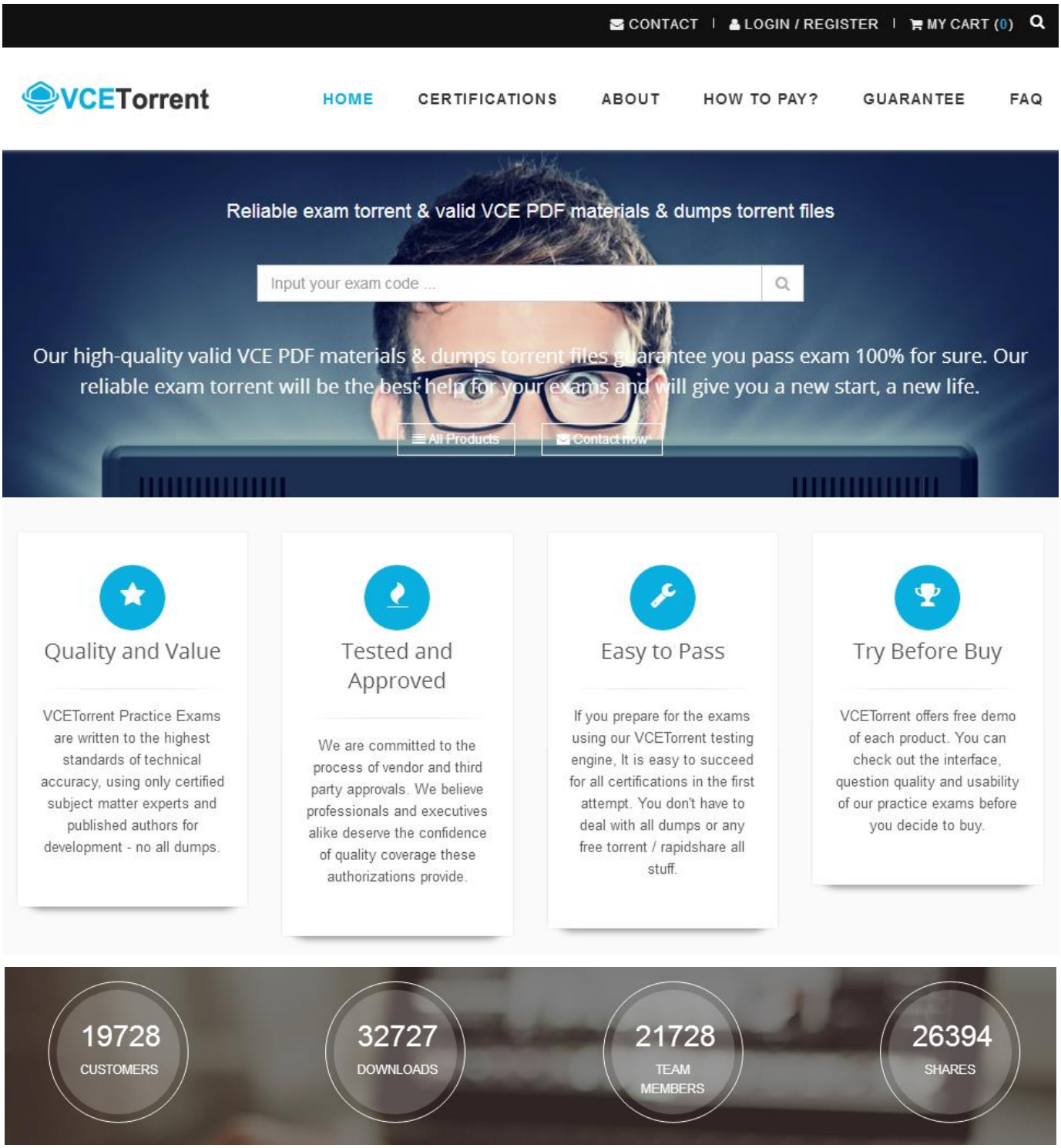
VCETorrent



http://www.vcetorrent.com

Reliable exam torrent & valid VCE PDF materials & dumps torrent files

Exam : **MS-101-Deutsch**

Title : Microsoft 365 Mobility and Security (MS-101 Deutsch Version)

Vendor : Microsoft

Version : DEMO

QUESTION NO: 1
Sie müssen die Anforderungen für die Rechtsabteilung erfüllen
Welche drei Aktionen sollten Sie im Security & Compliance Admin Center nacheinander ausführen? Verschieben Sie zum Beantworten die entsprechenden Aktionen aus der Liste der Aktionen in den Antwortbereich und ordnen Sie sie in der richtigen Reihenfolge an.

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:

Actions	Answer Area
Create a data loss prevention (DLP) policy.	Assign eDiscovery permissions.
Create an eDiscovery case.	Create an eDiscovery case.
Create a label.	Create a hold.
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Reference:
https://www.sherweb.com/blog/ediscovery-office-365/
Topic 1, Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review

your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
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.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
Problem Statements
Requirements
Business Goals
Technical Requirements
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 shows which Microsoft 36S 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 US. PII data to other New York office users. 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.

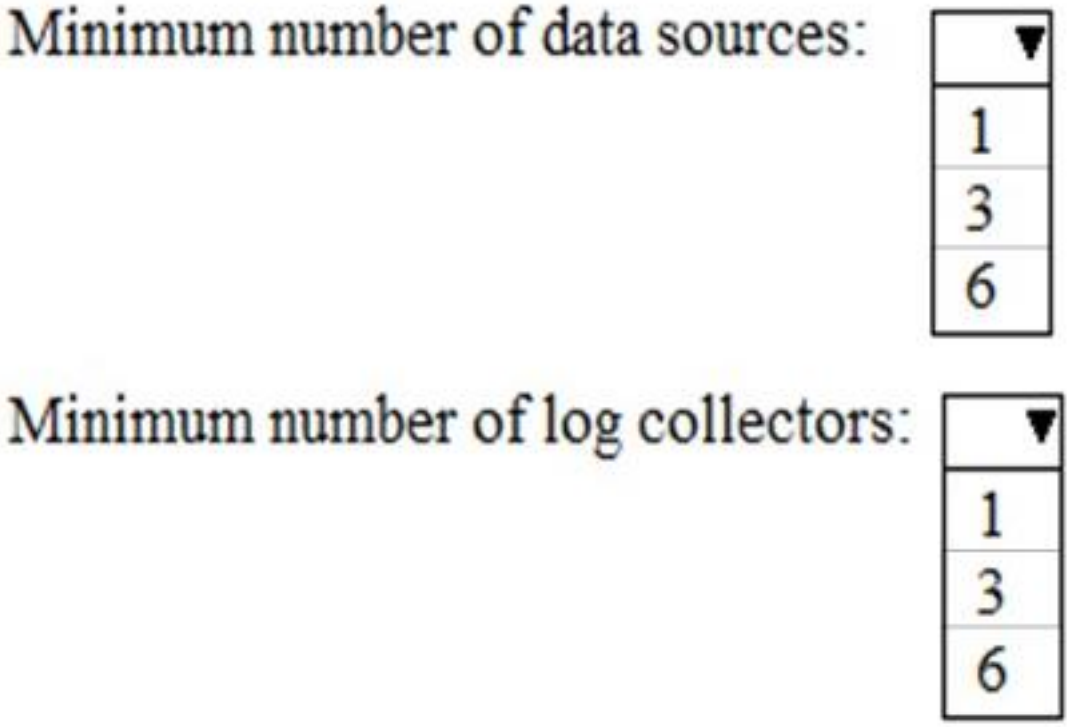
QUESTION NO: 2
Sie müssen dem Sicherheitsadministrator eine Lösung empfehlen. Die Lösung muss den technischen Anforderungen entsprechen.
Was sollten Sie in die Empfehlung aufnehmen?
A. Privilegierte Identitätsverwaltung für Microsoft Azure Active Directory (Azure AD)
B. Identitätsschutz für Microsoft Azure Active Directory (Azure AD)
C. Bedingte Zugriffsrichtlinien für Microsoft Azure Active Directory (Azure AD)
D. Authentifizierungsmethoden für Microsoft Azure Active Directory (Azure AD)

Answer: B
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#sign-in-risk states clearly that Sign-in risk

