



MS-500.58q

MS-500

MS-500

Microsoft 365 Security Administration

Score: 800/1000

Version:

Time Limit: 120 Minutes

Implement and manage identity and access

Case Study (2 questions)

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 identifies 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 wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question 1

Which IP address space should you include in the MFA configuration?

- ☐ 131.107.83.0/28
- ☐ 192.168.16.0/20
- ☐ 172.16.0.0/24
- ☐ 192.168.0.0/20

Question 2

You need to create Group2.

What are two possible ways to create the group?

- ☐ an Office 365 group in the Microsoft 365 admin center
- ☐ a mail-enabled security group in the Microsoft 365 admin center
- ☐ a security group in the Microsoft 365 admin center
- ☐ a distribution list in the Microsoft 365 admin center
- ☐ a security group in the Azure AD admin center

Case Study (3 questions)

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

Question 3

Which role should you assign to User1?

- ☐ Global administrator
- ☐ User administrator
- ☐ Privileged role administrator
- ☐ Security administrator

Question 4

You need to meet the technical requirements for User9. What should you do?

- ☐ Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
- ☐ Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
- ☐ Assign the Security administrator role to User9
- ☐ Assign the Global administrator role to User9

Question 5

Which user passwords will User2 be prevented from resetting?

- ☐ User6 and User7
- ☐ User4 and User6
- ☐ User4 only
- ☐ User7 and User8
- ☐ User8 only

(10 questions)**Question 6**

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 conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- ☐ an app protection policy in Microsoft Intune
- ☐ a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- ☐ a device compliance policy in Microsoft Intune

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 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?

- ☐ Yes
- ☐ No

Question 8

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 Application event log on Server1.

Does that meet the goal?

- ☐ Yes
- ☐ No

Question 9

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?

- ☐ From the Azure Active Directory admin center, create a new certificate
- ☐ Enable Application Proxy in Azure AD
- ☐ From Active Directory Administrative Center, create a Dynamic Access Control policy
- ☐ From the Azure Active Directory admin center, configure authentication methods

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 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?

- ☐ Yes
- ☐ No

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 Password Hash Synchronization settings.

Does that meet the goal?

- ☐ Yes
- ☐ No

Question 12

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?

- ☐ Azure Active Directory
- ☐ Cloud App Security
- ☐ Security & Compliance
- ☐ Microsoft 365

Question 13

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?

- ☐ Security & Compliance permissions
- ☐ Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- ☐ Microsoft Azure AD group management
- ☐ Microsoft Office 365 user management

Question 14

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

- ☐ a user risk policy
- ☐ a sign-in risk policy
- ☐ a named location in Azure Active Directory (Azure AD)
- ☐ an Azure MFA Server

Question 15

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?

- ☐ Yes
- ☐ No

Implement and manage threat protection

Case Study (1 questions)

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 identifies 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 wants to minimize the deployment of additional servers and services in the Active Directory forest.

Question 16

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

- ☐ Configure port mirroring
- ☐ Create the ForceDefenderPassiveMode registry setting
- ☐ Download and install the Microsoft Monitoring Agent
- ☐ Run WindowsDefenderATPOnboardingScript.cmd

(14 questions)**Question 17**

You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.

You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.

Which type of device configuration profile should you use?

- ☐ Endpoint protection
- ☐ Device restrictions
- ☐ Identity protection
- ☐ Windows Defender ATP

Question 18

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?

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

Question 19

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?

- ☐ ATP anti-phishing
- ☐ DKIM
- ☐ Anti-spam
- ☐ Anti-malware

Question 20

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?

- ☐ Configure auditing in the Office 365 Security & Compliance center.
- ☐ Turn off Delayed updates for the Azure ATP sensors.
- ☐ Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
- ☐ Integrate SIEM and Azure ATP.

Question 21

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?

- ☐ Set the action to Block
- ☐ Add an exception
- ☐ Add a condition
- ☐ Set the action to Dynamic Delivery

Question 22

You have a Microsoft 365 tenant.

You have 500 computers that run Windows 10.

You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.

You need to ensure that the computers connect to Windows Defender ATP.

How should you prepare Intune for Windows Defender ATP?

- ☐ Configure an enrollment restriction
- ☐ Create a device configuration profile
- ☐ Create a conditional access policy
- ☐ Create a Windows Autopilot deployment profile

Question 23

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?

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

Question 24

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?

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

Question 25

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1.

How long after the Azure ATP cloud service is updated will Sensor1 be updated?

