vce trainer



Reference Solution for MS-101.86q

MS-101

MS-101

Microsoft 365 Mobility and Security

Score: 800/1000

Version:

Licensed to Berend Post berend.post@it-university.nl

Time Limit: 120 Minutes

Licensed to Berend Post berend.post@it-university.nl

Implement modern device services

(24 questions)

Question 1

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.

What should you configure?

- ☐ Enrollment restrictions from the Device Management admin center
- ☐ device enrollment managers from the Device Management admin center
- ☐ MAM User scope from the Azure Active Directory admin center
- ☒ MDM User scope from the Azure Active Directory admin center

Explanation:

References:

https://docs.microsoft.com/en-us/intune/windows-enroll

Question 2

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☐ Deploy applications to Windows 10 devices.
- ☒ Deploy VPN profiles to iOS devices.
- ☐ Deploy VPN profiles to Windows 10 devices.
- ☒ Publish applications to Android devices.

Explanation:

References:

https://docs.microsoft.com/en-us/sccm/comanage/overview

https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles

Licensed to Berend Post berend.post@it-university.nl

Question 3

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com and a Microsoft 365 subscription.

The company recently hired four new users who have the devices shown in the following table.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

You configure the Microsoft 365 subscription to ensure that the new devices enroll in Microsoft Intune automatically.

Which users have a device that can enroll in Microsoft Intune automatically?

- ☐ User1, User2, User3, and User4
- ☒ User2 only
- ☐ User1 and User2 only
- ☐ User1, User2, and User3 only

Question 4

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do from the Security & Compliance admin center?

- ☐ Create a data loss prevention (DLP) policy that has a Content is shared condition.
- ☐ Modify the default safe links policy.
- ☐ Create a data loss prevention (DLP) policy that has a Content contains condition.
- ☒ Create a new safe links policy.

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients

Licensed to Berend Post berend.post@it-university.nl

Question 5

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices.

You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices.

You need to recommend a Windows 10 deployment method.

What should you recommend?

- ☐ a provisioning package
- ☒ an in-place upgrade
- ☐ wipe and load refresh
- ☐ Windows Autopilot

Explanation:

References:

https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure

Licensed to Berend Post berend.post@it-university.nl

Question 6

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 7

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices.

Your company uses the following types of devices:
Windows 10
Windows 8.1
Android
iOS

Which devices can be managed by using co-management?

- ☐ Windows 10 and Windows 8.1 only
- ☐ Windows 10, Android, and iOS only
- ☐ Windows 10 only
- ☒ Windows 10, Windows 8.1, Android, and iOS

Explanation:

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

Question 8

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users.

What should you use?

- ☒ Windows Autopilot
- ☐ Windows Update
- ☐ Subscription Activation
- ☐ an in-place upgrade

Explanation:

References:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

Question 9

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.

You need to create Microsoft Intune device configuration profiles to meet the following requirements:

Configure Wi-Fi connectivity to a secured network named ContosoNet.
Require passwords of at least six characters to lock the devices.

What is the minimum number of device configuration profiles that you should create?

- ☐ 4
- ☒ 2
- ☐ 1

Licensed to Berend Post berend.post@it-university.nl

Question 10

You have a Microsoft 365 tenant.

You have a line-of-business application named App1 that users access by using the My Apps portal.

After some recent security breaches, you implement a conditional access policy for App1 that uses Conditional Access App Control.

You need to be alerted by email if impossible travel is detected for a user of App1. The solution must ensure that alerts are generated for App1 only.

What should you do?

- ☒ From Microsoft Cloud App Security, create a Cloud Discovery anomaly detection policy.
- ☐ From Microsoft Cloud App Security, modify the impossible travel alert policy.
- ☐ From Microsoft Cloud App Security, create an app discovery policy.
- ☐ From the Azure Active Directory admin center, modify the conditional access policy.

Explanation:

References:

https://docs.microsoft.com/en-us/cloud-app-security/cloud-discovery-anomaly-detection-policy

Licensed to Berend Post berend.post@it-university.nl

Question 11

Your company has 10 offices.

The network contains an Active Directory domain named contoso.com. The domain contains 500 client computers. Each office is configured as a separate subnet.

You discover that one of the offices has the following:

Computers that have several preinstalled applications
Computers that use nonstandard computer names
Computers that have Windows 10 preinstalled
Computers that are in a workgroup

You must configure the computers to meet the following corporate requirements:

All the computers must be joined to the domain.
All the computers must have computer names that use a prefix of CONTOSO.
All the computers must only have approved corporate applications installed.

You need to recommend a solution to redeploy the computers. The solution must minimize the deployment time.

What should you recommend?

- ☒ a provisioning package
- ☐ wipe and load refresh
- ☐ Windows Autopilot
- ☐ an in-place upgrade

Explanation:

Explanation:

By using a Provisioning, IT administrators can create a self-contained package that contains all of the configuration, settings, and apps that need to be applied to a device.

Incorrect Answers:

C: With Windows Autopilot the user can set up pre-configure devices without the need consult their IT administrator.

D: Use the In-Place Upgrade option when you want to keep all (or at least most) existing applications.

References:

https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot

Licensed to Berend Post berend.post@it-university.nl

Question 12

You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Select when Quality Updates are received
- ☒ Select when Preview Builds and Feature Updates are received
- ☐ Turn off auto-restart for updates during active hours
- ☒ Manage preview builds
- ☐ Automatic updates detection frequency

Explanation:

References:

https://insider.windows.com/en-us/for-business-organization-admin/

Question 13

You have Windows 10 Pro devices that are joined to an Active Directory domain.

You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise.

You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services.

What are two prerequisites of the deployment? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☐ computers that have biometric hardware features
- ☒ Microsoft Intune enrollment
- ☒ Microsoft Azure Active Directory (Azure AD)
- ☐ smartcards
- ☐ TPM-enabled devices

Explanation:

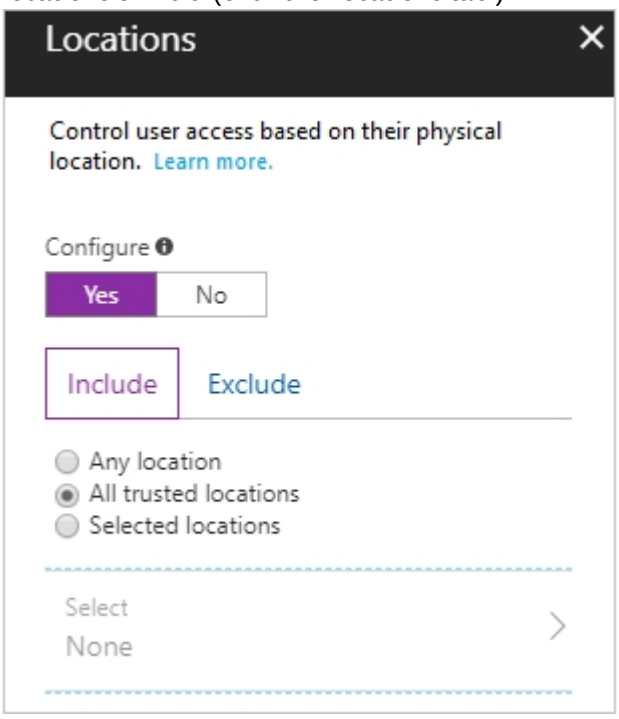
References:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-sso-base

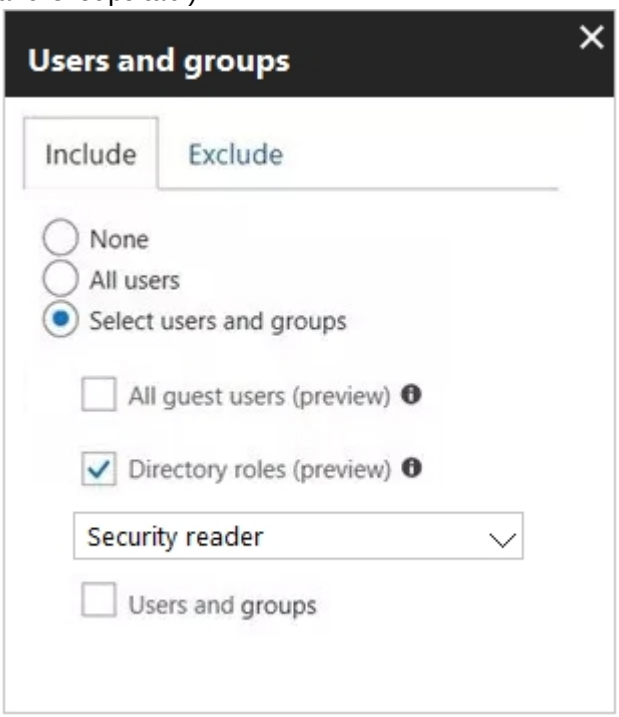
Licensed to Berend Post berend.post@it-university.nl

Question 14

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office.

