Microsoft.SC-401.v2026-05-18.q196

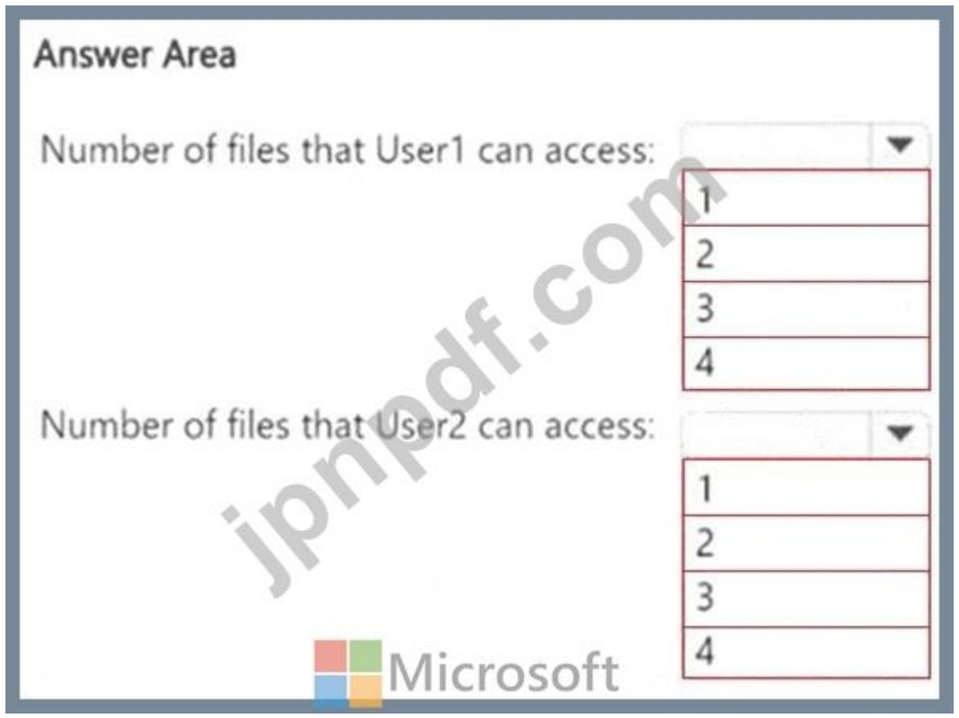
試験コード:	SC-401
試験名称:	Administering Information Security in Microsoft 365
認定資格:	Microsoft
無料問題数:	196
バージョン:	v2026-05-18
アクセス数:	133
ページビュー数:	1960
https://www.jpnpdf.com/Microsoft.SC-401.v2026-05-18.q196-mondaishu.html	

最新問題: **1**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を使用する予定です。
辞職を申し出たユーザーや雇用終了日が近いユーザーによる Microsoft SharePoint Online からのデータ盗難を検出するインサイダー リスク管理ポリシーを作成する必要があります。
まず何をすべきでしょうか?
A. 物理バッジコネクタを構成します。
B. Office インジケーターを構成します。
C. HR データ コネクタを構成します。
D. デバイスを Microsoft Defender for Endpoint にオンボードします。
Answer: C (メーッセージを残す**)**

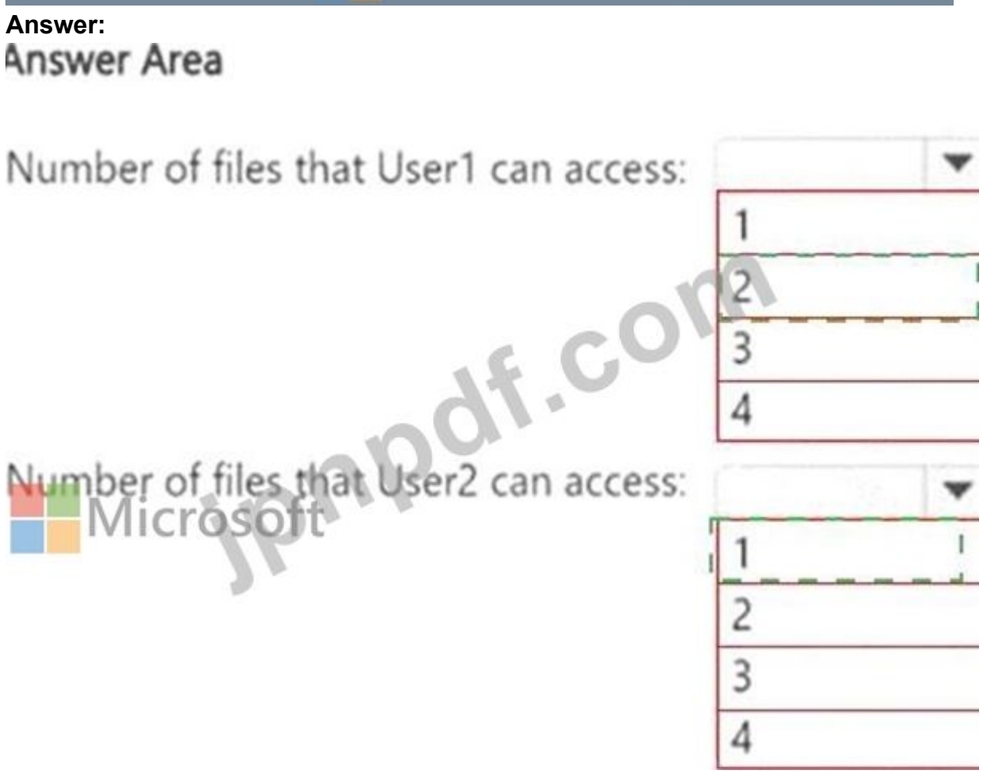
最新問題: **2**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク7
製品廃止保持ラベルは、Exchange メールボックスと SharePoint クラシック サイトおよびコミュニケーション サイトにのみ公開する必要があります。

Answer:
保持ラベルを特定の場所に公開するには、まずラベルを作成し、次にMicrosoft Purviewポータルで静的保持ラベルポリシーを作成し、「特定の場所を選択」を選択して、ポリシーの適用範囲としてExchangeメールボックスとSharePointサイトを選択します。Exchangeの場合は、「すべてのExchangeメールボックス」を選択するか、特定のメールボックスを選択できます。SharePointの場合は、ポリシー設定でクラシックサイトとコミュニケーションサイトを個別に追加する必要があります。
静的ポリシーでラベルを公開する
ステップ 1: Microsoft Purview ポータルで、[データ ライフサイクル管理] > [ポリシー] > [ラベル ポリシー] に移動します。
ステップ 2: [ラベルの公開] をクリックし、[公開するラベルの選択] をクリックして、[製品の廃止] ラベルを選択します。
ステップ 3: [ポリシー スコープ] セクションで [静的] を選択し、[次へ] をクリックします。
ステップ 4: [ラベルを公開する場所を選択] 画面で、[特定の場所を選択する] を選択します。
ステップ5: Exchangeの場合:
Exchangeメールボックスを選択します。すべてのExchangeメールボックスに適用するか、リストから特定のメールボックスを選択することができます。
ステップ 6: SharePoint の場合:
SharePointサイトを選択します。クラシックサイトとコミュニケーションサイトの両方について、特定のサイトコレクションのアドレスを手動で追加する必要があります。追加したサイトの横にチェックマークが表示され、次の画面で検索できるようになります。
ステップ 7: [次へ] をクリックし、ポリシーの名前と説明を入力して、[送信] をクリックしてポリシーを作成します。
参照：
https://learn.microsoft.com/en-us/purview/create-apply-retention-labels

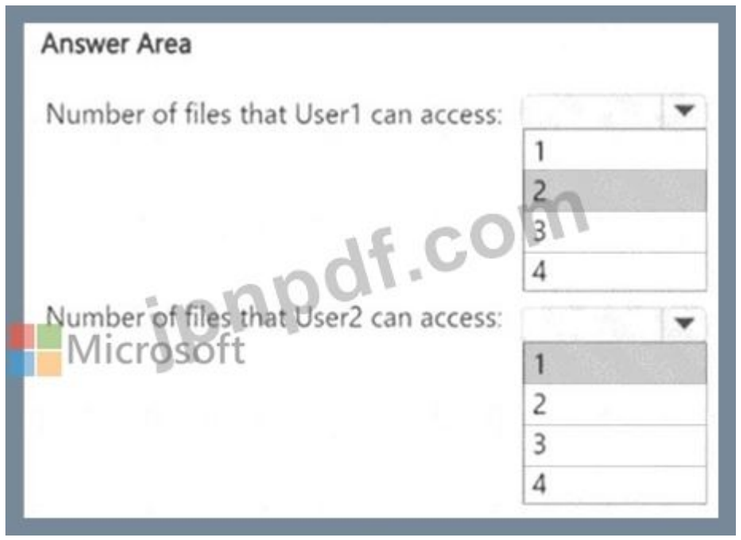
最新問題**: 3**
ホットスポット
DLPpolicy1 をオンにした後、User1 と User2 は Site2 内のいくつのファイルにアクセスできますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



DLP ポリシーがファイル アクセスに与える影響を理解する
DLP ポリシー (DLPpolicy1) は Site2 に適用され、次の場合にアクセスを制限します。
コンテンツには SWIFT コードが含まれています。
インスタンス数は2以上です。
ファイル分析（SWIFTコード数に基づく）

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	□ No restriction (SWIFT codes < 2)
File2.bmp	4	□ Restricted (SWIFT codes ≥ 2)
File3.txt	3	□ Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	□ Restricted (SWIFT codes ≥ 2)

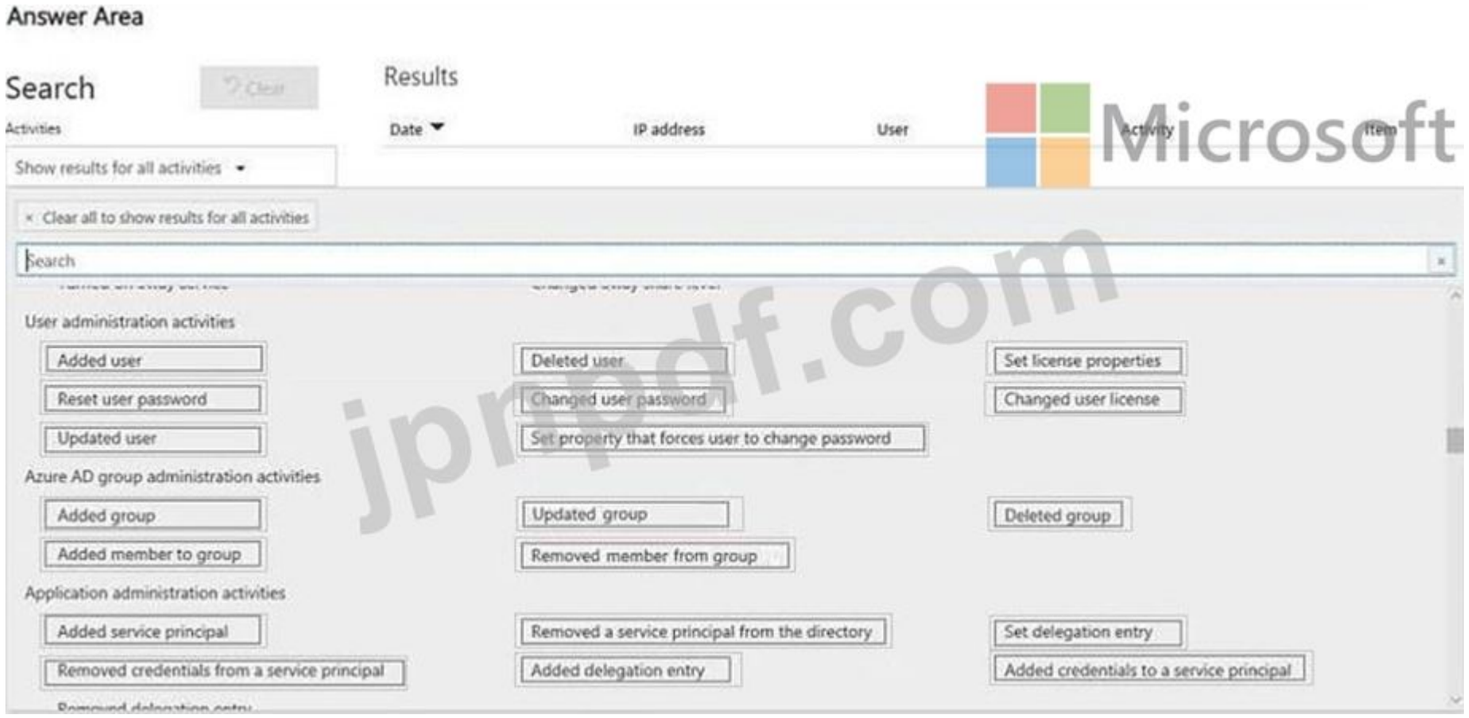
アクセス可能なままのファイル（DLP によって制限されていないもの）:
File1.docx (SWIFT コードが 1 つだけ含まれています # 制限しきい値未満) DLP ポリシー適用後のユーザー アクセス:

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

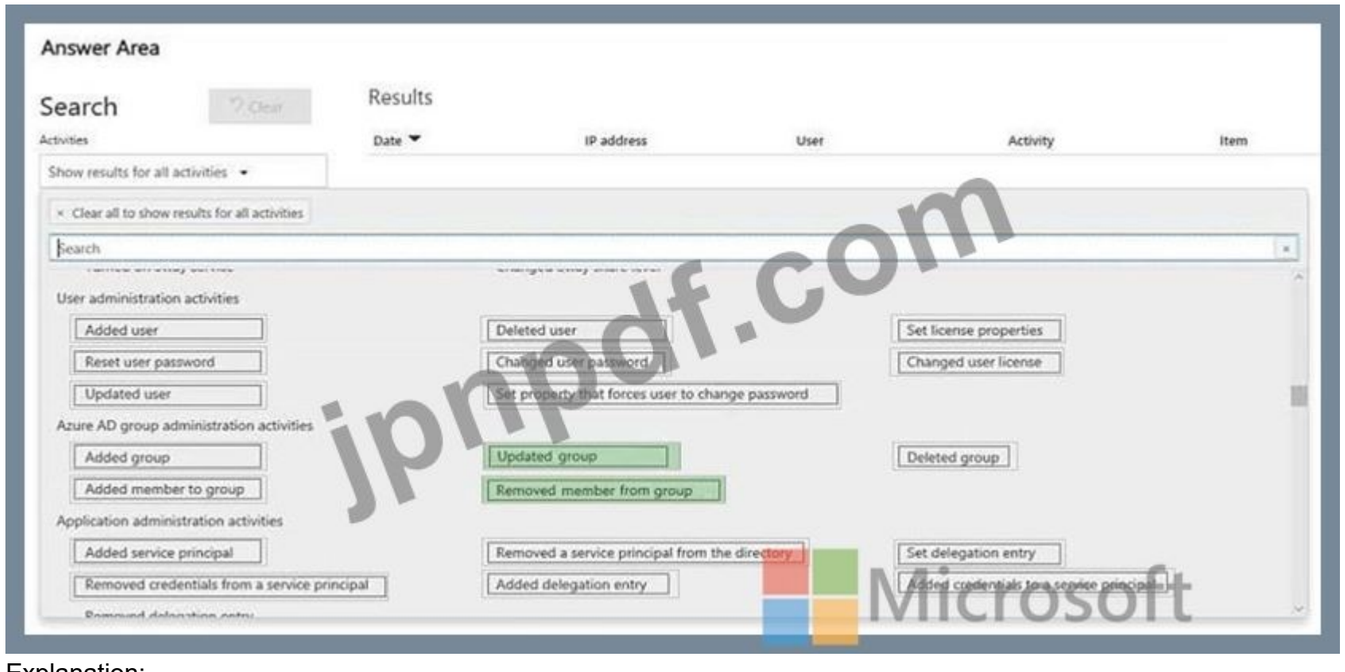
ユーザー1（サイト所有者）:
より高い権限を持ち、DLP 制限をオーバーライドできます (管理者の介入を通じて)。
2 つのファイルにアクセスできます (File1.docx + 別のファイルへのオーバーライド アクセス)。
ユーザー2（サイト訪問者）:
読み取り専用アクセスがありますが、DLP により制限されたファイルへのアクセスがブロックされます。
他のファイルはすべて制限されているため、1 つのファイル (File1.docx) にのみアクセスできます。

最新問題: **4**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
最近、会社の開発者が Azure ストレージ アカウント キーをプレーン テキストで第三者に電子メールで送信していることが分かりました。
Azure ストレージ アカウント キーを電子メールで送信する場合は、電子メールが暗号化されていることを確認する必要があります。
解決策: テキスト パターンに一致するメール フロー ルールを構成します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
Exchange トランスポート ルールで 「テキスト パターン」条件を使用しても機能しません。
Exchange トランスポート ルールで使用される条件は 「メッセージに次の機密情報のいずれかが含まれています...」となり、機密情報の種類として 「Azure アカウント ストレージ キー」を選択します。
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mail-flow-rules/conditions-and-exceptions?view=exchserver-2019

最新問題: **5**
ホットスポットに関する質問
Microsoft 365 サブスクリプションをお持ちです。監査が有効になっています。
User1 という名前のユーザーは、Group1 という名前の動的セキュリティ グループのメンバーです。
User1 が Group1 のメンバーではなくなったことがわかります。
User1 が Group1 から削除された理由を特定するには、監査ログを検索する必要があります。
検索ではどの 2 つのアクティビティを使用する必要がありますか? 回答するには、回答領域で適切なアクティビティを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ボックス1: グループからメンバーを削除

監査ログアクティビティ

Microsoft Entra グループ管理アクティビティ

次の表は、管理者またはユーザーが Microsoft 365 グループを作成または変更したとき、または管理者が Microsoft 365 管理センターまたは Azure 管理ポータルを使用してセキュリティ グループを作成したときに記録されるグループ管理アクティビティを示しています。
* グループからメンバーを削除しました
メンバーがグループから削除されました。
* グループを更新しました
グループのプロパティが変更されました。
* など
ボックス2: 更新されたグループ
参照：
https://learn.microsoft.com/en-us/purview/監査ログアクティビティ

最新問題: **6**
Site1 という名前の Microsoft SharePoint Online サイトと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Member of
User1	Members group of Site1
User2	Owners group of Site1
Admin1	SharePoint Administrator role

次の図に示すように、DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

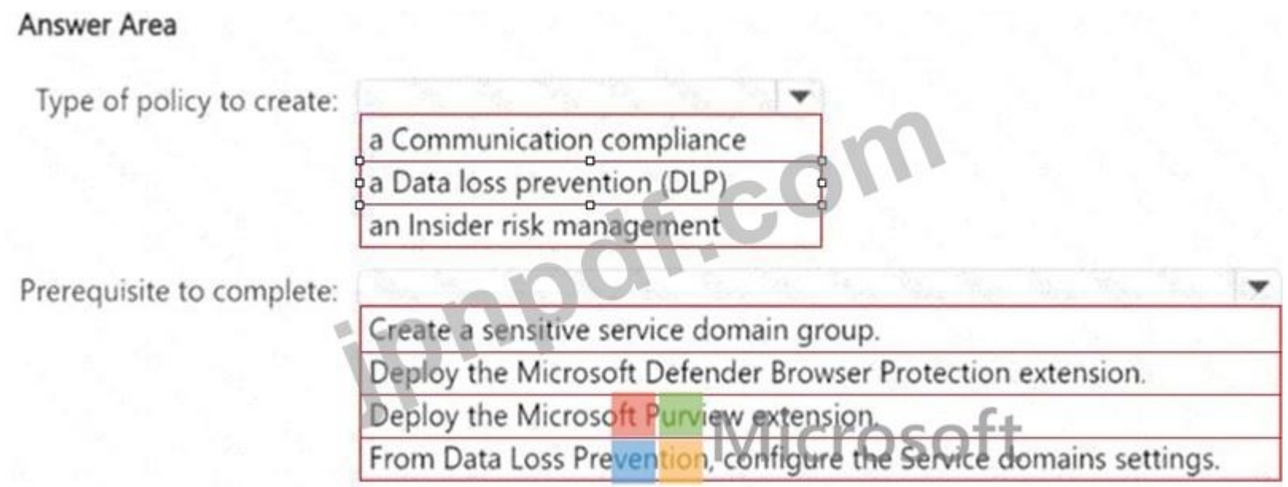
DLP1 を Site1 に適用します。
ユーザー1はサイト1にFile1というファイルをアップロードします。File1はDLP1ルールのいずれにも一致しません。ユーザー2はFile1を更新し、DLP1ルールに一致するデータを追加します。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

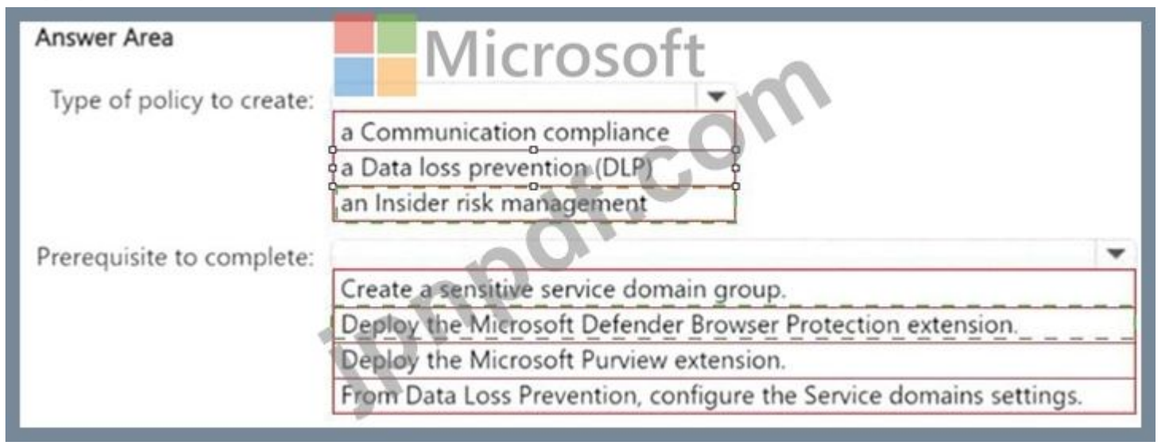
Answer:

Explanation:

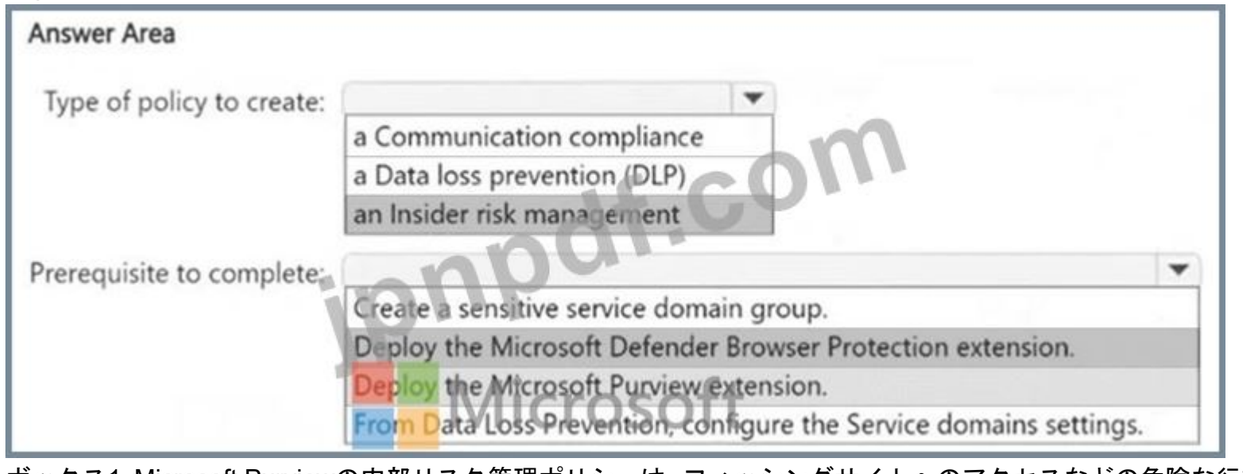
最新問題**: 7**
ホットスポット
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
ユーザーがフィッシング Web サイトにアクセスしたときにインシデントが生成されるようにする必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



ボックス1 :Microsoft Purviewの内部リスク管理ポリシーは、フィッシングサイトへのアクセスなどの危険な行動を検出するように設定できます。これらのポリシーは、ユーザーのアクティビティを監視し、アラートを生成し、組織が潜在的なセキュリティ脅威を調査するのに役立ちます。

ボックス2 :Microsoft Defender ブラウザ保護拡張機能は、安全でないウェブサイトやフィッシングサイトを検出し、その検出結果をインサイダーリスク管理ポリシーと統合するのに役立ちます。この拡張機能はMicrosoft EdgeおよびGoogle Chromeと連携し、危険なブラウジングアクティビティを識別してアラートをトリガーします。

最新問題: **8**
ホットスポットに関する質問
Microsoft Purview とジャストインタイム (JIT) 保護を使用する Microsoft 365 E5 サブスクリプションをご利用の場合、次の表に示すユーザーが含まれています。

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

サブスクリプションには、次の表に示すデバイスが含まれています。

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

デバイスには次の表に示すファイルが含まれています。

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

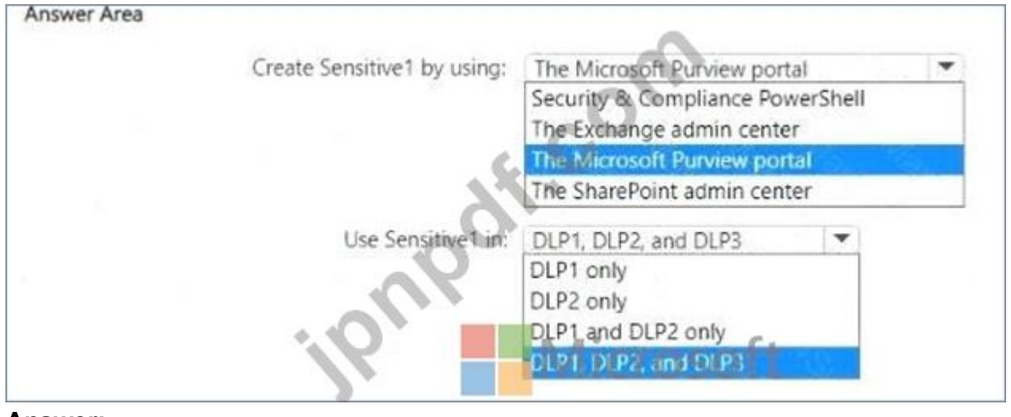
Answer:

Explanation:
ステートメント1 - いいえ。ユーザー1はJIT保護の対象です。ファイル1.docxはデバイス1上にあり、デバイス1はMicrosoft Defenderにオンボードされています。しかし、ファイル1.docxはファイル分類の評価を受けていないため、JITは保護を適用できません。ユーザー2がデバイス2にサインインし、ファイル2.pdfをメールに添付しようとした場合、JITはブロックします。
ステートメント 2 - いいえ。User2 は JIT 保護用に構成されていません (JIT は適用されません)。
File2.pdf は分類対象として評価されましたが、User2 は JIT 保護の対象外であるため、ブロックは発生しません。User3 が File3.xlsx をネットワーク共有にコピーしようとすると、JIT によって監査イベントが生成されます。
ステートメント3 - いいえ。User3はJIT保護の対象です。ただし、Device3はMicrosoft Defenderにオンボードされていないため、JIT保護はDevice3に対してアクションを実行できません。File3.xlsxは評価されていないため、たとえデバイスがオンボードされていたとしても、JITはアクションを実行するための分類データを取得できません。

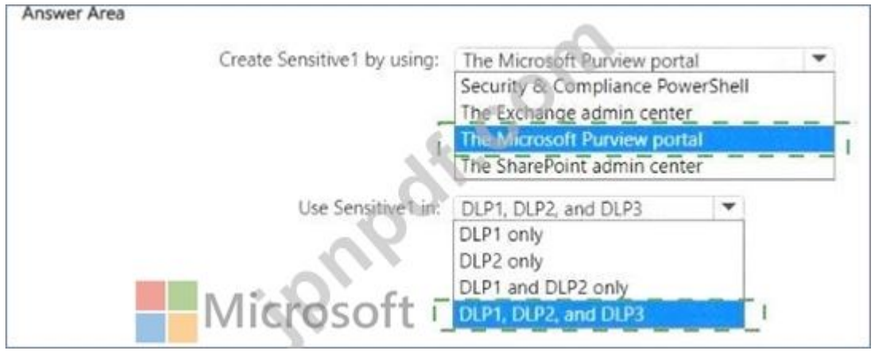
最新問題: **9**
次の表に示すデータ損失防止 (DLP) ポリシーが含まれる Microsoft 365 E5 サブスクリプションがあります。

Name	Applied to
DLP1	Microsoft Exchange Online email
DLP2	Microsoft SharePoint Online sites
DLP3	Microsoft Teams chat and channel messages

Template1 .docx という名前のカスタム従業員情報フォームがあります。
Template1.docx のドキュメント フィンガープリントを使用する、Sensitive! という名前の機密情報の種類を作成する予定です。
Sensitive1 を作成するには何を使用すればよいですか。また、Sensitive1 はどの DLP ポリシーで使用できますか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ステップ1 - 要件
Sensitive1 という名前のカスタムの機密情報の種類を作成します。
この SIT は、Template1.docx のドキュメント フィンガープリントから作成されます。
次に、DLP ポリシーで Sensitive1 を使用します。
ステップ 2 - カスタムの機密情報タイプはどこで作成しますか?
カスタム SIT (ドキュメント フィンガープリントを含む) は、Microsoft Purview コンプライアンス ポータルでのみ作成できます。
Exchange 管理センター、SharePoint 管理センター、または PowerShell で直接作成することはできません。
創造への答え: Microsoft Purview ポータル
参考: ドキュメント フィンガープリントを使用してカスタムの機密情報タイプを作成する手順 3 - カスタムの機密情報タイプはどこで使用できますか?
作成されたカスタム SIT はテナント全体で有効となり、DLP をサポートするすべてのワークロードで使用できるようになります。
Exchangeメール
SharePoint Online サイト
ワンドライブ
Teams チャットとチャネル メッセージ
表では、DLP ポリシーは次のとおりです。
DLP1 # Exchange Online メール
DLP2 # SharePoint Online サイト
DLP3 # Teams チャットとチャネル メッセージ
Sensitive1 はカスタム SIT であるため、3 つのポリシーすべてで使用できます。
使用法の回答: DLP1、DLP2、および DLP3

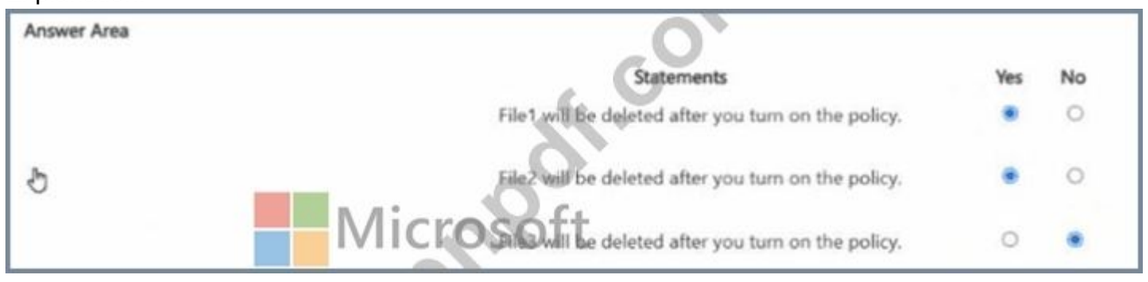
最新問題: 10
次の表に示すファイルがあります。

Name	Location	Date modified	Date created
File1	Microsoft SharePoint Online site	June 01, 2022	December 28, 2015
File2	Microsoft OneDrive account	February 02, 2021	January 02, 2015
File3	Microsoft Exchange Online public folder	May 01, 2010	May 01, 2010

展示に示されているように、保持ポリシーを設定します。（展示ボをクリックしてください。）保持期間の開始日はアイテムの作成日に基づきます。現在の日付は207年1月1日です。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

Answer:

Explanation:

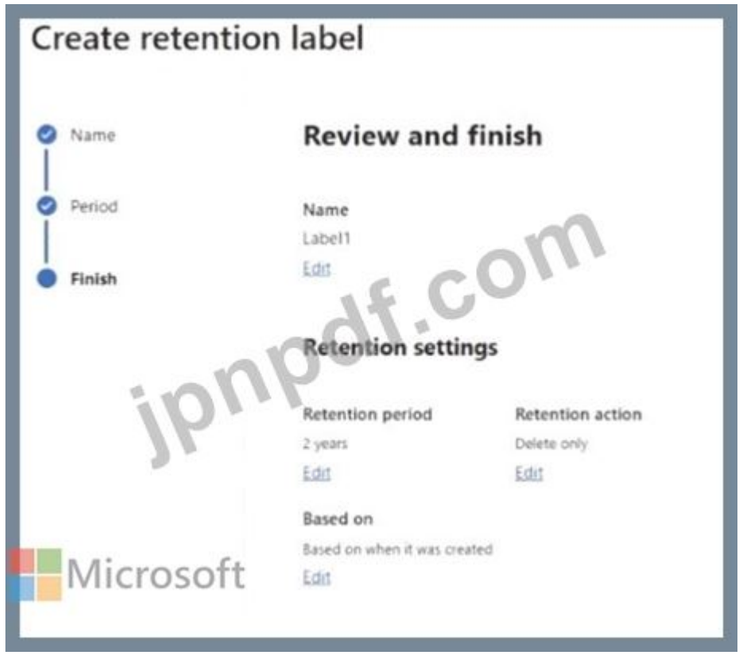


最新問題: **11**
Microsoft 365 サブスクリプションをお持ちの場合、保持ポリシーを作成し、Exchange Online メールボックスに適用します。
できるだけ早く、アイテム保持ポリシー タグをメールボックス アイテムに割り当てることができるようにする必要があります。
何をすべきでしょうか?

A. Exchange Online PowerShell から、Start-ManagedFolderAssistant を実行します。
B. Microsoft Purview ポータルから、データ損失防止 (DLP) ポリシーを作成します。
C. Microsoft Purview ポータルからラベル ポリシーを作成します。
D. Exchange Online PowerShell から、start -RetentionAutoTagLearning を実行します。

Answer: A (メーッセージを残す)
Exchange Online のアイテム保持ポリシータグ (MRM) は、管理フォルダーアシスタント (MFA) によって適用されます。新しく作成された Exchange アイテム保持ポリシーをメールボックスのアイテムに直ちに適用するには、メールボックスまたはメールボックスセットに対して Start-ManagedFolderAssistant を使用して手動で MFA を呼び出します。Purview で DLP ポリシーまたはラベルポリシーを作成しても、MRM 処理は高速化されません。

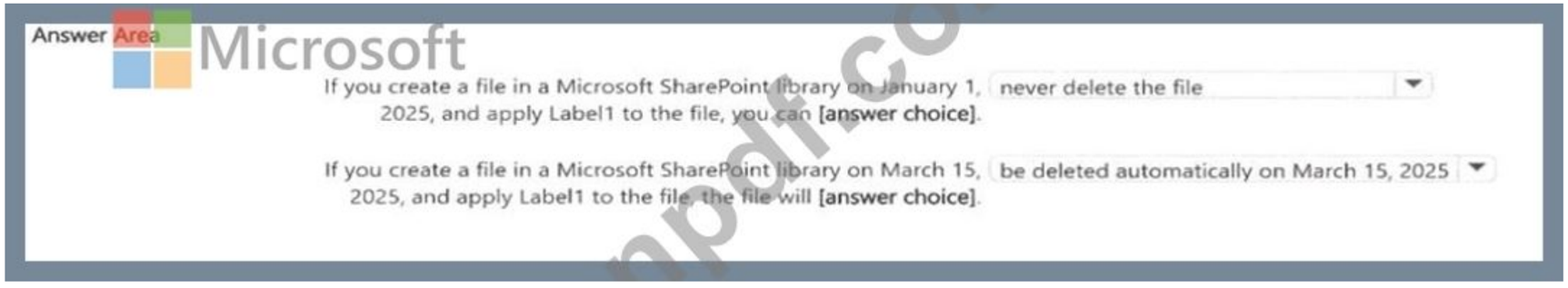
最新問題: **12**
Microsoft 365 サブスクリプションをお持ちです。
次の図に示すように、Label1 という名前の保持ラベルを作成します。



Label! を SharePoint サイトに公開します。
ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:



最新問題**: 13**

次の表に示すデバイスが含まれる Microsoft 36S ES サブスクリプションがあります。

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

社内リスク管理を実施し、フォレンジック証拠を取得する予定です。フォレンジック証拠の収集をサポートするデバイスはどれですか？また、サポートされる各デバイスを準備するには何をする必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

質問は、Microsoft 365 E5 (Microsoft Purview) における Insider Risk Management のフォレンジック証拠収集に関するものです。
ステップ 1 - サポートされているデバイスはどれですか?