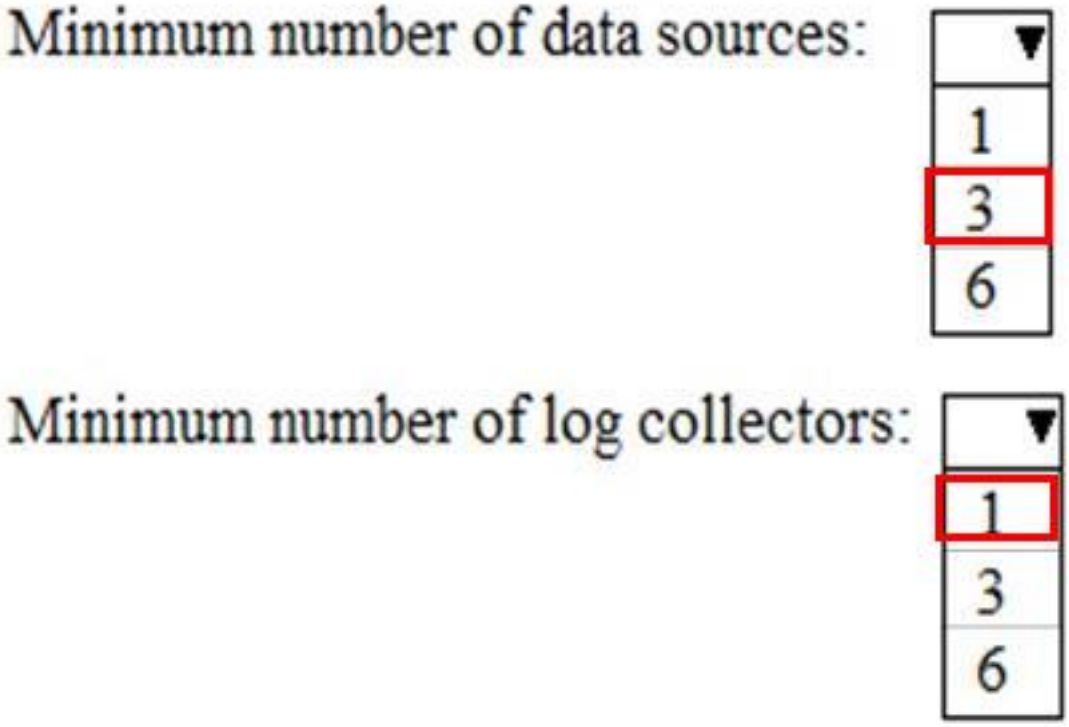
QUESTION NO: 3
Welchen Bericht sollten die New Yorker Wirtschaftsprüfer einsehen?
A. DLP-Richtlinienübereinstimmung
B. DLP-Fehlalarme und Überschreibungen
C. DLP-Vorfälle
D. Top Absender und Empfänger
Answer: C
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies
This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

QUESTION NO: 4
Sie müssen die technischen Voraussetzungen für das Abrufen großer Dokumente erfüllen.
Was solltest du erstellen?
A. Eine DLP-Richtlinie (Data Loss Prevention) aus dem Security & Compliance Admin Cente r
B. Eine Warnungsrichtlinie aus dem Security & Compliance Admin Center
C. Eine Dateirichtlinie von Microsoft Cloud App Security
D. Eine Aktivitätsrichtlinie von Microsoft Cloud App Security
Answer: D
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

QUESTION NO: 5
Sie müssen die technischen Voraussetzungen für die Protokollanalyse erfüllen.
Wie viele Datenquellen und Protokollsammler sollten mindestens mit Microsoft Cloud App Security erstellt werden? Wählen Sie zum Beantworten die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.



Answer:



Reference:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

QUESTION NO: 6
Sie müssen die technischen Anforderungen für die EU-PII-Daten erfüllen.
Was solltest du erstellen?

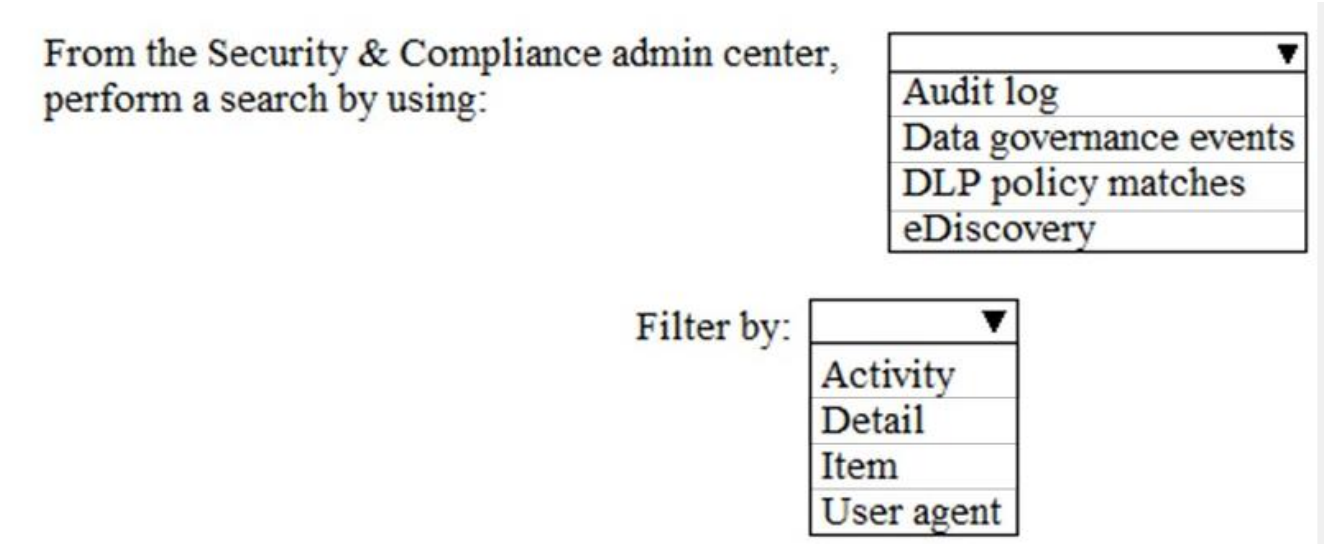
A. Eine Aufbewahrungsrichtlinie aus dem Security & Compliance Admin Center.

B. Eine Aufbewahrungsrichtlinie aus dem Exchange-Verwaltungscenter

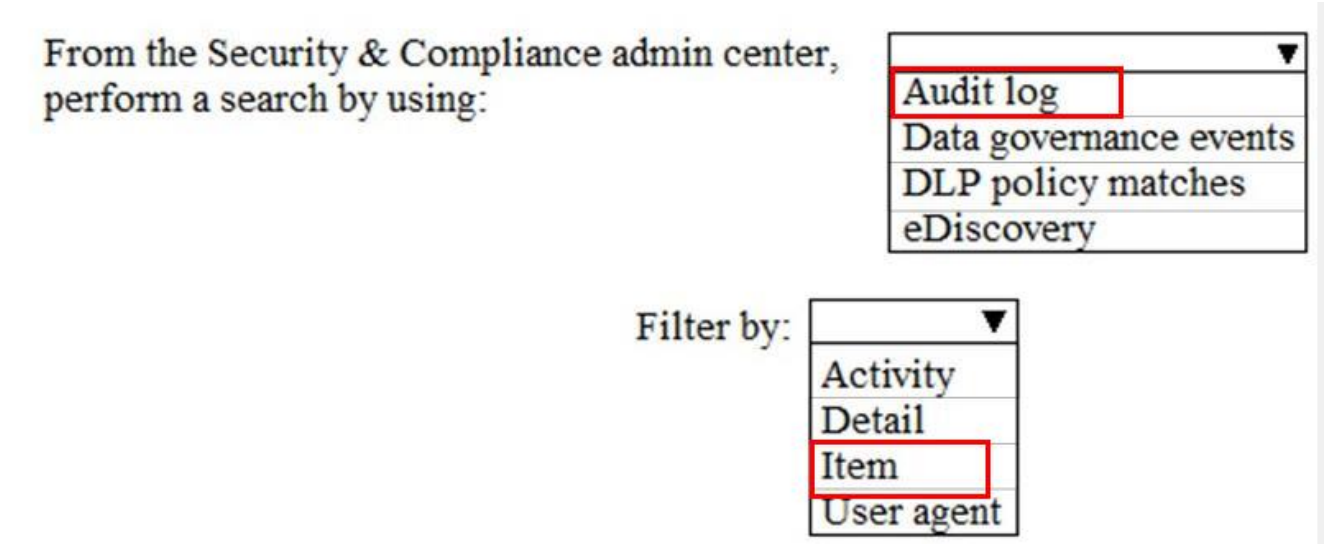
C. Eine DLP-Richtlinie (Data Loss Prevention) aus dem Exchange-Verwaltungscenter
D. Eine DLP-Richtlinie (Data Loss Prevention) aus dem Security & Compliance Admin Cente r
Answer: A
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

QUESTION NO: 7
Sie müssen die PII-Daten der USA schützen, um die technischen Anforderungen zu erfüllen. Was solltest du erstellen?
A. Eine DLP-Richtlinie (Data Loss Prevention), die eine Domänenausnahme enthält
B. Eine Sicherheits- und Compliance-Aufbewahrungsrichtlinie, die Inhalte mit vertraulichen Daten erkennt
C. Eine Sicherheits- und Compliance-Warnrichtlinie, die eine Aktivität enthält
D. Eine DLP-Richtlinie (Data Loss Prevention), die eine Benutzerüberschreibung enthält
Answer: A
Explanation:
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

QUESTION NO: 8
Sie müssen die technischen Anforderungen für den SharePoint-Administrator erfüllen. Was tun? Wählen Sie zum Beantworten die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.



Answer:



Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results

Topic 2, Contoso, Ltd

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 ES subscription.

Existing Environment

Requirement

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 are 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.

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.
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 automaticity.
* 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 (W1P) for the Windows 10 devices.

