

* MS-500 Practice Questions Verified by Expert Senior Certified Staff

* MS-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year