Microsoft のドキュメントによると、インサイダー リスク調査のためのフォレンジック証拠収集は、以下でのみサポートされています。
ウィンドウズ10
ウィンドウズ11
以下ではサポートされていません:
macOS
アンドロイド
iOS
参考: Microsoft Purview Insider Risk Management におけるフォレンジック証拠収集
したがって、Device1 (Windows 11) と Device2 (Windows 10) のみが対象となります。
ステップ 2 - どのような準備が必要ですか?
法医学的証拠を収集するには、サポートされているデバイスが次の条件を満たしている必要があります。
Microsoft Purview にオンボードされます (Microsoft Defender for Endpoint 統合経由)。
Microsoft Purview クライアントをインストールしておきます。
これにより、ファイルのコピー、USB 転送、印刷などのユーザー アクションをキャプチャして、インサイダー リスク アラートのフォレンジック証拠を提供できるようになります。
正しいオプション: デバイスを Microsoft Purview にオンボードし、Microsoft Purview クライアントをインストールする

最新問題: 14
Site1 と Site2 という名前の 2 つの Microsoft SharePoint Online サイトを含む Microsoft 365 サブスクリプションがあります。
次の要件を満たすためにポリシーを使用する予定です。
- 文書に機密の透かしを追加する
Project1 または Project2 という単語が含まれています。
- 文書にクレジットが含まれている場合は、文書を7年間保管する
カード情報。
- 保存されているすべての文書に 社内使用のみ」の透かしを追加します。
サイト2。
- Site1 に保存されているすべてのドキュメントに 機密」の透かしを追加します。
必要となる機密情報タイプの最小数を推奨する必要があります。
推奨する機密情報の種類はいくつありますか?
A. 1
B. 2
C. 3
D. 4
Answer: C (メーッセージを残す**)**
（１）文書 Pro-ject1」または Project2」という単語が含まれている場合は、文書に Confidential」の透かしを追加します。
2 - 保存）文書にクレジットカード情報が含まれている場合は、文書を7年間保存します。
（3サイト 2に保存されているすべての文書に 社内使用のみ」の透かしを追加します。
(1 同じものを使用できます) Site1 に保存されているすべてのドキュメントに Confidential の透かしを追加します。
参照：
https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about

最新問題: **15**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク8
次の要件を満たすコンテンツに従業員レコード保持ラベルが自動的に適用されるようにする必要があります。
- 英国固有の納税者参照番号の機密情報タイプのみが含まれています
- Exchange メール、SharePoint サイト、OneDrive アカウント、または Microsoft 365 グループに配置されている
Answer:
下記の説明を参照してください。
Explanation:
特定の機密情報の種類を使用するように保持ラベルを構成するには、Microsoft Purview ポータルで、その機密情報の種類を含むコンテンツにラベルを適用する自動ラベル付けポリシーを作成する必要があります。まず、保持ラベル自体とその保持設定を作成し、次に自動ラベル付けポリシーを作成します。 "機密情報を含むコンテンツにラベルを適用する"を選択し、目的の機密情報の種類を選択し、適用場所を指定して、保持ラベルを選択します。
ステップ 1: Microsoft Purview ポータルにサインインします。
手順 2: レコード管理を使用している場合 (はい): [ソリューション] > [レコード管理] > [ポリシー] > [ラベル ポリシー] > [ラベルの自動適用] 手順 3: この自動ラベル付けポリシーの名前と説明を入力し、[次へ] を選択します。
ステップ 4: "このラベルを適用するコンテンツの種類を選択してください"で、利用可能な条件の 1 つを選択します。
特定の種類の機密情報を含むコンテンツにラベルを自動的に適用する手順 5: 英国の個人識別情報 (PII) データ テンプレートで、英国固有納税者参照番号の機密情報の種類を選択します。
機密情報に対する自動適用保持ラベルポリシーを作成すると、Microsoft Purview データ損失防止 (DLP) ポリシーを作成するときと同じポリシーテンプレートの一覧が表示されます。各テンプレートは、特定の種類の機密情報を検索するように事前構成されています。次の例では、機密情報の種類は "プライバシー"カテゴリと "英国の個人識別情報 (PII) データ"テンプレートから選択されています。

ステップ6:　管理ユニットの割り当て」ページでは、デフォルトの「ワルディレクトリ」のままにしておきます。現在、このポリシーでは管理ユニットはサポートされていません。
手順 7: [作成する保持ポリシーの種類を選択] ページで、[アダプティブ] または [静的] を選択します。
[静的を選択]
ステップ 8: [静的] を選択した場合: [場所の選択] ページで、任意の場所をオンまたはオフに切り替えます。
選択:
Exchangeメール
SharePoint サイト
OneDriveアカウント
Microsoft 365 グループ

Status	Location	Applicable Content	Included	Excluded
On	Exchange mailboxes	Items in user, shared, and resource mailboxes: emails, calendar items with an end date, notes, tasks with an end date, and Public folders. Doesn't apply to items in Microsoft 365 Group mailboxes. More details	All mailboxes Edit	None Edit
On	SharePoint classic and communication sites	Files in classic sites or communication sites or team sites that aren't connected to a Microsoft 365 group, and files in all document libraries (including default ones like Site Assets). More details	All sites Edit	None Edit
On	OneDrive accounts	All files in users' OneDrive accounts. More details	All user accounts Edit	None Edit
On	Microsoft 365 Group mailboxes & sites	Items in the Microsoft 365 Group mailbox, and files in the corresponding group-connected SharePoint team site. Doesn't apply to files in SharePoint classic or communication sites or SharePoint team sites that aren't connected to Microsoft 365 Groups. More details	All microsoft 365 groups Edit	None Edit

ステップ 9: プロンプトに従って保持ラベルを選択し、ポリシーをシミュレーション モードで実行するかオンにするか (選択した条件に該当する場合) を選択して、構成の選択内容を確認して送信します。
参照：
https://learn.microsoft.com/en-us/purview/apply-retention-labels-automatically
https://learn.microsoft.com/en-us/purview/retention-settings#locations

最新問題: **16**
Microsoft 365 テナントがあります。
次のものを作成します。
- 機密ラベル
- 自動ラベル付けポリシー
自動ラベル付けポリシーによって検出されたすべてのデータに機密ラベルが適用されていることを確認する必要があります。
まず何をすべきでしょうか?
A. Enable-TransportRule コマンドレットを実行します。
B. インサイダーリスク管理を有効にします。
C. 学習可能な分類器を作成する
D. ポリシーをシミュレーション モードで実行します。

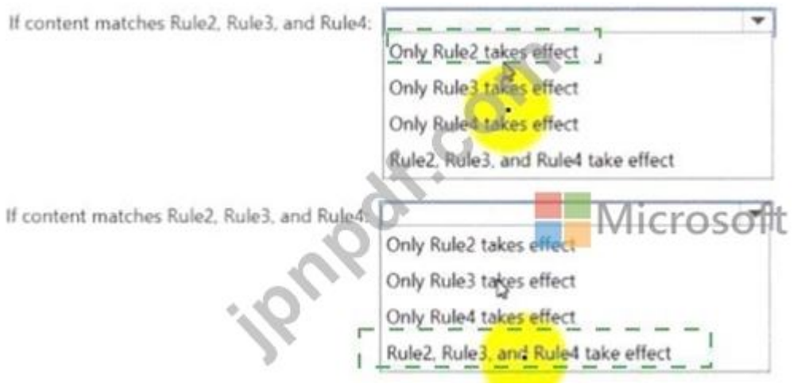
Answer: D (メーッセージを残す)
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-label-automatically を適用します

最新問題: 17
次の表に示すような高度な DIP ルールを持つデータ損失防止 (DIP) ポリシーがあります。

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

コンテンツが複数の高度な DIP ルールに一致する場合にどのルールを適用するかを特定する必要があります。
どのルールを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

Answer:



Explanation:

最新問題: 18

ホットスポットに関する質問

次のファイルを含む Microsoft SharePoint Online サイトがあります。

Name	Modified by	Data loss prevention (DLP) status
File1.docx	Manager1	None
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

次の表に示すように、ユーザーにはサイトの役割が割り当てられます。

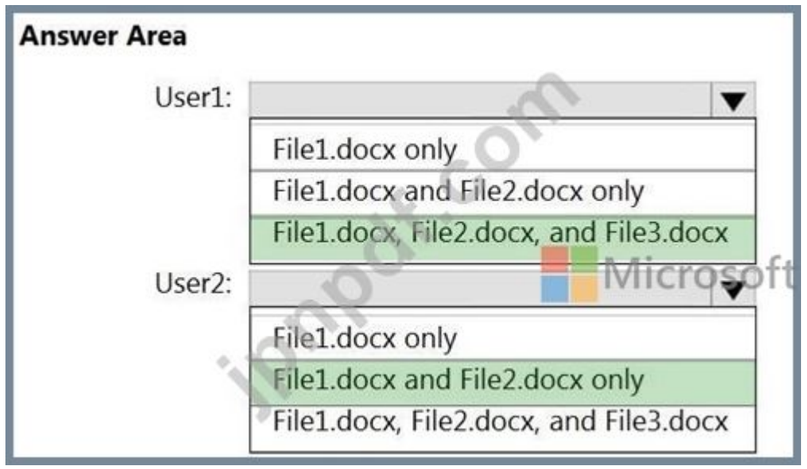
Name	Role
User1	Site owner
User2	Site member

User1 と User2 が開くことができるファイルはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:



Explanation:

ユーザー1: ユーザー1はサイト所有者であるため、サイト内のすべてのファイルに対する完全な権限を持ちます。File3.docx はDLPによってブロックされていますが、サイト所有者はDLP制限を無効にしたり管理したりすることで、すべてのファイルにアクセスできます。

ユーザー2 :ユーザー2はサイトメンバーであるため、ブロックされない限り、ファイルを閲覧および編集する標準権限を持ちます。ファイル1.docxにはDLPアクションが設定されていないため、ユーザー2はアクセスできます。ファイル2.docxはDLPに一致しますが、ブロックされていないため、ユーザー2は引き続きアクセスできます。ファイル3.docxはDLPによってブロックされているため、ユーザー2はアクセスできません。

最新問題**: 19**

ホットスポットに関する質問

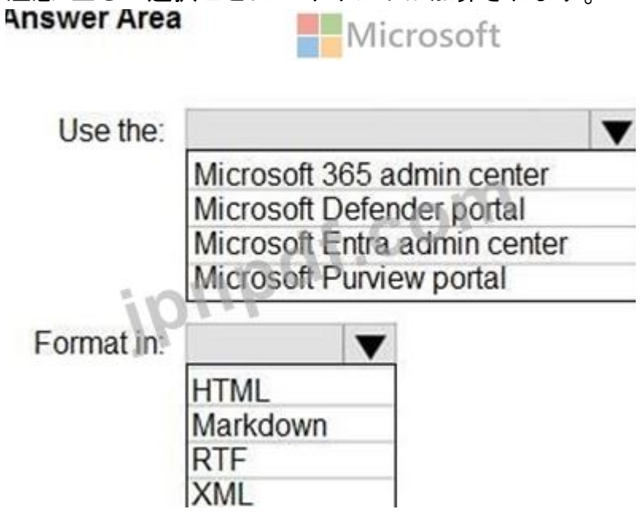
Microsoft 365 E5 サブスクリプションをお持ちです。

インサイダー リスク管理を実装しています。

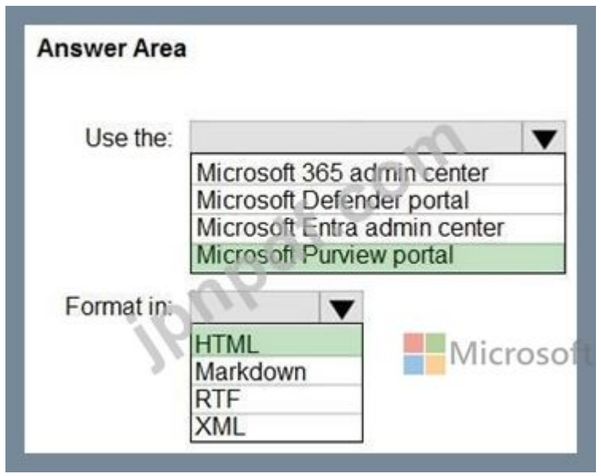
インサイダー リスク管理通知テンプレートを作成し、通知テンプレートのメッセージ本文をフォーマットする必要があります。

テンプレートをどのように構成すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ボックス1: Microsoft Purviewポータル

インサイダーリスク管理通知テンプレートを作成する

新しいインサイダー リスク管理通知テンプレートを作成するには、Microsoft Purview ポータルのインサイダー リスク管理ソリューションの通知作成ツールを使用します。

ボックス2: HTML

通知用のHTML

通知用に単純なテキストベースの電子メール メッセージ以外のものを作成する場合は、通知テンプレートのメッセージ本文フィールドで HTML を使用して、より詳細なメッセージを作成できます。

参照：

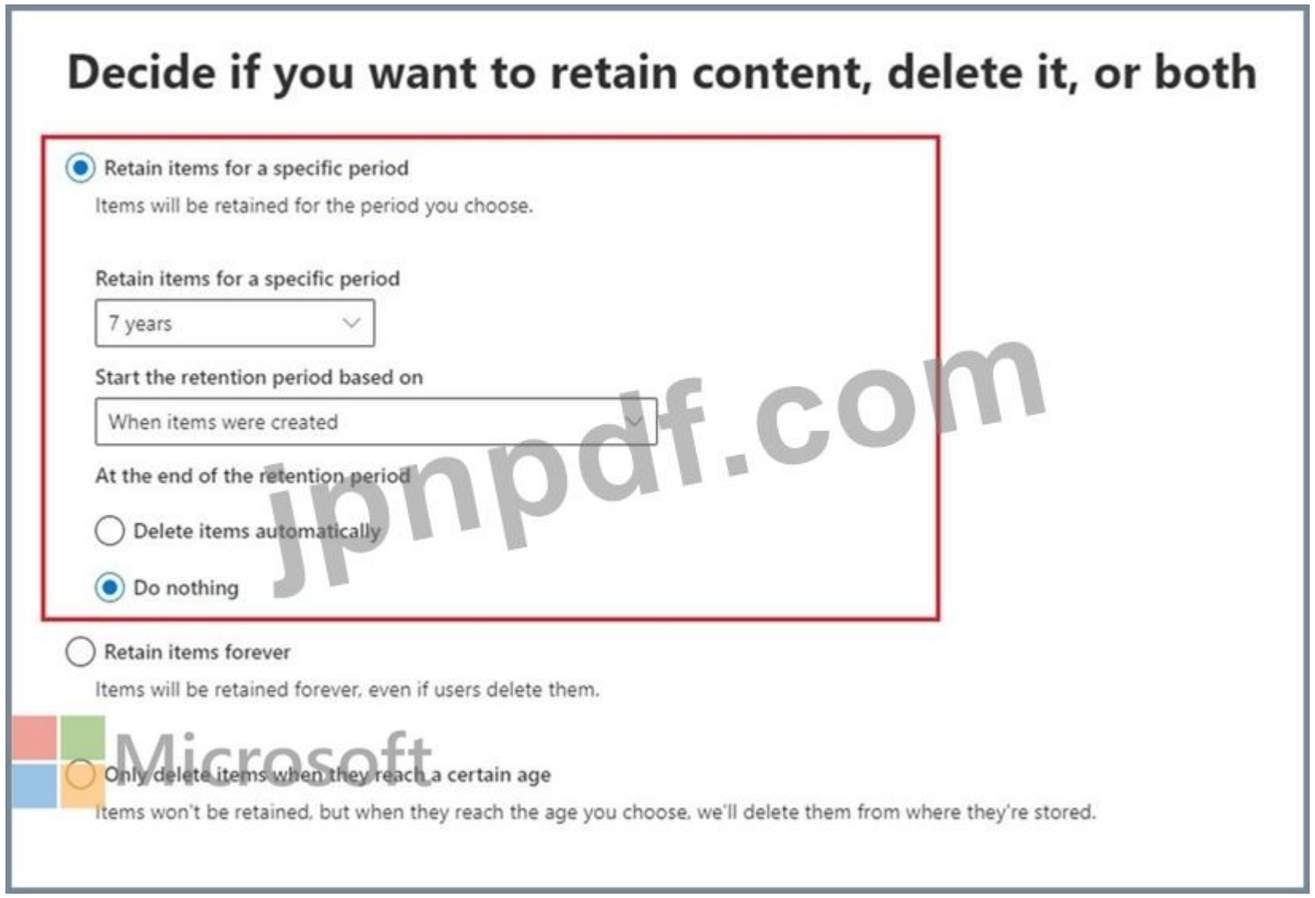
https://learn.microsoft.com/en-us/purview/insider-risk-management-notices

最新問題**: 20**

シミュレーション

ユーザー名とパスワード

必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com"を入力して Enter キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXXX
タスク3
2025 年 6 月 1 日から 10 年間アイテムを保持する保持ラベルを作成する必要があります。
保存期間が経過した後はアイテムを削除する必要があります。
現時点ではラベルを公開したり自動適用したりする必要はありません。
Answer:
保持ラベルを作成するには、Microsoft Purview ポータルにサインインし、"ソリューション"> "レコード管理"> "ポリシー"に移動します。"ラベルの発行"を選択し、プロンプトに従ってラベルの設定、保持期間、および期間終了後の動作を構成します。
ステップ1 :Microsoft Purviewポータルにサインインします。Microsoft 365アプリランチャーにアクセスし、"コンプライアンス"を選択するとアクセスできます。
ステップ 2: Microsoft Purview ポータルで、[ソリューション] > [レコード管理] > [ポリシー] に移動し、[ラベルの公開] をクリックします。
ステップ3: 保持ラベルを作成して構成する
次の選択を行ってください。
アイテムを特定の期間保持する: 10年を選択
保存期間の開始日: 開始日として2025年6月1日を選択
保持期間の終了時: アイテムを自動的に削除します。



参照：
https://learn.microsoft.com/en-us/purview/retention-settings

最新問題**: 21**
Microsoft Teams を使用する Microsoft 565 E5 テナントがあり、User1 と User2 という 2 人のユーザーがいます。User1 と User2 の Teams チャットとチャネルメッセージの場所に適用されるデータ漏洩防止 (DIP) ポリシーを作成します。
どの Teams エンティティに DLP 保護が適用されますか?
A. 1:1/n チャット、一般チャンネル、プライベートチャンネル
B. 1:1/n チャットとプライベートチャンネルのみ
C. 1:1/n チャットと一般チャンネルのみ
Answer: A (メーッセージを残す**)**

最新問題**: 22**
Microsoft 565 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を使用する予定です。
辞職を申し出たユーザーや雇用終了日が近いユーザーによる Microsoft SharePoint Online からのデータ盗難を検出するインサイダー リスク管理ポリシーを作成する必要があります。
まず何をすべきでしょうか?

A. HR データ コネクタを構成します。
B. Office インジケーターを構成します。
C. 物理バッジコネクタを構成します。
D. デバイスを Microsoft Defender for Endpoint にオンボードします。
Answer: A (メーッセージを残す**)**
ステップ1 - シナリオ
辞職届を提出したユーザーや退職が近いユーザーによる SharePoint Online からのデータ盗難を検出する Microsoft Purview Insider リスク管理ポリシーを作成する必要があります。
ステップ2 - インサイダーリスク管理の仕組みを理解する
インサイダーリスクポリシーは、潜在的なリスクイベントを特定するシグナルに基づいています。これらのシグナルには以下が含まれます。
人事データ（退職日 退職通知）。
Office アクティビティ インジケーター (ファイルのダウンロード、共有、印刷)。
デバイスインジケーター (USB へのファイルのコピー、印刷)。
物理的なアクセス (バッジイン/バッジアウト)。
ステップ3 - ここでHR信号が必要な理由
辞職または解雇のリスク イベントを検出するには、まず Microsoft Purview が HR によってフラグが付けられたユーザーを認識する必要があります。
これは、HR システム (Workday、SAP SuccessFactors、または CSV インポート) から従業員の退職/退職データをインポートする HR データ コネクタを構成することによって行われます。
この HR データ コネクタがないと、Purview は従業員の退職または解雇のタイムラインを把握できず、ポリシーは機能しません。
ステップ4 - 他の選択肢を選ばない理由
B). Officeインジケーターの設定 :リスクの高いアクティビティ（ダウンロード、共有）を検出しますが、退職ステータスを判定することはできません。人事シグナルによってリスクのあるユーザーが特定された後に使用されます。
C). 物理バッジコネクタを構成する: 異常な物理アクセスを検出するのに役立ちますが、辞任ベースの検出とは無関係です。
D). Microsoft Defender for Endpoint へのデバイスのオンボード: 人事部門の辞職検出ではなく、デバイス アクティビティ シグナルに必要です。
ステップ5 - Microsoftリファレンス
Microsoftのドキュメントには、「人事部門の退職/解雇トリガーを使用するには、退職および解雇データをインサイダーリスク管理にインポートするように人事コネクタを構成する必要があります。」と記載されています。参考 :Microsoft Purviewにおけるインサイダーリスク管理

最新問題**: 23**
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Description
User1	• User 1 is a regional manager. • User1 is assigned the Reader role. • Three department managers report to User1.
User2	• User2 is the human resources (HR) department manager. • User2 has no Microsoft Entra roles assigned. • Five HR department users report to User2.
User3	• User3 is a developer. • User3 reports to User2. • User3 is the only user in the compliance department. • User3 is assigned the Compliance Administrator role.
User4	• User4 is the assistant of User1. • User4 has no Microsoft Entra roles assigned. • User4 handles a high volume of confidential data on behalf of User1.

Microsoft Purview インサイダー リスク管理では、どのユーザーが潜在的に大きな影響を与えるユーザーとしてフラグが付けられますか?

A. ユーザー1とユーザー2のみ
B. ユーザー2とユーザー3のみ
C. ユーザー1、ユーザー2、ユーザー3、ユーザー4
D. User1、User2、User3のみ
Answer: C (メーッセージを残す**)**

最新問題: **24**
Microsoft 365 E5 サブスクリプションをお持ちです。
次のものにデータ損失防止 (DLP) ポリシーを適用する必要があります。
- Microsoft Exchange Online メールボックス
- Microsoft SharePoint Online サイト
- Microsoft Power BI ワークスペース
- Microsoft OneDriveアカウント
- オンプレミスリポジトリ
目標を達成するために必要な DLP ポリシーの最小数はいくつですか?

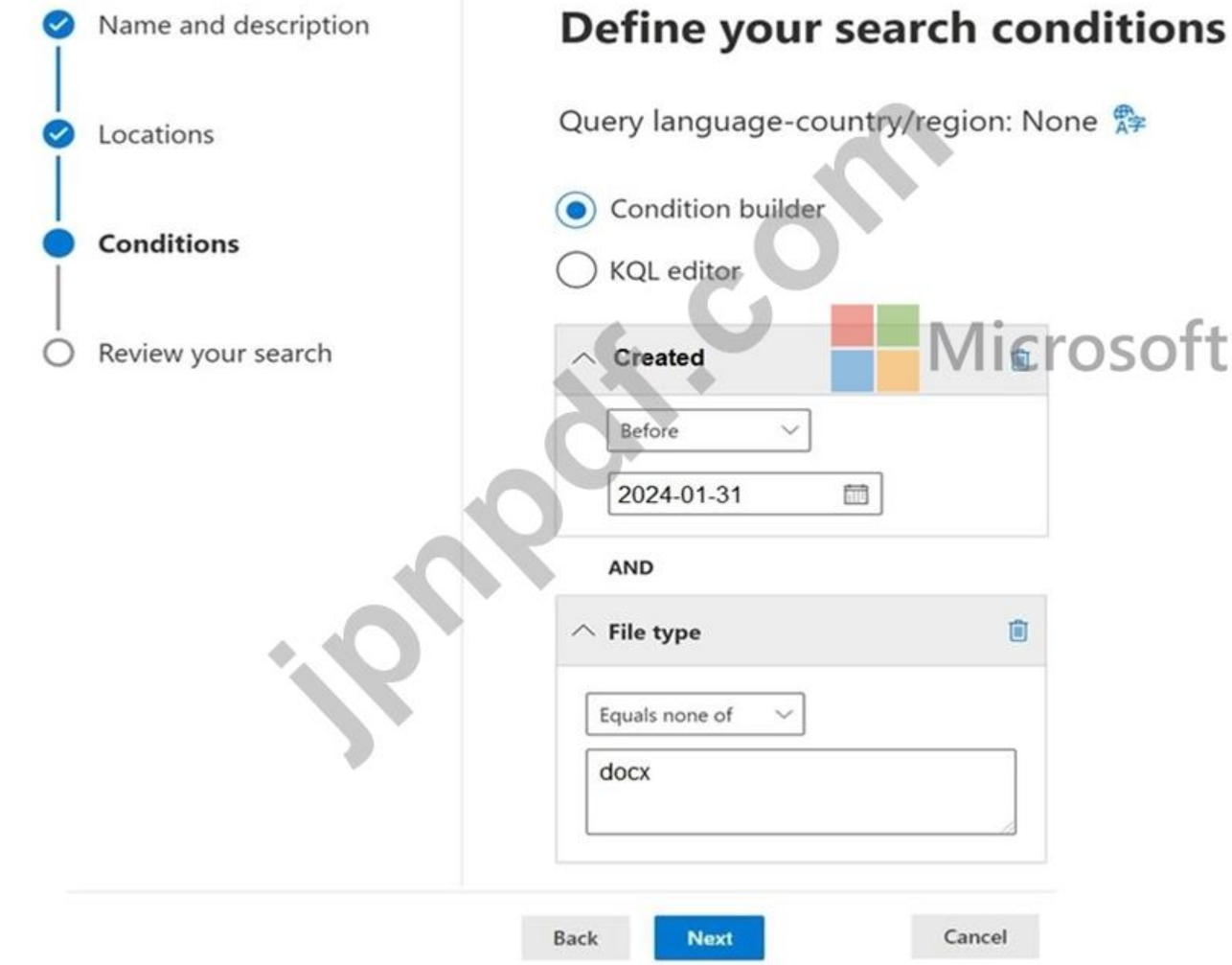
A. 1
B. 5
C. 4
D. 2
E. 3
Answer: D (メーッセージを残す**)**

最新問題: **25**
Microsoft 365 サブスクリプションをお持ちの場合、保持ポリシーを作成し、Exchange Online メールボックスに適用します。
できるだけ早く、アイテム保持ポリシー タグをメールボックス アイテムに割り当てることができるようにする必要があります。
何をすべきでしょうか?
A. Microsoft Purview ポータルから、データ損失防止 (DLP) ポリシーを作成します。
B. Microsoft Purview ポータルからラベル ポリシーを作成します。
C. Exchange Online PowerShell から、Start-ManagedFolderAssistant を実行します。
D. Exchange Online PowerShell から、Start-RetentionAutoTagLearning を実行します。
Answer: (解答を表示する**)**
管理フォルダー アシスタント (MFA) は、保持ポリシーで構成されたメッセージ保持設定を適用および処理する Exchange メールボックス アシスタントです。
Exchange 2013と同様に、Exchange 2016およびExchange 2019の管理フォルダーアシスタントは、常時実行されるスロットルベースのアシスタントです。MFAをスケジュールする必要がなく、MFAによって消費されるシステムリソースを調整できます。管理フォルダーアシスタントは、メールボックスサーバー上のすべてのメールボックスを、ワークサイクルと呼ばれる一定の期間内に処理するように構成できます。既定では、MFAのワークサイクルは1日です サーバー上のすべてのメールボックスは毎日MFAによって処理されます)。
指定されたメールボックスを直ちに処理するように MFA を強制することもできます。
参照：
https://learn.microsoft.com/en-us/exchange/policy-and-compliance/mrm/configure-managed-folder-assistant

最新問題: **26**
ホットスポットに関する質問
Microsoft 365 サブスクリプションをお持ちです。
Site1 という名前の Microsoft SharePoint Online サイトがあります。Site1 には、次の表に示すファイルを含むドキュメント ライブラリがあります。

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

Microsoft Purview コンプライアンス ポータルから、Site1 に対して、次の図に示すように、日付が YYYY-MM-DD 形式の Search1 という名前のコンテンツ検索を作成します。

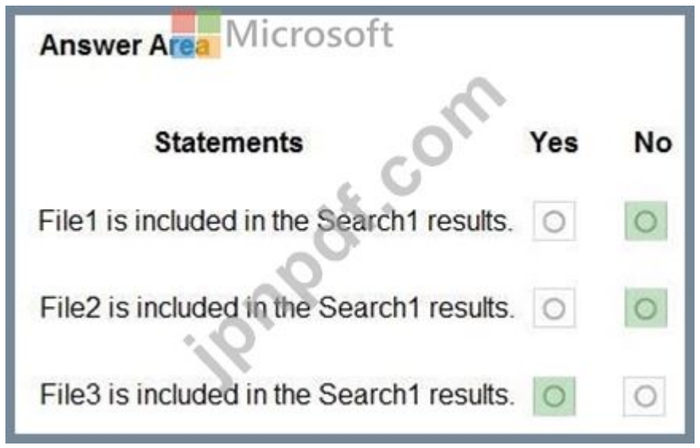


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
File1 is included in the Search1 results.	○	○
File2 is included in the Search1 results.	○	○
File3 is included in the Search1 results.	○	○

Answer:



Explanation:
ボックス1: いいえ
File1 のファイルタイプは DOCX です。
Search1 のファイル タイプは docx のいずれにも該当しません。
File1 は Search1 に含まれません。
ボックス2: いいえ
ファイル2は2024年2月5日に作成されます。
Search1 には、ファイルが 2024 年 1 月 1 日より前に作成されるという条件があります。
File2 は Search1 に含まれません。
ボックス3: はい
File3 のファイルタイプは PNG ですが、docx とは異なります。
ファイル3は2023年5月4日に作成され、2024年1月1日より前です。
File3 は Search1 に含まれます。

最新問題**: 27**
次の表に示すアダプティブ スコープを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type	Query
Scope1	Users	FirstName starts with User
Scope2	SharePoint Online sites	SiteTitle starts with Site

次の表に示す保持ポリシーを作成します。

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

どの保持ポリシーが保存ロックをサポートしていますか?

A. RPolicy2のみ

B. RPolicy3のみ

C. RPolicy1 と RPolicy2 のみ

D. RPolicy1 と RPolicy3 のみ

E. RPolicy1、RPolicy2、およびRPolicy3

Answer: B (メーッセージを残す**)**

保持ロックを使用して、保持ポリシーと保持ラベル ポリシーへの変更を制限します。重要 現在、アダプティブ ポリシー スコープは保持ロックをサポートしていません。

参照：

https://learn.microsoft.com/en-us/purview/retention-preservation-lock

最新問題**: 28**

シミュレーション

ユーザー名とパスワード

必要に応じて次のログイン資格情報を使用します。

ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。

パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。

Microsoft 365 ユーザー名:

admin@WWLx121586.onmicrosoft.com

Microsoft 365 パスワード: XXXXXXXXX

Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin.microsoft.com"を入力して Enter キーを押します。

以下の情報は技術サポートのみを目的としています。

ラボインスタンス: XXXXXXXXX

タスク2

件名に "Falcon"という単語が含まれる外部受信者に送信される電子メールが、"Highly Confidential \ All Employees"という名前の RMS テンプレートを使用して暗号化されるようにする必要があります。

Answer:

件名に "Falcon"を含むメールを外部の受信者に暗号化するには、まずRMS暗号化で情報保護の機密ラベルを作成し、次にPurviewコンプライアンスポータルでメールフロールールを作成し、外部に送信され、件名に "Falcon"と入力します。

タスク 1: 情報保護の機密ラベルを設定する

ステップ 1: Microsoft Purview コンプライアンス ポータルにアクセスし、情報保護に移動します。

ステップ 2: "ラベル"タブを開き、"ラベルの作成"をクリックします。

ステップ3 :ウィザードに従って新しいラベルを設定します。ラベル設定ページで 「暗号化」を有効にし、適用するRMSテンプレートを選択します。
タスク2: メールフロールールを作成する
ステップ 4: Purview コンプライアンス ポータルにアクセスし、メール フロー ルールに移動します。
ステップ 5: [新しいルール] をクリックします。
ステップ 6: 条件を設定します。
条件 1: 「件名に...が含まれる」を選択し、「Falcon」と入力します。
条件 2: 「受信者の所在地...」を選択し、「外部」を選択します。
ステップ7: アクションを設定します。
「機密ラベルを適用...」を選択し、前の手順で作成したラベルを選択します。
ステップ 8: ルールを確認して保存します。
参照 :
https://learn.microsoft.com/en-us/purview/ome

最新問題**: 29**
次の表に示すリソースが含まれる Microsoft 365 IS サブスクリプションがあります。

Name	Type	Member of
User1	User	*None*
User2	User	Group1
Group1	Group	*None*

サブスクリプションには、デバイス 1 という名前の Windows 11 デバイスが含まれており、Microsoft Purview Information Protection クライアントがインストールされています。デバイス i には、次の表に示すリソースが含まれています。

Name	Type	Path
File1.png	File	C:\Temp
File2.docx	File	D:\Folder1
Folder2	Folder	D:\

Label1 という名前の機密ラベルを User1 と Group1 に公開します。
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	○	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	○
User2 can apply Label1 to File2.docx by using the information protection client.	○	○

Answer:
Answer Area

Statements	Yes	No
User1 can apply Label1 to File1.png by using the information protection client.	○	○
User1 can apply Label1 to Folder2 by using the information protection client.	○	○
User2 can apply Label1 to File2.docx by using the information protection client.	○	○

Explanation:

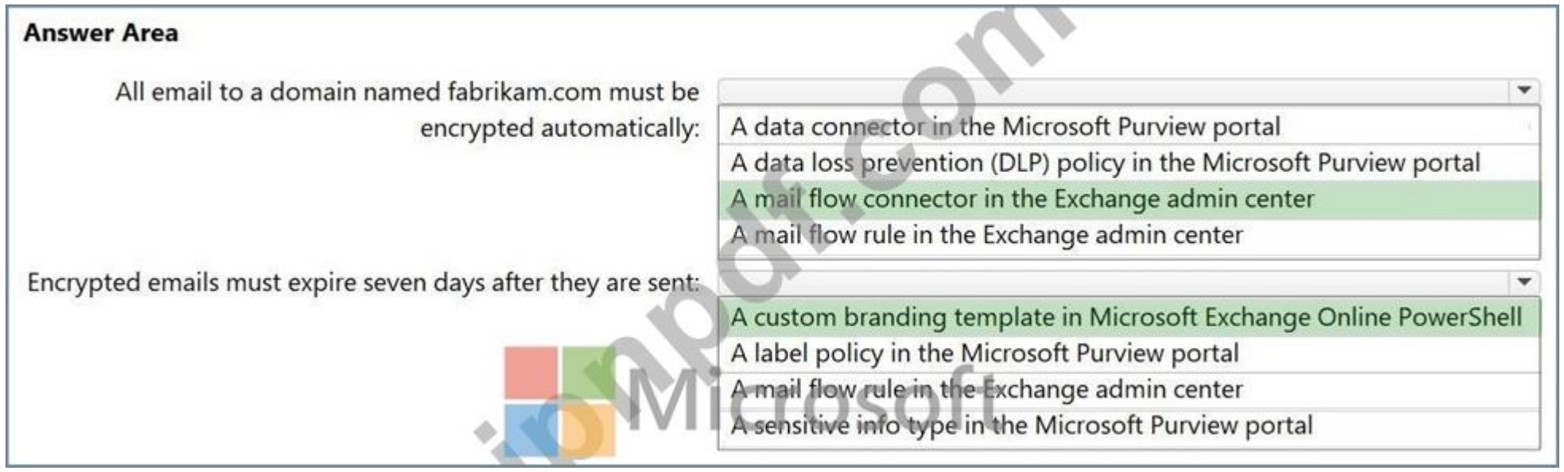
最新問題**: 30**
ホットスポットに関する質問
contoso.com という名前の Microsoft 365 テナントに Microsoft Purview Advanced Message Encryption を実装しています。
次の要件を満たす必要があります。
- fabrikam.comというドメイン宛のすべてのメールは暗号化する必要がある
自動的に。
- 暗号化された電子メールは送信後 7 日で期限切れになります。
各要件に対して何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