QUESTION NO: 9
Sie müssen die technischen Anforderungen und geplanten Änderungen für Intune erfüllen.
Was tun? Wählen Sie zum Beantworten die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.
Answer Area

Settings to configure in Azure AD:	Device settings Mobility (MDM and MAM) Organizational relationships User settings
Settings to configure in Intune:	Device compliance Device configuration Device enrollment Mobile Device Management Authority

Answer:
Answer Area

Settings to configure in Azure AD:	Device settings **Mobility (MDM and MAM)** Organizational relationships User settings
Settings to configure in Intune:	Device compliance Device configuration **Device enrollment** Mobile Device Management Authority

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

QUESTION NO: 10
Sie müssen sicherstellen, dass Benutzer1 die Geräte registrieren kann, um die technischen Anforderungen zu erfüllen. Was tun?
A. Weisen Sie im Azure Active Directory-Verwaltungscenter Benutzer1 den Cloud-Geräteadministrator zu.
B. Konfigurieren Sie im Azure Active Directory-Verwaltungscenter die Einstellung Maximale Anzahl von Geräten pro Benutzer.
C. Fügen Sie im Intune Admin Center Benutzer1 als Geräteregistrierungsmanager hinzu.
D. Konfigurieren Sie im Intune Admin Center die Registrierungsbeschränkungen.
Answer: C
Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 11
Sie müssen die Kompatibilitätsanforderungen für Windows 10-Geräte erfüllen.
Was sollten Sie im Intune Admin Center erstellen?
A. Richtlinien zur Gerätekonformität
B. Ein Gerätekonfigurationsprofil

C. eine Anwendungsrichtlinie
D. Eine App-Konfigurationsrichtlinie
Answer: C

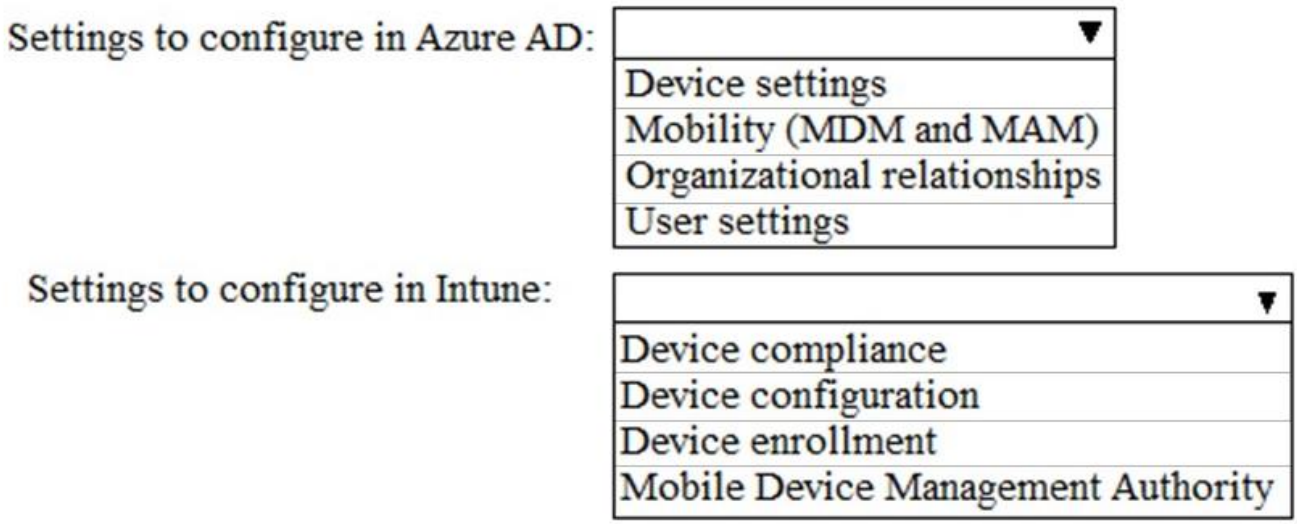
QUESTION NO: 12
Sie müssen den Microsoft Store for Business erstellen.
Welcher Benutzer kann den Shop erstellen?
A. User2
B. User3
C. User4
D. User5
Answer: C
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

QUESTION NO: 13
Ihr Unternehmen verfügt über ein Microsoft 365-Abonnement. Das Abonnement umfasst 500 Geräte mit Windows 10 und 100 Geräte mit iOS.
Sie müssen Microsoft Intune-Gerätekonfigurationsprofile erstellen, um die folgenden Anforderungen zu erfüllen:
* Konfigurieren Sie die Wi-Fi-Konnektivität zu einem gesicherten Netzwerk namens ContosoNet.
* Zum Sperren der Geräte sind Passwörter mit mindestens sechs Zeichen erforderlich.
Wie viele Gerätekonfigurationsprofile sollten Sie mindestens erstellen?
A. 2
B. 1
C. 4
Answer: A

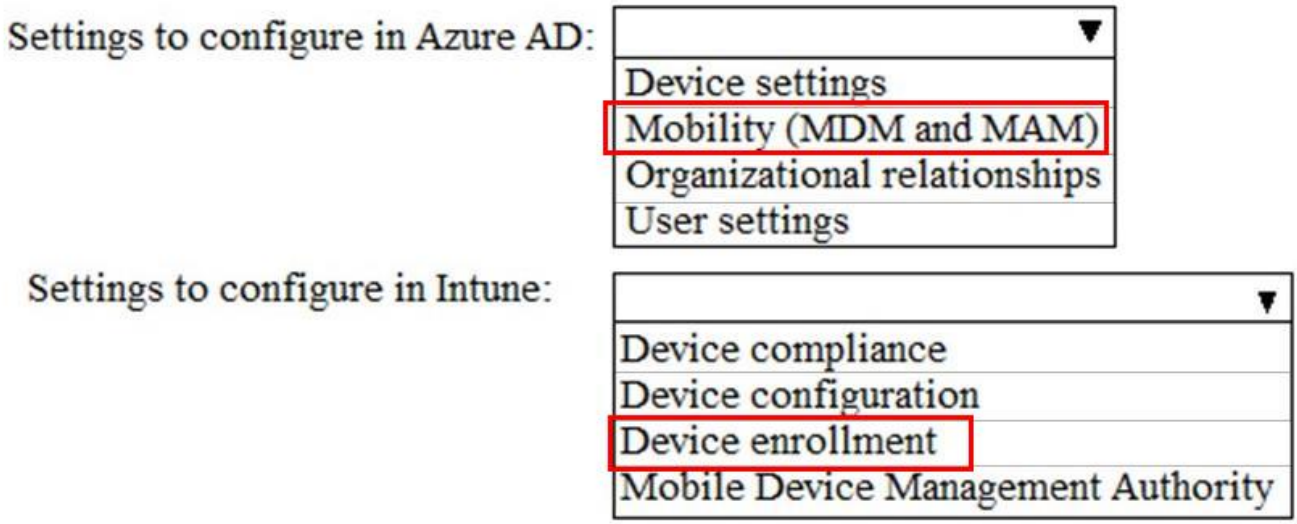
QUESTION NO: 14
Sie müssen sicherstellen, dass die Supporttechniker die technischen Anforderungen für die mobilen Bürogeräte in Montreal erfüllen können.
Was ist das Minimum an engagierten Support-Technikern?
A. 1
B. 4
C. 7
D. 31
Answer: B
Reference:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 15

Sie müssen die Intune-Anforderungen für Windows 10-Geräte erfüllen.
Was tun? Wählen Sie zum Beantworten die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.



Answer:



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

QUESTION NO: 16
Wie lange werden die Computer in den einzelnen Büros ab März von Microsoft unterstützt?
Um zu antworten, wählen Sie die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.


Seattle:
6 months
18 months
24 months
30 months
5 years
New York:
6 months
18 months
24 months
30 months
5 years

Answer:

Reference:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

QUESTION NO: 17
Auf welchem Server sollte der Azure ATP-Sensor installiert werden?
A. Server 1
B. Server 2
C. Server 3
D. Server 4
E. Server 5
Answer: A
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

QUESTION NO: 18

Auf welchem Server sollten Sie den Defender als Identitätssensor verwenden?