Licensed to Berend Post berend.post@it-university.nl

You need to ensure that the members of the Security reader group can sign in in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege.

What should you do?

- ☐ From the conditional access policy, configure the device state.
- ☐ From the Azure Active Directory admin center, create a custom control.
- ☐ From the Device Management admin center, create a device compliance policy.
- ☒ From the Azure Active Directory admin center, create a named location.

Explanation:

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Question 15

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You create the Mobility (MDM and MAM) settings.

Does this meet the goal?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 16

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You unjoin Device1 from the Active Directory domain.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 17

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

You have a Microsoft 365 subscription.

You need to ensure that administrators can manage the configuration settings for all the Windows 10 devices in your organization.

What should you configure?

- ☐ the Enrollment restrictions
- ☒ the mobile device management (MDM) authority
- ☐ the Exchange on-premises access settings
- ☐ the Windows enrollment settings

Explanation:

References:

https://docs.microsoft.com/en-us/intune/mdm-authority-set

Licensed to Berend Post berend.post@it-university.nl

Question 18

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

References:

https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/

Licensed to Berend Post berend.post@it-university.nl

Question 19

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.

Your network contains an on-premises Active Directory domain. The domain contains 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the ReadyForWindows status of App2 to Highly adopted.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

Explanation:

App1 has a “low install count” (2% or less) so will be Ready to upgrade. We just need to change the setting for App2.

References:

https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps

Licensed to Berend Post berend.post@it-university.nl

Question 20

HOTSPOT

Your company has a Microsoft 365 tenant.

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

The device type restrictions are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

The device limit restrictions are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	Wet Region	5	Engineering
Default	All users	10	All users

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

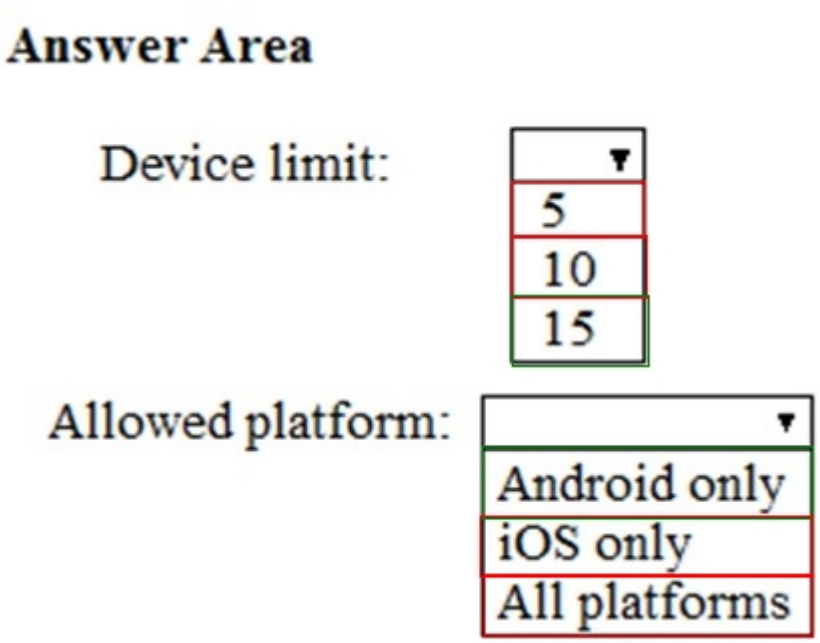
NOTE: Each correct selection is worth one point.

Answer Area

Device limit: [▼]
- 5
- 10
- 15

Allowed platform: [▼]
- Android only
- iOS only
- All platforms

Licensed to Berend Post berend.post@it-university.nl



Solution:

Question 21

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to a Configuration Manager device collection.

Does this meet the goal?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 22

HOTSPOT

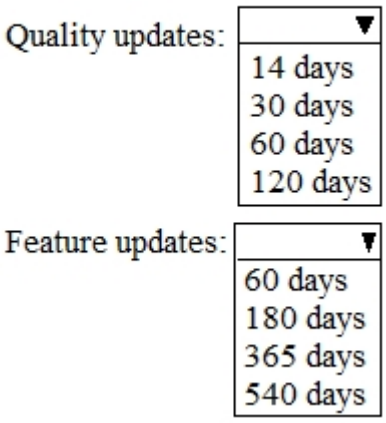
Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer Area



Solution:

Explanation:

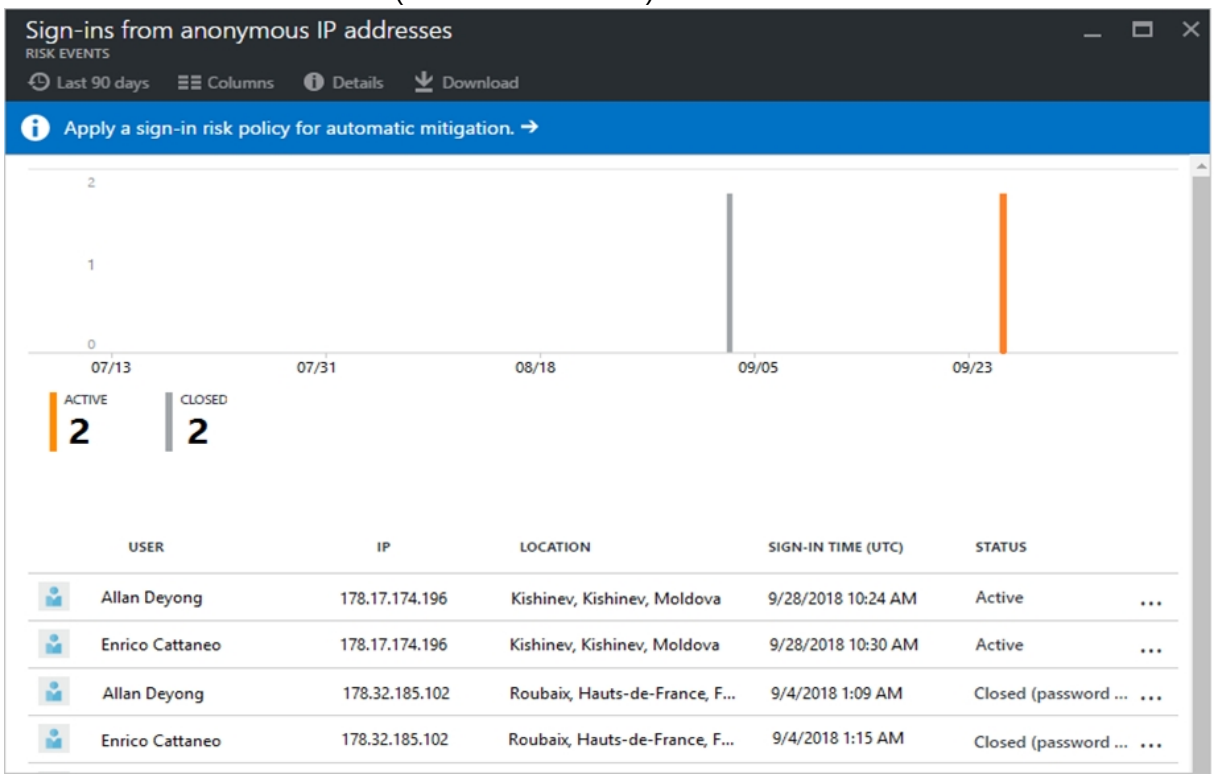
References:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb

Licensed to Berend Post berend.post@it-university.nl

Question 23

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified as risky.

