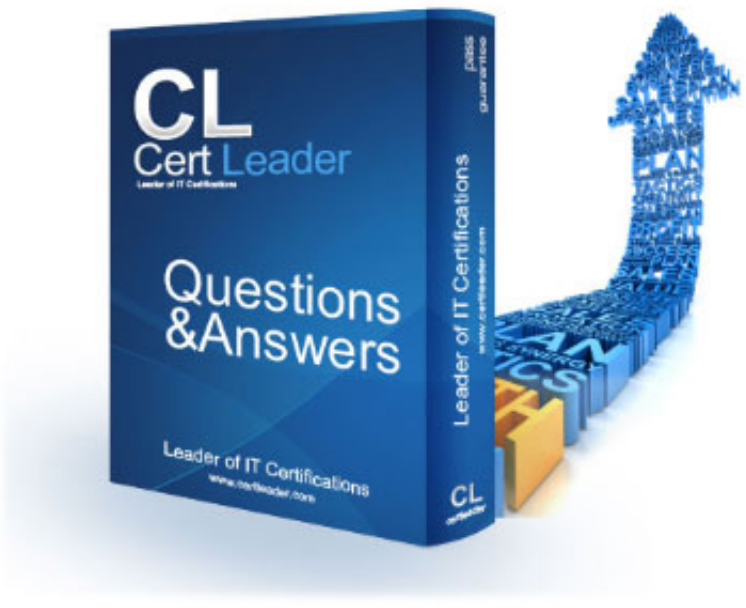
MS-500 Dumps

Microsoft 365 Security Administrator

https://www.certleader.com/MS-500-dumps.html



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 plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.
Which other settings should you configure? 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 3
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 4
HOTSPOT
You install Azure ATP sensors on domain controllers.
You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.
You need to meet the security requirements for Azure ATP reporting.
What should you configure? 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:
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy

NEW QUESTION 5
You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.
What should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Create an access review.
B. Assign the Global administrator role to User1.
C. Assign the Guest inviter role to User1.
D. Modify the External collaboration settings in the Azure Active Directory admin center.

Answer: AC

NEW QUESTION 6
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 7
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.

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

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.

The tenant contains the groups shown in the following table.

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

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

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

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 8
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.

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 9
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 10
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
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.

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 assigning the Compliance Manager Reader role to User1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 11
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 Source Anchor settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 12
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.
The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Clock the Exhibit tab.)

In contoso.com, you create the users shown in the following table.

What is the effect of the configuration? 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 15
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 17
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 21
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 26
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 28
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 31
You have a Microsoft 365 E5 subscription.
You implement Advanced Threat Protection (ATP) safe attachments policies for all users.
User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be

blocked.
What should you do from ATP?

A. Set the action to Block
B. Add an exception
C. Add a condition
D. Set the action to Dynamic Delivery

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing

NEW QUESTION 35
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.

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 38
HOTSPOT
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

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

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

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 40
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 44
Your company has 500 computers.
You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.
You need to recommend a remediation solution that meets the following requirements: Windows Defender ATP administrators must manually approve all remediation for the executives
Remediation must occur automatically for all other users
What should you recommend doing from Windows Defender Security Center?

A. Configure 20 system exclusions on automation allowed/block lists
B. Configure two alert notification rules
C. Download an offboarding package for the computers of the 20 executives
D. Create two machine groups

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groupswindows-defender-advanced-threat-protection

NEW QUESTION 45
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 create a new label in the global policy and instruct the user to resend the email message.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 49
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 53
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 54
HOTSPOT
Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.
The company has the offices shown in the following table.

The tenant contains the users shown in the following table.

You create the Microsoft Cloud App Security policy shown in the following exhibit.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 58
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 63
You have a Microsoft 365 subscription.
Some users access Microsoft SharePoint Online from unmanaged devices.
You need to prevent the users from downloading, printing, and synching files. What should you do?
A. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
B. From the SharePoint admin center, configure the Access control settings
C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Answer: B

NEW QUESTION 64
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:

NEW QUESTION 67
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 69
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 70
You recently created and published several labels policies in a Microsoft 365 subscription.
You need to view which labels were applied by users manually and which labels were applied automatically.
What should you do from the Security & Compliance admin center?

A. From Search & investigation, select Content search
B. From Data governance, select Events
C. From Search & investigation, select eDiscovery
D. From Reports, select Dashboard

Answer: B

NEW QUESTION 75
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 80
HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Policy1 if configured as showing in the following exhibit.

Policy2 is configured as shown in the following exhibit.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence

NEW QUESTION 83
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.

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 85
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 90
You have a Microsoft 365 subscription.
Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.
You need to ensure that the labels will be available for manual assignment as soon as possible. What should you do?

A. From the Security & Compliance admin center, create a label policy
B. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
C. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Answer: C

NEW QUESTION 93
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 97
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. Mastered

B. Not Mastered

Answer: A

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

NEW QUESTION 99
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 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 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 102
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 107
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.

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 109
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.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 114
You have a Microsoft 365 subscription.
You create a retention policy and apply the policy to Exchange Online mailboxes.
You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.
What should you do?

A. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy
D. From the Security & Compliance admin center, create a label policy

Answer: D

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

NEW QUESTION 115
You have a Microsoft 365 subscription.
You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.
What should you create first?

A. A retention label in Microsoft Office 365
B. A custom sensitive information type
C. A Data Subject Request (DSR)
D. A safe attachments policy in Microsoft Office 365

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-thedsr-case-tool#more-information-about-using-the-dsr-case-tool

NEW QUESTION 116
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 117
You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses. You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy. You need to enable mailbox intelligence for all users. What should you do first?

A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect).
B. Purchase the ATP add-on.
C. Select Directory extension attribute sync in Microsoft Azure Active Directory Connect {Azure AD Connect).
D. Migrate the on-premises mailboxes to Exchange Online.

Answer: B

NEW QUESTION 121
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 Security 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 122
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 127
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 129
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your MS-500 Exam with Our Prep Materials Via below:

https://www.certleader.com/MS-500-dumps.html