A. Server1

B. Server2

C. Server3

D. Server4

E. Server5

Answer: A

Explanation:

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

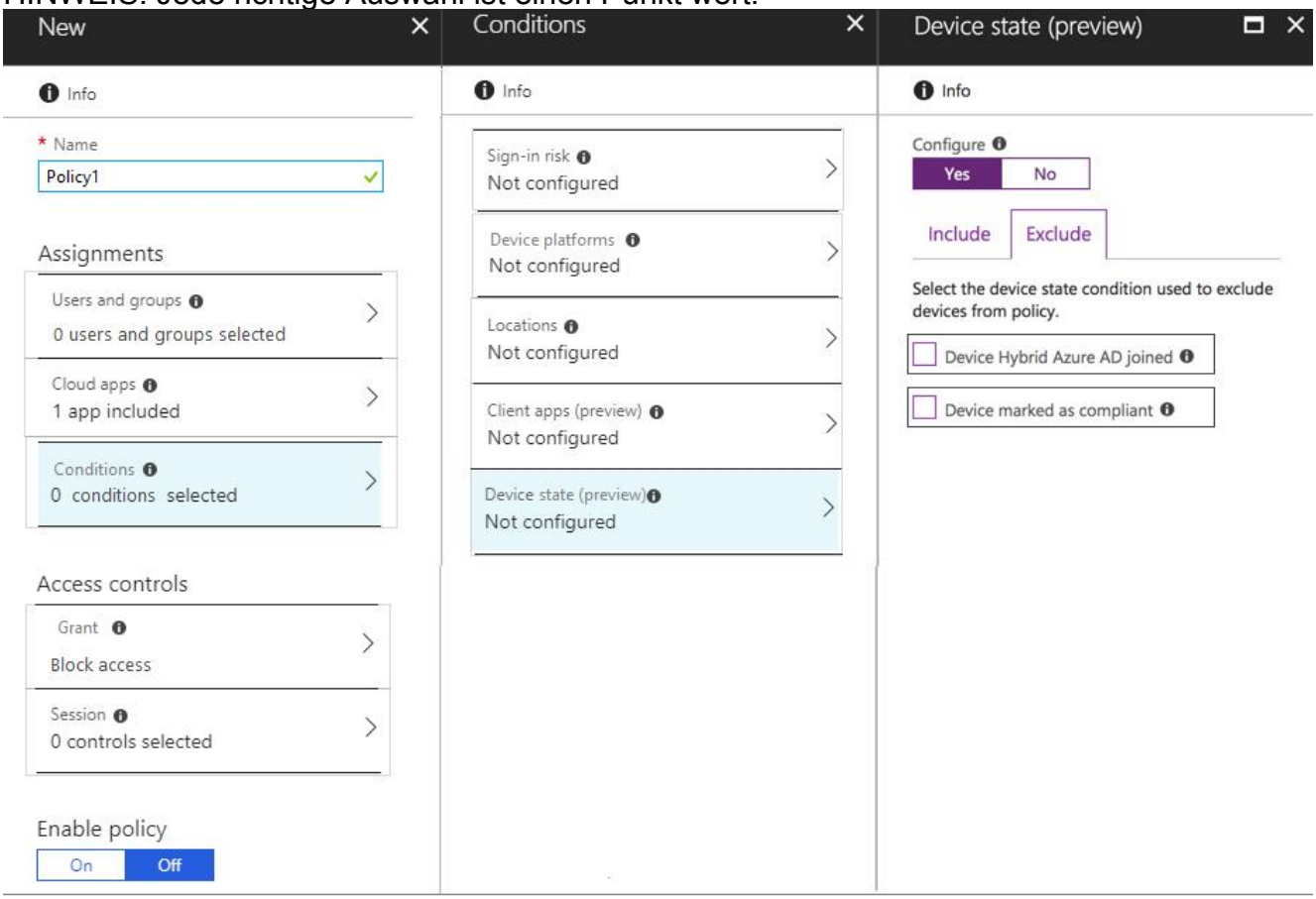
QUESTION NO: 19

Sie müssen eine Richtlinie für bedingten Zugriff konfigurieren, um die Compliance-Anforderungen zu erfüllen.

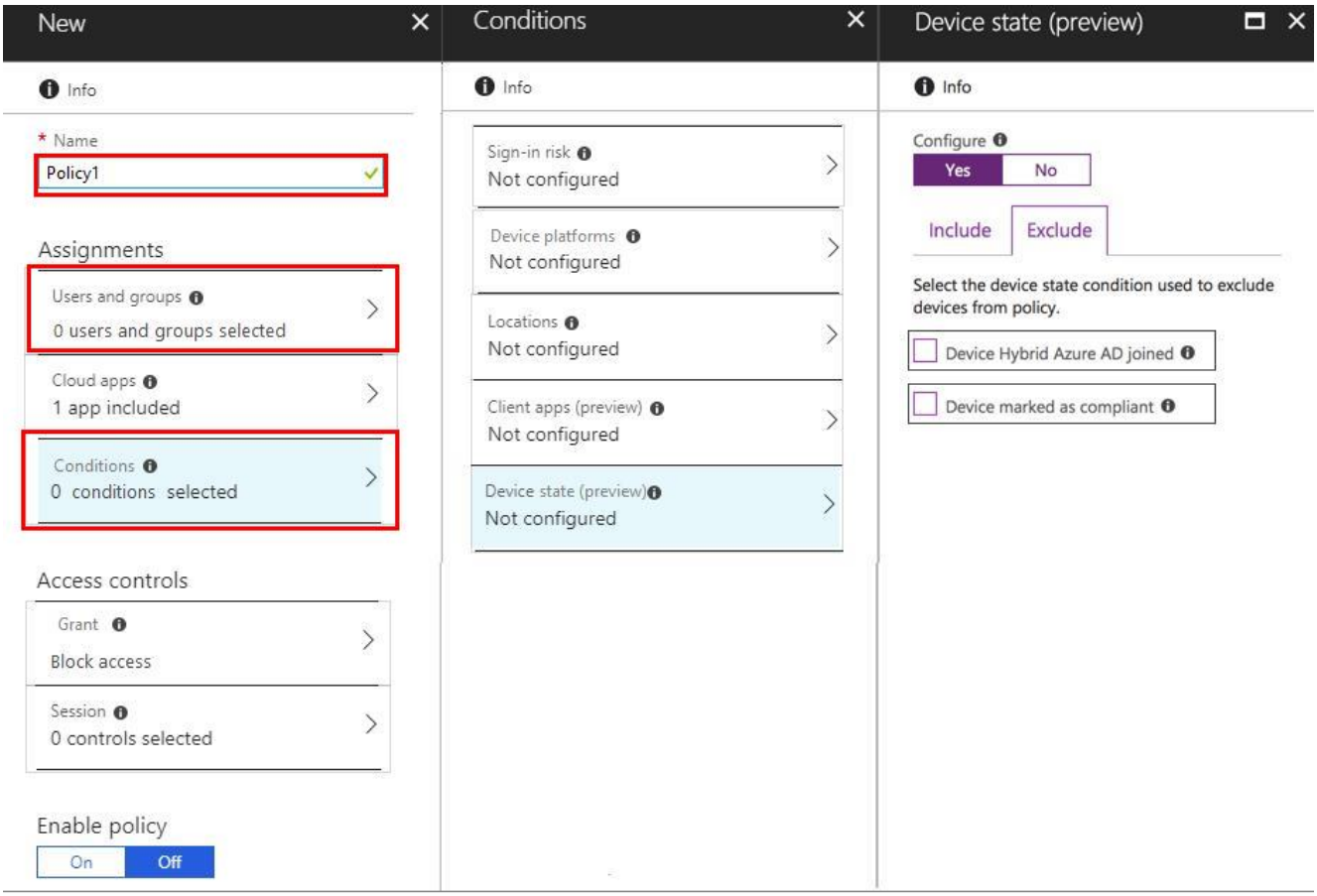
Sie fügen Exchange Online als Cloud-App hinzu.

Welche zwei zusätzlichen Einstellungen sollten Sie in Policy1 konfigurieren? Um zu antworten, wählen Sie im Antwortbereich die entsprechenden Optionen aus.

HINWEIS: Jede richtige Auswahl ist einen Punkt wert.



Answer:



QUESTION NO: 20
Sie haben einen Microsoft 365 E5-Mandanten.
Sie müssen eine Richtlinie erstellen, die eine Warnung auslöst, wenn ungewöhnliche Microsoft Office 365-Nutzungsmuster erkannt werden.
Was sollten Sie zum Erstellen der Richtlinie verwenden?

A. das Microsoft 365 Admin Center

B. das Microsoft Apps Admin Center

C. das Compliance-Portal von Microsoft Purview

D. das Microsoft Defender für Cloud Apps-Portal

Answer: D

QUESTION NO: 21
Hinweis: Diese Frage ist Teil einer Reihe von Fragen, die dasselbe Szenario darstellen. Jede Frage in der Reihe enthält eine eindeutige Lösung, mit der die angegebenen Ziele erreicht werden können. Einige Fragensätze haben möglicherweise mehr als eine richtige Lösung, während andere möglicherweise keine richtige Lösung haben.
Nachdem Sie eine Frage in diesem Abschnitt beantwortet haben, können Sie NICHT mehr darauf zurückkommen. Infolgedessen werden diese Fragen nicht im Überprüfungsbildschirm angezeigt.
Ihr Netzwerk enthält eine Active Directory-Domäne mit dem Namen contoso.com, die mit Microsoft Azure Active Directory (Azure AD) synchronisiert wird.
Sie verwalten Windows 10-Geräte mit Microsoft System Center Configuration Manager

(Current Branch).
Sie konfigurieren ein Pilotprojekt für die gemeinsame Verwaltung.
Sie fügen der Domäne ein neues Gerät mit Name Device1 hinzu. Sie installieren den Configuration Manager-Client auf Gerät1.
Sie müssen sicherstellen, dass Sie Device1 mit Microsoft Intune und Configuration Manager verwalten können.
Lösung: Definieren Sie eine Configuration Manager-Gerätesammlung als Pilotsammlung. Fügen Sie der Sammlung Device1 hinzu.
Erfüllt dies das Ziel?