What should you do?

- ☐ From the Security & Compliance admin center, create a classification label.
- ☐ From the Security & Compliance admin center, add the users to the Security Readers role group.
- ☐ From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- ☒ From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Explanation:

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Licensed to Berend Post berend.post@it-university.nl

Question 24

A user receives the following message when attempting to sign in to https://myapps.microsoft.com:

"Your sign-in was blocked. We've detected something unusual about this sign-in. For example, you might be signing in from a new location, device, or app. Before you can continue, we need to verify your identity. Please contact your admin."

Which configuration prevents the users from signing in?

- ☐ Microsoft Azure Active Directory (Azure AD) Identity Protection policies
- ☒ Microsoft Azure Active Directory (Azure AD) conditional access policies
- ☐ Security & Compliance supervision policies
- ☐ Security & Compliance data loss prevention (DLP) policies

Explanation:

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Licensed to Berend Post berend.post@it-university.nl

Case Study (2 questions)

Case Study
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company has the employees and devices shown in the following table.

Location	Employees	Laptops	Desktops	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 recently purchased a Microsoft 365 E5 subscription.

Existing Environment

The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain.

The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.

The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.

Licensed to Berend Post berend.post@it-university.nl

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.

Requirements
Planned Changes

Contoso plans to implement the following changes:

Implement Microsoft 365.
Manage devices by using Microsoft Intune.
Implement Azure Advanced Threat Protection (ATP).
Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements

Contoso identifies the following technical requirements:

When a Windows 10 device is joined to Azure AD, the device must enroll in Intune automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
User1 must be able to enroll all the New York office mobile devices in Intune.
Azure ATP sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.
Compliance Requirements

Contoso identifies the following compliance requirements:

Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices.

Question 25

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- ☐ 1
- ☒ 4

Licensed to Berend Post berend.post@it-university.nl

- ☐ 7
- ☐ 31

Explanation:

References:

https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

Question 26

You need to create the Microsoft Store for Business.

Which user can create the store?

- ☐ User2
- ☐ User3
- ☒ User4
- ☐ User5

Explanation:

References:

https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

Licensed to Berend Post berend.post@it-university.nl

Implement Microsoft 365 security and threat management

(24 questions)

Question 27

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription.

You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- ☐ Enable Microsoft Office 365 Cloud App Security.
- ☒ Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- ☐ Enable Microsoft Office 365 Analytics.

Question 28

Your network contains an on-premises Active Directory domain.

Your company has a security policy that prevents additional software from being installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the BEST answer.

- ☐ Deploy an Azure ATP sensor, and then configure port mirroring.
- ☐ Deploy an Azure ATP sensor, and then configure detections.
- ☐ Deploy an Azure ATP standalone sensor, and then configure detections.
- ☒ Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 29

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.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint admin center, you modify the sharing settings.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 30

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- ☐ From the Exchange admin center, create an in-place eDiscovery & hold.
- ☐ From the Security & Compliance admin center, create a data governance event.
- ☒ From the Exchange admin center, create an anti-malware policy.
- ☐ From the Exchange admin center, create a mail-flow rule.

Explanation:

Reference:

https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spam-and-anti-malware-protection

Licensed to Berend Post berend.post@it-university.nl

Question 31

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678A

Licensed to Berend Post berend.post@it-university.nl

Question 32

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

Licensed to Berend Post berend.post@it-university.nl

Question 33

You have a Microsoft 365 subscription.

Your company purchases a new financial application named App1.

From Cloud Discovery in Microsoft Cloud App Security, you view the Discovered apps page and discover that many applications have a low score because they are missing information about domain registration and consumer popularity.

You need to prevent the missing information from affecting the score.

What should you configure from the Cloud Discover settings?

- ☐ Organization details
- ☐ Default behavior
- ☐ Score metrics
- ☒ App tags

Explanation:

References:

https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries

Licensed to Berend Post berend.post@it-university.nl

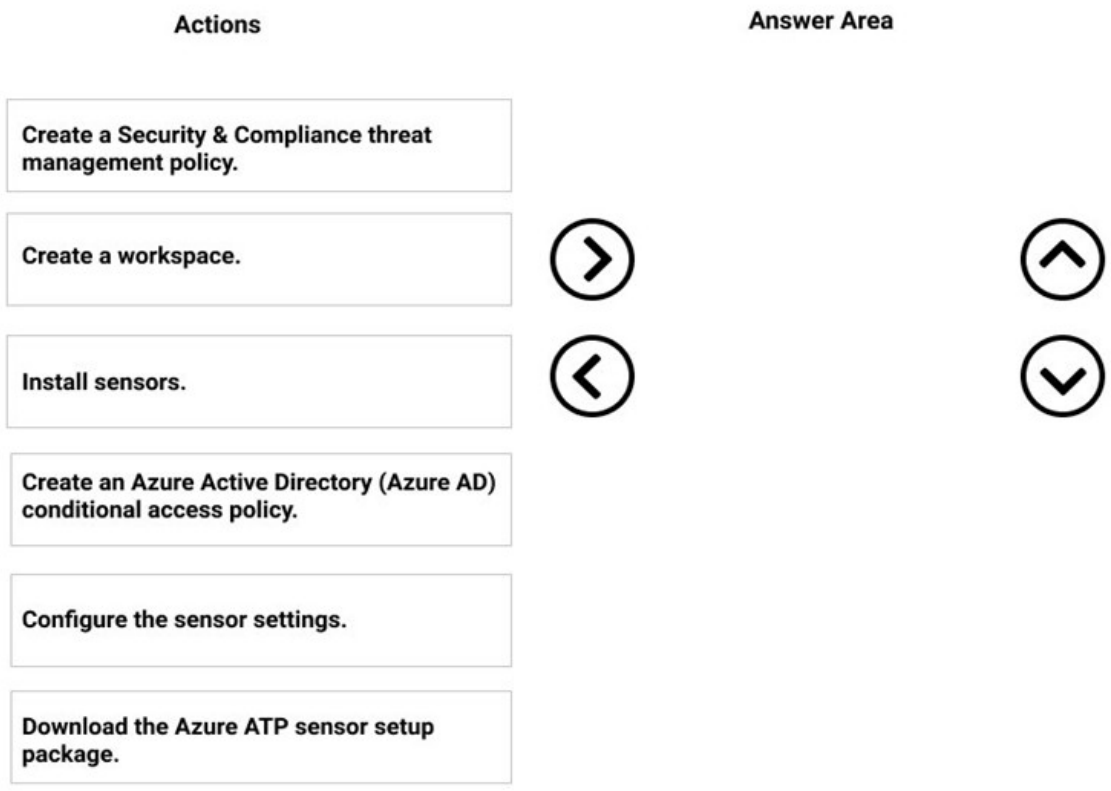
Question 34

DRAG DROP

You create a Microsoft 365 subscription.