All email to a domain named fabrikam.com must be encrypted automatically:
- A data connector in the Microsoft Purview portal
- A data loss prevention (DLP) policy in the Microsoft Purview portal
- A mail flow connector in the Exchange admin center
- A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days after they are sent:
- A custom branding template in Microsoft Exchange Online PowerShell
- A label policy in the Microsoft Purview portal
- A mail flow rule in the Exchange admin center
- A sensitive info type in the Microsoft Purview portal

Answer:



Explanation:

ボックス1: Exchange管理センターのメールフロールール

Microsoft Purview Advanced Message Encryption を使用して特定のドメインに送信されるすべての電子メールを自動的に暗号化するには、管理者はまず、必要な暗号化設定で機密ラベルを構成し、次に Microsoft Purview ポータルで Exchange メール フロー ルール (トランスポート ルールとも呼ばれる) を作成して、ターゲット ドメインに送信される条件を満たすメッセージにその機密ラベルを適用する必要があります。

ボックス 2: Microsoft Exchange Online PowerShell のカスタムブランドテンプレート OME ポータルを使用して暗号化されたメールにアクセスする外部受信者にユーザーが送信するメールに、メッセージの有効期限を設定できます。PowerShell で有効期限を指定する *カスタムブランドテンプレート* を使用することで、受信者が組織から送信した暗号化されたメールを閲覧および返信する際に OME ポータルを使用するように強制できます。

参照：

https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules

https://learn.microsoft.com/en-us/purview/ome-advanced-expiration

最新問題**: 31**

Microsoft 36S ES サブスクリプションをお持ちです。

Microsoft Purview Data Security Posture Management for AI ポータルから、AI データ セキュリティに関する推奨事項を確認します。リスクの高いユーザーが機密データを AI Web サイトに貼り付けたりアップロードしたりできないようにするワンクリック ポリシーを作成する予定ですか? ポリシーはどのように構成しますか? 回答するには、回答領域で適切なオプションを選択します。注: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Answer Area

Explanation:

この質問は、Microsoft Purview の AI 向けデータセキュリティ態勢管理ポータル内でワンクリックポリシーを作成する方法に関するものです。これらのポリシーは、機密データや AI ウェブサイトに関連するリスクを軽減するように設計されています。この特定のシナリオにおける正しい構成は、「まずテストする」を選択し、「デバイス、インスタンス、および SharePoint サイト」にポリシーを適用することです。この構成は、データ損失防止 (DLP) および同様のポリシーの導入に関する Microsoft の推奨プラクティスに基づいています。

ポリシーモード: 「まずはテストしてみましょう」

マイクロソフトは、新しいポリシーを適用する前に、その影響と有効性を評価するためにテストモードの使用を推奨しています。このアプローチにより、ユーザーのワークフローへの意図しない中断を防止できます。テストモードでは、ポリシーは指定されたアクティビティをブロックすることなく監視および監査します。アラートとレポートが生成されるため、管理者はポリシーの動作を確認し、必要な調整を行うことができます。これは「小規模から始めて拡張する」という原則に合致しており、機密データの転送をブロックするように設計されたポリシーが、正当なビジネス活動を意図せず妨げることがないようにします。

ポリシーの範囲: 「デバイス、インスタンス、および SharePoint サイト」

このポリシーは、ユーザーがAIウェブサイトに機密データを貼り付けたりアップロードしたりすることをブロックすることを目的としています。そのためには、あらゆる潜在的なデータ流出ポイントを網羅する包括的な適用範囲が必要です。

デバイス :これはユーザーのローカルデバイスを対象とし、マシン上で実行されているアプリケーションからのデータのアップロードや貼り付けを防止します。これはエンドポイントからのデータ制御に不可欠です。

インスタンス :これは、AIウェブサイトを含むSaaS（Software as a Service）インスタンスを指します。インスタンスにポリシーを適用することで、これらの外部サービスへのデータ転送が監視および制御されます。

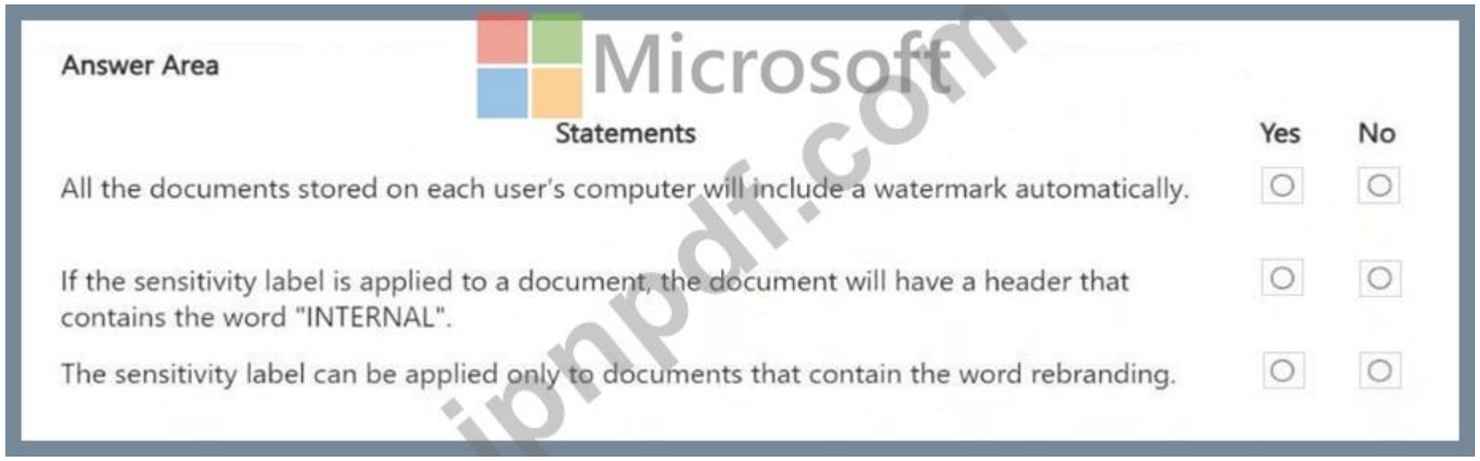
SharePoint サイト :SharePoint に保存されているデータは、機密情報の一般的なソースです。ポリシーの適用範囲に SharePoint サイトを含めることで、これらの場所からデータが直接コピーされ、AI ウェブサイトにアップロードされることを防ぎ、包括的なセキュリティ体制を実現します。

「デバイス、インスタンス、SharePoint サイト」を選択すると、最も一般的なソースと宛先にわたるデータを監視・保護するようにポリシーが構成され、AIサービスへのデータ流出に対する強力な防御が実現します。この包括的なアプローチは、Microsoft 365 における最新のデータセキュリティ戦略の基盤となります。

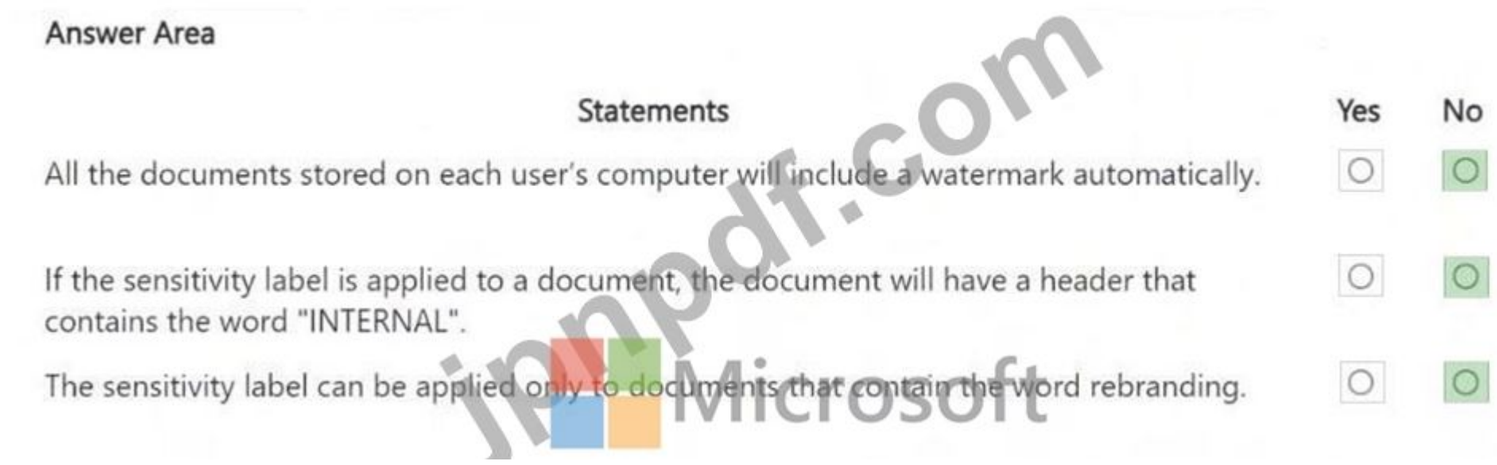
この情報は、Microsoft Purview に関する Microsoft の公式ドキュメント、特にデータ損失防止 (DLP) ポリシーと AI 向けデータセキュリティ態勢管理に関するセクションで確認できます。「まずテスト」というベストプラクティスと、機密データの保護範囲の広範さが一貫して推奨されています。

最新問題: 32
ホットスポットに関する質問
次の図に示すように、Microsoft Entra テナント内のすべてのユーザーに公開されている Microsoft 365 機密ラベルがあります。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。



Answer:



Explanation:
ステートメント 1 - いいえ。機密ラベルにはコンテンツのマーキング (透かし: INTERNAL) が含まれますが、これはラベルが手動または自動で適用されたドキュメントにのみ適用され、デフォルトではすべてのドキュメントに適用されるわけではありません。
ステートメント2 - いいえ。機密ラベルは透かしのみを指定し、ヘッダーは指定しません。ヘッダーマーキングが設定されている場合は、ラベル設定に明示的に表示されます。
ステートメント3 - いいえ。自動ラベル付けが「ebranding」という単語を含むドキュメントにのみラベルを適用するように設定されているという表示はありません。自動ラベル付けはオプション設定であり、明示的な設定が必要です。

最新問題**: 33**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションがあり、User、User2、User3 という 3 人のユーザーが登録されています。このサブスクリプションには、次の表に示すグループが含まれています。

Name	Members
Group1	User1
Group2	User2, User3
Group3	User2, User2, User3

サブスクリプションには、次の表に示すデバイスが含まれています。

Name	Platform
Device1	Windows
Device2	Android
Device3	macOS

すべてのデバイスは Microsoft Purview にオンボードされています。

次の表に示すデータ損失防止 (DLP) ポリシーがあります。

Name	Assigned to	Description
Policy1	Group1	Restrict copying data to USB devices.
Policy2	Group2	Restrict copying data to a clipboard.
Policy3	Group3	Restrict accessing corporate content in Microsoft 365 locations.

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	○	○
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	○	○
When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online.	○	○

Answer:

Answer Area

Statements	Yes	No
When User1 signs in to Device1, the user will be restricted from copying data to a USB storage device.	○	○
When User2 signs in to Device2, the user will be restricted from copying data to the clipboard.	○	○
When User3 signs in to Device3, the user will be restricted from accessing corporate content in Microsoft SharePoint Online.	○	○

Explanation:

ボックス1: はい

User1 は Group1 と Group3 のメンバーです。

デバイス1はWindowsです。

Policy1 は Group1 に割り当てられ、USB [これが意図された単語であると仮定します] デバイスへのコピーを制限します。

注記：

サポートされているアクション: デバイス

DLP に対して、オンボード Windows デバイスに対するこれらのユーザー アクティビティを許可、監査のみ、上書きしてブロック、またはブロック (アクション) するように指示できます。

ボックス2: いいえ
User2 は Group2 と Group3 のメンバーです。
デバイス1はAndroidです。
デバイスアクションは Android デバイスには適用されません。
ボックス3: はい
User3 は、Group 1、Group2、および Group3 のメンバーです。
デバイス1はmacOSです。
Policy3 は Group3 に割り当てられ、Microsoft 365 の場所にある企業コンテンツへのアクセスを制限します。
参照：
https://learn.microsoft.com/en-us/purview/dlp-policy-reference

最新問題**: 34**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーが ChatGPT および Google Gemini に機密データをアップロードできないようにする必要があります。
ソリューションは次の要件を満たす必要があります。
* クレジットカード番号が ChatGPT および Gemini に貼り付けられないようにします。
* 機密データを含む文書が ChatGPT および Gemini にアップロードされないようにします。
各要件に応じてどの Microsoft Purview ソリューションを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:

Explanation:

最新問題: **35**

Microsoft 36S サブスクリプションをお持ちです。

Microsoft Exchange Online では、次の図に示すメール フロー ルールを構成します。

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

メールフロールールは、メッセージにOMEv2保護（OMEv2で保護」）を適用するように構成されています。OMEv2を使用する場合：

コンシューマー メール システム (Gmail など) の受信者はリンクで保護されたメッセージを受信し、コンテンツを表示するには Office 365 メッセージ暗号化ポータルに対して認証する必要があります。

Microsoft 365 の受信者 (外部テナントの場合でも) は Outlook/OWA でネイティブの読み取りエクスペリエンスを得られ、保護されたメッセージは Microsoft 365 ID を使用して自動的に復号化され、直接開かれます。別の OME ポータル ワークフローは必要ありません。

これらの動作は、さまざまな受信者タイプとクライアントにおけるOMEv2ユーザーエクスペリエンスについてMicrosoftによって文書化されています。詳細は、Microsoft Purview Office 365 Message Encryptionの概要と、外部のMicrosoft 365および一般ユーザー向けメール受信者のユーザーエクスペリエンスをご覧ください。

最新問題**: 36**

プロジェクトの終了時に、多数のファイルを含むMicrosoft SharePoint Onlineライブラリにプロジェクトドキュメントをアップロードします。以下は、プロジェクトドキュメントのファイル名の例です。

- aei_AA989.docx
- bci_WS098.docx
- cei_DF112.docx
- ebc_QQ454.docx

- ecc_BB565.docx
この命名形式を使用するすべてのドキュメントには、プロジェクト ドキュメントというラベルを付ける必要があります。
自動適用保持ラベル ポリシーを作成する必要があります。
ファイルを識別するには何を使用すればよいですか?
A. 機密情報の種類
B. 保持ラベル
C. 学習可能な分類器
Answer: A (メーッセージを残す**)**

最新問題**: 37**
Trainable1 という名前のトレーニング可能な分類子を含む Microsoft 365 E5 サブスクリプションがあります。
次の表に示す項目を作成する予定です。

Name	Type
Label1	Sensitivity label
Label2	Retention label
Policy1	Retention label policy
DLP1	Data loss prevention (DLP) policy

Trainable 1 を使用できるアイテムはどれですか?
A. ラベル2のみ
B. ラベル1とラベル2のみ
C. Label1とPolicy1のみ
D. ラベル2、ポリシー1、DLP1のみ
E. ラベル1、ラベル2、ポリシー1、およびDLP1
Answer: D (メーッセージを残す**)**
Microsoft Purview のトレーニング可能な分類器は、コンテンツのパターンに基づいて非構造化データを自動的に識別・分類するために使用されます。この分類器は、以下の用途で使用できます。
1. 保持ラベル（ラベル2）→ サポートされています
*トレーニング可能な分類子を保持ラベルにリンクして、ドキュメントを自動的に分類し、保持ポリシーを適用できます。
2. 保持ラベルポリシー（ポリシー1)→サポート
*保持ラベル ポリシーは、トレーニング可能な分類子を自動的に使用するなど、保持ラベルを適用する方法と場所を定義します。
3. データ損失防止（DLP）ポリシー（DLP1）→サポート
*トレーニング可能な分類子を DLP ポリシーで使用して、機密コンテンツを自動的に検出し、保護することができます。

最新問題**: 38**
次の図に示すように、Alert2 という名前の Microsoft 365 アラートがあります。

Alertのステータスを管理する必要がありますか？Aletteをどのステータスに変更できますか？

A. 調査のみ

B. 調査中。アクティブ、または却下

C. 却下のみ

D. ステータスを変更できません。

E. アクティブまたは調査中のみ

Answer: (解答を表示する**)**

最新問題: **39**

ホットスポット

Microsoft 365 E5 サブスクリプションには、Group1 と Group2 という 2 つの Microsoft 365 グループが含まれています。どちらのグループも以下のリソースを使用しています。

グループメールボックス

Microsoft Teams チャネル メッセージ

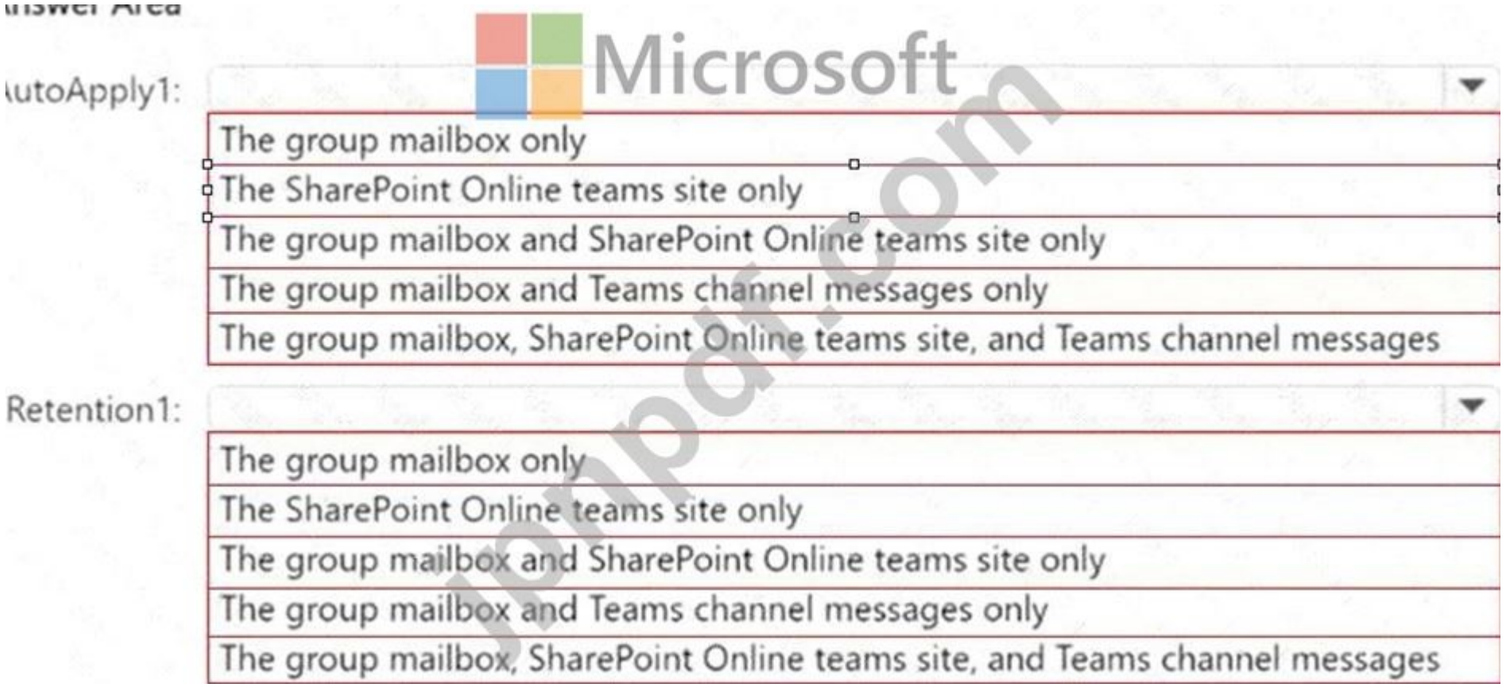
Microsoft SharePoint Online チームサイト

次の表に示すオブジェクトを作成します。

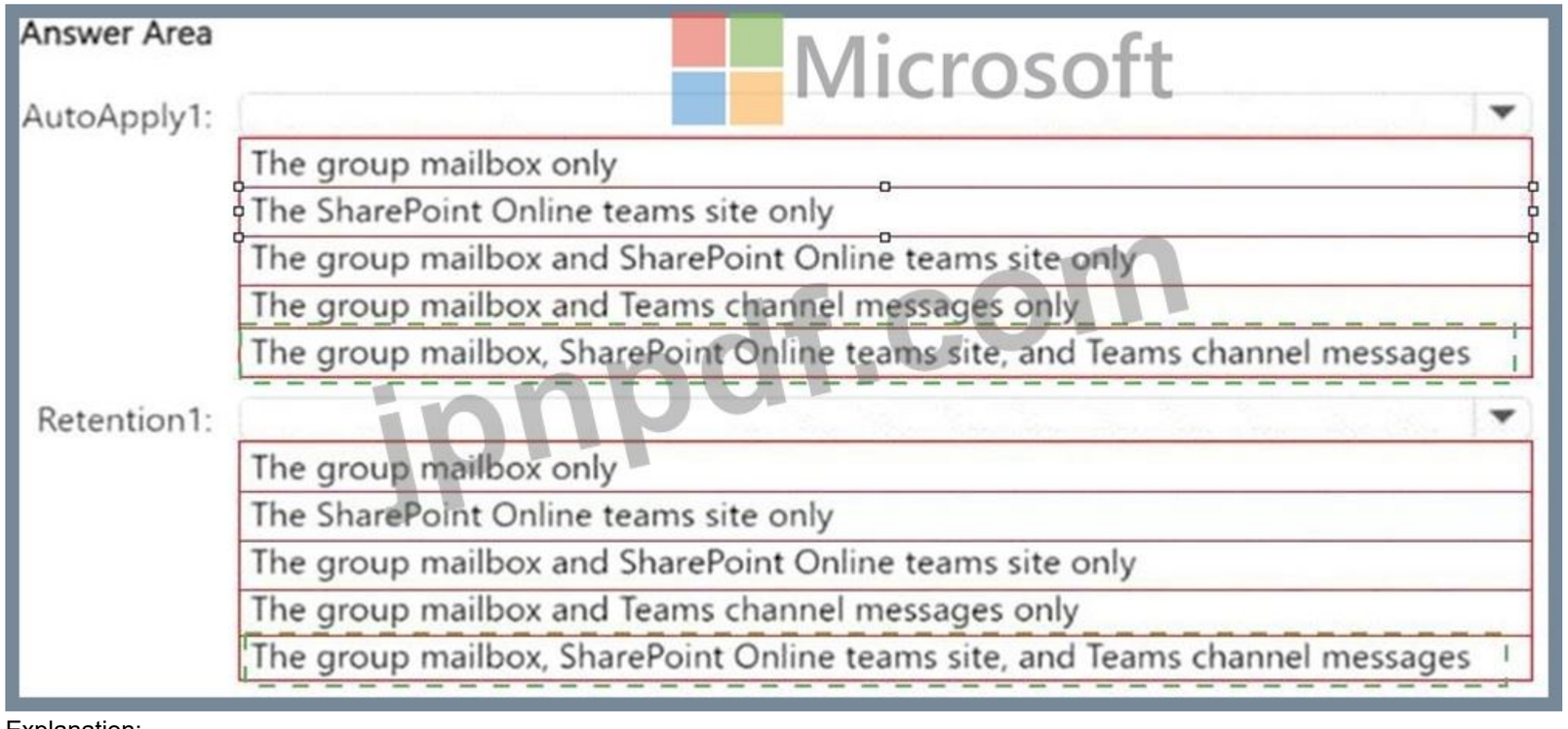
Name	Type	Description
RLabel1	Retention label	*None*
AutoApply1	Auto-labeling policy	Applies RLabel1 to Group1
Retention1	Retention policy	Applied to Group2

AutoApply1 と Retention1 はどのリソースに適用されますか? 回答するには、回答領域で適切なオプションを選択してください。

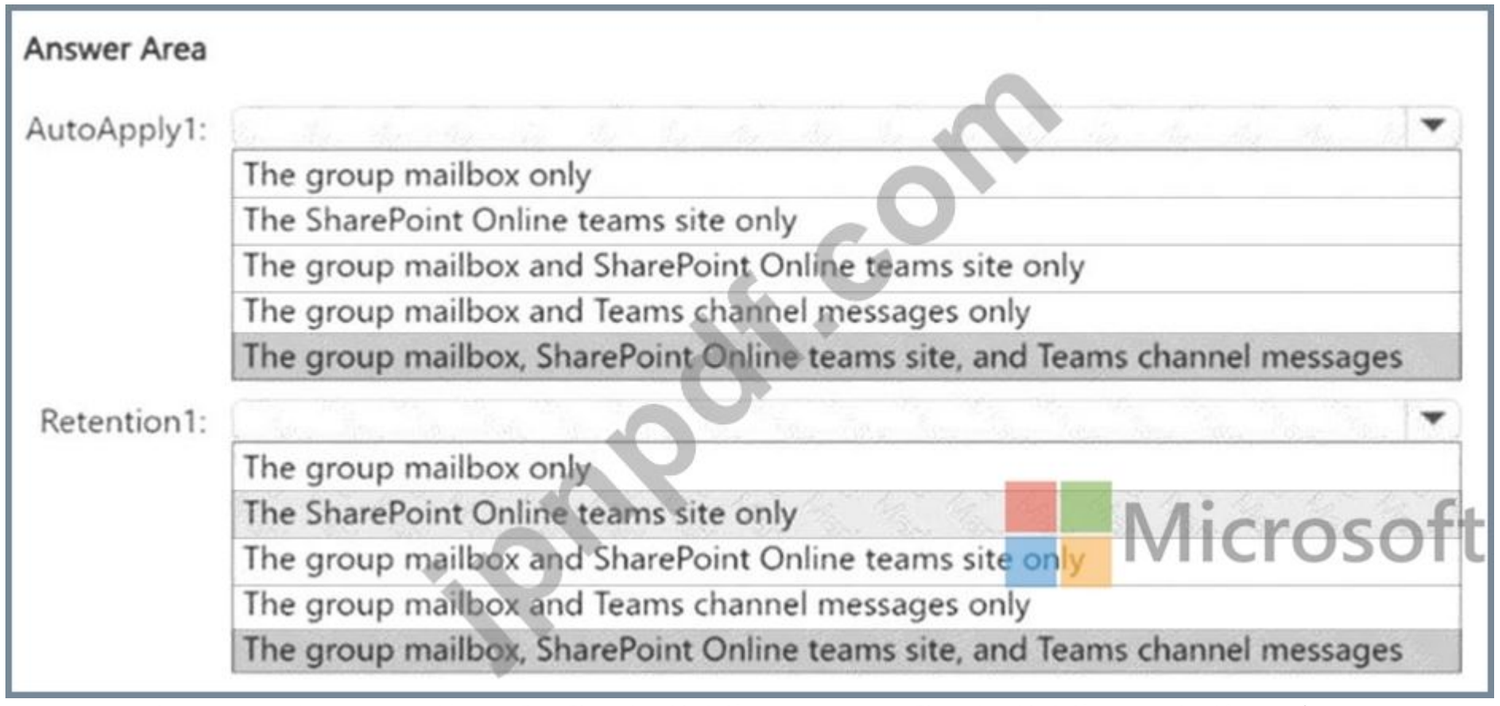
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

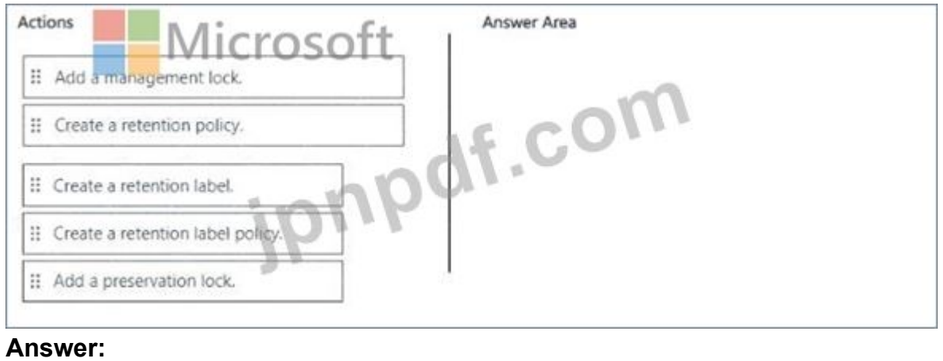


Explanation:

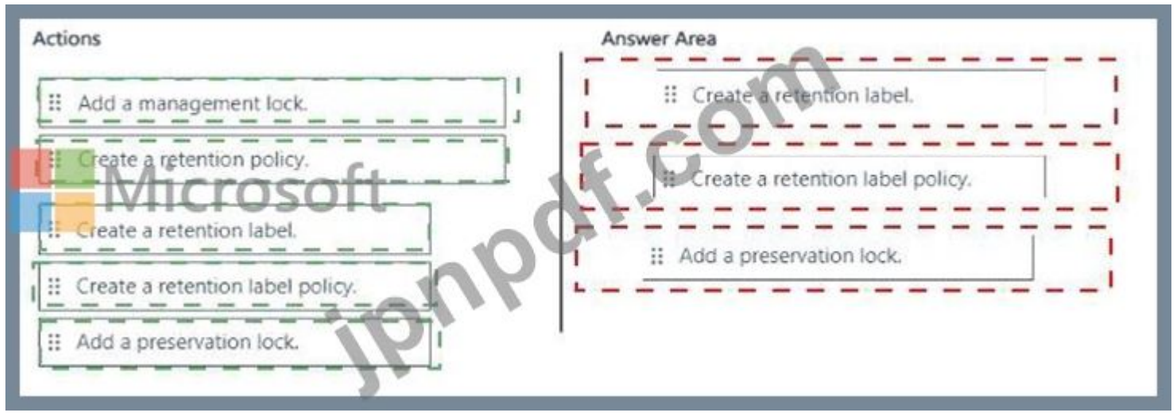


AutoApply1 は、RLabel1 を Group1 に適用する自動ラベル付けポリシーです。自動ラベル付けポリシーは、グループ リソース用に構成されている場合、グループ メールボックス、SharePoint Online サイト、および Teams チャネル メッセージ全体に保持ラベルを適用できます。
Retention1 は Group2 に適用される保持ポリシーです。Microsoft 365 グループの保持ポリシーは、グループ メールボックス、SharePoint Online チーム サイト、Teams チャネル メッセージなど、すべてのグループ リソースに適用されます。
AutoApply1 と Retention1 はどちらもグループ全体に影響するため、グループ メールボックス、SharePoint Online チーム サイト、Teams チャネル メッセージなど、関連するすべてのリソースに適用されます。

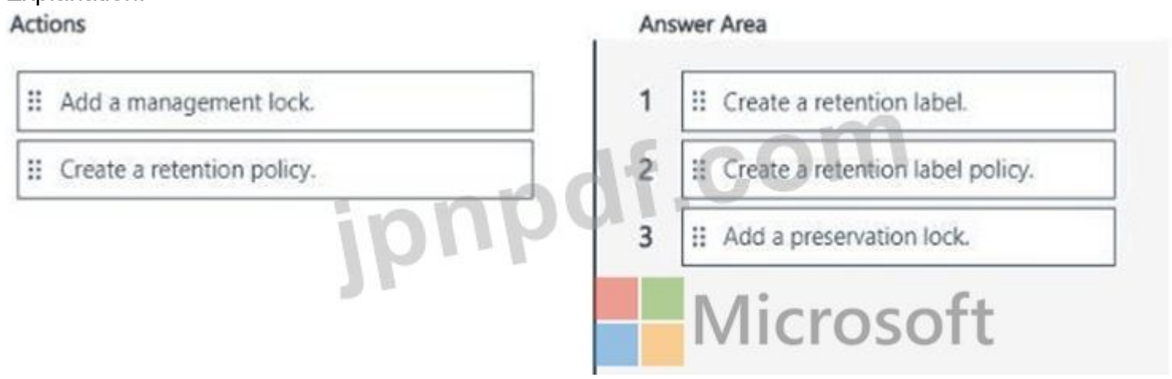
最新問題: **40**
Microsoft 365 テナントがあります。
新しい規制要件では、特許IDを含むすべての文書にラベルを付け、10年間保管した後、削除することが定められています。保管設定を適用するために使用するポリシーは、いかなる者によっても無効化または削除されてはなりません。
規制要件を実装する必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:



Explanation:



最新問題: 41

ホットスポット

次の表に示すデバイス構成を含む Microsoft 365 E5 サブスクリプションがあります。

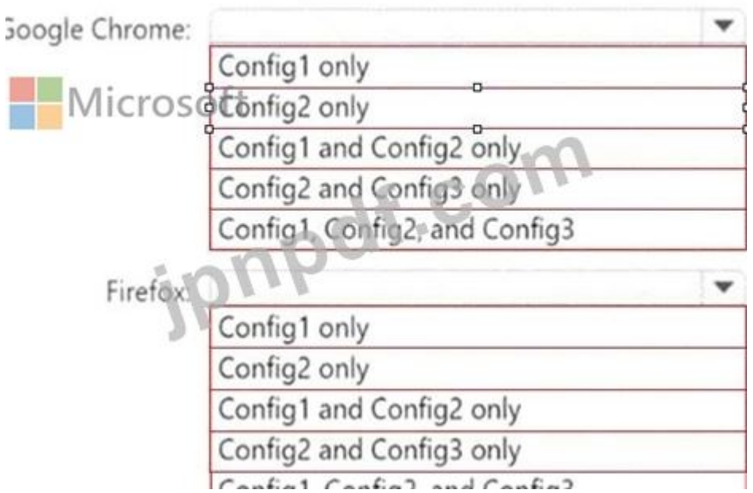
Name	Platform
Config1	Windows 11
Config2	macOS
Config3	Android

各構成では、Google Chrome または Firefox のいずれかをデフォルトのブラウザとして使用します。

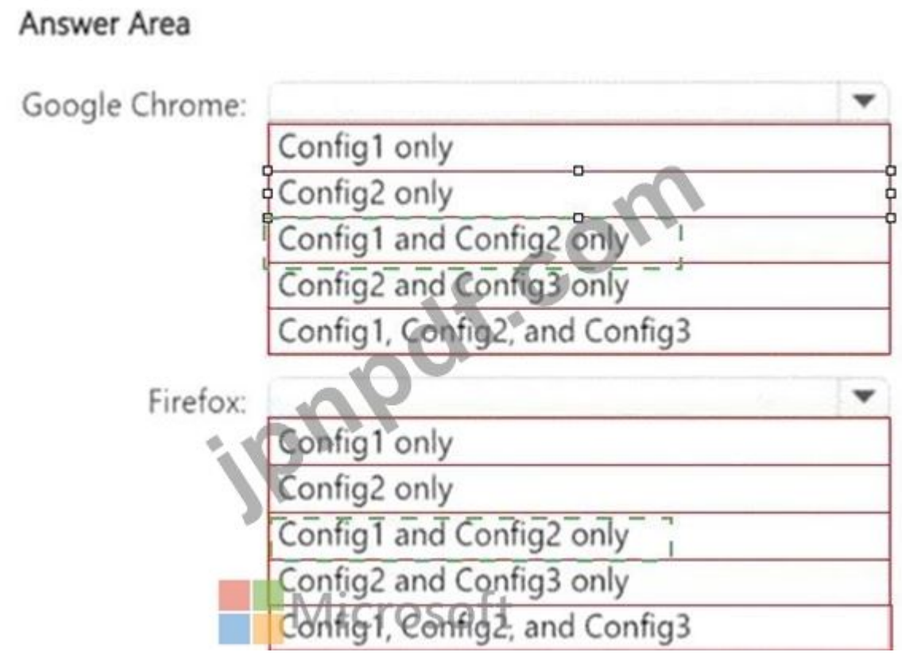
Microsoft Purview を実装し、構成に Microsoft Purview ブラウザ拡張機能を展開する必要があります。