A. Ja

B. NEIN

Answer: A

Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

QUESTION NO: 22
Hinweis: Diese Frage ist Teil einer Reihe von Fragen, die dasselbe Szenario darstellen. Jede Frage in der Reihe enthält eine eindeutige Lösung, mit der die angegebenen Ziele erreicht werden können. Einige Fragensätze haben möglicherweise mehr als eine richtige Lösung, während andere möglicherweise keine richtige Lösung haben.
Nachdem Sie eine Frage in diesem Abschnitt beantwortet haben, können Sie NICHT mehr darauf zurückkommen. Infolgedessen werden diese Fragen nicht im Überprüfungsbildschirm angezeigt.
Ihr Netzwerk enthält eine Active Directory-Domäne mit dem Namen contoso.com, die mit Microsoft Azure Active Directory (Azure AD) synchronisiert wird.
Sie verwalten Windows 10-Geräte mit Microsoft System Center Configuration Manager (Current Branch).
Sie konfigurieren ein Pilotprojekt für die gemeinsame Verwaltung.
Sie fügen der Domäne ein neues Gerät mit Name Device1 hinzu. Sie installieren den Configuration Manager-Client auf Gerät1.
Sie müssen sicherstellen, dass Sie Device1 mit Microsoft Intune und Configuration Manager verwalten können.
Lösung: Sie erstellen ein Gerätekonfigurationsprofil im Geräteverwaltungs-Admin Center.
Erfüllt dies das Ziel?

A. Ja

B. Nein

Answer: B

Explanation:
It looks like the given answer is correct. There is an on-premises Active Directory synced to

Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client
Topic 3, Litware Inc.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
General Overviews
Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.
Environment
Existing Environment
The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment
Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.
Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

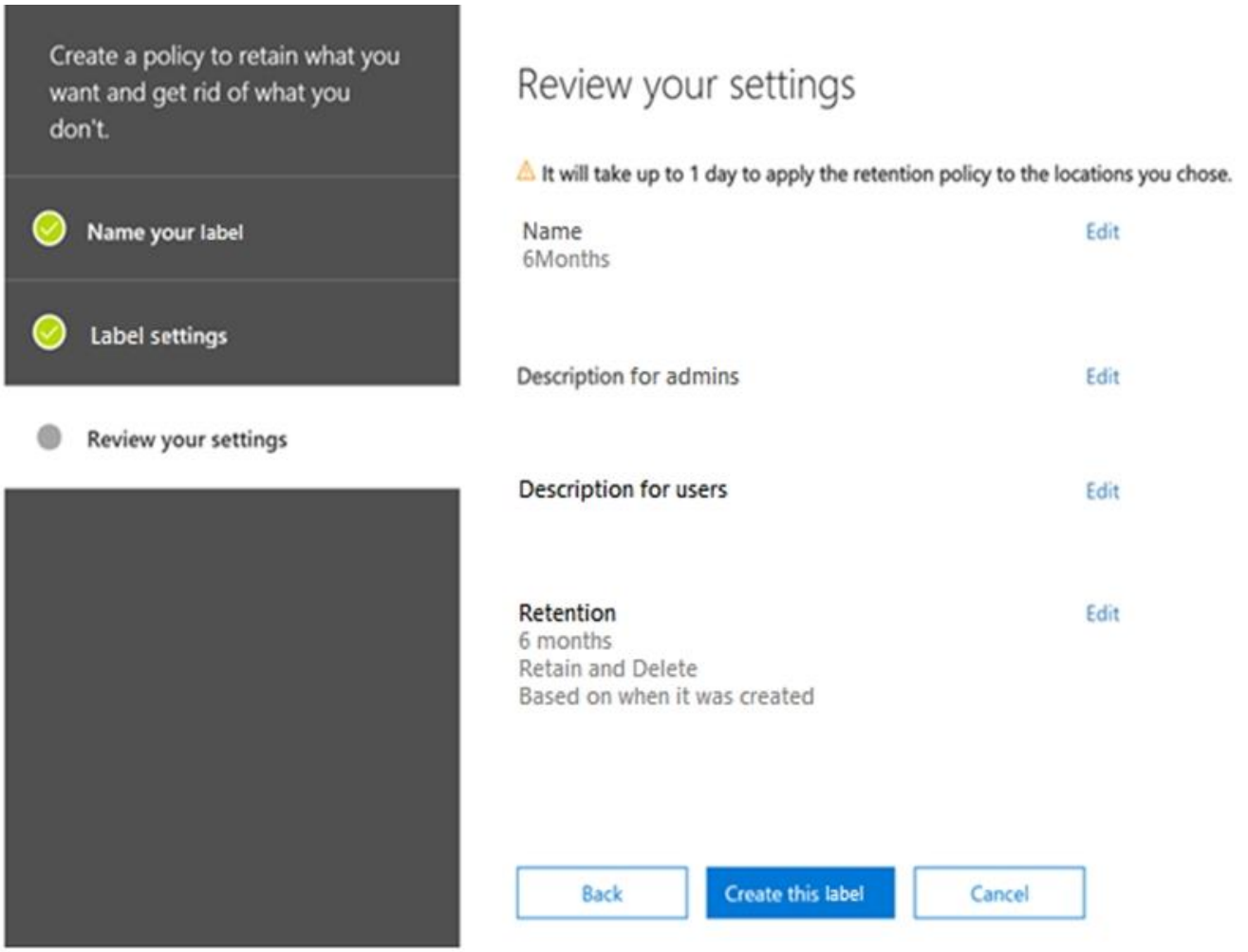
Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.
The verified domain is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Audit log search is turned on for the litware.com tenant.
Problem Statements
Litware identifies the following issues:
Users open email attachments that contain malicious content.
Devices without an assigned compliance policy show a status of Compliant.
User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

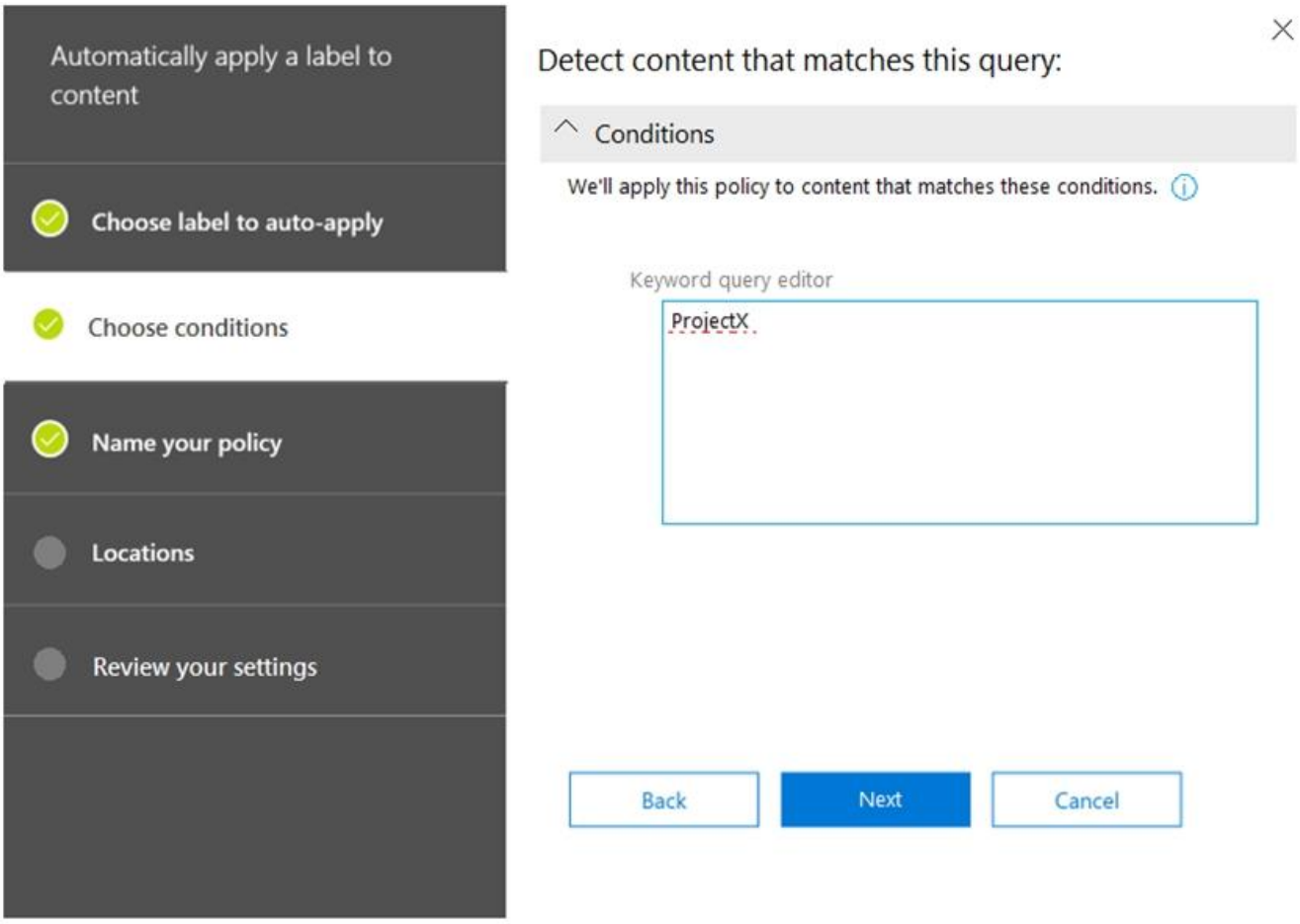
Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Azure AD.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Azure AD
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

QUESTION NO: 23
Sie haben einen Microsoft 365-Mandanten.
Sie erstellen ein Aufbewahrungsetikett wie in der Ausstellung Aufbewahrungsetikett gezeigt.
(Klicken Sie auf die Registerkarte Retention Label.)