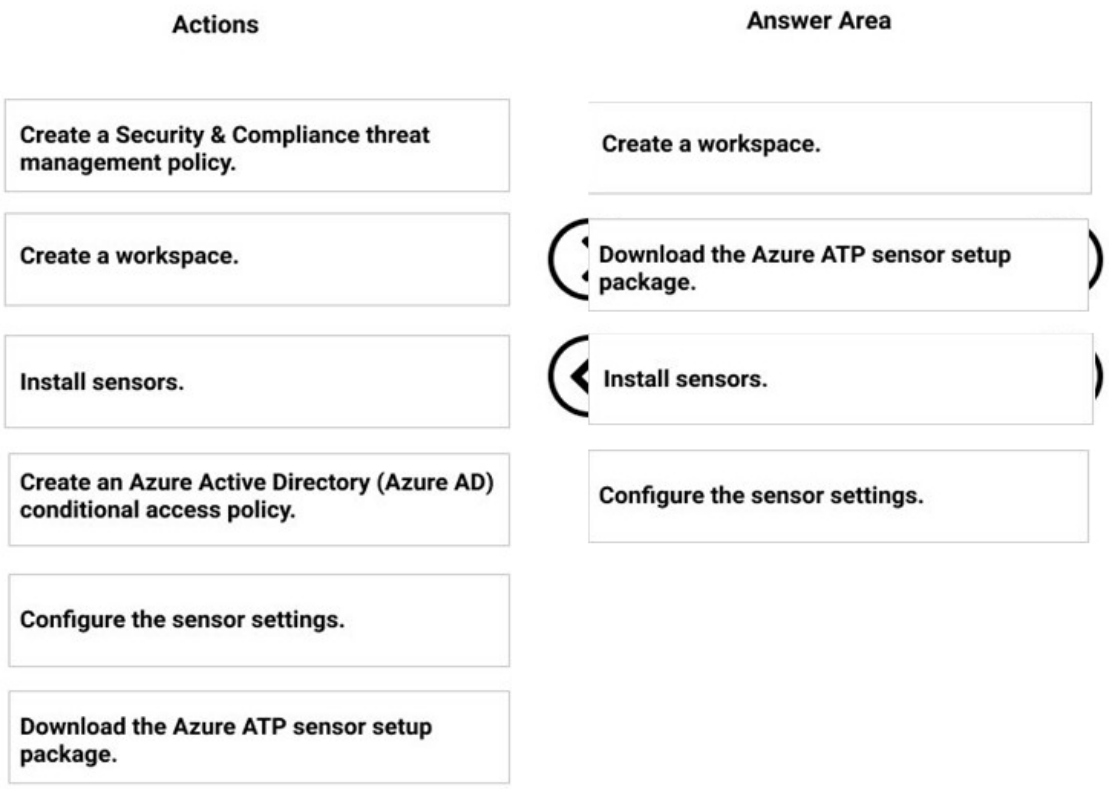
You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Licensed to Berend Post berend.post@it-university.nl

Solution:



Explanation:

References:

https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/

Licensed to Berend Post berend.post@it-university.nl

Question 35

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Security administrator role to User1.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

References:

https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

Question 36

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus.

What should you do?

- ☐ From the Exchange admin center, create an in-place eDiscovery & hold.
- ☐ From the Security & Compliance admin center, create a safe attachments policy.
- ☐ From the Security & Compliance admin center, create a data loss prevention (DLP) policy.
- ☒ From the Security & Compliance admin center, create an alert policy.

Explanation:

Reference:

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

Licensed to Berend Post berend.post@it-university.nl

Question 37

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.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 38

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a trusted location and a compliance policy

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

Licensed to Berend Post berend.post@it-university.nl

References:

https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678

Question 39

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

References:

https://docs.microsoft.com/en-us/cloud-app-security/manage-admins

Question 40

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender Advanced Threat Protection (ATP).

You need to create a filtered view that displays which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

- ☐ the threat intelligence API
- ☒ Automated investigations
- ☐ Threat analytics
- ☐ Advanced hunting

Explanation:

Licensed to Berend Post berend.post@it-university.nl

References:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alerts-windows-defender-advanced-threat-protection

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automated-investigations-windows-defender-advanced-threat-protection

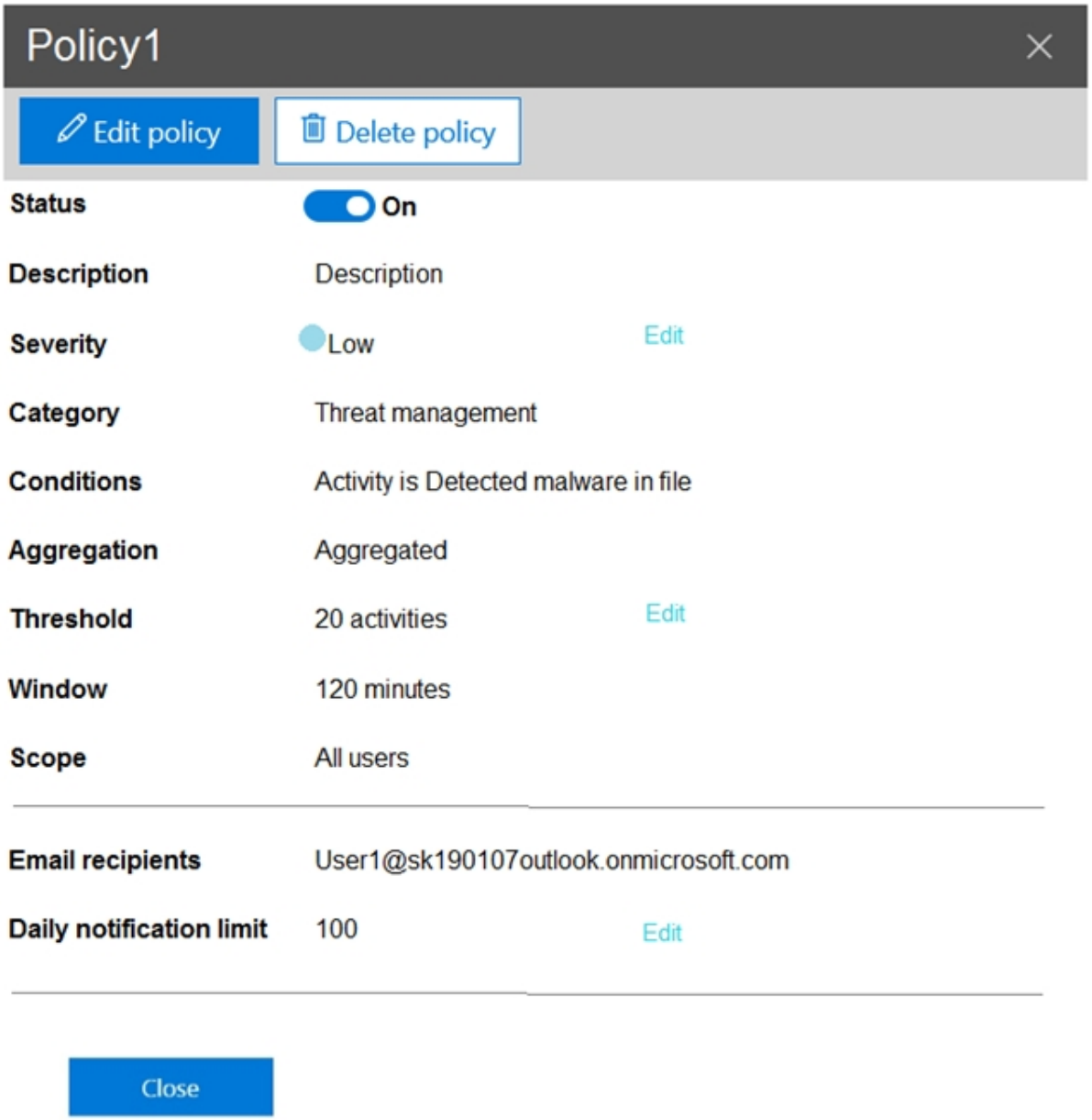
Licensed to Berend Post berend.post@it-university.nl

Question 41

HOTSPOT

You have Microsoft 365 subscription.

You create an alert policy as shown in the following exhibit.