各拡張機能はどの構成にデプロイできますか? 回答するには、回答領域で適切なオプションを選択してください。

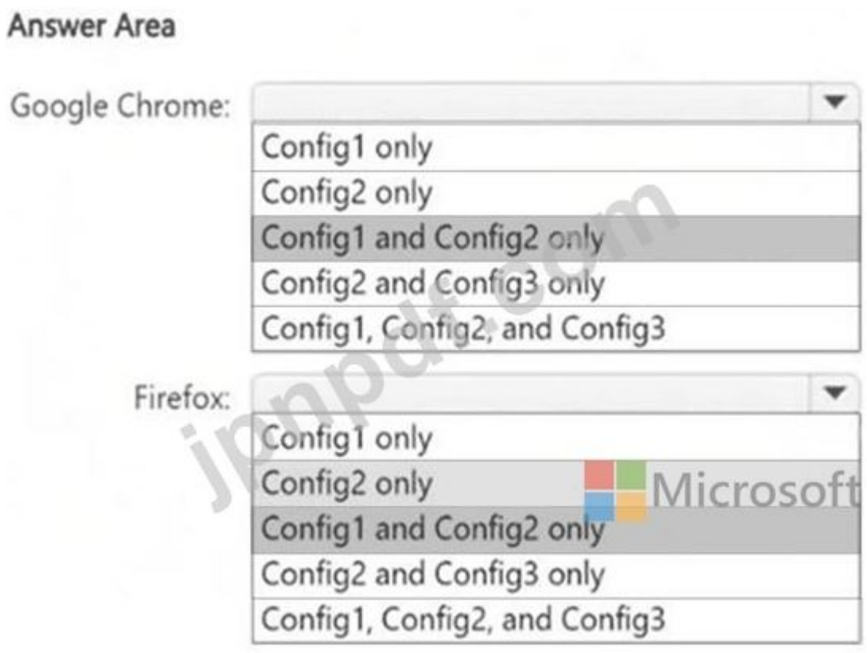
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



エンドポイント DLP 用の Microsoft Purview ブラウザー拡張機能は以下でサポートされています。
Windows 10/11 (構成1)
macOS (構成2)
Android (Config3) ではサポートされていません
Microsoft Purview は Android 上のブラウザ拡張機能をサポートしていないため、Config3 は Google Chrome と Firefox の両方から除外されます。

最新問題: **42**
デバイスの場所にデータ損失防止 (DIP) ポリシーが適用されています。このポリシーは、米国のパスポート番号を含む文書を保護します。ユーザーから、Pokeyのせいで旅行管理ウェブサイトに文書をアップロードできないという報告があります。
ユーザーが旅行管理ウェブサイトにドキュメントをアップロードできるようにする必要があります。保護されたコンテンツが他の場所にアップロードされるのを防ぐソリューションが必要です。
どの Microsoft 365 エンドポイント データ損失防止 (エンドポイント DIP) 設定を構成する必要がありますか?
A. サービスドメイン
B. 許可されていないブラウザ
C. ファイルパスの除外
D. 許可されていないアプリ
Answer: A (メーッセージを残す**)**
問題: エンドポイント DLP によってブロックされているため、ユーザーは米国のパスポート番号が記載された文書を正当な旅行管理 Web サイトにアップロードできません。
解決策: エンドポイント DLP でサービス ドメインを構成します。これにより、機密情報のアップロードが許可される特定の信頼できるドメインを定義しながら、承認されていない他のドメインへのアップロードをブロックできるようになります。
他の人はなぜダメなのですか?
許可されていないブラウザ: ブラウザを制限/ブロックリストしますが、ここでの問題ではありません。
ファイル パスの除外: Web アップロードとは関係なく、ローカル フォルダー/パスを監視から除外します。
許可されていないアプリ: ブラウザベースのサイトではなく、デスクトップ アプリを制限します。

参照：
Microsoft Learn: エンドポイント DLP のサービス ドメインを構成する

最新問題: **43**
社内でMicrosoft Purview Advanced Message Encryptionの機能をテストする必要があります。テストでは、以下の情報を確認する必要があります。
* 取得したデフォルトのテンプレート名
* 暗号化と復号化の検証ステータス
どの PowerShell コマンドレットを実行する必要がありますか?
A. テスト-OAuth接続
B. テスト-ClientAccessRule
C. テスト-IRMConfiguration
D. テストメールフロー
Answer: C (メーッセージを残す**)**
Microsoft Purview Advanced Message Encryption（Azure Information Rights Management を基盤とする）をテストするには、Test-IRMConfiguration コマンドレットを使用します。このコマンドレットは、構成、テンプレートの可用性、暗号化/復号化の状態を検証します。
Test-OAuthConnectivity # は OAuth 認証をテストします。
Test-ClientAccessRule # はクライアント アクセス ルールをテストします。
Test-Mailflow # メール ルーティングをテストします。
参考: Test-IRMConfiguration コマンドレット

最新問題: **44**
Microsoft 36515 サブスクリプションがあり、その中に Site1 という名前の Microsoft SharePoint Online サイトが含まれています。Site1 には、File1、File2、および File3 という名前の 3 つのタイルが含まれています。
次の表に示すデータ損失防止 (DIP) ポリシーを作成します。

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

各タイルの DIP ルールの一致を次の表に示します。

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

アクティビティ エクスプローラーに追加される DIP ポリシー一致イベントの数はいくつですか。また、DLP インシデント レポートに追加されるポリシー一致の数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。

Answer:

Explanation:

最新問題**: 45**
ホットスポットに関する質問
Microsoft Purview Audit (Premium) を使用する Microsoft 365 E5 サブスクリプションをお持ちで、
10 年間の監査ログ保持アドオン ライセンス。
サブスクリプションには、次の表に示す監査保持ポリシーが含まれています。

Name	Users	Record type	Activities	Duration	Priority
RP1	User1	SharePoint	Created site collection	1 Year	30
RP2	User1	SharePoint	*None*	3 Years	20
RP3	User1	SharePoint	Created site collection	3 Years	40
RP4	User1	SharePoint	Renamed site	6 Months	10

SharePoint Online 管理センターから、User1 は次の表に示すアクションを実行します。

Name	Description
Action1	Archives a site
Action2	Creates a site collection
Action3	Renames a site

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	○
Action2 will be retained for three years.	○	○
Action3 will be retained for six months.	○	○

Answer:

Answer Area

Statements	Yes	No
Action1 will be retained for one year.	○	●
Action2 will be retained for three years.	○	●
Action3 will be retained for six months.	●	○

Explanation:

ボックス1: いいえ

アクション1はサイトをアーカイブします。

アーカイブ サイトのアクティビティは、どの監査保持ポリシーにも指定されていません。

指定されたアクティビティがないため、RP2 が適用されます。

RP2の有効期間は3年です。

ボックス2: いいえ

アクション2はサイト コレクションを作成します。

RP1 および RP3 は、サイト コレクション アクティビティの作成に適用されます。

RP1 の優先度は 30、RP3 の優先度は 40 です。
RP1 の方が優先度が高くなります (値が低くなります)。
RP1 の有効期間は 1 年です。
ボックス3: はい
アクション3はサイトの名前を変更します。
RP4 は名前が変更されたサイト アクティビティに適用されます。
RP4 の有効期間は 6 か月です。
参照：
https://learn.microsoft.com/en-us/purview/監査ログ保持ポリシー

最新問題**: 46**
Sensitivity1 という名前の機密ラベルを持つ Microsoft 365 E5 サブスクリプションがあります。
Microsoft Exchange Online メールボックスに Sensitivity1 を適用する自動ラベル付けポリシーを作成する予定です。
2 月 1 日に、自動ラベル付けポリシーを作成し、デフォルト設定を使用してシミュレーション モードを有効にします。
シミュレーション モードではポリシーは変更されません。
このポリシーはいつ最初に有効になりますか?
A. 決して
B. 2月15日
C. 2月6日
D. 2月2日
Answer: B (メーッセージを残す)

最新問題**: 47**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーは次のアプリを使用してメールボックスにアクセスします。
* Microsoft 365 向け Outlook
* ウェブ上のOutlook
* Outlook Mobile（iOS、Android）
次の設定を持つ、DLP1 という名前のデータ損失防止 (DLP) ポリシーを作成します。
* 場所; Exchangeメール
* ステータス: オン
* ユーザー通知: オン
* ポリシーヒントでユーザーに通知: 有効
DIP1 を使用してコンテンツが一致したときにポリシーヒントを表示するアプリはどれですか?

A. Microsoft 365 向け Outlook のみ
B. Web 上の Outlook のみ
C. Microsoft 365 用 Outlook および Web 上の Outlook のみ
D. Microsoft 365 用 Outlook および Outlook Mobile (iOS、Android) のみ
E. Microsoft 365 の Outlook、Web 上の Outlook、および Outlook Mobile (iOS、Android)
Answer: C (メーッセージを残す)
DLP のポリシー ヒント: ポリシー ヒントは、ユーザーのアクション (機密コンテンツを電子メールで送信するなど) が DLP ポリシーと競合する場合に表示されるメッセージです。
Exchange 電子メールの場所については、次のアプリでポリシー ヒントがサポートされています。
Microsoft 365 用 Outlook (デスクトップ クライアント) #
ウェブ上の Outlook (OWA) #
Outlook Mobile (iOS/Android) # モバイルアプリではポリシーのヒントは表示されません。代わりに、DLPアクション（ブロック/制限）が表示されます。
/send incident report) は引き続き適用されますが、ユーザーにはポリシーヒント通知は表示されません。
したがって：
サポート対象: Microsoft 365 用 Outlook、Outlook on the web。
サポートされていません: Outlook モバイル アプリ。
参照：
Microsoft Learn: DLP のポリシーのヒント
引用: 「ポリシー ヒントは、Outlook on the web および Outlook 2013 以降でサポートされています。ポリシー ヒントは Outlook モバイル アプリではサポートされていません。」

最新問題**: 48**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を実装する予定です。
HR データ コネクタを実装します。
データ コネクタによってインポートされるデータを準備する必要があります。
どのような形式でデータを準備すればよいですか?
A. JSON
B. CSV
C. TSV
D. XML
E. PRN
Answer: (解答を表示する)
Microsoft Purview Insider Risk Management を導入し、HR データコネクタを使用する場合は、CSV（カンマ区切り値）形式でHRデータを準備する必要があります。Microsoft Purview は、ユーザーの雇用情報、退職日、役割変更、その他のHR関連属性のインポートにCSVファイルに対応しているため、この形式が必須となります。

最新問題**: 49**
次の表に示すように、Microsoft Defender for Endpoint にオンボードされたデバイスを持つ Microsoft 365 E5 テナントがあります。

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

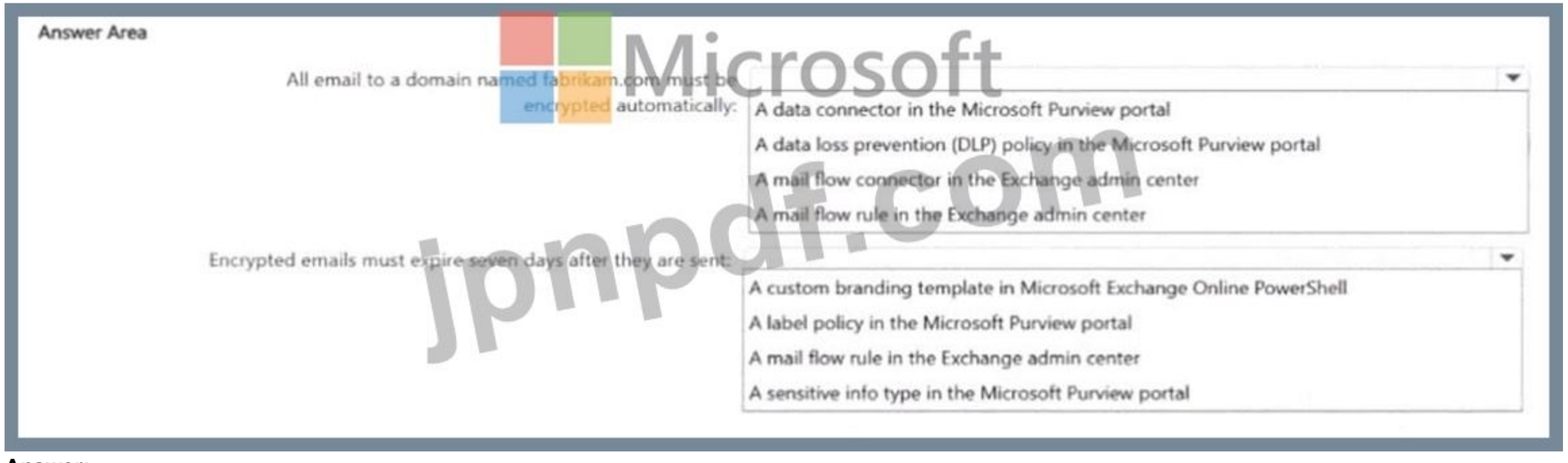
Microsoft 365 エンドポイント データ損失防止 (エンドポイント DLP) の使用を開始する予定です。
エンドポイント DLP をサポートするデバイスはどれですか?
A. デバイス1のみ
B. デバイス1とデバイス2のみ
C. デバイス1とデバイス4のみ
D. デバイス1、デバイス2、デバイス4のみ
E. デバイス1、デバイス2、デバイス3、デバイス4
Answer: B (メーッセージを残す**)**
Microsoft 365 エンドポイントデータ損失防止 (エンドポイント DLP) は、Windows 10 および Windows でのみサポートされています。
11台のデバイス。現時点ではmacOSとiOSには対応していません。
提供された表から:
デバイス1 (Windows 11) - サポートされています
デバイス2 (Windows 10) - サポートされています
デバイス3 (iOS) - サポートされていません
デバイス4 (macOS) - サポートされていません
したがって、デバイス 1 とデバイス 2 のみがエンドポイント DLP をサポートします。

最新問題: **50**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
最近、会社の開発者が Azure ストレージ アカウント キーをプレーン テキストで第三者に電子メールで送信していることが分かりました。
Azure ストレージ アカウント キーを電子メールで送信する場合は、電子メールが暗号化されていることを確認する必要があります。
解決策: Exchange 電子メールの場所のみが選択されたデータ損失防止 (DLP) ポリシーを作成します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**
Exchange 管理センターのメールフロー ルールとセキュリティ センターの DLP ポリシーはどちらも同じことを実現でき、メッセージ本文で検出された機密情報の種類に基づいて電子メールを暗号化します。

最新問題: **51**
Microsoft 365 E5 サブスクリプションをお持ちです。

Label1 という名前の機密ラベルを作成し、Label1 をすべてのユーザーとグループに公開します。
SharePoint サイトには次のファイルがあります。
* ファイル1.doc
* ファイル2.docx
* ファイル3.xlsx
* ファイル4.txt
Label1 を適用できるファイルを特定する必要があります。
どのファイルを識別する必要がありますか?
A. File2.docx と File3.xlsx のみ
B. File1.doc、File2.docx、File3.xlsx、およびFile4.txt
C. File1.doc、File2.docx、およびFile3.xlsxのみ
D. File2.docxのみ
Answer: (解答を表示する**)**

最新問題**: 52**
contoso.com という名前の Microsoft 365 テナントに Microsoft Purview Advanced Message Encryption を実装する場合、次の要件を満たす必要があります。
* (abrikam.com というドメイン宛のすべてのメールは自動的に暗号化される必要があります。
* 暗号化されたメールは送信後7日で期限切れになります
各要件に対して何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

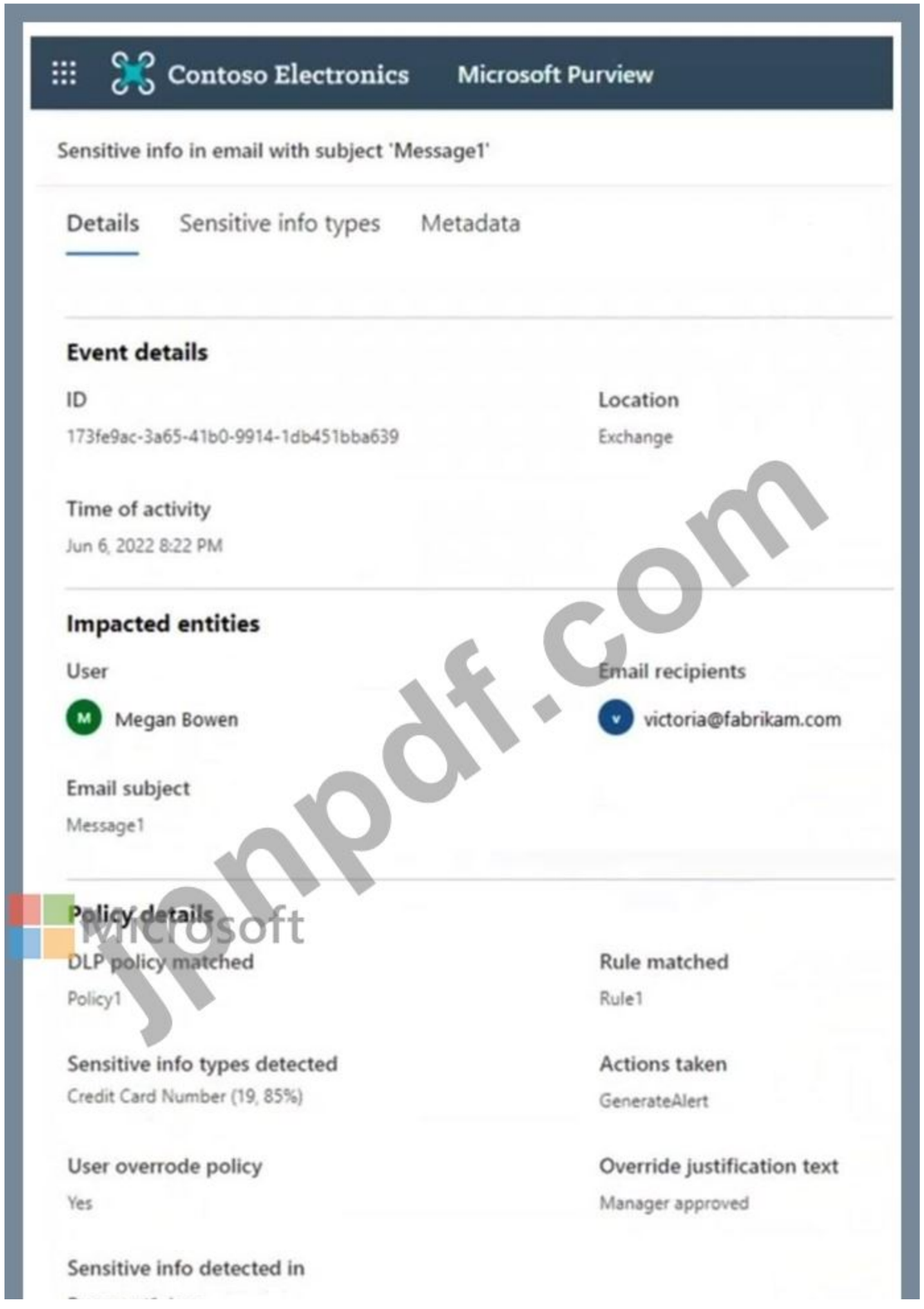
Explanation:

要件1 - fabrikam.comへのすべてのメールを自動的に暗号化する
特定の外部ドメイン (fabrikam.com) に送信されるメールの暗号化を強制するには:
Exchange 管理センター (EAC) でメール フロー ルール (トランスポート ルール) を構成します。
このルールは、メッセージが受信者のドメインなどの条件に一致する場合に、Office Message Encryption (OME) を自動的に適用できます。
参考: メールフロールールを定義して電子メールメッセージを暗号化する
正解: Exchange管理センターのメールフロールール
要件2 - 暗号化されたメールは7日後に期限切れになる必要がある
暗号化された電子メールの有効期限とアクセス制御を構成するには:
暗号化設定で Microsoft Purview 機密ラベルを使用します。
Purview ポータルのラベル ポリシーでは、暗号化を強制したり、アクセス権を設定したり、有効期限を定義したりできます (例: 7 日後にアクセスを取り消す)。
機密情報の種類またはメール フロー ルールでは有効期限を構成できません。
参考: 機密ラベルの暗号化設定を構成する
正解: Microsoft Purview ポータルのラベル ポリシー

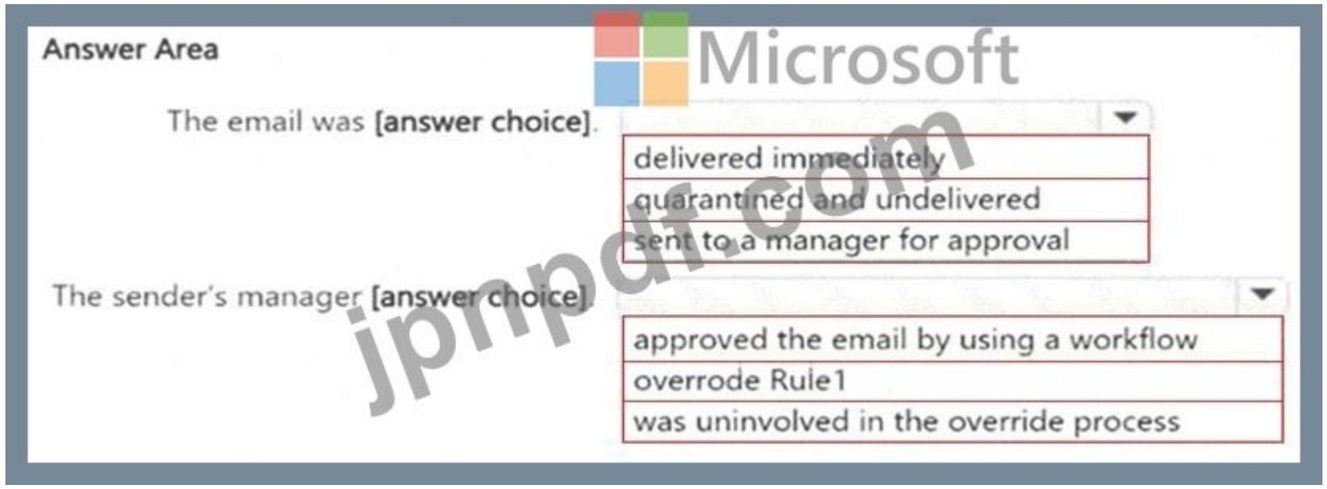
最新問題**: 53**
Microsoft 365 E5 サブスクリプションがあり、そこには Channel1 という Microsoft Teams チャネルが含まれています。Channel1 には研究開発ドキュメントが含まれています。
サブスクリプションに Microsoft 365 Copilot を実装する予定です。
Channel1 に保存されているファイルの内容が、Copilot によって生成された回答に含まれて、権限のないユーザーに表示されるのを防ぐ必要があります。
何を使うべきでしょうか?
A. データ損失防止 (DLP)
B. Microsoft Purview インサイダーリスク管理

C. Microsoft Purview 情報バリア (IB)
D. 機密ラベル
Answer: (解答を表示する**)**
Channel1 に保存されているファイルの内容が Microsoft 365 Copilot の応答に含まれないようにし、権限のないユーザーがアクセスできないようにするには、Microsoft Purview 秘密度ラベルを使用する必要があります。
機密ラベルを使用すると、機密ファイルを分類、保護、アクセス制限できます。ラベルベースの暗号化とアクセス制御ポリシーを設定することで、Channel1 内のファイルへのアクセスや操作を、承認されたユーザーのみが行えるようにすることができます。Microsoft 365 Copilot は機密ラベルを尊重します。つまり、ファイルに制限付きアクセスのラベルが付けられている場合、Copilot は承認されていないユーザー向けのレスポンスを生成する際にそのラベルを使用しません。

最新問題**: 54**
ホットスポット
Microsoft 365 E5 サブスクリプションをお持ちです。
次の図に示すデータ損失防止 (DLP) アラートを受信します。

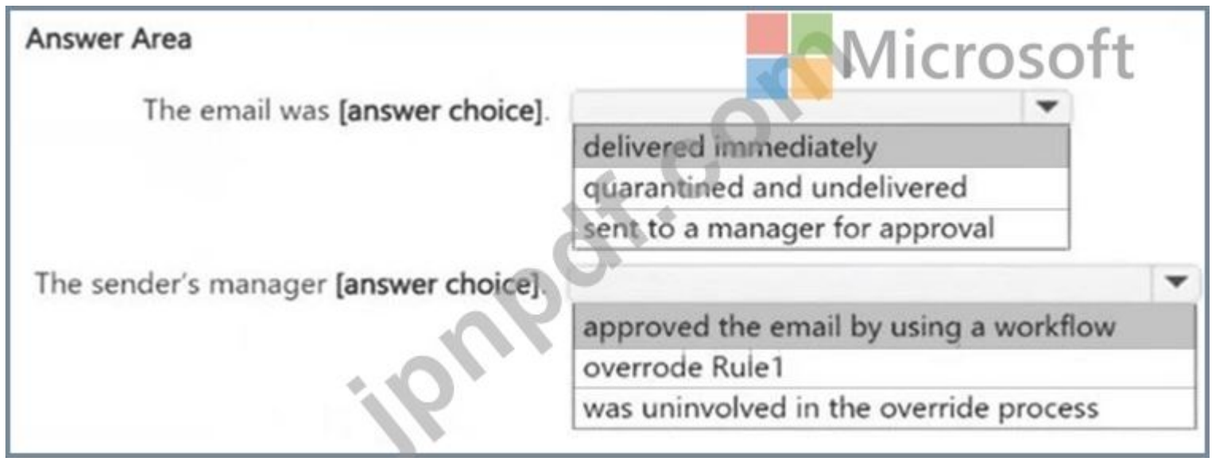

Contoso Electronics
Microsoft Purview
Sensitive info in email with subject 'Message1'
Details
Sensitive info types
Metadata
Event details
ID
173fe9ac-3a65-41b0-9914-1db451bba639
Location
Exchange
Time of activity
Jun 6, 2022 8:22 PM
Impacted entities
User
Megan Bowen
Email recipients
victoria@fabrikam.com
Email subject
Message1
Policy details
DLP policy matched
Policy1
Rule matched
Rule1
Sensitive info types detected
Credit Card Number (19, 85%)
Actions taken
GenerateAlert
User overrode policy
Yes
Override justification text
Manager approved
Sensitive info detected in

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Explanation:



最新問題: **55**
次の表に示すグループを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type
Group1	Microsoft 365
Group2	Security

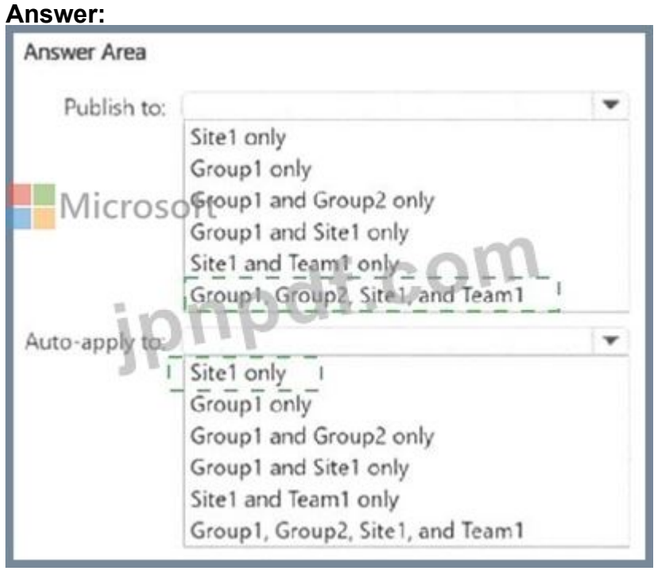
サブスクリプションには、次の表に示すリソースが含まれています。

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

Label1 という名前の機密ラベルを作成します。
Label1 を公開し、ラベルを自動的に適用する必要があります。
Label1 は何に公開できますか。また、何に Label1 を自動適用できますか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:



Explanation:

ボックス1: 機密ラベルの公開
機密ラベルは、Microsoft 365 グループ、セキュリティグループ、SharePoint Online サイト、Microsoft Teams に公開できます。以下の機能を備えています。
グループ1 (Microsoft 365 グループ) - サポートされています
グループ2 (セキュリティグループ) - サポートされています
サイト1 (SharePoint Online サイト) - サポートされています
Team1 (Microsoft Teams チーム) - サポート対象
つまり、Label1 を Group1、Group2、Site1、Team1 に公開できます。
ボックス2: 機密ラベルの自動適用
機密ラベルの自動適用ポリシーは以下で機能します:
SharePoint Online サイト (ドキュメント)
OneDrive (ドキュメント)
メール (メッセージ)の交換
ただし、ラベルはファイルやメールに適用され、グループやチームといったエンティティには適用されないため、Microsoft 365 グループやチームに直接自動適用することはできません。Site1 (SharePoint Online サイト)は自動適用をサポートしているため、これが正しいオプションです。

最新問題: **56**
EDM1 という名前の Microsoft Purview 完全データー致 (EDM) 分類子を持つ Microsoft 36S E5 サブスクリプションがあります。
次の表に示す Microsoft Purview ポリシーを作成する予定です。

Name	Type
DLP1	Data loss prevention (DLP)
Insider1	Insider risk management
Retention1	Retention

EDM1 を使用できるポリシーはどれですか?
A. DLP1 と Insider1 のみ

B. DLP1、インサイダー1、および保持1
C. DLP1のみ
D. 保持期間1のみ
E. Insider1とRetention1のみ
Answer: C (メーッセージを残す)

最新問題**: 57**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントと、Windows 11 を実行するコンピューターが 500 台あります。コンピューターは Microsoft Purview にオンボードされています。
Tailspin_scanner.exe というサードパーティ アプリケーションが複数のコンピューター上の保護された機密情報にアクセスしたことを発見しました。
Tailspin_scanner.exe はコンピューターにローカルにインストールされます。
アプリケーションが他のドキュメントにアクセスするのを妨げることなく、Tailspin_scanner.exe が機密ドキュメントにアクセスするのをブロックする必要があります。
解決策: Microsoft 365 エンドポイントのデータ損失防止 (エンドポイント DLP) 設定から、ファイル パスの除外にフォルダー パスを追加します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す)
ファイル パス除外へのフォルダー パスにより、特定のパスとファイルが DLP 監視から除外されます。
代わりに、許可されていないアプリのリストを使用してください。
参照：
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365- 全世界

最新問題**: 58**
Microsoft 365 E5 サブスクリプションがあり、その中に Site1 という Microsoft SharePoint Online サイトが含まれています。Site1 には、次の表に示すファイルが含まれています。

Name	Author
File1.docx	User1
File2.docx	User2
File3.docx	USER1

Microsoft Purview ポータルで、Content1 という名前のコンテンツ検索を作成し、次の図に示すように検索条件を構成します。

Content1 によって返されるファイルはどれですか?

A. File2.docxのみ

B. File3.docxのみ

C. File1.docx と File2.docx のみ

D. File1.docx と File3.docx のみ

E. Filet.docx、File2.docx、およびFile3.docx

Answer: D (メーッセージを残す)

Microsoft Purview、eDiscovery値のキーワードクエリと検索条件では大文字と小文字は区別されません。User1 (File1.docx) と USER1 (File3.docx) はどちらも検索条件 -Author:USER1 に一致します。

参照：

https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

最新問題: **59**

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。

このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 テナントと、Windows 11 を実行するコンピューターが 500 台あります。コンピューターは Microsoft Purview にオンボードされています。

Tailspin_scanner.exe というサードパーティ アプリケーションが複数のコンピューター上の保護された機密情報にアクセスしたことを発見しました。

Tailspin_scanner.exe はコンピューターにローカルにインストールされます。

アプリケーションが他のドキュメントにアクセスするのを妨げることなく、Tailspin_scanner.exe が機密ドキュメントにアクセスするのをブロックする必要があります。

解決策: Microsoft Defender for Cloud Apps から、アプリケーションを 昧承認」としてマークします。

これは目標を満たしていますか?

A. はい

B. いいえ

Answer: B (メーッセージを残す)

特定の危険なアプリの承認を解除するには、行末の3つの点をクリックします。 承認解除」を選択してください。アプリの承認を解除しても使用はブロックされませんが、Cloud Discoveryフィルターを使用してそのアプリの使用状況をより簡単に監視できるようになります。その後、承認されていないアプリについてユーザーに通知し、安全な代替アプリを提案することができます。
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-using?view=o365- 全世界

最新問題: **60**
機密ラベルを作成するための技術要件を満たす必要があります。
機密ラベル管理者の役割をどのユーザーに割り当てる必要がありますか?
A. 管理者1のみ
B. Admin1とAdmin4のみ
C. Admin1とAdmin5のみ
D. Admin1、Admin2、Admin3のみ
E. Admin1、Admin2、Admin4、Admin5のみ
Answer: D (メーッセージを残す)
すべての管理ユーザーが Microsoft 365 の機密ラベルを作成できる必要があるという要件を満たすには、適切なユーザーに機密ラベル管理者ロールを割り当てる必要があります。
機密ラベル管理者の役割と責任
このロールにより、ユーザーは次の操作を実行できます。
*Microsoft Purview で機密ラベルを作成および管理します。
*自動ラベル付けポリシーを公開および構成します。
*ラベルの暗号化とコンテンツのマーキングの設定を変更します。
表からの管理者ロールの確認:

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	□ No, read-only permissions.
Admin2	Compliance Data Administrator	□ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	□ Yes, has full compliance management, including labels.
Admin4	Security Operator	□ No, this role is focused on security alerts and response.
Admin5	Security Administrator	□ No, primarily focused on security policies and threat management.

機密ラベル管理者ロールを割り当てる必要があるユーザー:
*Admin2 (コンプライアンスデータ管理者)
*Admin3 (コンプライアンス管理者)
*Admin1 (グローバル リーダー) (すべての管理者がラベルを作成できるという要件を満たすには、このロールを割り当てる必要があります)。

最新問題: **61**
デバイスの場所にデータ損失防止 (DLP) ポリシーが適用されています。このポリシーは、米国のパスポート番号を含む文書を保護します。
ユーザーからは、ポリシーのせいで旅行管理 Web サイトにドキュメントをアップロードできないという報告があります。
ユーザーが旅行管理 Web サイトにドキュメントをアップロードできることを確認する必要があります。

ソリューションでは、保護されたコンテンツが他の場所にアップロードされるのを防ぐ必要があります。
どの Microsoft 365 エンドポイント データ損失防止 (エンドポイント DLP) 設定を構成する必要がありますか?
A. サービスドメイン
B. 許可されていないアプリ
C. 許可されていないブラウザ
D. ファイルパスの除外
Answer: A (メーッセージを残す**)**
ポリシーによって保護されている機密ファイルを Microsoft Edge から特定のサービス ドメインにアップロードできるかどうかを制御できます。
- リストモードが 「ブロック」に設定されている場合、ユーザーはこれらのドメインに機密アイテムをアップロードできません。アイテムがDLPポリシーに一致したためにアップロード操作がブロックされた場合、DLPは警告を生成するか、機密アイテムのアップロードをブロックします。
- リスト モードが [許可] に設定されている場合、ユーザーは機密アイテムをそれらのドメインにのみアップロードでき、他のすべてのドメインへのアップロード アクセスは許可されません。
参照：
https://docs.microsoft.com/ja-jp/microsoft-365/compliance/endpoint-dlp-using

最新問題: **62**
Microsoft 36S ES サブスクリプションがあり、そこには Device 1 という名前の Windows 11 デバイスと、User 1、User2、User3 という名前の 3 人のユーザーが含まれています。
Azure Information Protection (AIP) と Microsoft Purview Information Protection クライアントをデバイス 1 に展開する予定です。
計画された展開の一環として、ユーザーがデバイス1で次のアクションを実行できることを確認する必要があります。
* ユーザー 1 はクライアントの機能をテストします。
* ユーザー2 は Microsoft Rights Management コネクタをインストールして構成します。
* User3 は、情報保護スキャナーのサービス アカウントとして構成されます。
ソリューションでは、ユーザーのサインイン プロセスのセキュリティを最大限に高める必要があります。何をすべきでしょうか?
A. User2 と User3 を多要素認証 (MfA) から除外します。
B. パスワードレス認証のために User? と Usex3 を有効にします。
C. User1 と User? を多要素認証から除外する (Mf A}
D. ユーザー1、ユーザー1、ユーザー3をパスキー(FIDO2)認証用に有効にする
Answer: D (メーッセージを残す**)**
目標: AIP クライアント (User1) をテストし、Microsoft Rights Management コネクタ (User2) をインストール/構成し、AIP スキャナー サービス アカウント (User3) として機能するユーザーのサインイン セキュリティを最大限に高めます。
MFA からユーザーを除外するとセキュリティが低下するため、お勧めしません。
FIDO2 セキュリティ キー (パスキー) を使用したパスワードレスは、フィッシング耐性に優れた強力な認証を提供し、セットアップ中に対話型サインインを必要とする管理タスクやサービス シナリオを含む、Azure AD サインインで完全にサポートされます。
したがって、FIDO2 パスキー認証でこれら 3 つすべてを有効にすると、「セキュリティの最大化」の要件を最もよく満たすことができます。
参考文献:

Microsoft Entra ID - FIDO2 セキュリティ キーを使用したパスワードレス認証
https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-passwordless

最新問題: **63**
Microsoft 36S ES サブスクリプションをお持ちです。
Microsoft Purview Data Security Posture Management for AI ポータルから、AI データ セキュリティに関する推奨事項を確認します。リスクの高いユーザーが機密データを AI Web サイトに貼り付けたりアップロードしたりできないようにするワンクリック ポリシーを作成する予定ですか? ポリシーはどのように構成しますか? 回答するには、回答領域で適切なオプションを選択します。注: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

最新問題: **64**
Microsoft 365 サブスクリプションをお持ちです。
Microsoft Purview ポータルからコンテンツ検索を作成して実行します。
コンテンツ検索の結果をダウンロードする必要があります。
まず何を入手すべきでしょうか?