- ☐ 7 days
- ☐ 24 hours
- ☐ 1 hour
- ☐ 48 hours
- ☐ 12 hours

Question 26

Several users in your Microsoft 365 subscription report that they received an email message without 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.

- ☐ the Exchange admin center
- ☐ the Azure ATP admin center
- ☐ Outlook on the web
- ☐ the Security & Compliance admin center
- ☐ Microsoft Azure Security Center

Question 27

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?

- ☐ Configure 20 system exclusions on automation allowed/block lists
- ☐ Configure two alert notification rules
- ☐ Download an offboarding package for the computers of the 20 executives
- ☐ Create two machine groups

Question 28

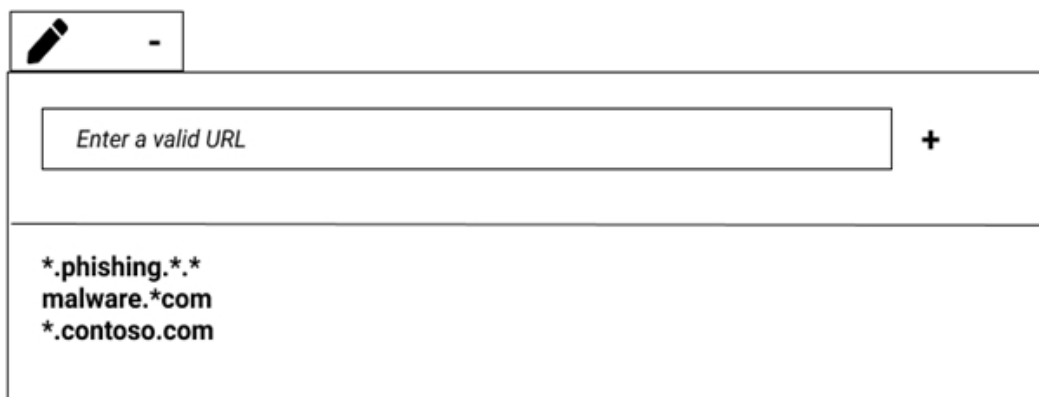
You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com.

You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
Block the following URLs:



Enter a valid URL +

- *.phishing.*
- malware.*com
- *.contoso.com

Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 365 ProPlus, Office for iOS and Android
 - ☒ Office Online of above applications
- For the locations selected above:
 - ☒ Do not track when users click safe links:
 - ☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- ☐ fabrikam.phishing.fabrikam.com
- ☐ malware.fabrikam.com
- ☐ fabrikam.contoso.com
- ☐ www.malware.fabrikam.com

Question 29

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?

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

Question 30

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.

Locations

ATP quarantine

The Junk Email folder of a user's mailbox

The Chutter folder a user's mailbox

Answer Area

Messages that contain word-filtered content:

Location

Messages that are classified as phishing:

Location

Implement and manage information protection

(8 questions)

Question 31

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?

- ☐ an app permission policy
- ☐ an activity policy
- ☐ a Cloud Discovery anomaly detection policy
- ☐ a session policy

Question 32

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?

- ☐ Yes
- ☐ No

Question 33

You create a data loss prevention (DLP) policy as shown in the following shown:

New DLP policy

What do you want to do if we detect sensitive info?

We'll automatically create activity reports so you can review the content that matches this policy. What else do you want to do?
Notify users when content matches the policy settings

☒ Show policy tips to users and send them an email notification.
Tips appear to users in their apps (like Outlook, and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)

Detect when a specific amount of sensitive info is being shared at one time.

☒ Detect when content that's being shared contains:
At least instances of the same sensitive info type.

☒ Send incident reports in email
By default, you and your global admin will automatically receive the email.
[Choose what to include in the report and who receives it](#)

☐ Restrict access or encrypt the content

[Back](#) [Next](#) [Cancel](#)

What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

- ☐ The user receives a notification and can send the email message
- ☐ The user receives a notification and cannot send the email message
- ☐ The email message is sent without a notification
- ☐ The email message is blocked silently

Question 34

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.

Answer Area

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

Users and groups, Cloud apps, and Session settings	V
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	V
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

Question 35

You have a Microsoft 365 subscription for a company named Contoso, Ltd. All data is in Microsoft 365.

Contoso works with a partner company named Litware, Inc. Litware has a Microsoft 365 subscription.

You need to allow users at Contoso to share files from Microsoft OneDrive to specific users at Litware.

Which two actions should you perform from the OneDrive admin center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Increase the permission level for OneDrive External sharing
- ☐ Modify the Links settings
- ☐ Change the permissions for OneDrive External sharing to the least permissive level
- ☐ Decrease the permission level for OneDrive External sharing
- ☐ Modify the Device access settings
- ☐ Modify the Sync settings

Question 36

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 syncing files.