Sie erstellen eine Beschriftungsrichtlinie, wie im Anhang zur Beschriftungsrichtlinie gezeigt. (Klicken Sie auf die Registerkarte Label Policy.)



Die Beschriftungsrichtlinie ist wie in der folgenden Tabelle gezeigt konfiguriert.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

Wählen Sie für jede der folgenden Anweisungen Ja aus, wenn die Anweisung wahr ist. Andernfalls wählen Sie Nein.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the work ProjectX.	○	○

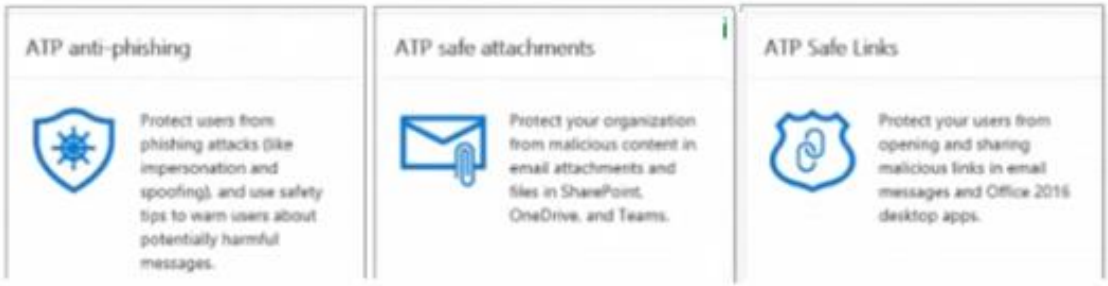
Answer:

Statements	Yes	No
Any sent email message that contains the word ProjectX will be deleted immediately.	○	○
Any sent email message that contains the word ProjectX will be retained for six months.	○	○
Users are required to manually apply a label to email messages that contain the work ProjectX.	○	○

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

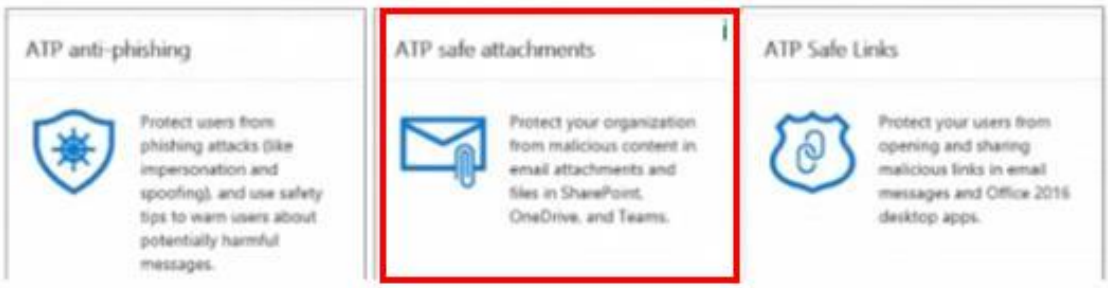
QUESTION NO: 24
Ihr Unternehmen verfügt über ein Microsoft 365-Abonnement.
Sie müssen Microsoft 365 konfigurieren, um die folgenden Anforderungen zu erfüllen:
* Malware, die in E-Mail-Anhängen gefunden wird, muss 20 Tage lang unter Quarantäne gestellt werden.
* Die E-Mail-Adresse der Absender Ihres Unternehmens muss überprüft werden.
Welche beiden Optionen sollten Sie im Security & Compliance Admin Center konfigurieren?
Wählen Sie zum Beantworten die entsprechenden Optionen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.

Answer Area

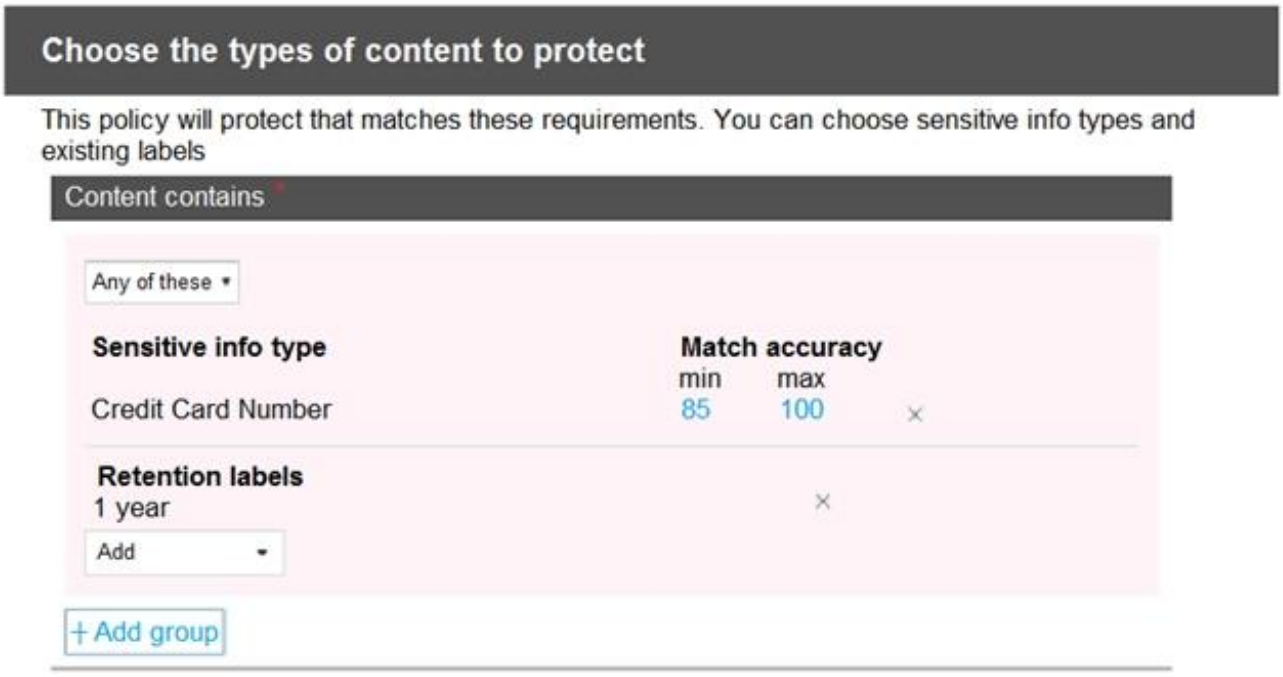


Answer:

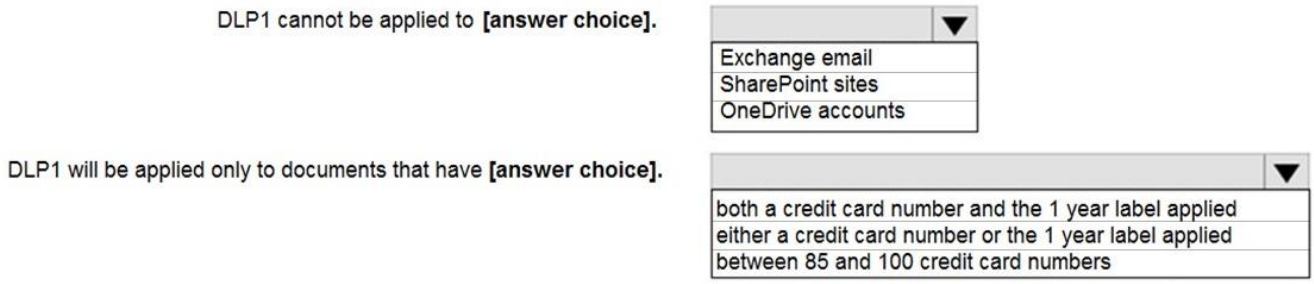
Answer Area



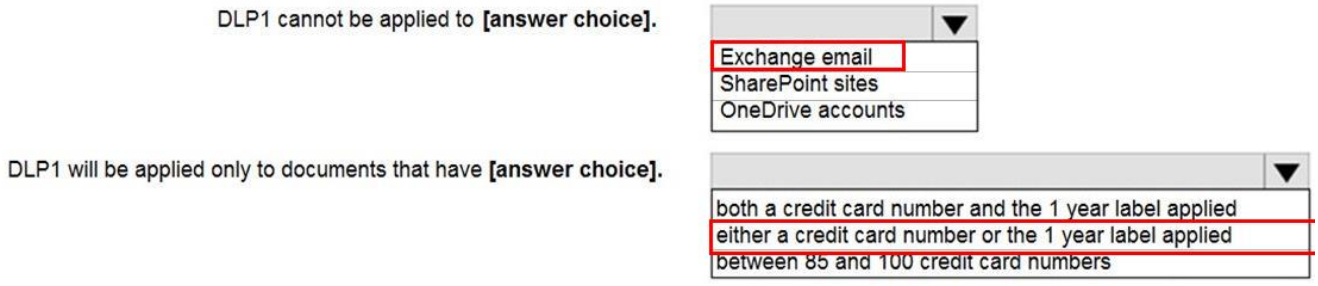
QUESTION NO: 25
Sie konfigurieren eine DLP-Richtlinie (Data Loss Prevention) mit dem Namen DLP1 (siehe folgende Abbildung).