A. エクスポートキー
B. ピン
C. パスワード
D. 証明書
Answer: A (メーッセージを残す**)**

最新問題: **65**
あなたの会社は複数の国にオフィスを持っています。
同社では、Microsoft Purview インサイダー リスク管理を使用する Microsoft 365 E5 サブスクリプションを保有しています。
次のアクションを実行する予定です。
*新しい国で、Office1 という名前のオフィスを開設します。
*User1という名前の新しいユーザーを作成します。
*Office1 にインサイダー リスク管理を展開します。
*User1 を Insider Risk Management Admins 役割グループに追加します。
User1 が Office1 内のユーザーとデバイスに対してのみインサイダー リスク管理タスクを実行できるようにする必要があります。
最初に何を作成すればよいですか?
A. 動的デバイスグループ
B. 動的なユーザーグループ
C. 行政単位
D. 管理グループ
Answer: (解答を表示する)
User1 が Office1 内のユーザーとデバイスに対してのみインサイダー リスク管理タスクを実行できるようにするには、まず Microsoft Entra ID (旧称 Azure AD) に管理単位を作成します。
管理単位を使用すると、特定のユーザー、デバイス、場所への権限を限定できます。Office1の管理単位を作成し、User1をその単位内のInsider Risk Management Adminsロールグループに割り当てることで、User1はOffice1内のユーザーとデバイスにのみアクセスできるようになります。

最新問題: **66**
EDM1 という名前の Microsoft Purview 完全データー致 (EDM) 分類子を持つ Microsoft 36S E5 サブスクリプションがあります。
次の表に示す Microsoft Purview ポリシーを作成する予定です。

Name	Type
DLP1	Data loss prevention (DLP)
Insider1	Insider risk management
Retention1	Retention

EDM1 を使用できるポリシーはどれですか?
A. DLP1のみ
B. 保持1のみ
C. DLP1 と Insider1 のみ
D. Insider1とRetention1のみ
E. DLP1、インサイダー1、および保持1
Answer: A (メーッセージを残す**)**
参考文献付きの包括的で詳細な説明

Exact Data Match (EDM) 分類子は、機密性の高い構造化データ (顧客 ID、アカウント番号など) を高い精度で識別するように設計されています。
EDM 分類子は、Microsoft Purview のデータ損失防止 (DLP) ポリシー内でのみ使用できます。
Insider リスク管理または保持ポリシーでは使用できません。
参考: Microsoft Purview の EDM 分類子
EDM 機密情報タイプは、データ損失防止ポリシーでのみ使用できます。」

最新問題: **67**
デバイスの場所にデータ損失防止 (DIP) ポリシーが適用されています。このポリシーは、米国のパスポート番号を含む文書を保護します。ユーザーから、Pokeyのせいで旅行管理ウェブサイトに文書をアップロードできないという報告があります。
ユーザーが旅行管理ウェブサイトにドキュメントをアップロードできるようにする必要があります。保護されたコンテンツが他の場所にアップロードされるのを防ぐソリューションが必要です。
どの Microsoft 365 エンドポイント データ損失防止 (エンドポイント DIP) 設定を構成する必要がありますか?
A. 許可されていないブラウザ
B. 許可されていないアプリ
C. サービスドメイン
D. ファイルパスの除外
Answer: C (メーッセージを残す**)**

最新問題: **68**
ホットスポット
Microsoft Purview とジャストインタイム (JIT) 保護を使用する Microsoft 365 E5 サブスクリプションをご利用の場合、次の表に示すユーザーが含まれています。

Name	JIT protection scope
User1	Included
User2	Not configured
User3	Included

サブスクリプションには、次の表に示すデバイスが含まれています。

Name	Microsoft Defender
Device1	Onboarded
Device2	Onboarded
Device3	Not onboarded

デバイスには次の表に示すファイルが含まれています。

Name	File classification evaluation status	Location
File1.docx	Not evaluated	Device1
File2.pdf	Evaluated	Device2
File3.xlsx	Not evaluated	Device3

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

Answer:

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

Explanation:

Answer Area

Statements	Yes	No
If User1 attempts to copy File1.docx to a removable USB drive, JIT will block the action.	○	○
If User2 signs in to Device2 and attempts to attach File2.pdf to an email, JIT will block the action.	○	○
If User3 attempts to copy File3.xlsx to a network share, JIT will generate an audit event.	○	○

ステートメント1 - いいえ。ユーザー1はJIT保護の対象です。ファイル1.docxはデバイス1上にあり、デバイス1はMicrosoft Defenderにオンボードされています。しかし、ファイル1.docxはファイル分類の評価を受けていないため、JITは保護を適用できません。ユーザー2がデバイス2にサインインし、ファイル2.pdfをメールに添付しようとした場合、JITはブロックします。
ステートメント2 - いいえ。User2はJIT保護の対象になっていません（JITは適用されません）。File2.pdfは分類のために評価されましたが、User2はJIT保護の対象ではないため、ブロックは発生しません。User3がFile3.xlsxをネットワーク共有にコピーしようとすると、JITによって監査イベントが生成されます。
ステートメント3 - いいえ。User3はJIT保護の対象です。ただし、Device3はMicrosoft Defenderにオンボードされていないため、JIT保護はDevice3に対してアクションを実行できません。File3.xlsxは評価されていないため、たとえデバイスがオンボードされていたとしても、JITはアクションを実行するための分類データを取得できません。

最新問題: **69**
Microsoft 365 E5 サブスクリプションをお持ちです。
インサイダー リスク管理を実装しています。
イベントがトリガーされたときに収集される履歴データの量を最大化する必要があります。
履歴データを収集できる最大日数はどれくらいですか?
A. 30
B. 60
C. 180
D. 90
Answer: D (メーッセージを残す)

最新問題: **70**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Exchange Online には、次の図に示すメール フロー ルールがあります。

Senders address

Matching Header

Priority

0

For rule processing errors

Ignore

Rule description

Apply this rule if

Is sent to 'Outside the organization'
and includes these words in the message subject '[Encrypt]'

Do the following

rights protect messages with RMS template: 'Do Not Forward'

Rule comments

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

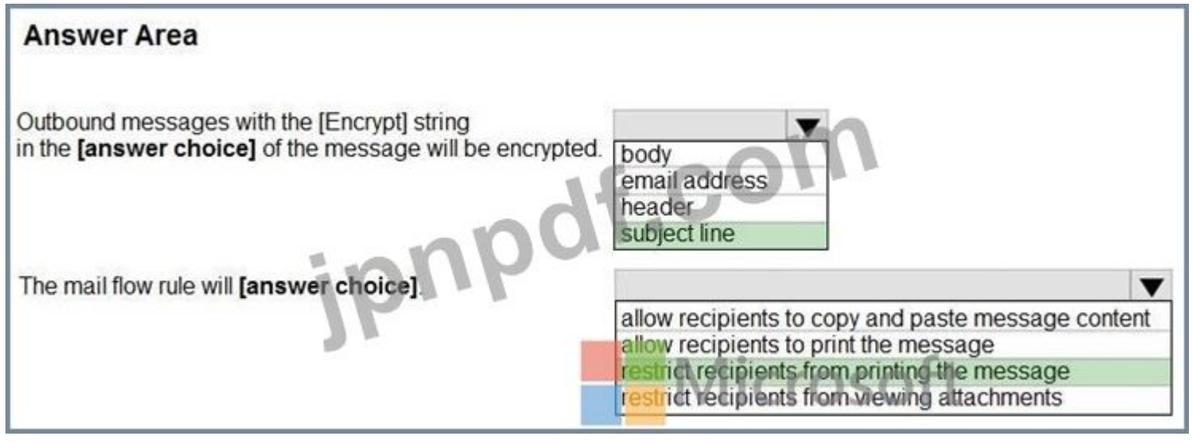
Outbound messages with the [Encrypt] string
in the **[answer choice]** of the message will be encrypted.

- body
- email address
- header
- subject line

The mail flow rule will **[answer choice]**.

- allow recipients to copy and paste message content
- allow recipients to print the message
- restrict recipients from printing the message
- restrict recipients from viewing attachments

Answer:



Explanation:

ボックス1: 件名

ボックス2: 受信者がメッセージを印刷できないように制限する

注: IRM は、メールメッセージに使用制限を適用する暗号化ソリューションです。機密情報が不正な人物によって印刷、転送、またはコピーされるのを防ぎます。

Microsoft 365 の IRM 機能では、Azure Rights Management (Azure RMS) が使用されます。

参照：

https://learn.microsoft.com/en-us/purvie　メール暗号化付き）

最新問題: 71

Microsoft 365 サブスクリプションをお持ちです。

Site1 という名前の Microsoft SharePoint Online サイトがあります。Site1 には、次の表に示すファイルを含むドキュメント ライブラリがあります。

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

Microsoft Purview コンプライアンス ポータルから、Site1 に対して、次の図に示すように、日付が YYYY-MM-DD 形式の Search1 という名前のコンテンツ検索を作成します。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

最新問題: **72**

次の表に示すグループを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type
Group1	Microsoft 365
Group2	Security

サブスクリプションには、次の表に示すリソースが含まれています。

Name	Type
Site1	Microsoft SharePoint Online site
Team1	Microsoft Teams team

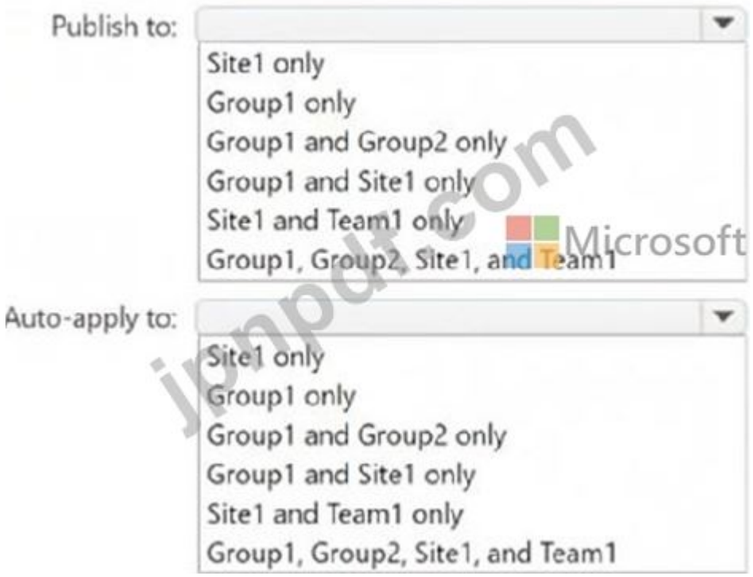
Label1 という名前の機密ラベルを作成します。

Label1 を公開し、ラベルを自動的に適用する必要があります。

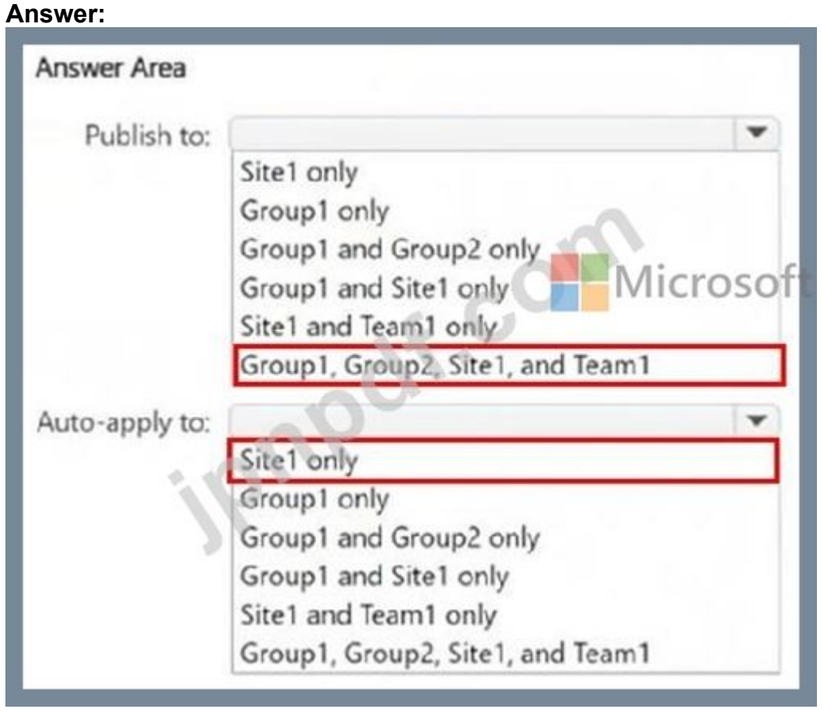
Label1 は何に公開できますか。また、何に Label1 を自動適用できますか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:



トピック1、Contoso株式会社

説明書

これはケーススタディです。ケーススタディは他の試験セクションとは別に時間制限がありません。各ケーススタディには、必要なだけの試験時間を使用できます。ただし、追加のケーススタディや他の試験セクションが課される場合があります。すべての試験セクションを指定された時間内に完了できるよう、時間を管理してください。画面上部の試験の進捗状況を確認し、このケーススタディに続く試験セクションを完了するのに十分な時間を確保してください。

ケーススタディの質問に回答するには、ケーススタディに記載されている情報を参照する必要があります。ケーススタディおよび関連する質問には、ケースで説明されているシナリオに関する詳細情報を提供

する資料やその他のリソースが含まれている場合があります。個々の質問で提供される情報は、ケーススタディの他の質問には適用されません。
このケーススタディの最後にレビュー画面が表示されます。レビュー画面では、次の試験セクションに進む前に回答を確認し、修正することができます。このケーススタディを終了した後は、戻ることはできません。
ケーススタディを始めるには
このケーススタディの最初の質問を表示するには、 次へ」ボタンを選択してください。質問の左側には、ビジネス要件、既存の環境、問題の説明などの情報へのリンクがメニューに表示されます。質問に回答する前に、これらの情報をすべてお読みください。質問に回答する準備ができたら、 質問」ボタンを選択して質問に戻ってください。
概要
Contoso 社は、モントリオールに本社を置き、シアトル、ボストン、ヨハネスブルグに 3 つの支社を持つコンサルティング会社です。
既存の環境
Microsoft 365 環境
Contoso 社には Microsoft 365 E5 テナントがあります。このテナントには、次の表に示す管理ユーザーアカウントが含まれています。

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

ユーザーは次の場所にデータを保存します。
*SharePoint サイト
*OneDriveアカウント
*メール交換
*Exchangeパブリックフォルダ
*Teamsチャット
*Teams チャネル メッセージ
研究部門のユーザーが文書を作成する際は、各文書に10桁のプロジェクトコードを追加する必要があります。999で始まるプロジェクトコードは機密情報です。
SharePoint Online 環境
Contoso には、Site1、Site2、Site3、Site4 という名前の 4 つの Microsoft SharePoint Online サイトがあります。
Site2 には、次の表に示すファイルが含まれています。

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

次の表に示すように、User1 と User2 という名前の 2 人のユーザーに Site2 のロールが割り当てられています。

User	Role
User1	Site owner
User2	Site visitor

Site3には、会社のプロジェクトに関連する文書が保存されています。文書はプロジェクトごとにフォルダ階層に整理されています。
Site4 には次の 2 つの保持ポリシーが適用されています。

*名前: Site4RetentionPolicy1
*ポリシーを適用する場所: サイト4
*2年以上前のアイテムを削除
*コンテンツを削除する基準: アイテムが作成された日時
*名前: Site4RetentionPolicy2
*ポリシーを適用する場所: サイト4
*アイテムを特定期間保管 :4年間
*保存期間の開始基準: アイテムが作成された日時
*保存期間の終了時: 何もしない
問題ステートメント
Contoso社の経営陣はデータ漏洩を懸念しています。研究部門の機密文書が漏洩するケースが複数回発生しました。
要件
計画された変更
Contoso では、次のデータ損失防止 (DLP) ポリシーを作成する予定です。
*名前: DLPpolicy1
*ポリシーを適用する場所: サイト2
*条件：
*コンテンツには、以下のいずれかの機密情報が含まれています: SWIFTコード
*インスタンス数: 2～任意
*アクション: コンテンツへのアクセスを制限する
技術要件
Contoso は次の技術要件を満たす必要があります。
*すべての管理ユーザーは DLP レポートを確認できる必要があります。
*可能な限り、最小権限の原則を使用する必要があります。
*すべてのユーザーについて、すべての Microsoft 365 データは少なくとも 1 年間保持する必要があります。
*機密文書は、Microsoft 365 を使用して検出および保護する必要があります。
*クレジットカード番号が含まれるSite1ドキュメントには、自動的にラベルが付けられる必要があります。
*すべての管理ユーザーは、Microsoft 365 の機密ラベルを作成できる必要があります。
※プロジェクト完了後、サイト3内のプロジェクト関連文書は10年間保管する必要があります。

最新問題: **73**
シミュレーション
ユーザー名とパスワード
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、"サインイン"ボックスにカーソルを置き、以下のユーザー名を選択します。
パスワードを入力するには、"パスワードを入力"ボックスにカーソルを置き、以下のパスワードを選択します。
Microsoft 365 ユーザー名:
admin@WWLx971455.onmicrosoft.com
Microsoft 365 パスワード: XXXXXXXXX
Microsoft Edge ブラウザーまたは Microsoft 365 ポータルが正常に読み込まれない場合は、タスク バーから Microsoft Edge ブラウザー アイコンを選択し、URL "https://admin microsoft.com"を入力して Enter

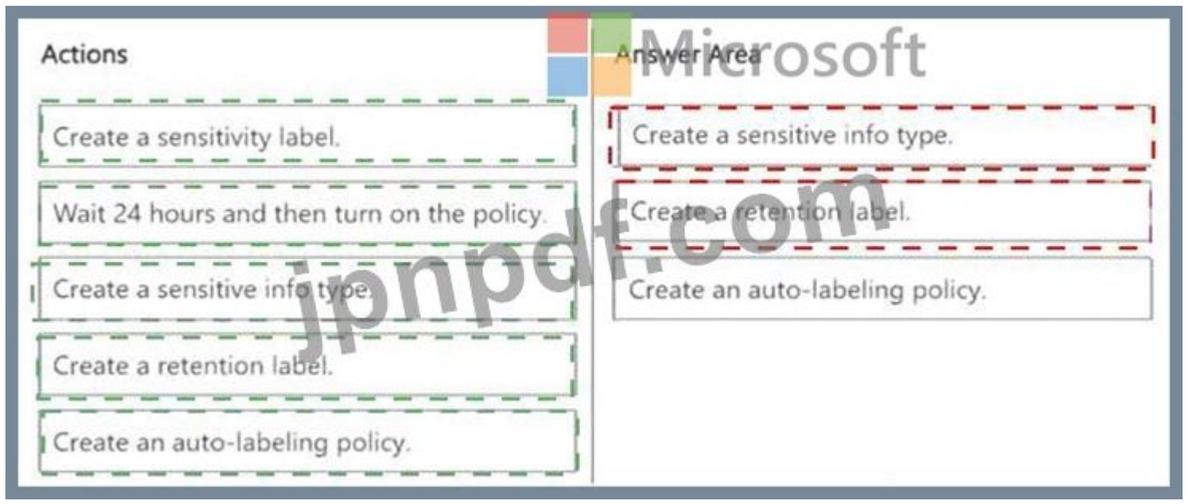
キーを押します。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: XXXXXXXX。
タスク9
次のキーワードを含むコンテンツに適用されるデータ損失防止 (DLP) ポリシーを作成する予定です。
- テールスピン
- 文学
- ファルコン
DLP ポリシーで使用できるキーワード リストを作成する必要があります。
Answer:
キーワードリスト内のすべての単語に一致する機密情報タイプを作成するには、
デフォルトの「いずれか」ではなく「すべて」の条件を使用します。このような機密情報タイプを作成する手順は次のとおりです。
手順 1: Microsoft 365 コンプライアンス センターにアクセスし、「機密情報の種類」ページに移動します。
ステップ 2: 「機密情報の種類を作成する」をクリックします。
ステップ 3: 作成する機密情報の種類として「キーワード辞書」を選択します。
ステップ 4: 機密情報の種類の名前と説明を入力します。
ステップ 5: 「キーワード」セクションで、一致させたいすべての単語をコンマで区切って入力します。
ここで登場 :Tailspin、Litware、Falcon
ステップ 6: 「条件を追加」をクリックし、条件タイプとして「任意」を選択します。
ステップ 7: 「作成」をクリックして機密情報タイプを作成します。
ステップ 8: 「作成」をクリックして機密情報タイプを作成します。
この構成では、DLP ポリシーは、スキャン対象のコンテンツにキーワード リスト内のいずれかの単語が存在する場合にのみ機密情報を検出します。
参照 :
https://learn.microsoft.com/en-us/answers/questions/1419105/how-to-create-sensitive- information-types-to-match

最新問題**: 74**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーは次のアプリを使用してメールボックスにアクセスします。
- Microsoft 365 向け Outlook
- ウェブ上のOutlook
- Outlook モバイル (iOS、Android)
次の設定を持つ、DLP1 という名前のデータ損失防止 (DLP) ポリシーを作成します。
- 場所: Exchangeメール
- ステータス: オン
- ユーザー通知: オン
- ポリシーヒントでユーザーに通知: 有効
DLP1 を使用してコンテンツが一致したときにポリシーヒントを表示するアプリはどれですか?
A. Microsoft 365 向け Outlook のみ
B. Web 上の Outlook のみ
C. Microsoft 365 用 Outlook および Web 上の Outlook のみ

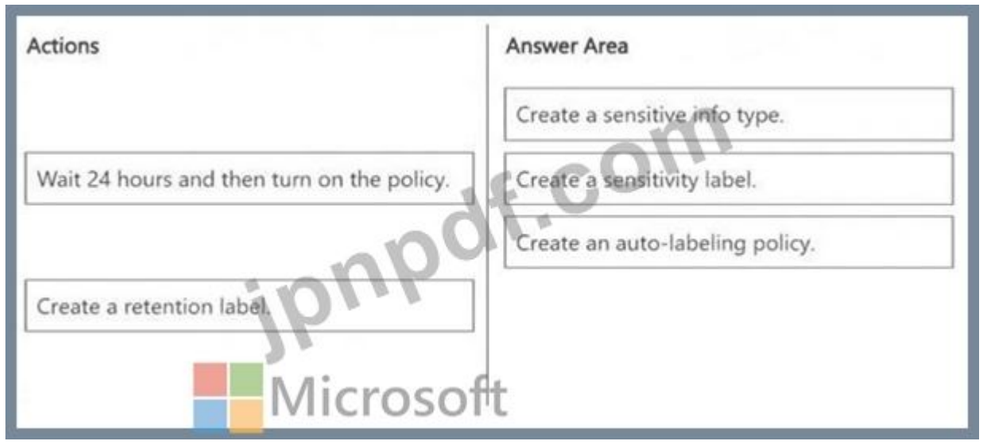
D. Microsoft 365 用 Outlook および Outlook Mobile (iOS、Android) のみ
E. Microsoft 365 用 Outlook、Web 上の Outlook、Outlook Mobile (iOS、Android)
Answer: C (メーッセージを残す)
PC 版 Outlook、Web 版 Outlook、iOS および Android 版 Outlook を比較する リファレンス:
https://support.microsoft.com/en-us/office/compare-outlook-for-pc-outlook-on-the-web-and-outlook-for-ios-android-b26a7bf5-0ac7-48ba-97af-984e0645dde5

最新問題: **75**
Site1 ドキュメントの技術要件を満たす必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

Answer:



Explanation:
アンケートの AI 生成コンテンツのスクリーンショットは不正確である可能性があります。



目標は、サイト1にあるクレジットカード番号を含むドキュメントに自動的にラベルを付けることです。これを実現するには、クレジットカード番号を検出する機密情報の種類に基づいた自動ラベル付けポリシーを備えた機密ラベルが必要です。
ステップ1: 機密情報の種類を作成する
ドキュメント内のクレジットカード番号を検出するには、機密情報タイプが必要です。
Microsoft Purview にはクレジットカード番号の機密情報タイプが組み込まれていますが、必要に応じてカスタムタイプを作成することもできます。
ステップ2: 機密ラベルを作成する
機密情報を含む文書を分類して保護するには、機密ラベルが必要です。
このラベルは、クレジットカードデータに暗号化、透かし、またはアクセス制御を適用できます。
ステップ3: 自動ラベル付けポリシーを作成する
自動ラベル付けポリシーにより、Site1 でクレジットカード番号が検出されると、機密ラベルが自動的に適用されます。
このポリシーは、ファイルをスキャンし、正しい機密ラベルを自動的に適用するように構成されています。
トピック1、Contoso社ケーススタディ1
説明書
これはケーススタディです。ケーススタディは他の試験セクションとは別に時間制限がありません。各ケーススタディには、必要なだけの試験時間を使用できます。ただし、追加のケーススタディや他の試験セクションが課される場合があります。すべての試験セクションを指定された時間内に完了できるよう、時間を管理してください。画面上部の試験の進捗状況を確認し、このケーススタディに続く試験セクションを完了するのに十分な時間を確保してください。
ケーススタディの質問に回答するには、ケーススタディに記載されている情報を参照する必要があります。ケーススタディおよび関連する質問には、ケースで説明されているシナリオに関する詳細情報を提供する資料やその他のリソースが含まれている場合があります。個々の質問で提供される情報は、ケーススタディの他の質問には適用されません。
このケーススタディの最後にレビュー画面が表示されます。レビュー画面では、次の試験セクションに進む前に回答を確認し、修正することができます。このケーススタディを終了した後は、戻ることはできません。
ケーススタディを始めるには
このケーススタディの最初の質問を表示するには、 次へ」ボタンを選択してください。質問の左側には、ビジネス要件、既存の環境、問題の説明などの情報へのリンクがメニューに表示されます。質問に回答する前に、これらの情報をすべてお読みください。質問に回答する準備ができたら、 質問」ボタンを選択して質問に戻ってください。
概要
Contoso 社は、モントリオールに本社を置き、シアトル、ボストン、ヨハネスブルグに 3 つの支社を持つコンサルティング会社です。
既存の環境
Microsoft 365 環境
Contoso 社には Microsoft 365 E5 テナントがあります。このテナントには、次の表に示す管理ユーザーアカウントが含まれています。

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

ユーザーは次の場所にデータを保存します。
SharePoint サイト
OneDriveアカウント
Exchangeメール
Exchange パブリックフォルダ
Teams チャット
Teams チャネル メッセージ
研究部門のユーザーが文書を作成する際は、各文書に10桁のプロジェクトコードを追加する必要があります。999で始まるプロジェクトコードは機密情報です。
SharePoint Online 環境
Contoso には、Site1、Site2、Site3、Site4 という名前の 4 つの Microsoft SharePoint Online サイトがあります。
Site2 には、次の表に示すファイルが含まれています。

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

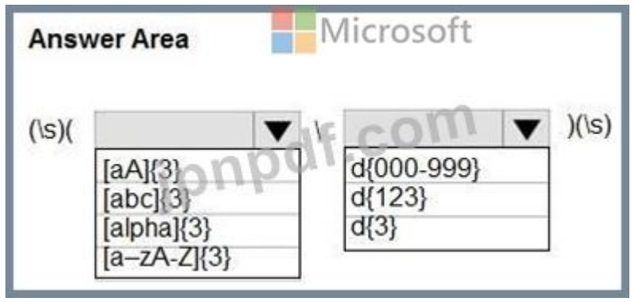
次の表に示すように、User1 と User2 という名前の 2 人のユーザーに Site2 のロールが割り当てられています。

User	Role
User1	Site owner
User2	Site visitor

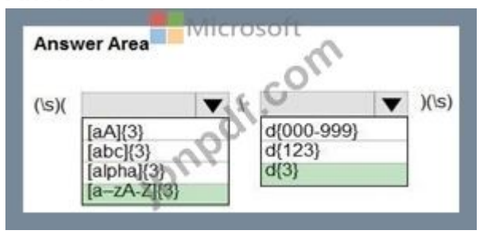
Site3には、会社のプロジェクトに関連する文書が保存されています。文書はプロジェクトごとにフォルダ階層に整理されています。
Site4 には次の 2 つの保持ポリシーが適用されています。
名前: Site4RetentionPolicy1
ポリシーを適用する場所: Site4
2年以上前のアイテムを削除
コンテンツを削除する基準: アイテムが作成された日時
名前: Site4RetentionPolicy2
ポリシーを適用する場所: Site4
アイテムを特定の期間保持する: 4 年間
保持期間の開始基準: アイテムが作成された日時
保存期間の終了時: 何もしない
問題ステートメント
Contoso社の経営陣はデータ漏洩を懸念しています。研究部門の機密文書が漏洩するケースが複数回発生しました。

要件
計画された変更
Contoso では、次のデータ損失防止 (DLP) ポリシーを作成する予定です。
名前: DLPpolicy1
ポリシーを適用する場所: Site2
条件:
コンテンツには、次のいずれかの機密情報タイプが含まれています: SWIFT コード
インスタンス数: 2～任意
アクション: コンテンツへのアクセスを制限する
技術要件
Contoso は次の技術要件を満たす必要があります。
すべての管理ユーザーは DLP レポートを確認できる必要があります。
可能な限り、最小権限の原則を使用する必要があります。
すべてのユーザーについて、すべての Microsoft 365 データは少なくとも 1 年間保持する必要があります。
機密文書は、Microsoft 365 を使用して検出し、保護する必要があります。
クレジットカード番号が含まれる Site1 ドキュメントには、自動的にラベルを付ける必要があります。
すべての管理ユーザーは、Microsoft 365 の機密ラベルを作成できる必要があります。
プロジェクトが完了した後、プロジェクトに関連する Site3 の文書は 10 年間保持する必要があります。

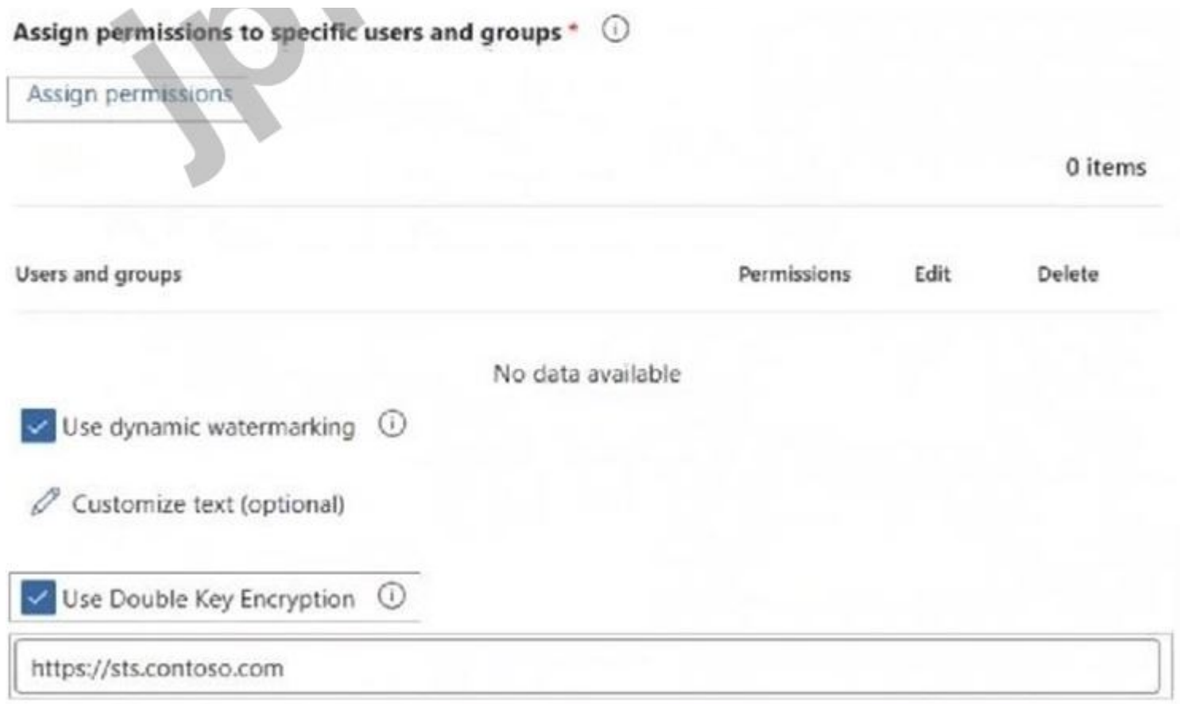
最新問題: **76**
ホットスポットに関する質問
プロジェクト コードを使用する形式は、プロジェクト タイプを表す 3 つの英字とそれに続く 3 つの数字 (例: Abc123) です。
プロジェクト コードの新しい機密情報タイプを作成する必要があります。
コンテンツを検出するために正規表現をどのように設定すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



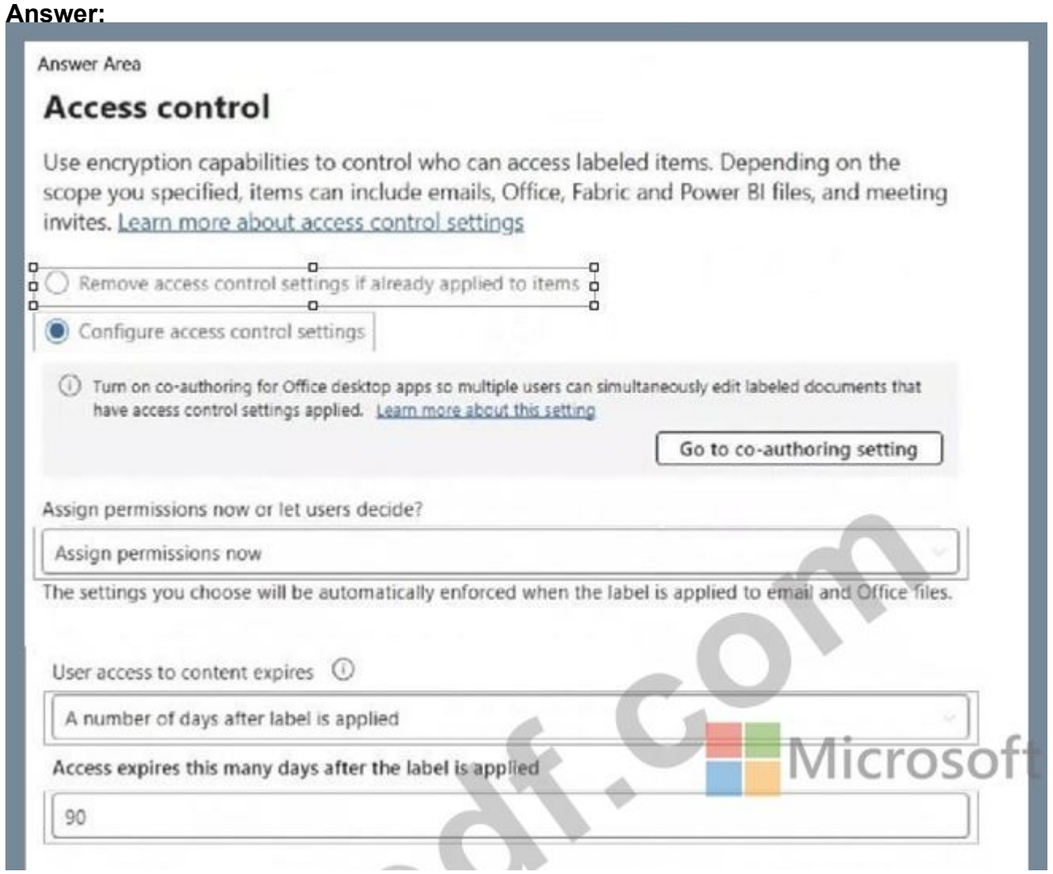
Answer:

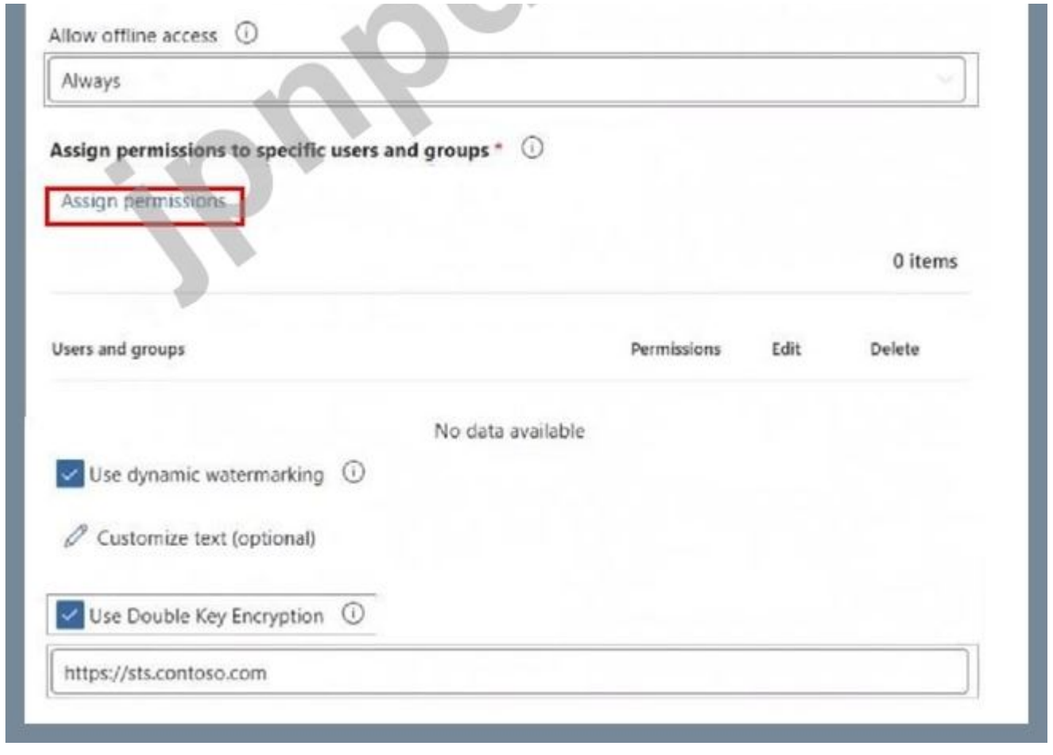


最新問題: **77**
label1 という名前の機密ラベルが含まれる Microsoft 365 E5 テナントがあります。
暗号化されたファイルの共同編集を有効にする予定です。
label1 が適用されたファイルが共同編集をサポートしていることを確認する必要があります。
どの 2 つの設定を変更する必要がありますか? 回答するには、回答領域で設定を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area

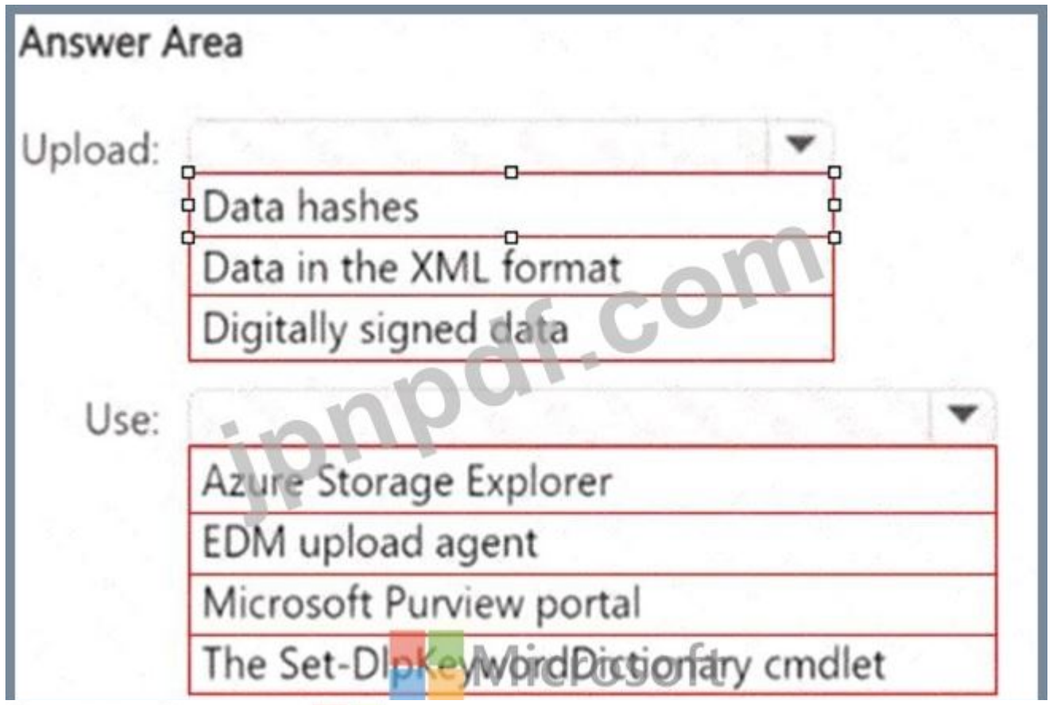

Assign permissions to specific users and groups *
Assign permissions
0 items
Users and groups
Permissions
Edit
Delete
No data available
Use dynamic watermarking
Customize text (optional)
Use Double Key Encryption
https://sts.contoso.com

Answer:

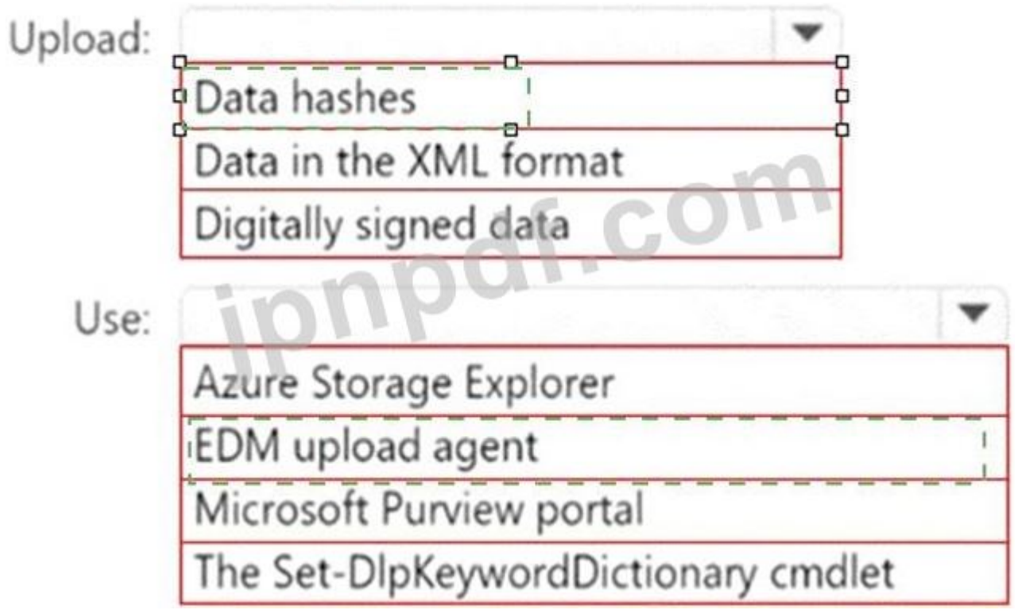

Answer Area
Access control
Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings
Remove access control settings if already applied to items
Configure access control settings
Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting
Go to co-authoring setting
Assign permissions now or let users decide?
Assign permissions now
The settings you choose will be automatically enforced when the label is applied to email and Office files.
User access to content expires
A number of days after label is applied
Access expires this many days after the label is applied
90



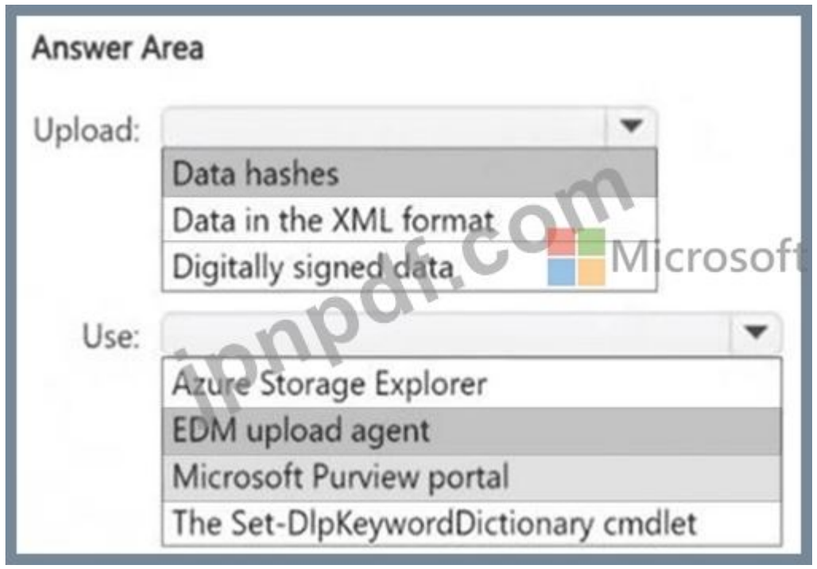
最新問題: **78**
ホットスポット
完全データ一致 (EDM) を使用するカスタムの機密情報の種類を作成する予定です。
Microsoft 365 にアップロードするものと、アップロードに使用するツールを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer Area



Explanation:

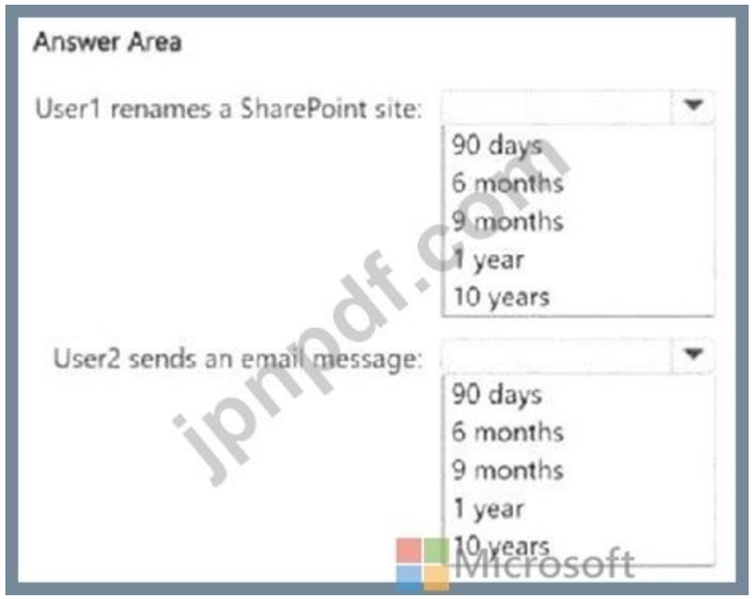


EDM は生データを保存しません。代わりに、プライバシーとセキュリティのために機密データのハッシュ バージョンを必要とします。
ハッシュ化されたデータをアップロードするために、Microsoft は EDM アップロード エージェントを提供しています。これにより、Microsoft 365 の EDM サービスによってデータが安全に処理され、認識されることが保証されます。

最新問題: **79**
ホットスポット
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
次の表に示す監査保持ポリシーを作成します。

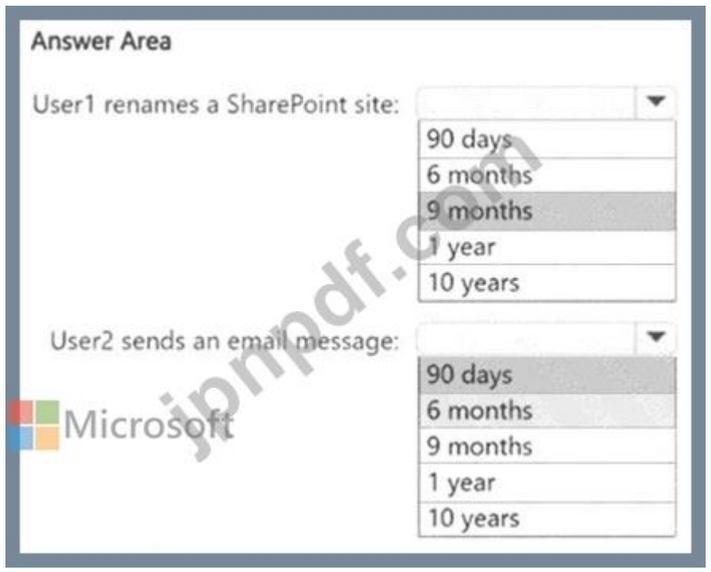
Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	*None*	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccesssed	User1	9 Months
30	AuditRetention3	Sharepoint	*None*	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	*None*	10 Years

ユーザーは次のアクションを実行します。
User1 が Microsoft SharePoint Online サイトの名前を変更します。
ユーザー2 が電子メール メッセージを送信します。
各アクションの監査ログ レコードはどのくらいの期間保持されますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Explanation:

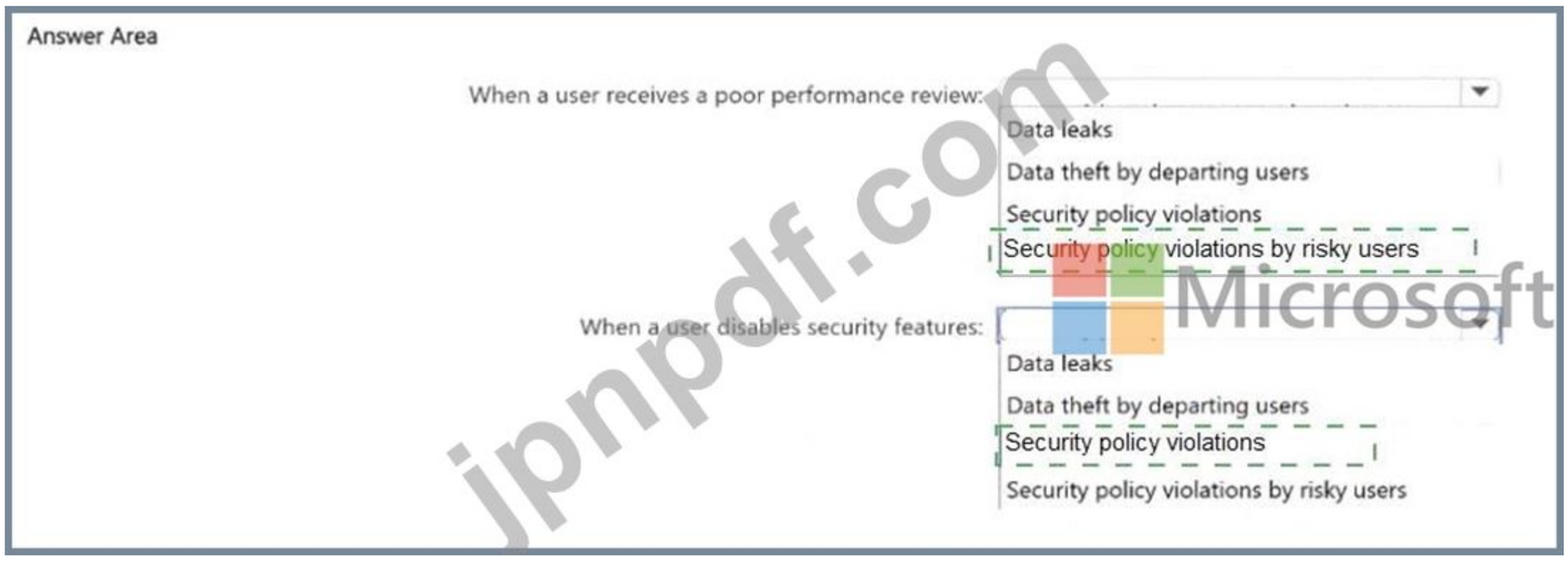


SharePoint のアクション ｢SiteRenamed｣は AuditRetention4 ポリシーの対象であり、User1 に適用され、ログを 9 か月間保持します。
ExchangeItem のアクション ｢送信｣は AuditRetention2 ポリシーの対象ですが、このポリシーは User1 にのみ適用されます。User2 は特定のポリシーの対象外であるため、Microsoft Purview における監査ログのデフォルトの保持期間は 90 日です。

最新問題: **80**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview インサイダー リスク管理を実装する予定です。
次の要件を満たすポリシー テンプレートを推奨する必要があります。
* ユーザーのパフォーマンス評価が低い場合のリスク指標とスコアリングが含まれます
* ユーザーがデバイスのセキュリティ機能を無効にした場合のリスク指標とスコアが含まれます。
各要件にはどのテンプレートを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:



Explanation:

最新問題: 81

Microsoft 365 E5 テナントがあります。
新しいキーワード辞書を追加する必要があります。
何を創造すべきでしょうか?
A. 学習可能な分類器
B. 保持ポリシー
C. 機密ラベル
D. 機密情報の種類
Answer: D (メーッセージを残す**)**
Microsoft Purview データ損失防止 (DLP) に新しいキーワード辞書を追加するには、機密情報タイプ (SIT) を作成する必要があります。
機密情報タイプ（SIT）を使用すると、キーワード辞書、正規表現、電子メール、ドキュメント、その他のMicrosoftドキュメント内の機密コンテンツを識別するための関数など、カスタム検出ルールを定義できます。
365 か所。キーワード辞書は、Microsoft Purview が DLP ポリシーのコンテンツを識別および分類するために使用できる、定義済みの単語/フレーズのリストです。
キーワード辞書を追加する手順:
1. Microsoft Purviewコンプライアンスポータルにアクセスする
2. データ分類 > 機密情報の種類に移動します
3. 新しい機密情報タイプを作成する
4. キーワード辞書を追加する
5. DLPポリシーに保存して使用する

最新問題**: 82**
Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
ユーザーが Site1 上の機密情報を外部の受信者と共有するときにアラートを生成する Microsoft Purview インサイダー リスク管理ソリューションを展開する必要があります。
実行すべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正解ごとに 1 ポイントが加算されます。
A. データ損失防止 (DLP) ポリシーを作成します。
B. インジケーターをオンにします。
C. 適応型保護を構成します。
D. 分析をオンにします。
E. インサイダー リスク ポリシーを作成します。
Answer: (解答を表示する**)**
A). DLP ポリシーを作成します。# 外部で共有されている機密情報を検出する必要があります。
B). 外部共有などの危険なアクティビティを検出するために、インサイダーリスクポリシーに必要なインジケーター # をオンにします。
C). 適応型保護を構成する # 適用のカスタマイズの場合はオプションですが、ここでは必須ではありません。
D). 分析をオンにする # ポリシーの影響を評価するのに役立ちますが、アラートを生成するために必須ではありません。
E). インサイダー リスク ポリシーを作成します # インサイダー リスク アラートを生成するために必要です。

最新問題**: 83**
Microsoft 365 E5 サブスクリプションをお持ちです。
データ損失防止 (DLP) ポリシーを作成し、選択します。
通知を使用してユーザーに通知し、機密情報の適切な使用について教育します。

どのアプリにポリシーヒントが表示されますか?
A. Outlook Win32 および iOS および Android 向け Outlook のみ
B. iOS および Android 向け Outlook のみ
C. Web 上の Outlook のみ
D. Web 上の Outlook、Outlook Win32、iOS および Android 向け Outlook
E. Web 上の Outlook および Outlook Win32 のみ
F. Outlook Win32 のみ
Answer: E (メーッセージを残す**)**

最新問題**: 84**
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
Policy1 という名前の通信コンプライアンス ポリシーを作成し、Microsoft Copilot の相互作用を検出するを選択します。
どの 2 つのトレーニング可能な分類器が Policy1 に自動的に追加されますか? それぞれの正解はソリューションの一部を示します。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. 不正開示
B. プロンプトシールド
C. 脅威
D. 企業妨害
E. 保護された資料
Answer: (解答を表示する**)**
プロンプト シールド: この分類子は、Microsoft Copilot などの生成 AI ツールに提供される安全でない、機密性の高い、または不適切なプロンプトを検出するように設計されています。
保護された資料: この分類子は、ユーザーが Copilot またはその他の生成 AI インタラクション内で機密、秘密、または保護された企業データを公開または使用しようとしたときにそれを検出します。
https://learn.microsoft.com/en-us/purview/communication-compliance-policies#policy-templates

最新問題**: 85**
次の表に示すアダプティブ スコープを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type	Query
Scope1	Users	`FirstName starts with User`
Scope2	SharePoint Online sites	`SiteTitle starts with Site`

次の表に示す保持ポリシーを作成します。

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

どの保持ポリシーが保存ロックをサポートしていますか?
A. RPolicy1、RPolicy2、およびRPolicy3
B. RPolicy1 と RPolicy2 のみ
C. RPolicy1 と RPolicy3 のみ
D. RPolicy2のみ
E. RPolicy3on1y
Answer: (解答を表示する**)**

最新問題: **86**

Microsoft 365 E5 テナントがあります。

「機密ラベル」展示に示されているように、機密ラベルがあります。（機密ラベル」タブをクリックします。）

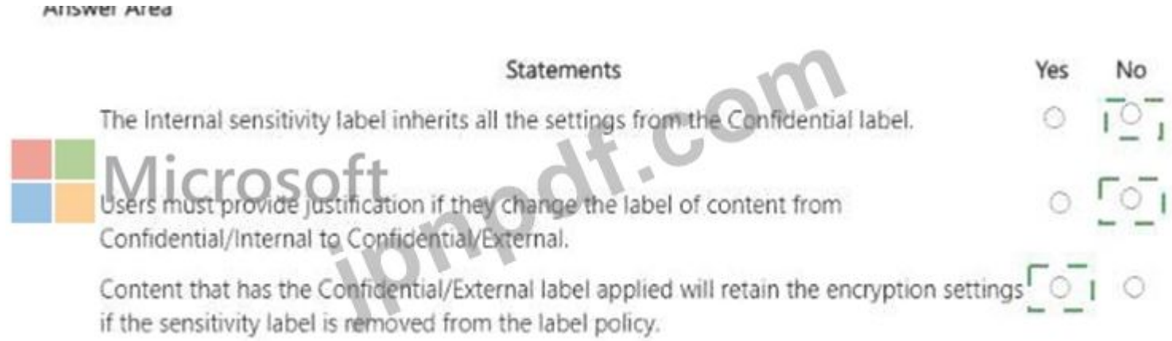
機密/外部の機密ラベルは、コンテンツに適用されたときにファイルと電子メールを暗号化するように構成されています。

機密ラベルは、「公開済み」展示に示されているとおりに公開されました。(「公開済み」タブをクリックします。)

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:



Explanation:

ステップ1 - 構成を確認する
ラベル: 公開、一般、機密、内部、外部。
ポリシーにも表示されます: 機密/内部および機密/外部。
ポリシー設定: ユーザーは、ラベルを削除したり、ラベルの分類を下げたりする正当な理由を示す必要があります。
機密/外部 # は適用時にコンテンツを暗号化します。
ステップ2 - 各ステートメントを分析する
ステートメント 1: 内部機密ラベルは、機密ラベルからすべての設定を継承します。
サブラベル (例: Confidential/Internal、Confidential/External) は親から設定を継承しません。
これらは組織のために親の下にグループ化された独立したラベルですが、各サブラベルには独自の保護設定を定義する必要があります。
答え: いいえ
ステートメント 2: ユーザーは、コンテンツのラベルを 「機密/内部」から 「機密/外部」に変更する場合、正当な理由を示す必要があります。
このポリシーでは、ラベルを削除する場合、または分類をダウングレードする（低下させる）場合にのみ正当な理由が必要です。
同じ親ラベルの 2 つのサブラベル (機密/社内 # 機密/社外) 間の変更は、横移動 (ダウングレードではない) と見なされます。
答え: いいえ
ステートメント 3: 機密/外部ラベルが適用されたコンテンツは、ラベル ポリシーから機密ラベルが削除されても、暗号化設定が保持されます。

公開されたポリシーからラベルが削除された場合、すでにラベルが付けられているコンテンツの保護設定 (暗号化など) は保持されます。
ラベル メタデータは、未公開の場合でもファイル/電子メールに適用されたままになります。
答え: はい
参考: 機密ラベルを削除または編集するとどうなるか

最新問題: **87**
Microsoft 365 サブスクリプションをお持ちです。
サブスクリプション用の暗号化メールをカスタマイズする必要があります。ソリューションは以下の要件を満たす必要があります。
*暗号化されたメールを送信する場合は、メールに会社のロゴが含まれていることを確認してください。
*管理作業を最小限に抑えます。
どの PowerShell コマンドレットを実行する必要がありますか?
A. Set-IRMConfiguration
B. Set-OMEConfiguration
C. Set-RMSTemplate
D. 新しいOME構成
Answer: B (メーッセージを残す**)**
Microsoft 365 で暗号化されたメールをカスタマイズするには（会社のロゴの追加など）、Office Message Encryption (OME) のブランド設定を変更する必要があります。Set-OMEConfiguration PowerShell コマンドレットを使用すると、次のようなブランド要素を構成できます。
*会社ロゴ
*カスタムテキスト
*背景色
このコマンドレットは、既存の OME ブランド設定を更新し、組織から送信される暗号化された電子メールに必要なカスタマイズが含まれるようにするために使用されます。

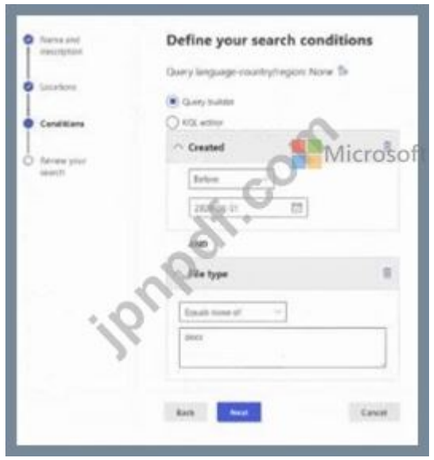
最新問題: **88**
次の表に示すユーザーを含む Microsoft 365 サブスクリプションがあります。

Name	Assigned license
User1	Microsoft 365 E3
User2	Microsoft 365 F3
User3	Microsoft 365 E5

各ユーザーの監査保持期間を確認します。
どのユーザーの監査ログが 9 か月間保持されますか?
A. ユーザー1とユーザー3
B. ユーザー2とユーザー3
C. ユーザー1、ユーザー2、ユーザー3
D. ユーザー3のみ
Answer: (解答を表示する)
最新問題: **89**
Microsoft 365 サブスクリプションをお持ちです。
Site1 という名前の Microsoft SharePoint Online サイトがあります。Site1 には、次の表に示すファイルを含むドキュメント ライブラリがあります。

Name	File type	Created on
File1	DOCX	December 1, 2023
File2	XLSX	February 5, 2024
File3	PNG	May 4, 2023

Microsoft Purview コンプライアンス ポータルから、Site1 に対して、次の図に示すように、日付が YYYY-MM-DD 形式の Search1 という名前のコンテンツ検索を作成します。

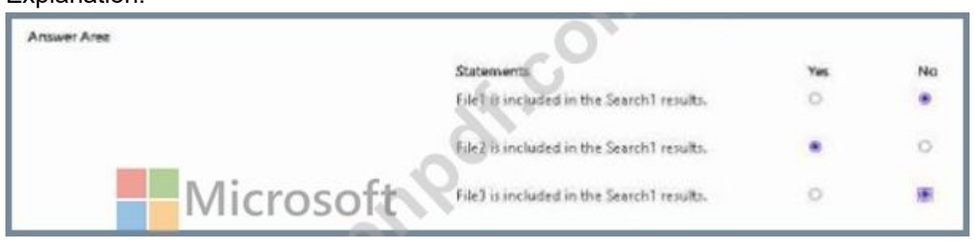


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:



最新問題**: 90**

機密情報の種類に使用される単語のリストを含む電子メールを受信します。

キーワード辞書のソースとして使用できるファイルを作成する必要があります。
リストはどの形式で保存すればよいですか?
A. 最初の行の各セルに1つの単語が含まれるXLSXファイル
B. 各単語のキーワードタグを含むXMLファイル
C. Dictionaryという名前のテーブルを含むACCDBデータベースファイル
D. 各行に1つの単語が含まれるテキストファイル
Answer: (解答を表示する**)**
辞書のキーワードはさまざまなソースから取得できますが、最も一般的なのは、サービスまたは PowerShell コマンドレットによってインポートされたファイル (.csv または .txt リストなど) です。
注記：
試験ではこの問題に複数のバージョンが出題されます。正解は2つあります。
1. カンマで区切られた単語を含むCSVファイル
2. 各行に1つの単語が含まれるテキストファイル
試験で表示される可能性のあるその他の誤った回答オプションは次のとおりです。
- タブで区切られた単語を含むTSVファイル
- 最初の行の各セルに1つの単語が含まれるXLSXファイル
- 各行に1つの単語が含まれるDOCXファイル
参照：
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-keyword- dictionary?view=o365-worldwide

最新問題: **91**
トレーニング可能な分類子をオプトインする Microsoft 365 テナントがあります。
User1 というユーザーがカスタムのトレーニング可能な分類子を作成できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 に割り当てるべきロールはどれですか?
A. グローバル管理者
B. コンプライアンス管理者
C. セキュリティオペレーター
D. セキュリティ管理者
Answer: A (メーッセージを残す**)**

最新問題: **92**
機密ラベル管理者の役割をどのユーザーに割り当てる必要がありますか?
機密ラベルを作成するための技術要件を満たす必要があります。
A. 管理者1のみ
B. Admin1とAdmin4のみ
C. Admin1とAdmin5のみ
D. Admin1、Admin2、Admin3のみ

E. Admin1、Admin2、Admin4、Admin5のみ
Answer: D (メーッセージを残す**)**
すべての管理ユーザーが Microsoft 365 の機密ラベルを作成できる必要があるという要件を満たすには、適切なユーザーに機密ラベル管理者ロールを割り当てる必要があります。
機密ラベル管理者の役割と責任
このロールにより、ユーザーは次の操作を実行できます。
Microsoft Purview で機密ラベルを作成および管理します。
自動ラベル付けポリシーを公開および構成します。
ラベルの暗号化とコンテンツのマーキングの設定を変更します。
表からの管理者ロールの確認:
コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

Admin	Role Assigned	Can Create Sensitivity Labels?
Admin1	Global Reader	□ No, read-only permissions.
Admin2	Compliance Data Administrator	□ Yes, can manage compliance data, including labels.
Admin3	Compliance Administrator	□ Yes, has full compliance management, including labels.
Admin4	Security Operator	□ No, this role is focused on security alerts and response.
Admin5	Security Administrator	□ No, primarily focused on security policies and threat management.

機密ラベル管理者ロールを割り当てる必要があるユーザー:
Admin2 ㄖンプライアンスデータ管理者）
Admin3 ㄖンプライアンス管理者）
Admin1 (グローバル リーダー) (すべての管理者がラベルを作成できるという要件を満たすには、このロールを割り当てる必要があります)。

最新問題: **93**
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Purview インサイダー リスク管理を展開します。
User1 に関連するインサイダー リスク管理イベントが特定のユーザーのみに表示されるようにする必要があります。
何を創造すべきでしょうか?
A. グローバル除外
B. インジケーターのバリアント
C. 優先ユーザーグループ
D. 検出グループ
Answer: D (メーッセージを残す**)**
ユーザーがサードパーティの生成 AI ウェブサイトと機密情報を共有するのを防ぐ必要があります。

A). 情報保護 # データを分類してラベル付けしますが、外部の AI サイトとの共有をブロックしません。
B). 情報バリア # Web アップロードではなく、ユーザー グループ間の通信を制限します (コンプライアンス ウォールなど)。
C). インサイダーリスク管理 # 危険な行為 (データの流出など) を検出しますが、データ共有を積極的にブロックすることはありません。
D). データ損失防止 (DLP) # 機密データがブラウザーや USB にコピーされたり、制限されたドメイン (ChatGPT、Bard など) にアップロードされたりするのを検出し、防止します。

最新問題: **94**
Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、User1 というユーザーと、次の表に示す機密ラベルが含まれています。

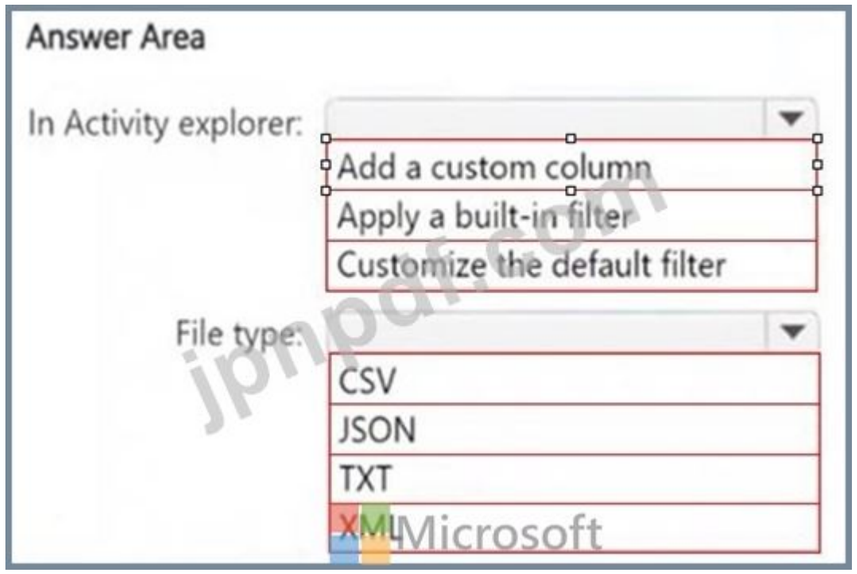
Name	Authenticated users: View content (VIEW)	Authenticated users: Copy and extract content (EXTRACT)	Authenticated users: Export content (EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

ラベルを User1 に公開します。
サブスクリプションには、次の表に示すファイルが含まれています。

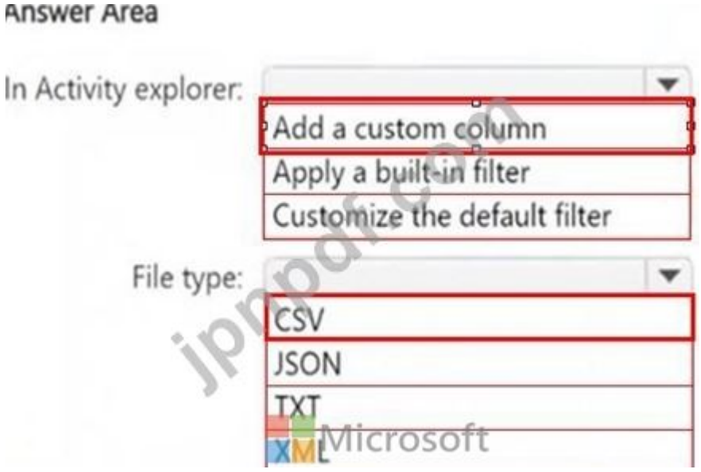
Name	Label
File1	Label1
File2	Label2
File3	Label3

Microsoft 365 Copilot は User1 のどのファイルを要約できますか?
A. ファイル2のみ
B. ファイル3のみ
C. ファイル2とファイル3のみ
D. ファイル1、ファイル2、ファイル3
Answer: A (メーッセージを残す**)**
Microsoft Learn によると、Microsoft 365 Copilot でファイル内のデータを要約するには、ユーザーはそのファイルに適用された機密ラベルに対する EXTRACT と VIEW の両方の使用権限を持っている必要があります。
これにより、Copilot は要約の目的でファイルの内容にアクセスして処理できるようになります。
ファイルが機密ラベルなしで Azure Rights Management を使用して暗号化されている場合でも、Copilot が機能するには同じアクセス許可 (EXTRACT および VIEW) が必要です。
参照：
https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-architecture-data-protection-auditing

最新問題: **95**
データ損失防止 (DLP) が実装された Microsoft 365 E5 サブスクリプションがあります。
アクティビティ エクスプローラーを使用して DLP アクティビティをエクスポートする予定です。
エクスポートされたファイルには、各 DLP ルールの一致で検出された機密情報の種類が表示される必要があります。
データをエクスポートする前にアクティビティ エクスプローラーで何を行う必要がありますか? また、ファイルはどのファイル形式でエクスポートされますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **96**

ホットスポットに関する質問

Contoso と Fabrikam という2つの Microsoft 365 サブスクリプションがあります。これらのサブスクリプションには、次の表に示すユーザーが含まれています。