What should you do?

- ☐ Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
- ☐ From the SharePoint admin center, configure the Access control settings
- ☐ From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- ☐ From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Question 37

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?

- ☐ Records Center
- ☐ Compliance Policy Center
- ☐ eDiscovery Center
- ☐ Enterprise Search Center
- ☐ Document Center

Question 38

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?

- ☐ Yes
- ☐ No

Manage governance and compliance features in Microsoft 365

Case Study (1 questions)

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

Question 39

What should User6 use to meet the technical requirements?

- ☐ Supervision in the Security & Compliance admin center
- ☐ Service requests in the Microsoft 365 admin center
- ☐ Security & privacy in the Microsoft 365 admin center
- ☐ Data subject requests in the Security & Compliance admin center

(19 questions)

Question 40

You have a Microsoft 365 subscription.

You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection.

From the Security & Compliance admin center, you create a label that designates personal data.

You need to auto-apply the new label to all the content in Site1.

What should you do first?

- ☐ From PowerShell, run Set-ManagedContentSettings.
- ☐ From PowerShell, run Set-ComplianceTag.
- ☐ From the Security & Compliance admin center, create a Data Subject Request (DSR).
- ☐ Remove Azure Information Protection from the Site1 files.

Question 41

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?

- ☐ From the Azure Active Directory admin center, open the audit log
- ☐ From the OneDrive admin center, select Device access
- ☐ From Security & Compliance, perform an eDiscovery search
- ☐ From Microsoft Cloud App Security, open the activity log

Question 42

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 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 assigning the Compliance Manager Reader role to User5.

Does that meet the goal?

- ☐ Yes
- ☐ No

Question 43

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?

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

Question 44

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 device configuration profile that has device restrictions configured
- ☐ a device configuration profile that has the Endpoint Protection settings configured
- ☐ a device configuration policy that has the System Security settings configured
- ☐ a device compliance policy that has the Device Health settings configured

Question 45

You have a Microsoft 365 subscription.

You create and run a content search from the Security & Compliance admin center.

You need to download the results of the content search.

What should you obtain first?

- ☐ an export key
- ☐ a password
- ☐ a certificate
- ☐ a pin

Question 46

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?

- ☐ From Search & investigation, select Content search
- ☐ From Data governance, select Events
- ☐ From Search & investigation, select eDiscovery
- ☐ From Reports, select Dashboard

Question 47

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?

- ☐ From Search & investigation, create a guided search.
- ☐ From Events, create an event.
- ☐ From Alerts, create an alert policy.
- ☐ From Search & investigation, create an eDiscovery case.

Question 48

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?

- ☐ Modify the priority order of label policies
- ☐ Wait six hours and ask the users to try again
- ☐ Create a label policy
- ☐ Create a new sensitive information type

Question 49

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E5 license.

How long will auditing data be retained?

- ☐ 30 days
- ☐ 90 days
- ☐ 365 days
- ☐ 5 years

Question 50

You have a Microsoft 365 subscription that includes a user named Admin1.

You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.

The solution must use the principle of least privilege.

What should you do?

- ☐ From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
- ☐ From the Exchange admin center, assign the Discovery Management admin role to Admin1.
- ☐ From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
- ☐ From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Question 51

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 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 assigning the Compliance Manager Reader role to User1.

Does that meet the goal?

- ☐ Yes
- ☐ No

Question 52

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?

- ☐ Yes
- ☐ No

Question 53

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?

- ☐ Yes
- ☐ No

Question 54

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.

- ☐ From the Cloud App Security admin center, create a file policy.
- ☐ From the SharePoint admin center, modify the Site Settings.
- ☐ From the SharePoint & Compliance admin center, create a label.
- ☐ From the SharePoint admin center, modify the records management settings.
- ☐ From the Security & Compliance admin center, publish a label.

Question 55

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-Mailbox -Identity "User1" -AuditEnabled \$true command.

Does that meet the goal?

- ☐ Yes
- ☐ No

Question 56

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?

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

Question 57

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?

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

Question 58

Your company has a Microsoft 365 subscription that includes a user named User1.

You suspect that User1 sent email messages to a competitor detailing company secrets.

You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.

What should you include in the recommendation?

- ☐ Enable In-Place Archiving for the mailbox of User1
- ☐ From the Security & Compliance, perform a content search of the mailbox of User1
- ☐ Place a Litigation Hold on the mailbox of User1
- ☐ Configure message delivery restrictions for the mailbox of User1