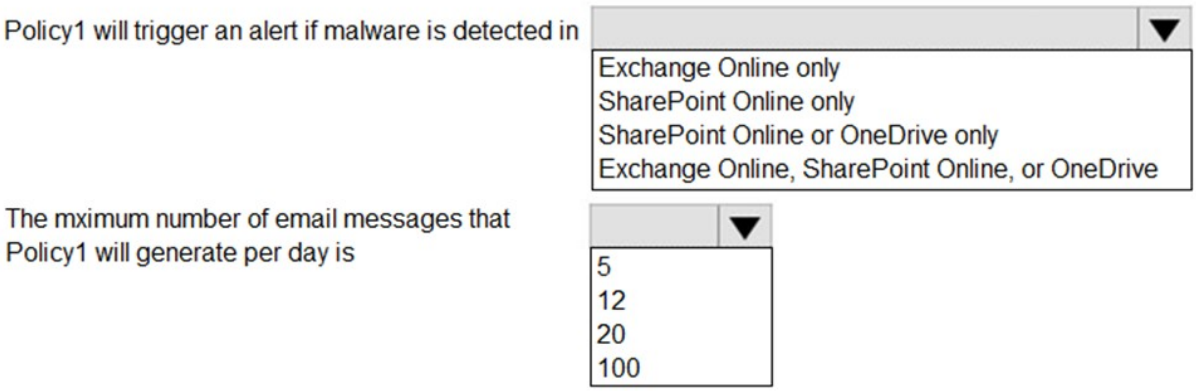


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

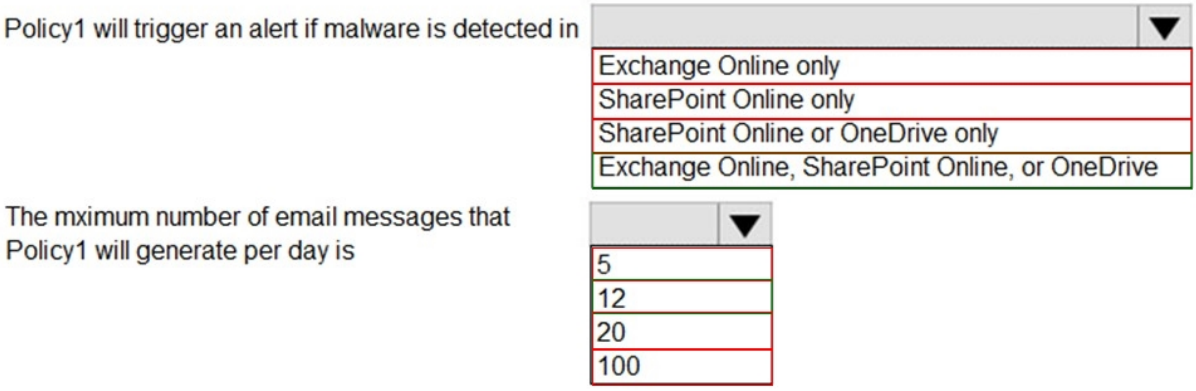
Licensed to Berend Post berend.post@it-university.nl

Answer Area



Solution:

Answer Area



Explanation:

Explanation:

Note: The Aggregation settings has a 120 minute window

Licensed to Berend Post berend.post@it-university.nl

Question 42

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices.

You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP-related data to be stored in the United States.

You plan to onboard all the devices to Windows Defender ATP.

You need to store the Windows Defender ATP data in Europe.

What should you first?

- ☐ Create a workspace.
- ☐ Onboard a new device.
- ☐ Delete the workspace.
- ☒ Offboard the test devices.

Question 43

You have a Microsoft Azure Active Directory (Azure AD) tenant.

The organization needs to sign up for Microsoft Store for Business. The solution must use the principle of least privilege.

Which role should you assign to the user?

- ☒ Global administrator
- ☐ Cloud application administrator
- ☐ Application administrator
- ☐ Service administrator

Explanation:

References:

https://docs.microsoft.com/en-us/microsoft-store/sign-up-microsoft-store-for-business

Licensed to Berend Post berend.post@it-university.nl

Question 44

The users at your company use Dropbox Business to store documents. The users access Dropbox Business by using the MyApps portal.

You need to ensure that user access to Dropbox Business is authenticated by using a Microsoft 365 identity. The documents must be protected if the data is downloaded to a device that is not trusted.

What should you do?

- ☐ From the Device Management admin center, configure conditional access settings.
- ☐ From the Azure Active Directory admin center, configure the device settings.
- ☒ From the Azure Active Directory admin center, configure the organizational relationships settings.
- ☐ From the Device Management admin center, configure Exchange on-premises access settings.

Question 45

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- ☒ From the Security & Compliance admin center, create a label and a label policy.
- ☐ From the Exchange admin center, create a mail flow rule.
- ☐ From the Security & Compliance admin center, start a message trace.
- ☐ From Exchange admin center, start a mail flow message trace.

Explanation:

References:

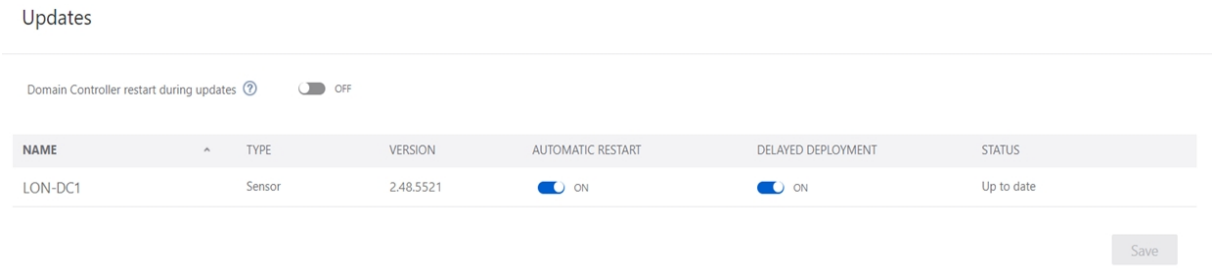
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

Licensed to Berend Post berend.post@it-university.nl

Question 46

You implement Microsoft Azure Advanced Threat Protection (Azure ATP).

You have an Azure ATP sensor configured as shown in the following exhibit.



How long after the Azure ATP cloud service is updated will the sensor update?

- ☐ 72 hours
- ☐ 12 hours
- ☐ 48 hours
- ☐ 7 days
- ☒ 24 hours

Explanation:

References:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-whats-new

Question 47

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.

You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the Security & Compliance admin center, you create a threat management policy.

Does this meet the goal?

- ☒ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

Question 48

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain.

You need to enable Windows Defender Credential Guard on all the computers.

What should you do?

- ☐ From the Security & Compliance admin center, configure the DKIM signatures for the domain.
- ☐ From a domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
- ☐ From the Security & Compliance admin center, create a device security policy.
- ☒ From a domain controller, create a Group Policy object (GPO) that enabled the Turn On Virtualization Based Security setting.

Explanation:

Reference:

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage

Question 49

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

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

- ☐ From Azure ATP, configure the notifications and reports.
- ☒ From Azure ATP, configure the data sources.
- ☐ From Windows Defender Security Center, configure the Machine management settings.
- ☐ From Windows Defender Security Center, configure the General settings.

Explanation:

References:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/integrate-wd-atp

Licensed to Berend Post berend.post@it-university.nl

Question 50

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a device configuration profile.

Does this meet the goal?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Manage Microsoft 365 governance and compliance

(33 questions)

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 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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Exchange admin center, you create a data loss prevention (DLP) policy.

Does this meet the goal?

- ☒ Yes
- ☐ No

Licensed to Berend Post berend.post@it-university.nl

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 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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User2 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 53

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the work ProjectX.

You need to export the results of the content search.

What do you need to download the report?

- ☐ a certification authority (CA) certificate
- ☒ an export key
- ☐ a password
- ☐ a user certificate

Explanation:

Licensed to Berend Post berend.post@it-university.nl

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results

Question 54

Your company has a Microsoft 365 subscription.

You need to identify which users performed the following privileged administration tasks:

Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
Opened a mailbox of which the user was not the owner
Reset a user password

What should you use?

- ☒ Microsoft Azure Activity Directory (Azure AD) audit logs
- ☐ Security & Compliance content search
- ☐ Microsoft Azure Activity Directory (Azure AD) sign-ins
- ☐ Security & Compliance audit log search

Explanation:

References:

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview

Licensed to Berend Post berend.post@it-university.nl

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 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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User3 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

Explanation:

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

Reference:

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups

Licensed to Berend Post berend.post@it-university.nl

Question 56

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint site.

What should you do?

- ☒ From the Security & Compliance admin center, create an alert policy.
- ☐ From the SharePoint site, create an alert.
- ☐ From the SharePoint admin center, modify the sharing settings.
- ☐ From the Security & Compliance admin center, create a data loss prevention (DLP) policy.

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

Question 57

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You sign for Microsoft Store for Business.

The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	*None*
User2	Basic Purchaser	*None*
User3	*None*	Application administrator
User4	*None*	Cloud application administrator

Microsoft Store for Business has the following Shopping behavior settings:

Allow users to shop is set to On
Make everyone a Basic Purchaser is set to Off

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

- ☐ User3 only
- ☐ User1 only
- ☒ User1 and User2 only
- ☐ User3 and User4 only

Explanation:

Explanation:

Licensed to Berend Post berend.post@it-university.nl

Allow users to shop controls the shopping experience in Microsoft Store for Education. When this setting is on, Purchasers and Basic Purchasers can purchase products and services from Microsoft Store for Education.