Verwenden Sie die Dropdown-Menüs, um die Antwortauswahl auszuwählen, die jede Anweisung basierend auf den in der Grafik dargestellten Informationen vervollständigt.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.



Answer:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide#using-a-retention-label-as-a-condition-in-a-dlp-policy

QUESTION NO: 26
Sie haben einen Microsoft 365-Mandanten.
Die Unternehmensrichtlinie erfordert, dass alle Windows 10-Geräte die folgenden Mindestanforderungen erfüllen:
Komplexe Passwörter verlangen.

Erfordern die Verschlüsselung von Datenträgern.
Aktivieren Sie den Echtzeitschutz von Microsoft Defender Antivirus.
Sie müssen verhindern, dass Geräte, die die Anforderungen nicht erfüllen, auf Ressourcen im Mandanten zugreifen.
Welche zwei Komponenten sollten Sie erstellen? Jede richtige Antwort stellt einen Teil der Lösung dar.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.

A. eine Konfigurationsrichtlinie
B. eine Compliance-Richtlinie
C. ein Sicherheits-Baseline-Profil
D. eine Richtlinie für den bedingten Zugriff
E. ein Konfigurationsprofil

Answer: B,D
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION NO: 27
Sie haben ein Microsoft 365 E5-Abonnement.
Sie planen, Microsoft 365-Compliance-Richtlinien zu implementieren, um die folgenden Anforderungen zu erfüllen:
* Identifizieren Sie Dokumente, die in Microsoft Teams und SharePoint Online gespeichert sind und personenbezogene Daten (PII) enthalten.
* Bericht über freigegebene Dokumente, die PII enthalten.
Was sollten Sie erstellen?

A. eine Benachrichtigungsrichtlinie
B. eine Richtlinie zur Verhinderung von Datenverlust (DLP)
C. eine Aufbewahrungsrichtlinie
D. eine Microsoft Cloud App-Sicherheitsrichtlinie

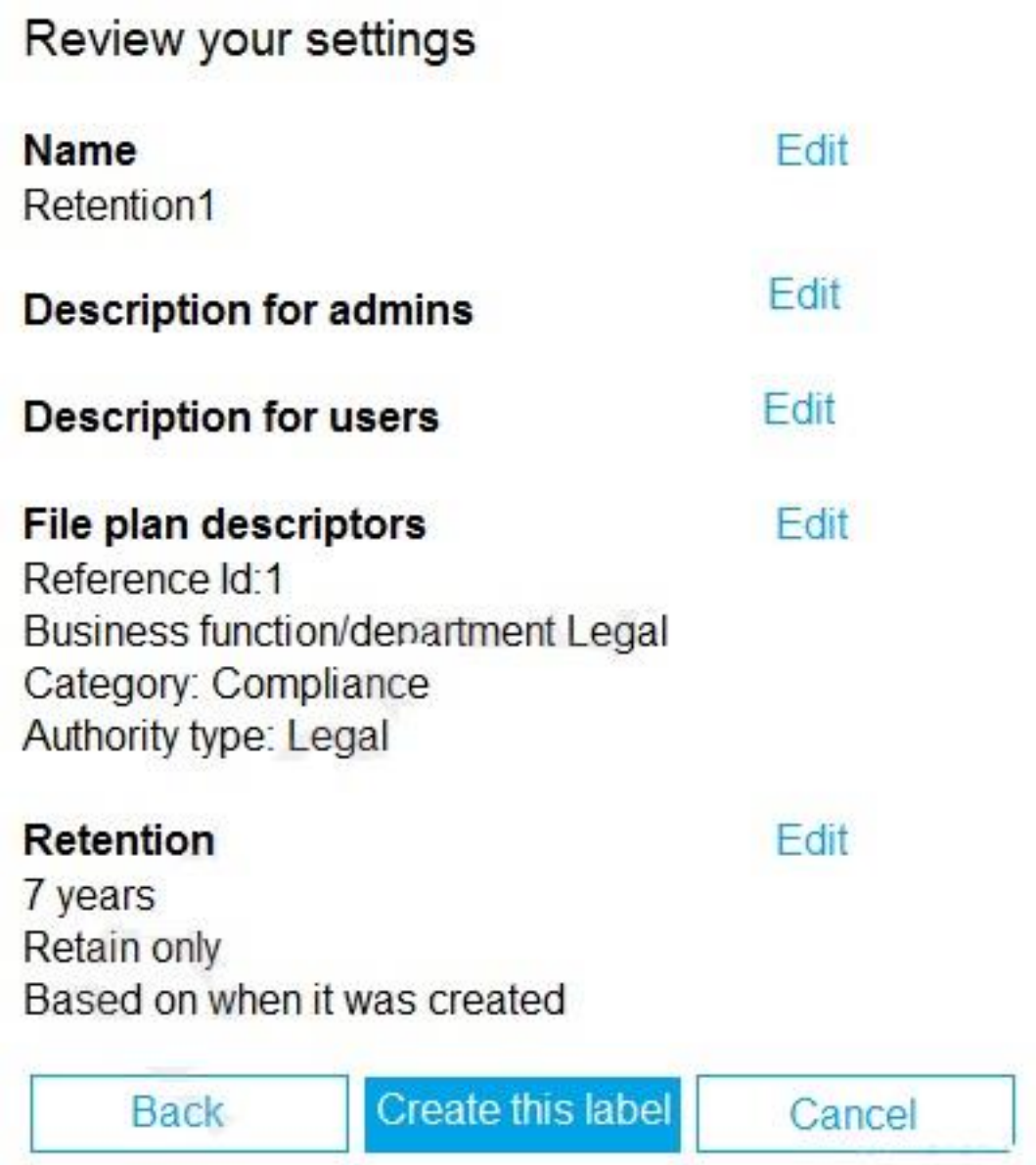
Answer: B
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

QUESTION NO: 28
Sie haben ein Microsoft 365 E5-Abonnement. Das Abonnement enthält Benutzer mit den folgenden Gerätetypen:
*Windows10
* Android
* Betriebssystem
Auf welchen Geräten können Sie die Endpoint DLP-Richtlinien konfigurieren?

A. Nur Windows 10
B. Nur Windows 10 und Android
C. Nur Windows 10 und macO
D. Windows 10, Android und iOS

Answer: C
Explanation:
Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide

QUESTION NO: 29
Sie haben einen Microsoft 365 E5-Mandanten.
Sie erstellen eine Aufbewahrungsbezeichnung namens Retention1 wie in der folgenden Abbildung gezeigt.



Wenn Benutzer versuchen, Retention1 anzuwenden, ist das Label nicht verfügbar.

Sie müssen sicherstellen, dass Retention1 für alle Benutzer verfügbar ist.
Was sollte man tun?