Name	Subscription	Email address
User1	Contoso	user1@contoso.com
User2	Contoso	user2@contoso.com
User3	Fabrikam	user3@fabrikam.com
User4	Fabrikam	user4@fabrikam.com

図に示すように、Sensitivity1」という機密ラベルがあります。（図のタブをクリックします）

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

- ○ Remove access control settings if already applied to items
- ◉ Configure access control settings

ⓘ Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting

Go to co-authoring setting

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

Never

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

2 items

Users and groups	Permissions	Edit	Delete
contoso.com	Co-Owner		
fabrikam.com	Reviewer		

☐ Use dynamic watermarking ⓘ

次の表に示すファイルがあります。

Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can edit rights for File1.	○	○
User2 can edit rights for File3.	○	○
User3 can print File2.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can edit rights for File1.	○	○
User2 can edit rights for File3.	○	○
User3 can print File2.	○	○

Explanation:

ボックス1: はい

User1 は Contoso サブスクリプションに含まれており、電子メール アドレスは user1@contoso.com です。機密ラベル Sensitiviy1 は contoso.com ユーザーに共同所有者のアクセス許可を割り当てています。

File1 には、自動ラベル付けポリシーを使用して Sensitiviy1 が自動的に適用されています。

ボックス2: はい

User2 は Contoso サブスクリプションに属しており、電子メール アドレスは user2@contoso.com です。機密ラベル Sensitiviy1 により、contoso.com ユーザーに共同所有者のアクセス許可が割り当てられています。

File3 には User1 によって Sensitiviy1 が適用されています。

ボックス3: いいえ
User3 は Fabrikam サブスクリプションに含まれており、電子メール アドレスは user3@fabrikam.com です。機密ラベル Sensitiviy1 によって、fabrikam.com ユーザーにレビュー担当者権限が割り当てられています。
File2 には User2 によって Sensitiviy1 が適用されています。
参照：
https://learn.microsoft.com/en-us/purview/暗号化の感度ラベル

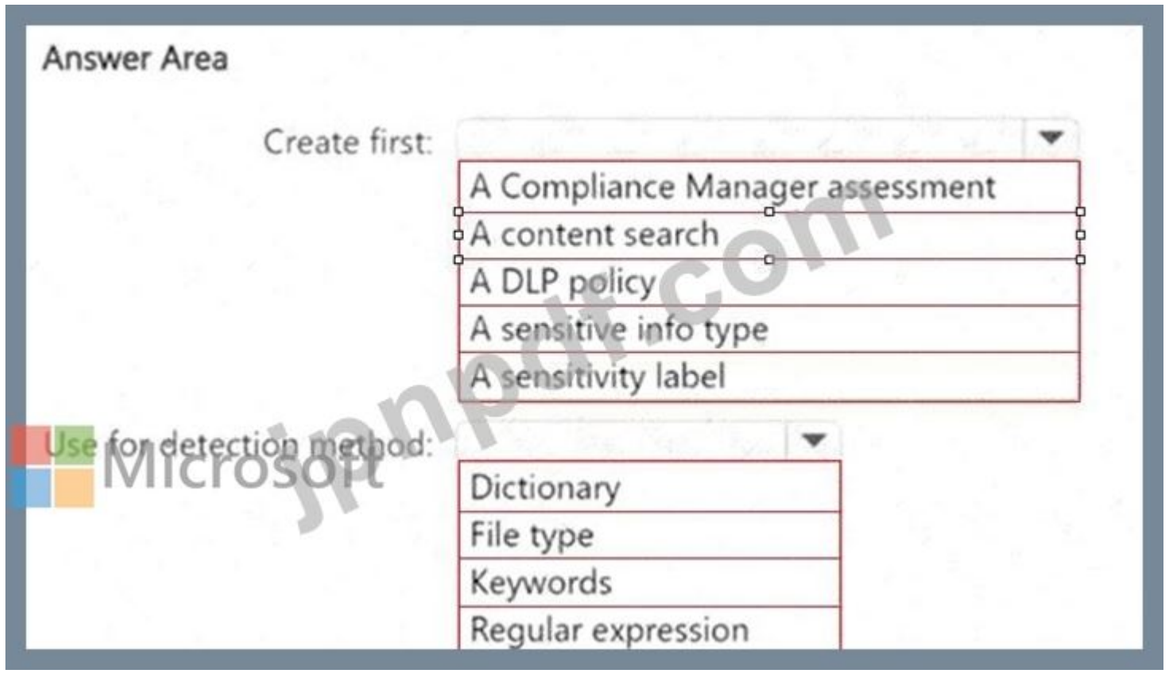
最新問題: **97**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションをお持ちです。次の要件を満たす
コンプライアンス ソリューションを実装する必要があります。
- 主要なセキュリティ関連のユーザーアクティビティのクリップをキャプチャします。
企業の機密データの流出。
- データ損失防止（DLP）機能とインサイダーリスクを統合
管理。
各要件には何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

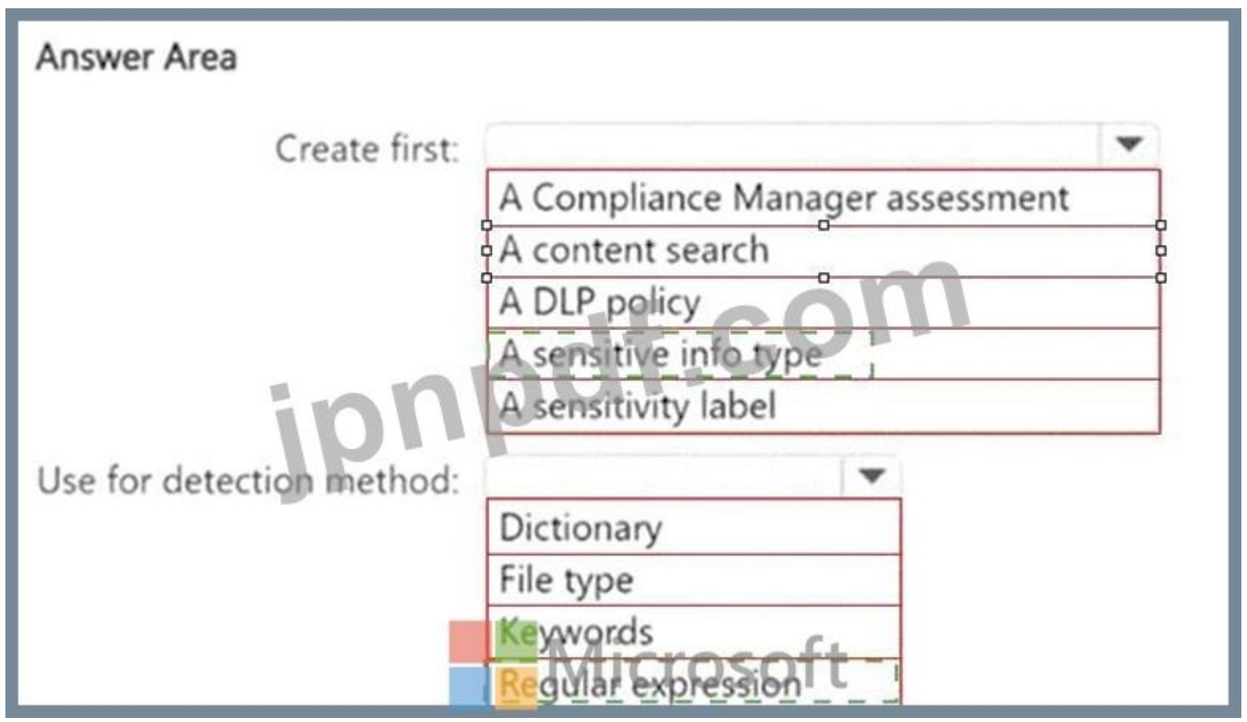
Answer Area

Explanation:
ボックス1 :Microsoft Purview Insider Risk Managementのフォレンジック証拠を利用することで、組織は機密データの流出未遂など、セキュリティ関連のユーザーアクティビティの画面録画をキャプチャできます。この機能は、リスクの高い行動に関するコンテキストを提供し、調査担当者がインシデントをより効果的に分析するのに役立ちます。
ボックス2 :Adaptive Protectionは、Microsoft Purview Insider Risk ManagementとDLPを連携させ、検出されたユーザーリスクに基づいて動的に保護を適用します。インサイダーリスクのシグナルに基づいて適用範囲を自動調整することでDLPポリシーを強化し、高リスクユーザーにはより厳格なデータ制御を提供しながら、低リスクユーザーの負担を最小限に抑えます。

最新問題**: 98**
ホットスポット
機密文書の技術要件を満たす必要があります。
最初に何を作成し、検出方法に何を使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



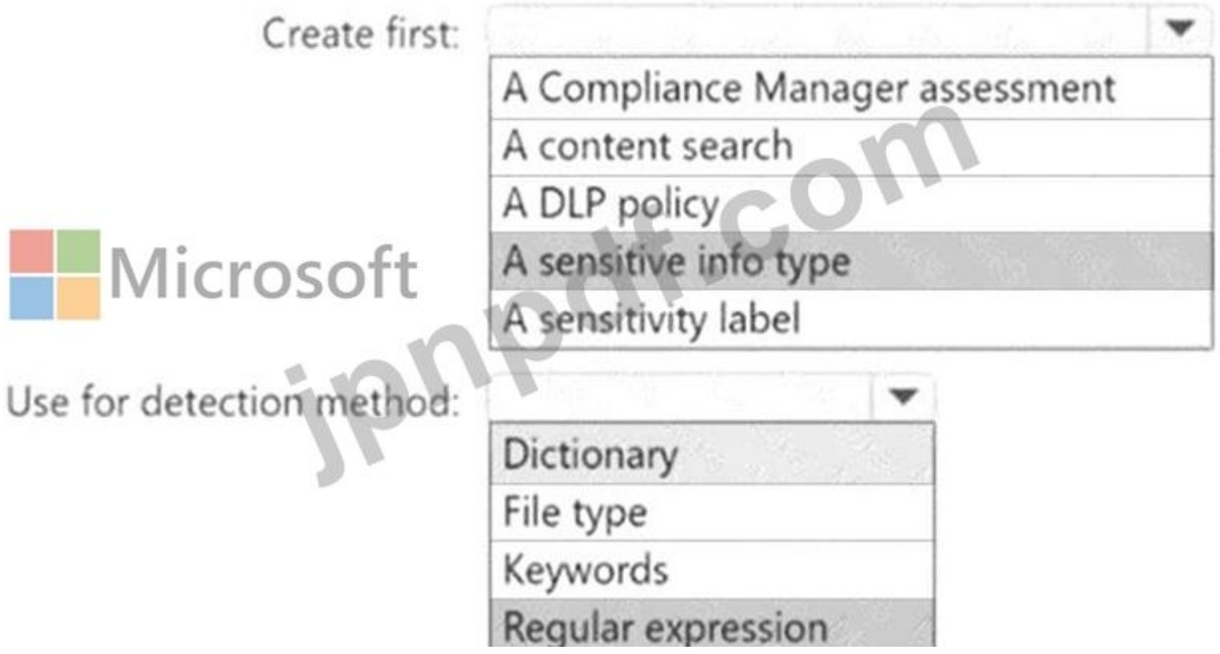
Answer:



Explanation:

コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

Answer Area



機密文書を検出して保護するには、次のコードで始まるプロジェクトコードを識別するカスタムルールが必要です。
999（機密情報であるため）。
ボックス1：機密情報タイプ（SIT）により、Microsoft Purview DLPポリシーは構造化データ（例プロジェクトコード）を認識できます。DLPポリシーでは、パターン、キーワード、または辞書用語に基づいてコンテンツを検出するために、機密情報タイプが必要です。機密ラベルだけでは検出ロジックは定義されません。これは、コンテンツが識別された後の分類と保護に使用されます。
ボックス 2: プロジェクト コードは構造化された 10 桁のパターンに従うため、999 で始まるプロジェクト コードを一致させるには正規表現 (Regex) を使用する必要があります。
正規表現パターンの例:
999\d{7}
このパターンは、「999」で始まる 10 桁の数字を検出します。

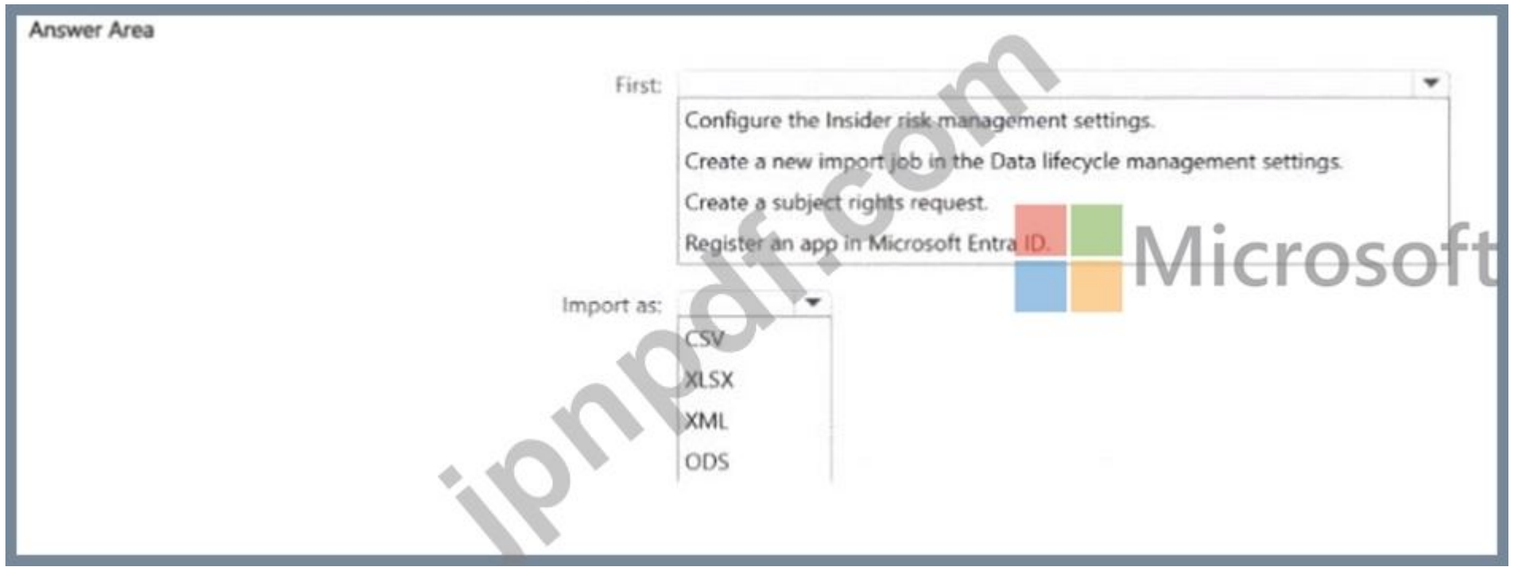
最新問題: **99**
DLP1 という名前のデータ損失防止 (DLP) ポリシーを含む Microsoft 365 E5 サブスクリプションがあります。DLP1 には、表に示す DLP ルールが含まれています。

Name	Priority	User notifications	Policy tip	If there's a match for this rule, stop processing additional DLP policies and rules
Rule1	0	On	Tip 1	Enabled
Rule2	1	On	Tip 2	Enabled
Rule3	2	On	Tip 3	Disabled
Rule4	3	On	Tip 4	Enabled

ドキュメントがすべてのルールに一致する場合、ユーザーにヒント 2 が表示されるようにする必要があります。
何を変えるべきでしょうか?
A. ルール2の優先度を0に設定する
B. ルール2の優先度設定を2にする

C. ルール3とルール4の優先度を0に設定する
D. このルールに一致する場合、追加のDLPポリシーとルールの処理を停止する設定をRule3で有効にする
Answer: A (メーッセージを残す**)**
確実に処理されるように、Rule2 の優先度を最高、値を最低の 0 に設定します。
注: Priorityパラメータは、ポリシーの処理順序を決定するポリシーの優先度値を指定します。値が小さいほど優先度が高く、値0が最高優先度となります。
参照：
https://techcommunity.microsoft.com/discussions/microsoft-365/dlp-policy-order/2197427

最新問題**: 100**
Microsoft 36S ES サブスクリプションをお持ちです。
Microsoft Purview ポータルを使用して、インサイダー リスク管理ポリシーで使用する人事 (HR) データをマッピングする予定です。
HR データをインポートするには、データ コネクタを追加する必要があります。
最初に何をすべきか、またどのような形式でデータをインポートすべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Explanation:

ステップ1 - 要件
このシナリオでは、Microsoft Purview Insider Risk Management を使用して人事データ（従業員の入社日、退職日、部署異動など）をインポートする必要があります。人事データコネクタを使用すると、インサイダーリスクポリシーで従業員のシグナルを利用し、危険なユーザーアクティビティを検出できます。
ステップ2 - 最初に何をすべきか
人事データをインポートする前に、Microsoft Purviewコンプライアンスポータルで Insider Risk Managementの設定を構成する必要があります。これは、人事データコネクタとポリシーを作成するための前提条件です。
参考：Microsoft PurviewでInsider Risk ManagementのHRデータを構成する 手順3 - インポート形式 Insider Risk ManagementのHRデータはCSVファイルとしてインポートされます。CSVには、ユーザープリンシパル名、イベントの種類、開始日、終了日などの必須フィールドが含まれている必要があります。その他の形式（XLSX、XML、ODS）は、Purview Insider Risk HRデータコネクタではサポートされていません。
参考: Insider Risk Management の HR コネクタ CSV スキーマ

最新問題**: 101**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションの質問に回答した後は、その質問に戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 エンドポイントのデータ損失防止 (エンドポイント DLP) を実装します。
Windows 11 を実行し、Microsoft 365 アプリがインストールされたコンピューターがあります。これらのコンピューターは Microsoft Entra テナントに参加しています。
エンドポイント DLP ポリシーがコンピューター上のコンテンツを保護できることを確認する必要があります。
解決策: Microsoft Purview Information Protection クライアントをコンピューターに展開します。

これは目標を満たしていますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
正しい：
* エンドポイント DLP 構成パッケージをコンピューターに展開します。
* コンピューターを Microsoft Defender for Endpoint にオンボードします。
正しくない：
* 統合ラベル付けクライアントをコンピューターに展開します。
* コンピューターを Microsoft Intune に登録します。
* Microsoft Purview Information Protection クライアントをコンピューターに展開します。
参照：
https://docs.microsoft.com/ja-jp/microsoft-365/compliance/endpoint-dlp-getting-started
https://docs.microsoft.com/ja-jp/microsoft-365/security/defender-endpoint/configure-endpoints

最新問題: **102**
ホットスポットに関する質問
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Role group
Admin1	Insider Risk Management Admins
Admin2	Insider Risk Management Analysts
Admin3	Risk Management Investigators
Admin4	Insider Risk Management Auditors

Case1 という名前の Microsoft Purview インサイダー リスク管理ケースを作成する予定です。
最初にどのインサイダー リスク管理オブジェクトを選択する必要がありますか? また、どのユーザーがデフォルトで Case1 の投稿者として追加されますか?
回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Object:

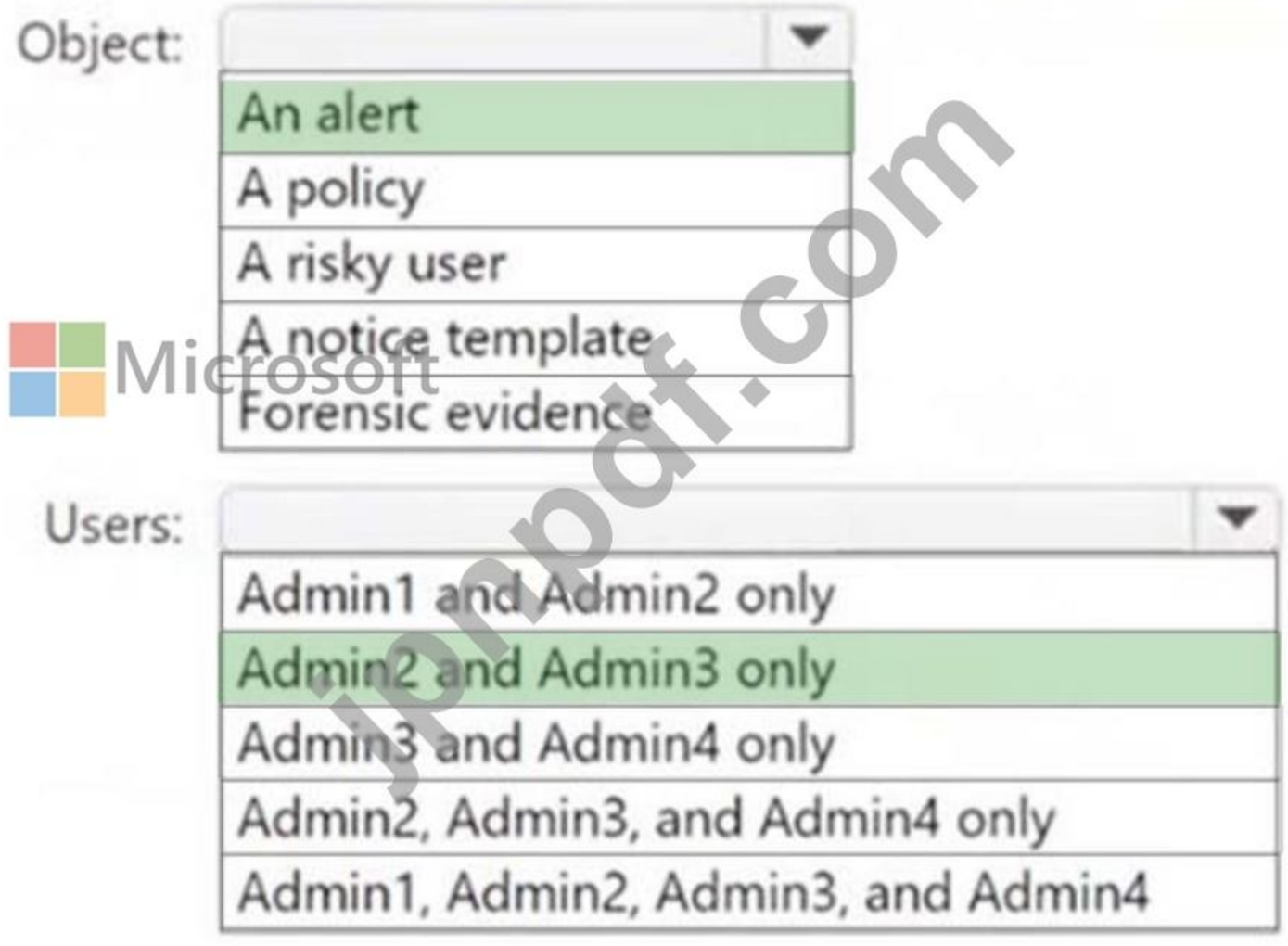
- An alert
- A policy
- A risky user
- A notice template
- Forensic evidence

Users:

- Admin1 and Admin2 only
- Admin2 and Admin3 only
- Admin3 and Admin4 only
- Admin2, Admin3, and Admin4 only
- Admin1, Admin2, Admin3, and Admin4

Answer:

Answer Area



Explanation:
ボックス1: 警告
Microsoft Purview インサイダー リスク管理でケースを作成するには、常にアラートから開始します。
ボックス2: Admin2とAdmin3のみ
調査と分析の役割を持つため、デフォルトでは Admin2 と Admin3 のみが貢献者として追加されます。

最新問題**: 103**
次の表に示すデバイスが含まれる Microsoft 36S ES サブスクリプションがあります。

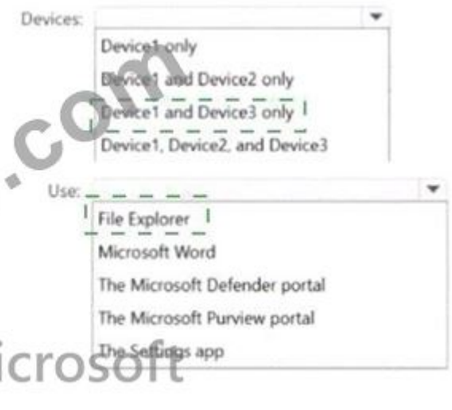
Name	Platform	Chipset
Device1	Windows 11	x64
Device2	Windows 11	ARM64
Device3	Windows 10	x86

Microsoft Purview Information Protection の機密ラベルを公開します。
情報保護クライアントをデバイスに導入する予定です。ソリューションでは、機密性の高い画像や文書にラベルを適用できる必要があります。情報保護クライアントをインストールできるデバイスはどれですか？また、ユーザーはラベルを適用するために何を使用する必要がありますか？
回答するには、回答エリアで適切なオプションを選択してください。

Answer Area

Answer:

Answer Area



Explanation:

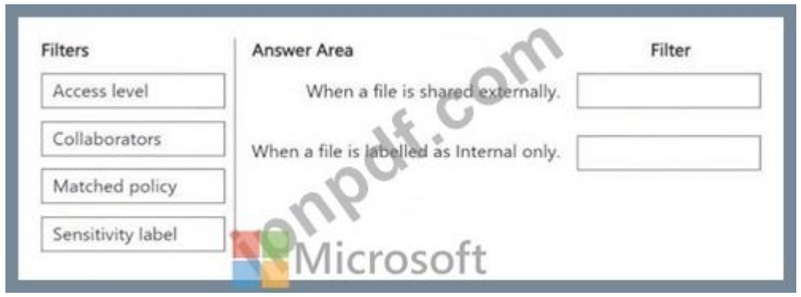
Answer Area

ステップ1 - 要件を理解する
このタスクは、Azure Information Protection (AIP) 統合ラベル付けクライアントを使用して、機密画像やドキュメントに Microsoft Purview Information Protection 機密ラベルを適用することです。
Purview の機密ラベルは Microsoft 365 アプリ (Word、Excel、Outlook、PowerPoint) に適用できますが、画像、PDF、その他のドキュメントなどの Office 以外のファイルにラベルを付けるには、ユーザーは AIP 統合ラベル付けクライアントを使用する必要があります。
AIP クライアントがインストールされている場合は、ファイルを右クリックしてファイル エクスプローラーで直接ラベルを適用できます。
ステップ2 - デバイスの互換性
AIP 統合ラベル付けクライアントは、Windows デバイスでのみ実行されます。
質問のコンテキスト (提供されたドロップダウンに基づく) では、リストされているすべてのデバイス (Device1、Device2、Device3) は互換性のある Windows エンドポイントです。
したがって、AIP クライアントは 3 つのデバイスすべてに展開できます。
ステップ3 - ユーザーがラベルを適用する方法
Office ドキュメントの場合、# ラベルは Word、Excel、PowerPoint 内のリボンから適用できます。
その他のファイル タイプ (画像、PDF、テキスト ファイルなど) の場合、# ラベルは AIP クライアント経由でファイル エクスプローラーを使用して適用する必要があります。
参照：
Azure Information Protection 統合ラベル付けクライアントをインストールして使用する Microsoft Purview でファイルとメールに機密ラベルを適用する

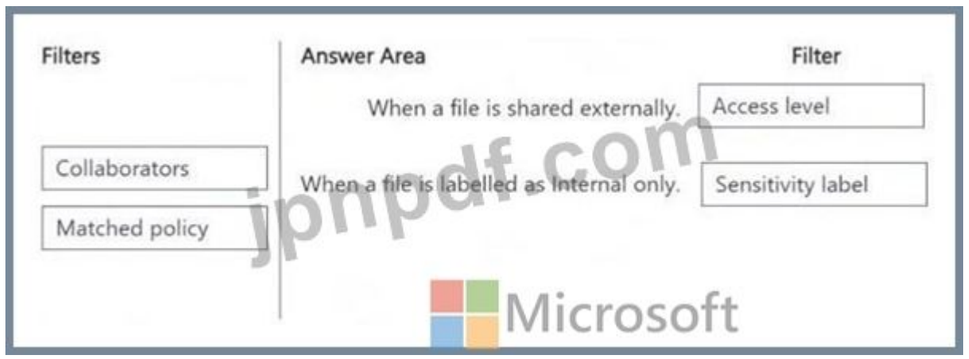
最新問題: **104**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーがデータ損失防止 (DLP) で保護されたドキュメントを次のサードパーティの Web サイトにアップロードできないようにする必要があります。
web1.contoso.com
web2.contoso.com
ソリューションでは管理の労力を最小限に抑える必要があります。
エンドポイント DLP のサービス ドメイン設定を何に設定する必要がありますか?
A. contoso.com
B. web*.contoso.com
C. *.contoso.com
D. web1.contoso.com と web2.contoso.com
Answer: (解答を表示する**)**
Microsoft 365 エンドポイントデータ損失防止（エンドポイント DLP）の「サービスドメイン」設定により、管理者は特定のドメインからのファイルアップロードをブロックまたは許可できます。これは、ユーザーが DLP で保護されたドキュメントを web1.contoso.com および web2.contoso.com にアップロードするのを防ぐことを目的としています。
サービス ドメインを「web1.contoso.com と web2.contoso.com」に設定すると、特定の 2 つのサードパーティ Web サイトが正確にターゲットとなり、管理の労力を最小限に抑えながら厳密な制御が保証されます。

最新問題: **105**
ドラッグアンドドロップの質問

Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションがあります。
次の条件が満たされたときにトリガーされる Defender for Cloud Apps ファイル ポリシーを展開する予定です。
- ファイルが外部と共有されています。
- ファイルは内部専用としてラベル付けされています。
各条件にどのフィルターを使用すべきでしょうか？適切なフィルターを正しい条件にドラッグしてください。各フィルターは1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:
Microsoft Defender for Cloud Apps の 「アクセス レベル」フィルターは、組織外で外部共有されているかどうかなど、ファイルがどのように共有されているかを識別するのに役立ちます。
「機密ラベル」フィルターは、内部のみなどの特定の Microsoft Purview 機密ラベルで分類されたファイルを追跡するために使用され、内部分類のファイルが適切に監視および保護されることを保証します。
「共同作業者」フィルターは、アクセス権はあるが外部共有を示していないユーザーを追跡します。
「一致したポリシー」フィルターは、事前定義されたポリシーに基づいてファイルを識別しますが、外部共有または機密ラベルを直接フィルター処理しません。

最新問題**: 106**
完全データー致 (EDM) を使用するカスタムの機密情報の種類を作成する予定です。
Microsoft 365 にアップロードするものと、アップロードに使用するツールを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Upload:

- Data hashes
- Data in the XML format
- Digitally signed data

Use:

- Azure Storage Explorer
- EDM upload agent
- Microsoft Purview portal
- The Set-DlpKeywordDictionary cmdlet

Answer:

Answer Area

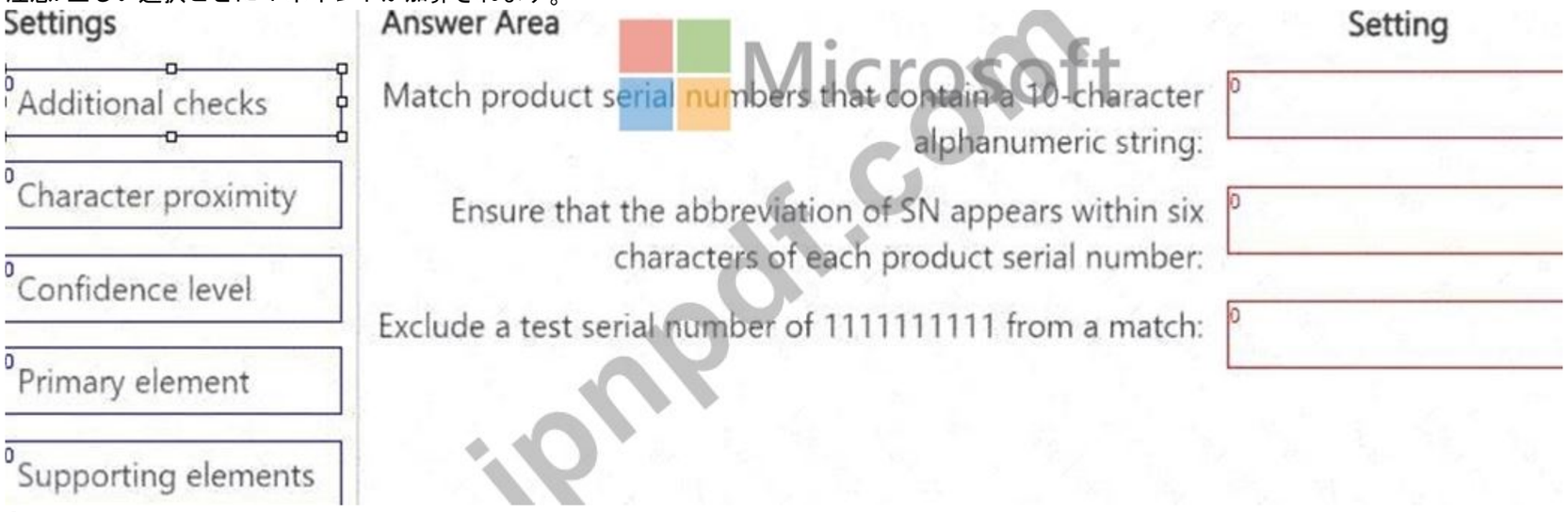
Upload:

- Data hashes
- Data in the XML format
- Digitally signed data

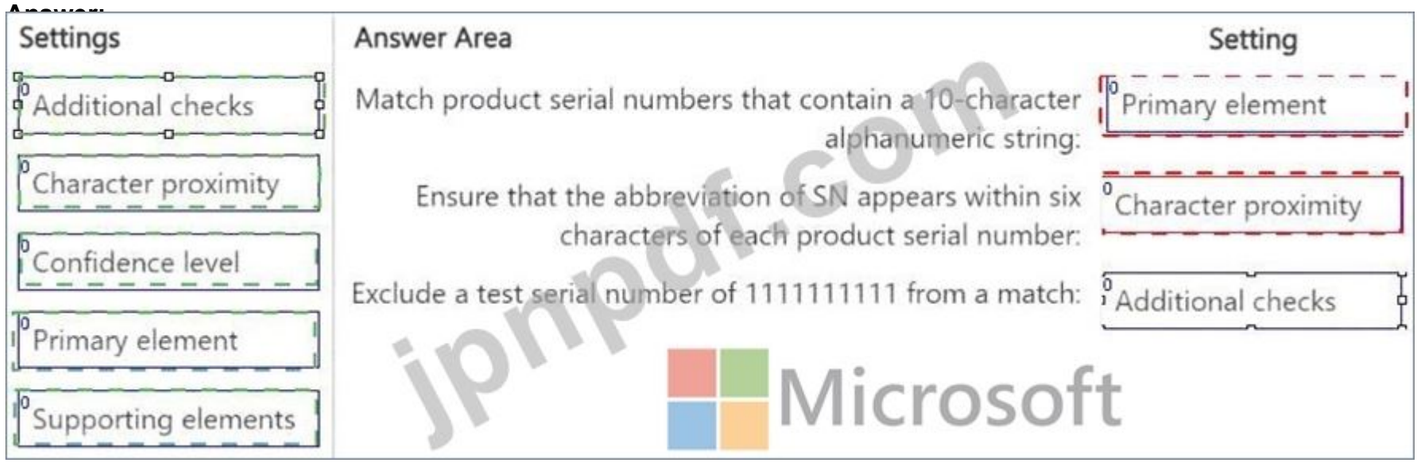
Use:

- Azure Storage Explorer
- EDM upload agent
- Microsoft Purview portal
- The Set-DlpKeywordDictionary cmdlet