References:

https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business

Question 58

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 Azure Active Directory (Azure AD) tenant named contoso.com.

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User1 to modify the Azure ATP sensor configuration.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

Explanation:

Only Azure ATP administrators can modify the sensors.

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups

Question 59

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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 60

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Cloud App Security admin center, you create an access policy.

Does this meet the goal?

- ☐ Yes
- ☒ No

Licensed to Berend Post berend.post@it-university.nl

Question 61

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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-ComplianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- ☒ Yes
- ☐ No

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search

https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps

Question 62

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

What should you do?

- ☐ From the SharePoint Online admin center, view the usage reports.
- ☒ From the Security & Compliance admin center, perform an audit log search.
- ☐ From the Microsoft 365 admin center, view the usage reports.
- ☐ From the Microsoft 365 admin center, view the properties of the user's user account.

Explanation:

References:

Licensed to Berend Post berend.post@it-university.nl

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

Question 63

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do?

- ☒ From the Security & Compliance admin center, create an eDiscovery case.
- ☐ From the Exchange admin center, create a mail flow rule.
- ☐ From the Security & Compliance admin center, start a message trace.
- ☐ From Microsoft Cloud App Security, create an access policy.

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case

Question 64

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of a mailbox.

You need to view the content of the mail messages found by the search as quickly as possible.

What should you select from the Content search settings?

- ☐ Export report
- ☒ Export results
- ☐ Re-run
- ☐ View results

Explanation:

Explanation:

There is no 'View Results" option. You can preview results but that will only show up to 100 emails. To guarantee you're getting all results, you'll need to export them to a PST file.

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/microsoft-365/compliance/limits-for-content-search

Question 65

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 66

You have a Microsoft 365 subscription.

You configure a data loss prevention (DLP) policy.

You discover that users are incorrectly marking content as false positive and bypassing the DLP policy.

You need to prevent the users from bypassing the DLP policy.

What should you configure?

- ☐ incident reports
- ☐ actions
- ☐ exceptions
- ☒ user overrides

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 67

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

- ☐ Security Administrator
- ☒ Records Management
- ☐ Compliance Administrator
- ☐ eDiscovery Manager

Explanation:

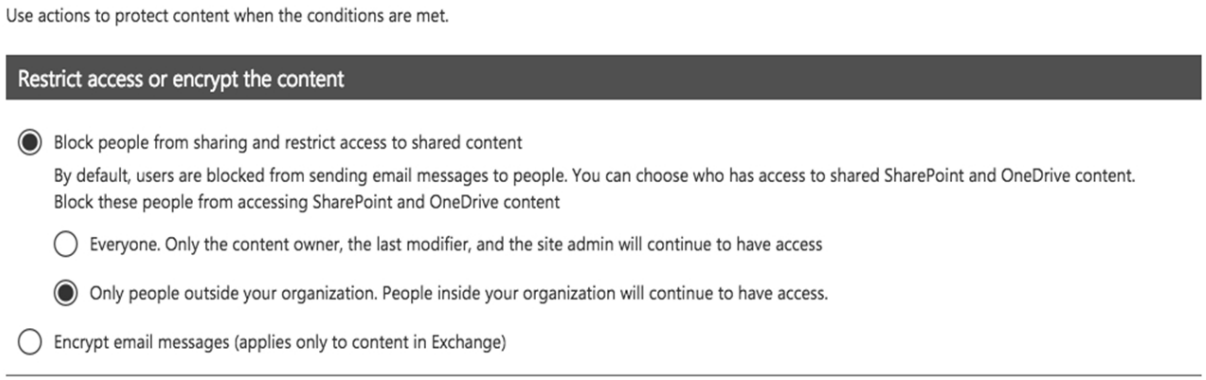
References:

https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager

Question 68

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the Exhibit tab.)



You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com.

What should you configure?

- ☐ an exception
- ☒ an action
- ☐ a condition
- ☐ a group

Explanation:

Licensed to Berend Post berend.post@it-university.nl

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work

Question 69

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

- ☐ From the SharePoint admin center, configure hybrid search.
- ☐ From the SharePoint admin center, create a managed property.
- ☐ From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.
- ☒ From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Explanation:

References:

https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps

Licensed to Berend Post berend.post@it-university.nl

Question 70

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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From the Azure Active Directory admin center, you create a conditional access policy.

Does this meet the goal?

- ☐ Yes
- ☒ No

Question 71

You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

- ☐ A conditional access policy.
- ☐ A compliance policy.
- ☒ An app protection policy.
- ☐ An app configuration policy.

Explanation:

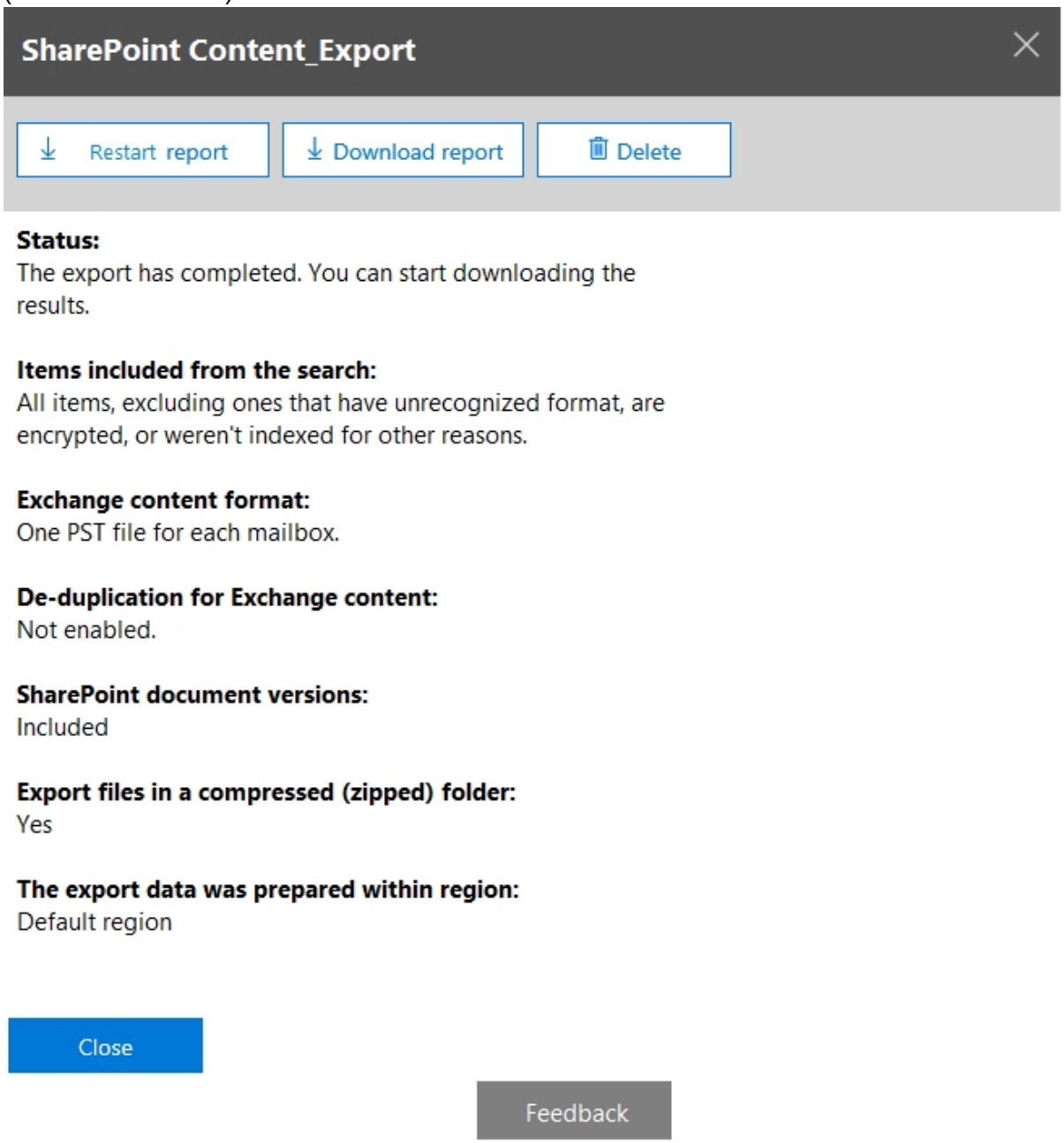
References:

https://docs.microsoft.com/en-us/intune/app-protection-policy

Licensed to Berend Post berend.post@it-university.nl

Question 72

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



What will be excluded from the export?