A. Erstellen Sie eine neue Label-Richtlinie

B. Ändern Sie die Einstellung des Autoritätstyps für die Aufbewahrung!

C. Ändern Sie die Geschäftsfunktions-/Abteilungseinstellung für Aufbewahrung 1.

D. Verwenden Sie eine Dateiplan-CSV-Vorlage zum Importieren von Aufbewahrung1.

Answer: A

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide

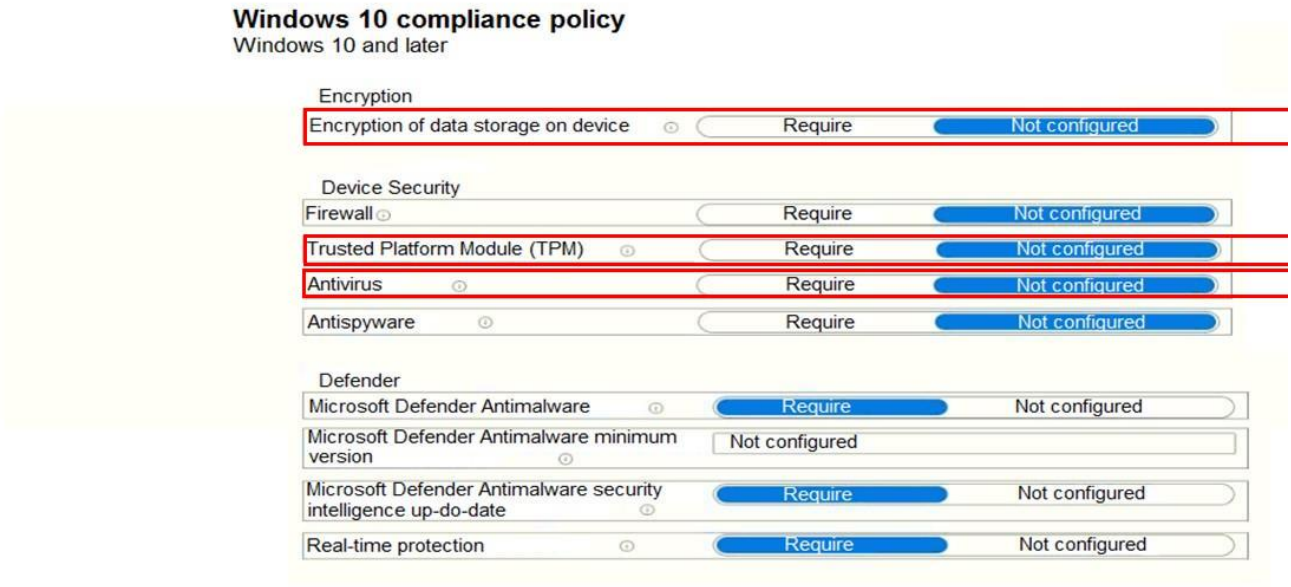
QUESTION NO: 30

Sie haben einen Microsoft 365 E5-Mandanten, der 500 Windows 10-Geräte und eine Windows 10-Konformitätsrichtlinie enthält.
Sie stellen eine Antivirenlösung eines Drittanbieters auf den Geräten bereit.
Sie müssen sicherstellen, dass die Geräte als konform gekennzeichnet sind.
Welche drei Einstellungen sollten Sie in der Compliance-Richtlinie ändern? Wählen Sie zum Antworten die entsprechenden Einstellungen im Antwortbereich aus.
HINWEIS: Jede richtige Auswahl ist einen Punkt wert.

Answer Area

Answer:

Answer Area

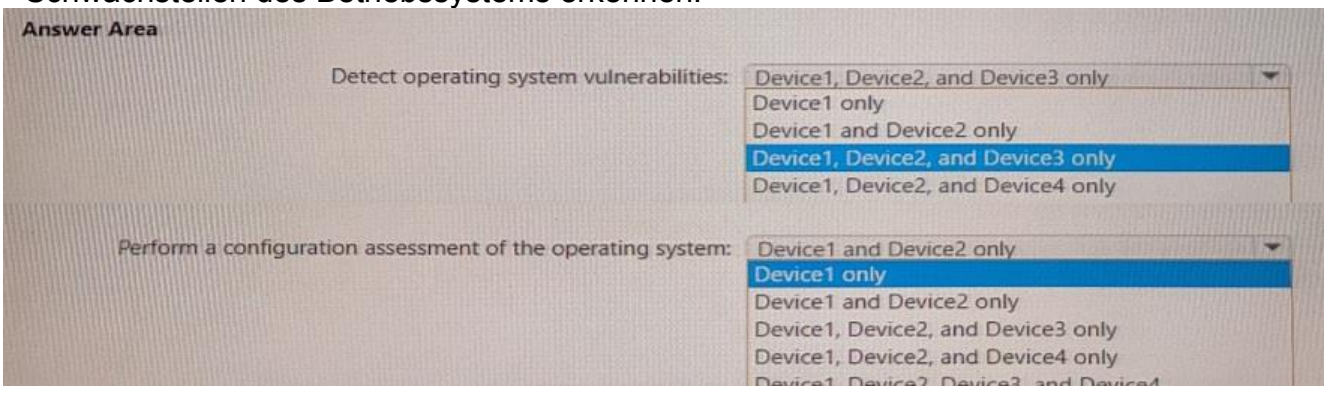


Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows

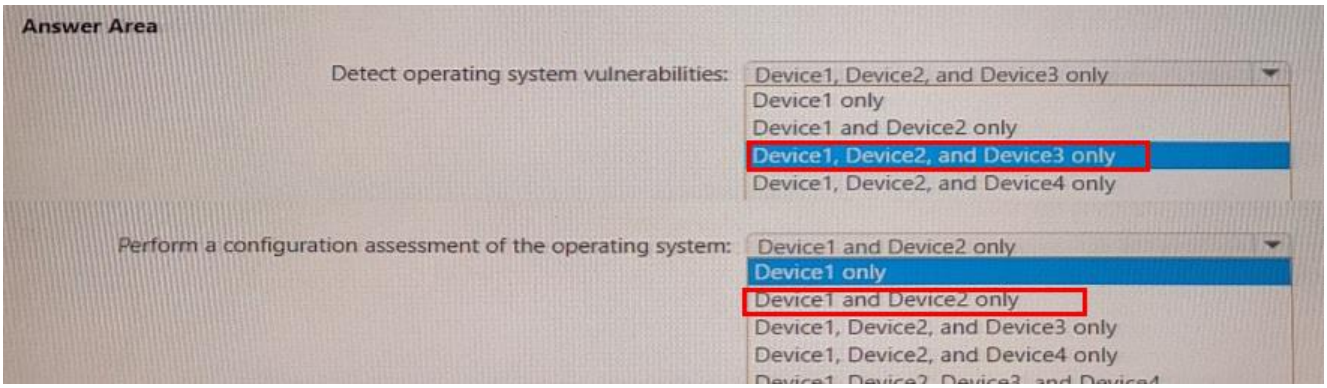
QUESTION NO: 31
Sie haben ein Microsoft 365 E5-Abonnement, das die in der folgenden Tabelle aufgeführten Geräte enthält.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

Alle Geräte sind in Microsoft Defender for Endpoint integriert
Sie planen, Microsoft Defender Vulnerability Management zu verwenden, um die folgenden Anforderungen zu erfüllen:
* Schwachstellen des Betriebssystems erkennen.



Answer:



QUESTION NO: 32
Ihr Unternehmen verfügt über einen Microsoft 365 E5-Mandanten, der einen Benutzer namens User1 enthält.
Sie überprüfen den Compliance-Score des Unternehmens.
Sie müssen Benutzer1 die folgende Verbesserungsaktion zuweisen: Self-Service-Kennwortrücksetzung aktivieren.
Was sollten Sie zuerst tun?
A. Deaktivieren Sie im Compliance Manager die automatisierten Tests.
B. Aktivieren Sie im Azure Active Directory Admin Center die Self-Service-Kennwortzurücksetzung (SSPR).
C. Ändern Sie im Microsoft 365 Admin Center die Einstellungen für die Self-Service-Kennwortzurücksetzung (SSPR).
D. Fügen Sie im Azure Active Directory Admin Center User1 zur Compliance-Administratorrolle hinzu.
Answer: D
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal

QUESTION NO: 33
Sie haben ein Microsoft 365-Abonnement.
Im Security & Compliance Admin Center erstellen Sie eine Inhaltssuche für ein Postfach.
Sie müssen den Inhalt der von der Suche gefundenen E-Mails so schnell wie möglich anzeigen.
Was sollten Sie aus den Einstellungen für die Inhaltssuche auswählen?
A. Bericht exportieren
B. Ergebnisse exportieren
C. Wiederholen
D. Ergebnisse anzeigen
Answer: B
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.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/limits-for-content-search

QUESTION NO: 34
Sie haben ein Microsoft 365-Abonnement.
Alle Benutzer haben ihre E-Mails in Microsoft Exchange Online gespeichert.
Im Postfach eines Benutzers mit dem Namen "Benutzer1" müssen Sie eine Kopie aller E-Mail-Nachrichten aufbewahren, die das Wort "Project X" enthalten.
Was solltest du zuerst tun?
A. Erstellen Sie im Security & Compliance Admin Center eine DLP-Richtlinie (Data Loss Prevention).
B. Erstellen Sie im Security & Compliance Admin Center ein Etikett und eine Etikettenrichtlinie.
C. Erstellen Sie im Security & Compliance Admin Center ein Etikett und eine Etikettenrichtlinie.
D. Starten Sie im Security & Compliance Admin Center eine Nachrichtenverfolgung.
E. Starten Sie im Exchange-Verwaltungscenter eine Ablaufverfolgung für Nachrichten
Answer: A
Explanation:
A DLP policy contains a few basic things:
Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.
When and how to protect the content by enforcing rules comprised of:
Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that's been shared with people outside your organization.
Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

QUESTION NO: 35
Ihr Netzwerk enthält eine lokale Active Directory-Domäne mit dem Namen contoso.com. Die Domäne enthält 1.000 Windows 10-Geräte.
Sie führen eine PoC-Bereitstellung (Proof of Concept) von Windows Defender Advanced Threat Protection (ATP) für 10 Testgeräte durch. Während des Onboarding-Vorgangs konfigurieren Sie Windows Defender-ATP-bezogene Daten, die in den USA gespeichert werden sollen.
Sie planen, alle Geräte in Windows Defender ATP zu integrieren.
Sie müssen die Windows Defender-ATP-Daten in Europa speichern.
Was solltest du zuerst?
A. Erstellen Sie einen Arbeitsbereich.
B. Auf einem neuen Gerät.

C. Löschen Sie den Arbeitsbereich.
D. Offboarding der Testgeräte.
Answer: D