- ☐ a 60-MB DOCX file
- ☒ a 12-MB BMP file
- ☐ a 5-KB RTF file
- ☐ a 100-MB VSDX file

Explanation:

Explanation:

Unrecognized file formats are excluded from the search.

Licensed to Berend Post berend.post@it-university.nl

Incorrect Answers:

A: DOCX is a supported Microsoft PowerPoint file format.

C: RTF is a supported Rich Text File format.

D: VSDX is a supported Microsoft Visio file format.

Answer: B

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

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 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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- ☐ Yes
- ☒ No

Explanation:

References:

https://docs.microsoft.com/en-us/powershell/module/azurerm.resources/new-azurermroleassignment?view=azurermps-6.13.0

Licensed to Berend Post berend.post@it-university.nl

Question 74

You have a Microsoft 365 subscription.

You have a user named User1.

You need to ensure that User1 can place a hold on all mailbox content.

Which role should you assign to User1?

- ☒ eDiscovery Manager from the Security & Compliance admin center
- ☐ Compliance Management from the Exchange admin center
- ☐ User management administrator from the Microsoft 365 admin center
- ☐ Information Protection administrator from the Azure Active Directory admin center

Explanation:

References:

https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019

Licensed to Berend Post berend.post@it-university.nl

Question 75

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

Exempt apps: App2
Protected apps: App1
Windows Information Protection mode: Block
Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

You need to identify the apps from which you can open File1.abc.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can open File1.abc in App1.	○	○
You can open File1.abc in App2.	○	○
You can open File1.abc in App3.	○	○

Solution:

Answer Area

Statements	Yes	No
You can open File1.abc in App1.	○	○
You can open File1.abc in App2.	○	○
You can open File1.abc in App3.	○	○

Explanation:

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure

Question 76

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email. However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

- ☒ the locations of the DLP policy
- ☐ the user overrides of the DLP policy rule
- ☐ the status of the DLP policy
- ☐ the conditions of the DLP policy rule

Explanation:

References:

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

Question 77

You have a Microsoft 365 subscription.

All users are assigned a Microsoft 365 E3 license.

You enable auditing for your organization.

What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- ☐ 2 years
- ☐ 1 year
- ☐ 30 days
- ☒ 90 days

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 78

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users.

From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- ☒ An administrator creates a new Microsoft SharePoint site collection.
- ☒ An administrator creates a new mail flow rule.
- ☒ A user shares a Microsoft SharePoint folder with an external user.
- ☐ A user delegates permissions to their mailbox.
- ☐ A user purges messages from their mailbox.

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c

Question 79

You have a Microsoft 365 subscription.

You need to investigate user activity in Microsoft 365, including from where users signed in, which applications were used, and increases in activity during the past month. The solution must minimize administrative effort.

Which admin center should you use?

- ☐ Azure ATP
- ☒ Security & Compliance
- ☐ Cloud App Security
- ☐ Flow

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

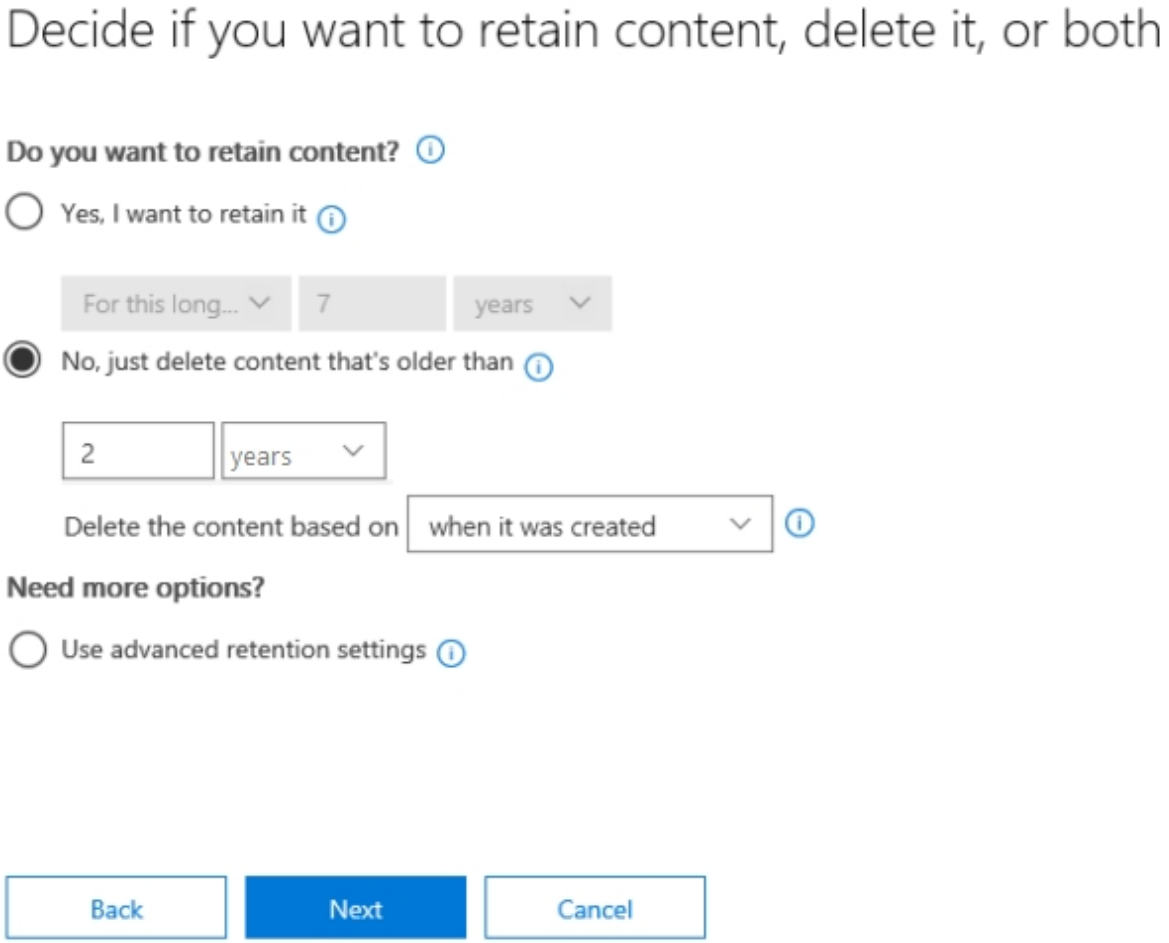
Question 80

HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

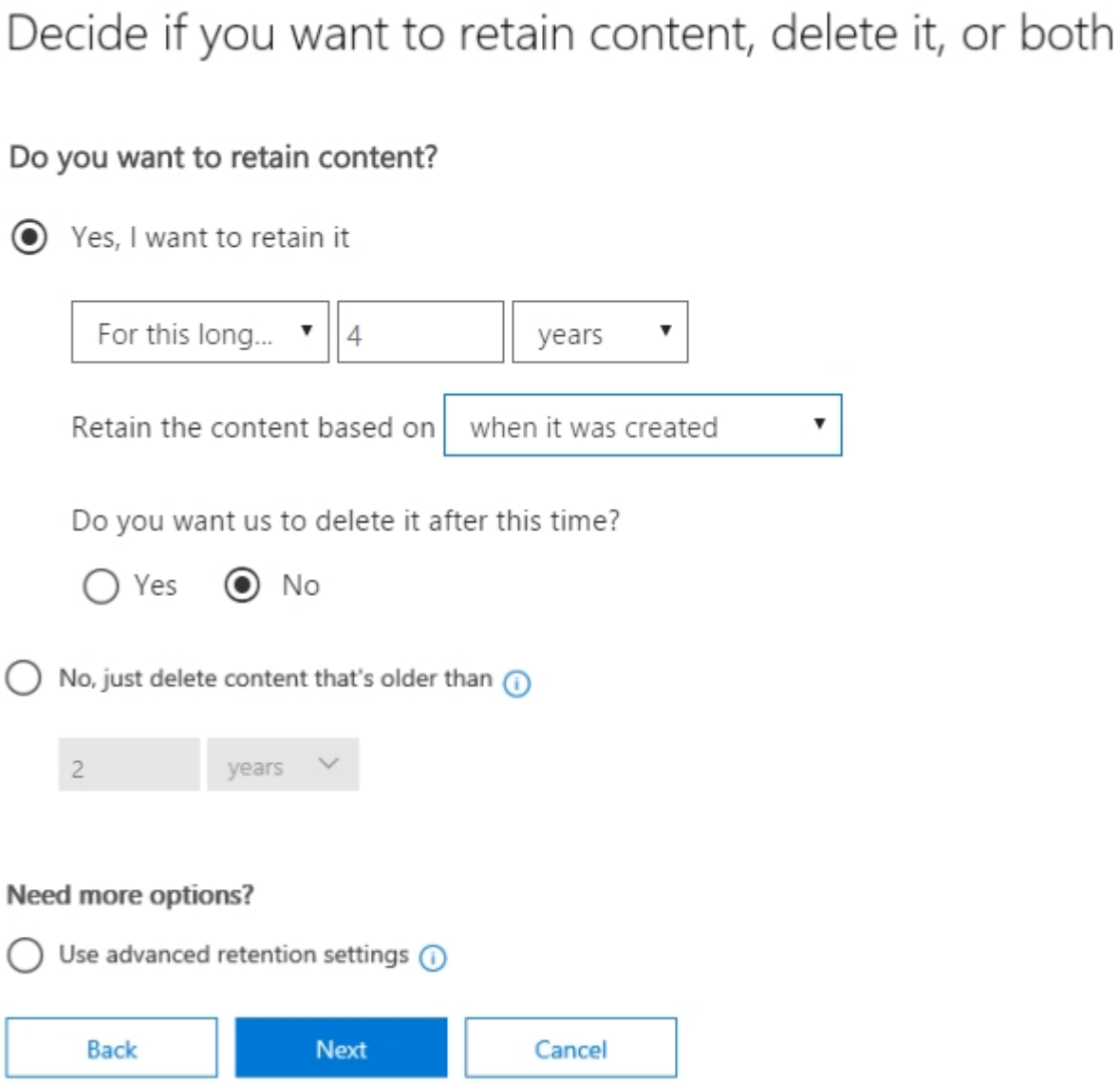
Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)



Policy2 is configured as shown in the Policy2 exhibit. (Click the Policy2 tab.)

Licensed to Berend Post berend.post@it-university.nl



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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Licensed to Berend Post berend.post@it-university.nl

Solution:

Answer Area

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	○	○
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	○	○

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence

Question 81

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS).

What should you do?

- ☐ From the Security & Compliance admin center, add SecAdmin1 to the eDiscovery Manager role group.
- ☐ From the Azure Active Directory admin center, add SecAdmin1 to the Security Reader role group.
- ☐ From the Security & Compliance admin center, add SecAdmin1 to the Compliance Administrator role group.
- ☒ From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Explanation:

Explanation:

The super user feature of the Azure Rights Management service from Azure Information Protection ensures that authorized people and services can always read and inspect the data that Azure Rights Management protects for your organization. However, the super user feature is not enabled by default. The PowerShell cmdlet Enable-AadrmSuperUserFeature is used to manually enable the super user feature.

References:

Licensed to Berend Post berend.post@it-university.nl

https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users

Question 82

HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1.

You need to prevent all users from disabling the policy or reducing the retention period.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

[▼] -Identity "Policy1" [▼] $true

Set-ComplianceTag	-enabled
Set-HoldCompliancePolicy	-Force
Set-RetentionCompliancePolicy	-RestrictiveRetention
Set-RetentionPolicy	-RetentionPolicyTagLinks
Set-RetentionPolicyTag	-SystemTag

Solution:

Answer Area

[▼] -Identity "Policy1" [▼] $true

Set-ComplianceTag	-enabled
Set-HoldCompliancePolicy	-Force
Set-RetentionCompliancePolicy	-RestrictiveRetention
Set-RetentionPolicy	-RetentionPolicyTagLinks
Set-RetentionPolicyTag	-SystemTag

Explanation:

References:

https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps

Licensed to Berend Post berend.post@it-university.nl

Question 83

You have a Microsoft 365 tenant.

You discover that administrative tasks are unavailable in the Microsoft Office 365 audit logs of the tenant.

You run the Get-AdminAuditLogConfig cmdlet and receive the following output:

```
RunspaceId                       : 4cb214a3-c11d-4dbf-a59a-3c055d01a576
AdminAuditLogEnabled             : True
LogLevel                         : Verbose
TestCmdletLoggingEnabled         : False
AdminAuditLogCmdlets             : {*}
AdminAuditLogParameters          : {*}
AdminAuditLogExcludedCmdlets     : {}
AdminAuditLogAgeLimit            : 90.00:00:00
LoadBalancerCount                : 3
RefreshInterval                  : 10
PartitionInfo                    : {}
UnifiedAuditLogIngestionEnabled  : False
UnifiedAuditLogFirstOptInDate    :
AdminDisplayName                 :
ExchangeVersion                  : 0.10 (14.0.100.0)
Name                             : Default
DistinguishedName                : CN=Default,CN=Configuration,CN=Contoso.onmicrosoft.com,OU=Microsoft Exchange
                                   Hosted Organizations,DC=FFO,DC=extest,DC=microsoft,DC=com
Identity                         : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration/Default
ObjectCategory                   :
ObjectClass                      : {msExchAdminAuditLogConfig}
WhenChanged                      :
WhenCreated                      :
WhenChangedUTC                   :
WhenCreatedUTC                   :
ExchangeObjectId                 : 08075a1f-b49e-4769-983d-be2587651f3b
OrganizationId                   : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com - FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration
Id                               : FFO.extest.microsoft.com/Microsoft Exchange Hosted
Organizations/Contoso.onmicrosoft.com/Configuration/Default
Guid                             : 08075a1f-b49e-4769-983d-be2587651f3b
OriginatingServer                :
IsValid                          : True
ObjectState                      : New
```

You need to ensure that administrative tasks are logged in the Office 365 audit logs.

Which attribute should you modify?

- ☐ TestCmdletLoggingEnabled
- ☒ UnifiedAuditLogIngestionEnabled
- ☐ AdminAuditLogEnabled

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Case Study (3 questions)

Case Study
Overview

ADatum Corporation is an international financial services company that has 5,000 employees.

ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.

All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment
Current Infrastructure

ADatum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.

Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.

ADatum uses and processes Personally Identifiable Information (PII).

Problem Statements

ADatum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Requirements

Business Goals

ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates.

ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

ADatum identifies the following technical requirements:

Licensed to Berend Post berend.post@it-university.nl

Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question 84

You need to protect the U.S. PII data to meet the technical requirements.

What should you create?

- ☐ a data loss prevention (DLP) policy that contains a domain exception
- ☐ a Security & Compliance retention policy that detects content containing sensitive data
- ☒ a Security & Compliance alert policy that contains an activity
- ☐ a data loss prevention (DLP) policy that contains a user override

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/create-activity-alerts

Question 85

Which report should the New York office auditors view?

- ☒ DLP incidents
- ☐ Top Senders and Recipients
- ☐ DLP false positives and overrides
- ☐ DLP policy matches

Explanation:

References:

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

Licensed to Berend Post berend.post@it-university.nl

Question 86

You need to meet the technical requirement for the EU PII data.

What should you create?

- ☐ a data loss prevention (DLP) policy from the Security & Compliance admin center
- ☐ a data loss prevention (DLP) policy from the Exchange admin center
- ☐ a retention policy from the Exchange admin center
- ☒ a retention policy from the Security & Compliance admin center

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies

Licensed to Berend Post berend.post@it-university.nl