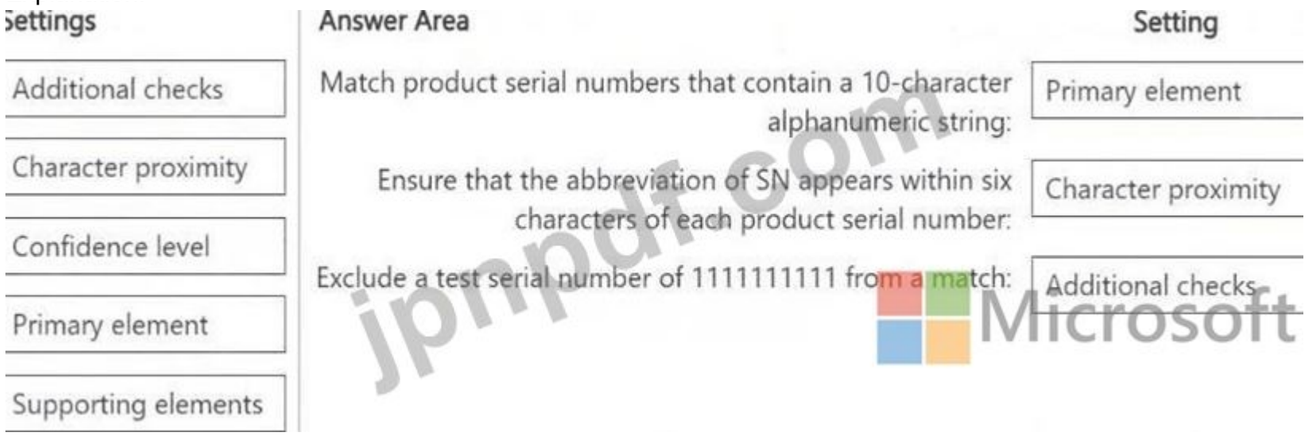
最新問題: **107**
ドラッグ＆ドロップ
データ損失防止 (DLP) が実装された Microsoft 365 E5 サブスクリプションがあります。
カスタムの機密情報タイプを作成する必要があります。ソリューションは以下の要件を満たす必要があります。
10 文字の英数字文字列を含む製品のシリアル番号を一致させます。
SN の略語が各製品シリアル番号の 6 文字以内に表示されていることを確認します。
テストシリアル番号 1111111111 を一致から除外します。
各要件に対してどのパターン設定を行うべきでしょうか？適切な設定を正しい要件にドラッグしてください。各設定は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: 108

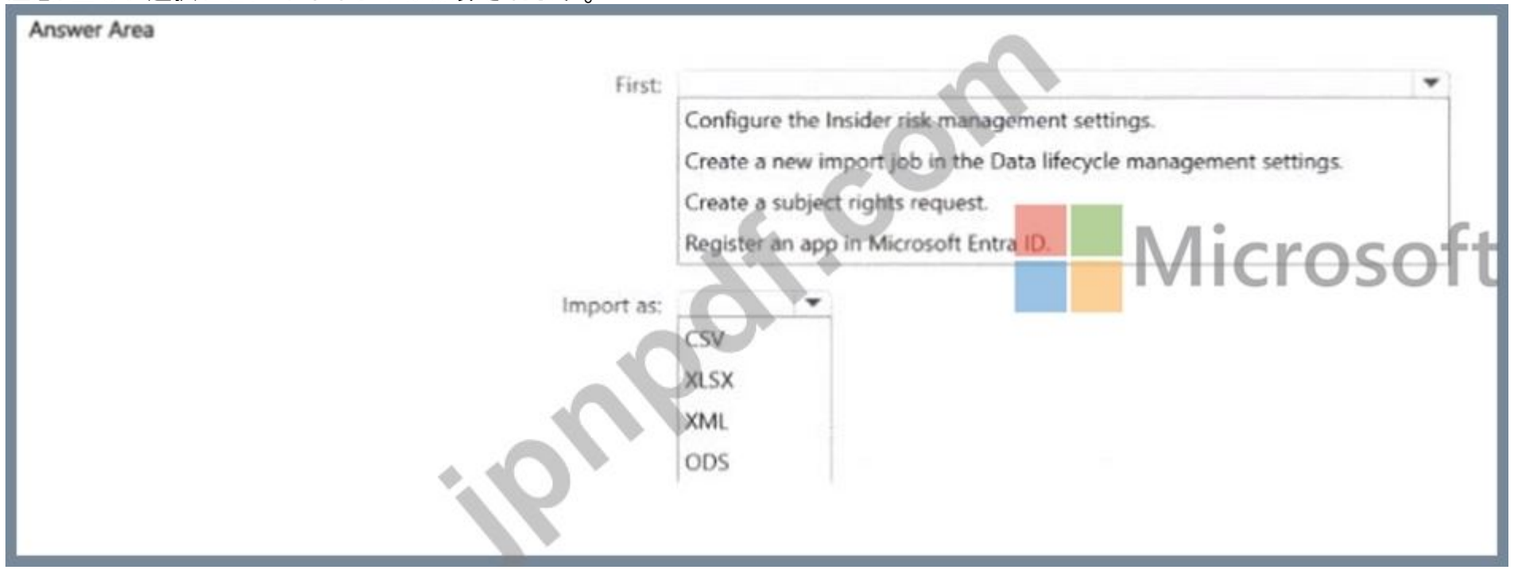
Microsoft 36S ES サブスクリプションをお持ちです。

Microsoft Purview ポータルを使用して、インサイダー リスク管理ポリシーで使用する人事 (HR) データをマッピングする予定です。

HR データをインポートするには、データ コネクタを追加する必要があります。

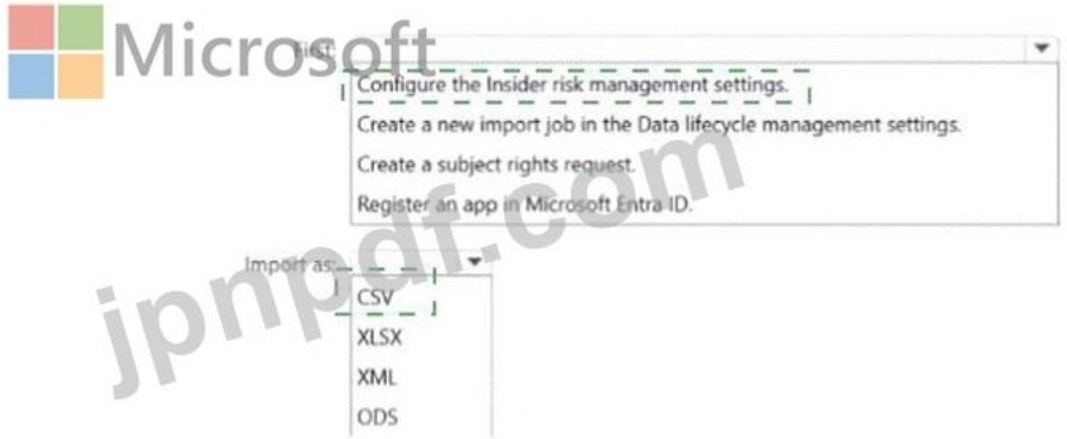
最初に何をすべきか、またどのような形式でデータをインポートすべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Answer Area



Explanation:

最新問題: 109

Microsoft 365 E5 サブスクリプションをお持ちです。

次の表に示す時間にトリガーされる、Policy1 および Policy2 という名前の 2 つのアラート ポリシーを作成します。

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

Microsoft Purview ポータルに追加されるアラートの数はいくつですか?

A. 2
B. 3
C. 4
D. 5
E. 6

Answer: (解答を表示する**)**

Microsoft Purview では、複数のアラート ポリシーによってアラートがトリガーされると、冗長性を回避するために、短期間 (通常 5 分) 内の重複したアラートが抑制されることがあります。
ステップバイステップの分析:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

10:00:04 の Policy1 は無視されます。これは、Policy1 がすでに 10:00:00 にトリガーされており、5 分以内であるためです。
10:00:31 の Policy2 は無視されます。これは、Policy2 がすでに 10:00:03 にトリガーされており、5 分以内であるためです。
10:01:01 の Policy1 は、前の Policy1 アラートから 1 分以上経過しているため、新しいアラートです。
10:04:45 の Policy1 は、前の Policy1 アラートから 3 分以上経過しているため、新しいアラートです。

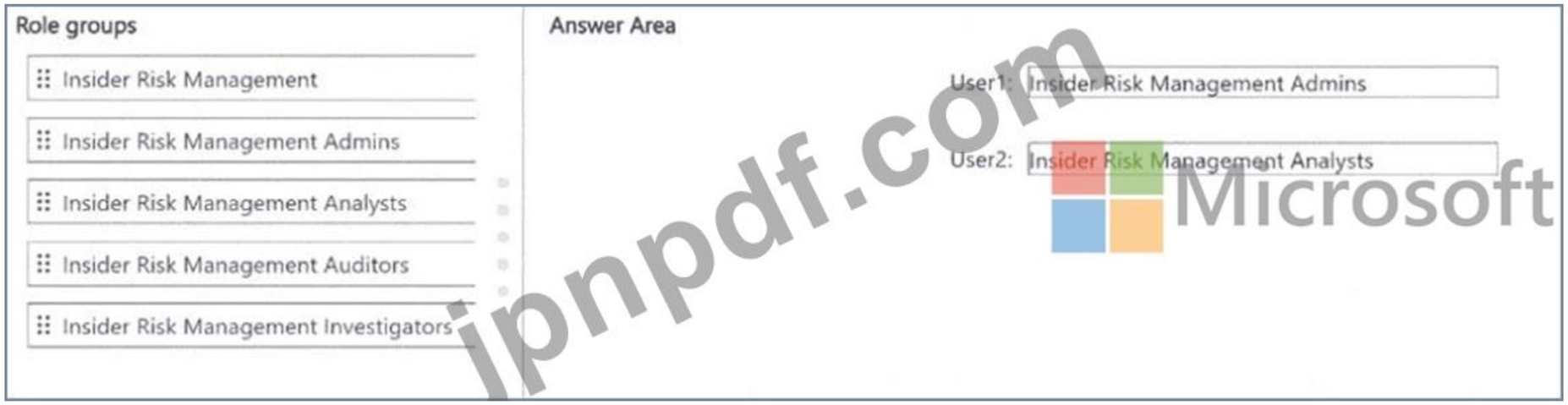
最新問題: **110**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft 365 Copilot の使用状況レポートを確認する必要があります。
レポートはどこから確認すればよいですか?
A. Microsoft Purview ポータルの情報保護
B. Microsoft 365 管理センター
C. Microsoft Purview ポータルの AI 向け DSPM
D. Microsoft Defender ポータル
Answer: B (メーッセージを残す**)**
Microsoft 365 Copilot 使用状況レポートを確認するには:
- Microsoft 365 管理センターに移動します。
- 〖レポート」> 使用状況」に移動します。

- 採用と使用状況の指標を表示するには、Copilot」を選択します。
管理センターでは、組織全体で Copilot がどのように使用されているかについての分析情報が提供され、エンゲージメントと有効性の追跡に役立ちます。
Microsoft Purview ポータルの AI 向けデータ セキュリティ ポスチャ管理 (DSPM) は、AI の使用状況に関する分析情報を提供しますが、標準的な使用状況メトリックではなく、セキュリティとコンプライアンスに重点を置いています。
https://learn.microsoft.com/en-us/purview/ai-microsoft-purview

最新問題**: 111**
Microsoft 365 E5 サブスクリプションがあり、そこには User! と User2 という 2 人のユーザーが含まれています。
インサイダーリスク管理を実装する必要があります。ソリューションは以下の要件を満たす必要があります。
* User1 がインサイダー リスク管理ポリシーを作成できることを確認します。
* ユーザー2がインサイダーリスク管理ポリシーを使用してキャプチャしたコンテンツを使用できることを確認する
* 最小権限の原則に従ってください。
各ユーザーをどのロールグループに追加すればよいでしょうか？適切なロールグループを適切なユーザーにドラッグしてください。各ロールグループは、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:



最新問題: **112**
Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
ユーザーが Site1 上の機密情報を外部の受信者と共有するときにアラートを生成する Microsoft Purview インサイダー リスク管理ソリューションを展開する必要があります。
実行すべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正解ごとに 1 ポイントが加算されます。
A. 分析をオンにします。
B. インジケーターをオンにします。
C. 適応型保護を構成します。
D. インサイダー リスク ポリシーを作成します。
E. データ損失防止 (DLP) ポリシーを作成します。
Answer: (解答を表示する)
インサイダー リスク ポリシーによってリスク評価に使用されるファイル共有や機密データへのアクセスなどのユーザー アクティビティの監視を有効にするには、インジケーターをオンにする必要があります。
インサイダー リスク ポリシーを作成すると、外部ユーザーへのデータ漏洩などのリスク シナリオを定義し、SharePoint Online (サイト 1) からの機密情報の共有など、ポリシー条件が満たされたときにアラートをトリガーできます。
参照：
https://learn.microsoft.com/en-us/purview/insider-risk-management-settings-policy-indicators

最新問題: **113**
Microsoft 365 サブスクリプションをお持ちです。
次の表に示す Microsoft Purview 監査ソリューションを使用するかどうかを評価しています。

Name	Description
Solution1	Control auditing by using audit log retention policies.
Solution2	Export audit records to a CSV file.
Solution3	Retain audit logs for one year.

Microsoft Purview Audit (Standard) を実装する予定です。
どのようなソリューションを使用できますか?

A. ソリューション1、ソリューション2、ソリューション3
B. ソリューション1とソリューション2のみ
C. ソリューション2のみ
D. ソリューション2とソリューション3のみ
E. ソリューション3のみ
Answer: C (メーッセージを残す)

最新問題: **114**
Channel1 という名前の Microsoft Teams チャネルを含む Microsoft 365 E5 サブスクリプションがあります。
Channel1 には研究開発文書が含まれています。
サブスクリプションに Microsoft 365 Copilot を実装する予定です。
Channel1 に保存されているファイルの内容が、Copilot によって生成された回答に含まれて、権限のないユーザーに表示されるのを防ぐ必要があります。
何を使うべきでしょうか?
A. データ損失防止 (DLP)
B. Microsoft Purview インサイダーリスク管理
C. Microsoft Purview 情報バリア
D. 機密ラベル
Answer: D (メーッセージを残す)
Channel1 に保存されているファイルの内容が Microsoft 365 Copilot の応答に含まれないようにし、権限のないユーザーがアクセスできないようにするには、Microsoft Purview 秘密度ラベルを使用する必要があります。
機密ラベルを使用すると、機密ファイルを分類、保護、アクセス制限できます。ラベルベースの暗号化とアクセス制御ポリシーを設定することで、Channel1内のファイルへのアクセスや操作を、承認されたユーザーのみが行えるようにすることができます。Microsoft 365 Copilotは機密ラベルを尊重します。つまり、ファイルに制限付きアクセスのラベルが付けられている場合、Copilotは承認されていないユーザー向けのレスポンスを生成する際にそのラベルを使用しません。

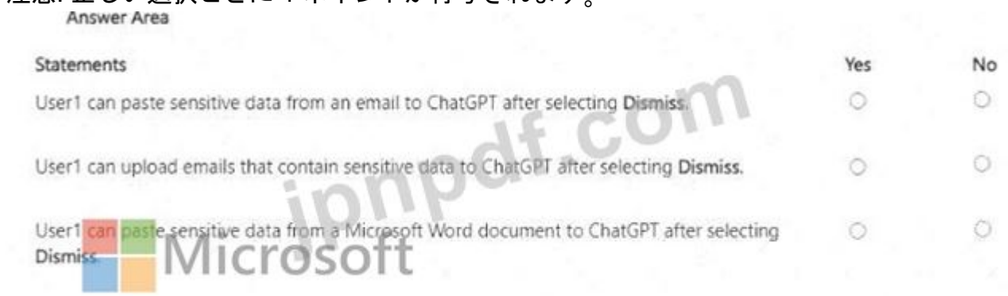
最新問題: **115**
Microsoft 365 E5 サブスクリプションがあり、User1 というユーザーが登録されています。このサブスクリプションには、「アクション」の図に示すように、エンドポイント データ損失防止 (エンドポイント DLP) ポリシーが含まれています。(「アクション」タブをクリックします。)

アップロード制限の図に示すように、制限されたクラウド サービス ドメインへのアップロードまたは許可されていないブラウザーからのアクセスの設定を構成します。([アップロード制限] タブをクリックします。)

サポートされているブラウザへの貼り付け設定は、貼り付けの制限」の図に示すように構成します。(貼り付けの制限」タブをクリックします。)

ユーザー 1 が ChatGPT にコンテンツを貼り付けると、エラー展示に示されているエラー メッセージが表示されます。
([エラー] タブをクリックします。)

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

Explanation:

最新問題: 116

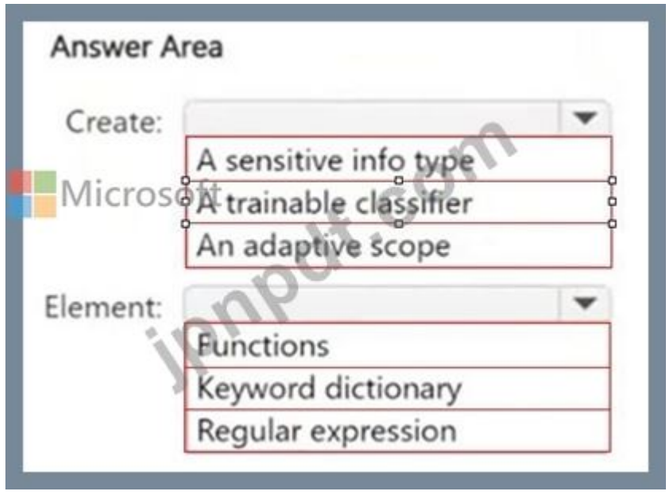
Microsoft 365 E5 サブスクリプションをお持ちです。

1,000 件の顧客名のリストが含まれる Customer.csv という名前のファイルがあります。

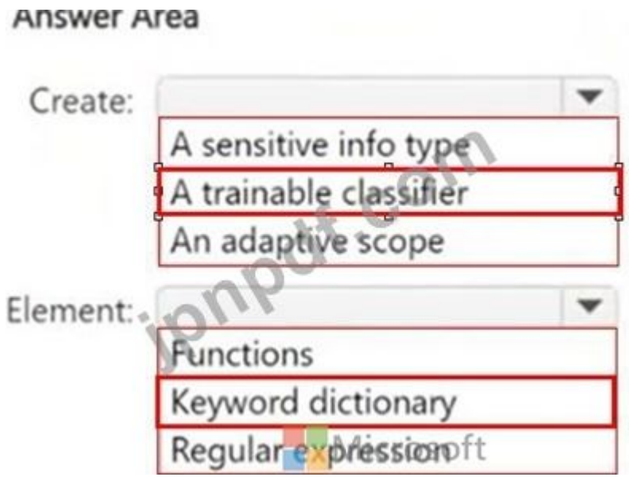
Customer.csv を使用して、Microsoft SharePoint Online ライブラリに保存されているドキュメントを分類する予定です。

Microsoft Purview ポータルで何を作成する必要がありますか? また、どのタイプの要素を選択する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **117**

Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という 3 人のユーザーと Filetdocx というファイルが含まれています。

次の図に示すように、Label1 という名前の機密ラベルを作成します。

Label1 を File1 に適用します。

Microsoft 365 Copilot はどのユーザー向けに File1 を要約できますか?

A. ユーザーなし

B. ユーザー1のみ

C. ユーザー1とユーザー2のみ

D. ユーザー1、ユーザー2、ユーザー3

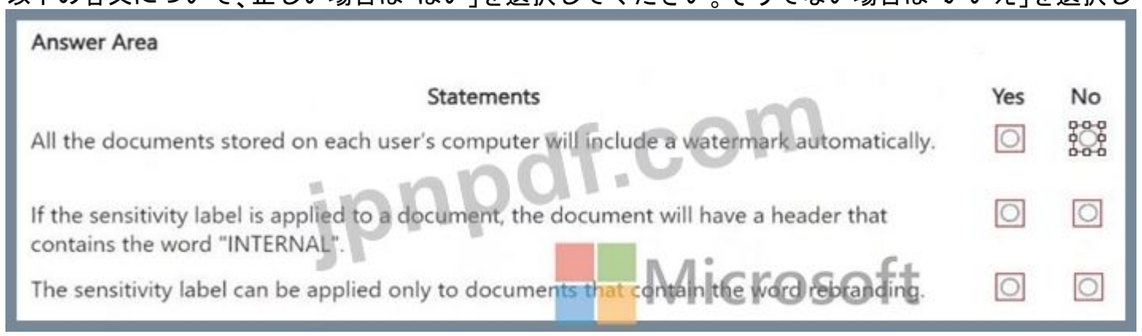
Answer: (解答を表示する**)**

機密ラベルLabel1は、権限（User1 = 共同作成者、User2 = レビュー担当者、User3 = 閲覧者）を割り当て、二重キー暗号化（DKE）を有効にします。Microsoft 365 Copilotは、サービスがユーザーの権限を使用して

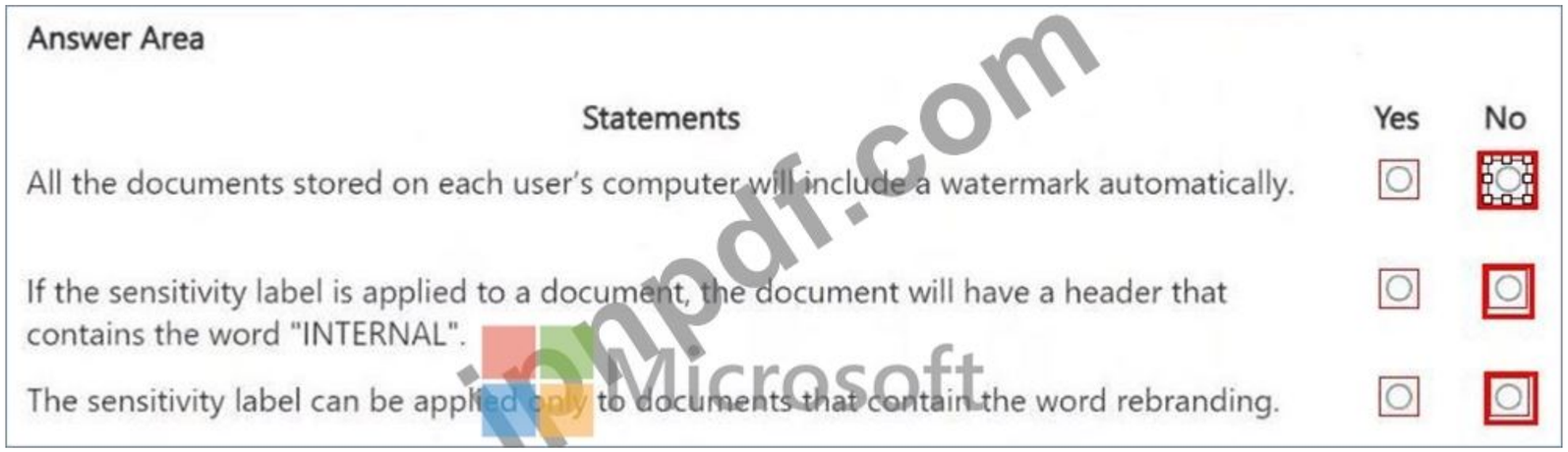
ファイルにアクセスできる場合にのみ、コンテンツを要約できます。二重キー暗号化で保護されたコンテンツは、Microsoftクラウドサービス（Copilotを含む）からアクセスできません。そのため、ユーザーがOfficeアプリでファイルを開くことができる場合でも、CopilotはDKEで保護されたファイルを開いたり処理したりすることはできません。
したがって、Microsoft 365 Copilot を使用して File1 を要約するユーザーはいません。
参考: Microsoft Purview Double Key Encryption - Copilot および検索インデックス作成を含む Microsoft クラウド サービスのサービス アクセス制限。

最新問題**: 118**
次の図に示すように、Microsoft Entra テナント内のすべてのユーザーに公開されている Microsoft 365 機密ラベルがあります。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。



Answer:



最新問題: 119

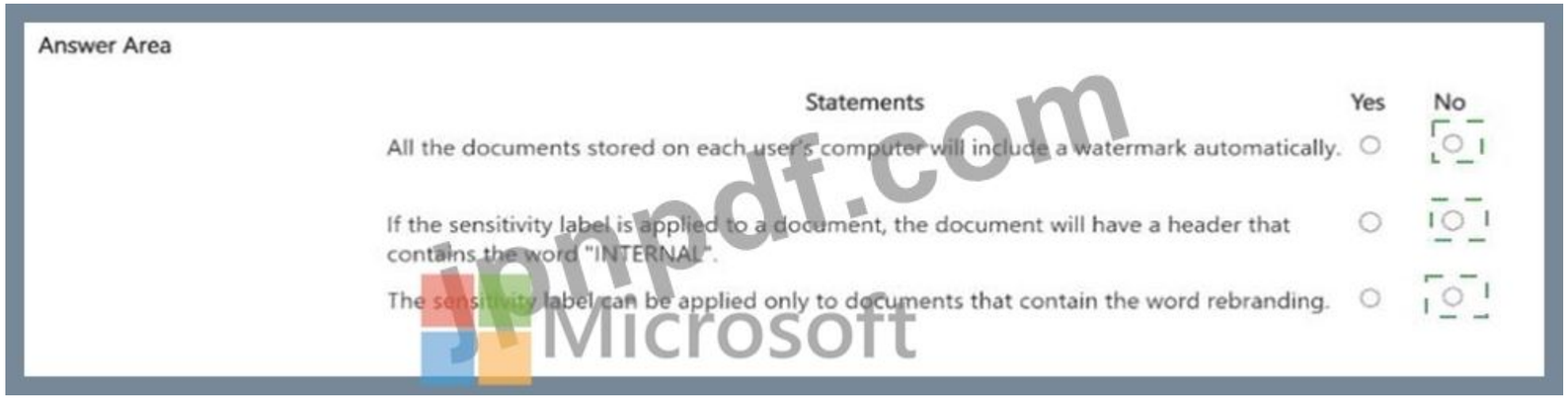
次の図に示すように、Microsoft Entra テナント内のすべてのユーザーに公開されている Microsoft 365 機密ラベルがあります。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択は1つにつき1点です。

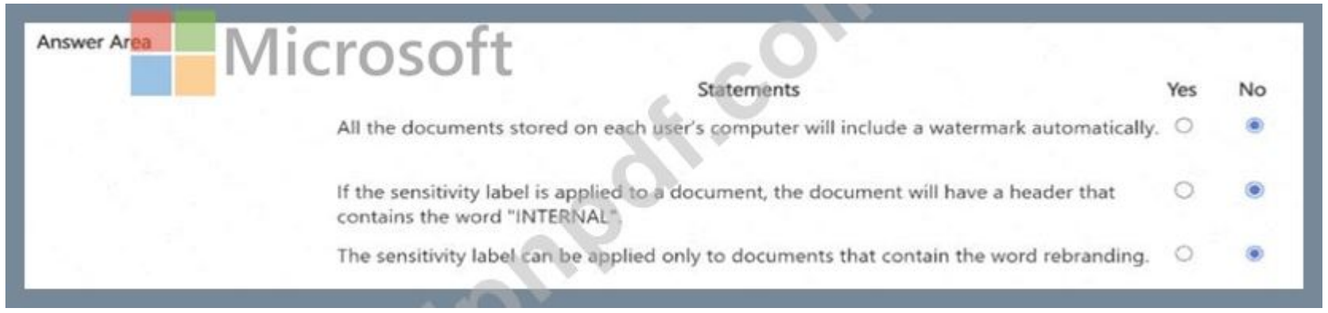
Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Answer:



Explanation:



最新問題: **120**

Contoso Confidential という名前の機密ラベルが含まれる Microsoft 365 サブスクリプションがあります。

Contoso Confidential をすべてのユーザーに公開します。

Contoso Confidential は、 構成」の図に示すように構成されています。([構成] タブをクリックします。)

Contoso Confidential のアクセス制御設定は、「アクセス制御」の図に示すように構成されています。
([アクセス制御]タブをクリックします。)

Edit sensitivity label

- Label details
- Scope
- Items
- Groups & sites
- Schematized data assets (preview)
- **Finish**

Review your settings and finish

Name
Contoso Confidential

Display name
Contoso Confidential
Edit

Description for users
Contoso Confidential
Edit

Scope
Files & other data assets, Email
Edit

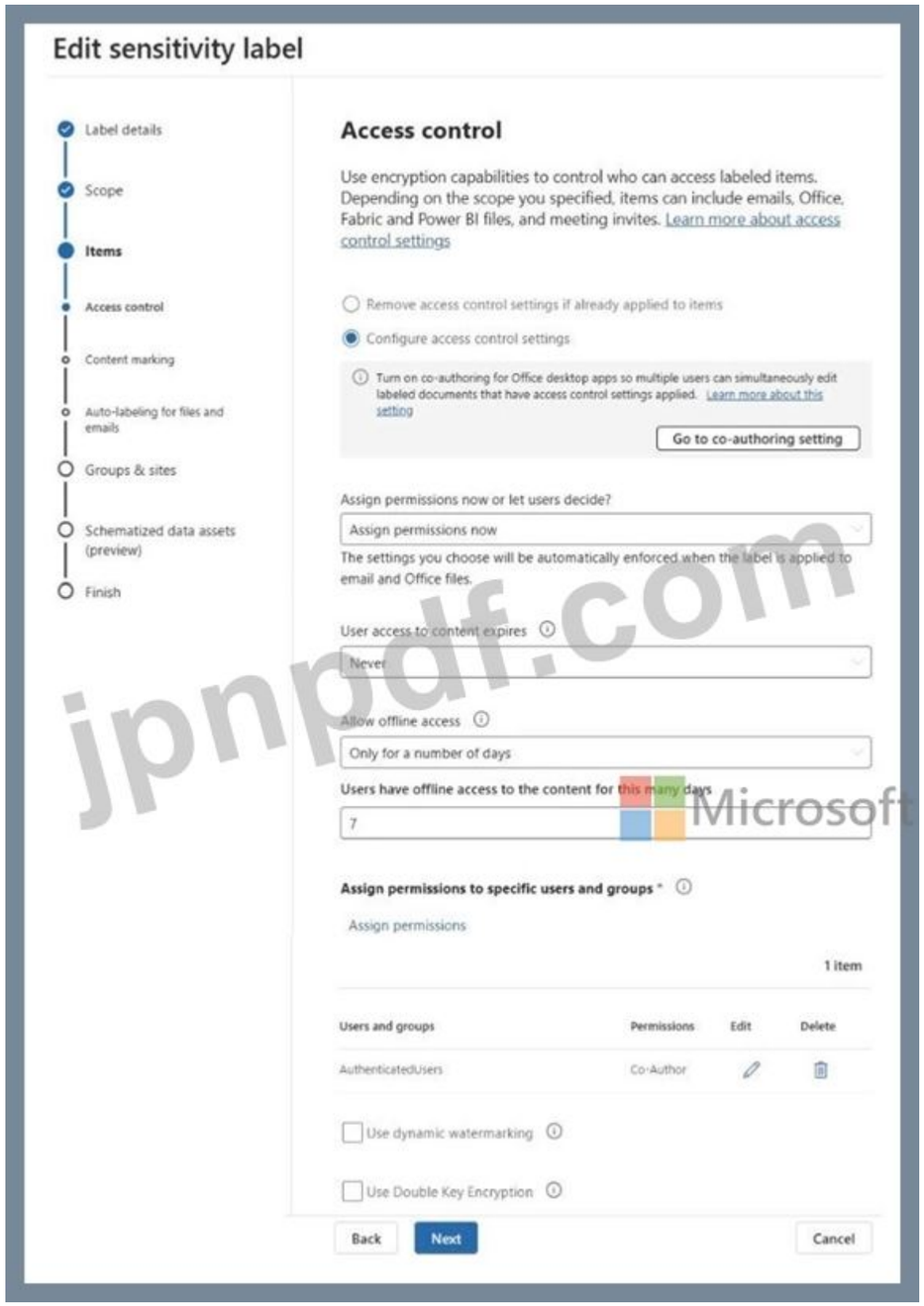
Access control
Access control
Edit

Content marking
Footer: Contoso Confidential Internal use only
Edit

Auto-labeling for files and emails
None
Edit

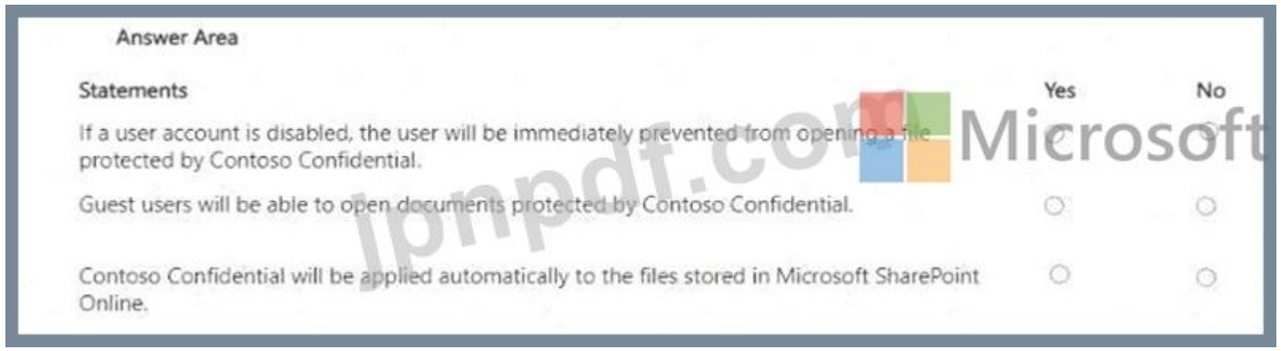
Auto-labeling for schematized data assets (preview)
None
Edit

Back | Save label | Cancel

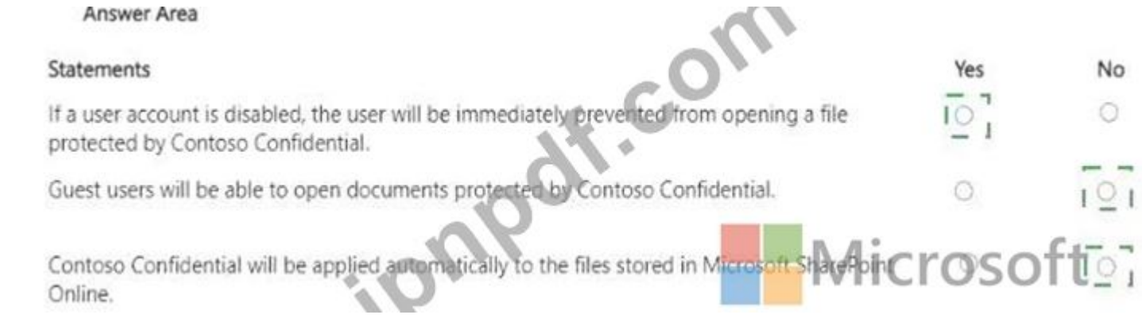


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ステップ1 - 構成を確認する
機密ラベル名: Contoso Confidential
範囲: ファイルとメール
アクセス制御:
ドキュメント/電子メールを暗号化します。
共同作成者権限を持つ AuthenticatedUsers に割り当てられた権限。
オフライン アクセスは 7 日間のみ許可されます。
自動ラベル付け = なし (構成されていません)。
コンテンツのマーキング: フッターが適用されました。
ステップ2 - 各ステートメントを分析する
ステートメント 1: ユーザー アカウントが無効になっている場合、ユーザーは Contoso Confidential によって保護されたファイルを開けなくなります。
暗号化された機密ラベルは、ユーザーがファイルにアクセスしようとするたびに Azure AD 認証を強制します。
Azure AD でアカウントが無効になっている場合、アクセスは直ちにブロックされます。
ステートメント 2: ゲスト ユーザーは、Contoso Confidential によって保護されたドキュメントを開くことができます。
アクセス制御は AuthenticatedUsers (内部ユーザー) に対してのみ構成されました。

このグループにはゲストまたは外部ユーザーは含まれません。
したがって、ゲスト ユーザーは保護されたドキュメントを開くことができません。
ステートメント 3: Contoso Confidential は、Microsoft SharePoint Online に保存されているファイルに自動的に適用されます。
ファイルとメールの自動ラベル付け = なし。
つまり、ラベル付けは自動ではなく、ユーザーが手動で適用する必要があります。
最終検証済み回答
ユーザー アカウントが無効になっている場合、ユーザーは Contoso Confidential で保護されたファイルを開けなくなります # はい ゲスト ユーザーは Contoso Confidential で保護されたドキュメントを開くことができます # いいえ Contoso Confidential は Microsoft SharePoint Online に保存されているファイルに自動的に適用されます # いいえ

最新問題: **121**
トレーニング可能な分類子をオプトインする Microsoft 365 テナントがあります。
User1 というユーザーがカスタムのトレーニング可能な分類子を作成できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 に割り当てるべきロールはどれですか?
A. セキュリティ管理者
B. コンプライアンス管理者
C. グローバル管理者
D. セキュリティオペレーター
Answer: (解答を表示する**)**
Microsoft Purview でカスタムのトレーニング可能な分類子を作成するには、コンプライアンス ポータルで権限を持っている必要があります。コンプライアンス管理者ロールは、トレーニング可能な分類子の作成と管理に必要な権限を提供します。セキュリティ ロールは脅威管理に重点を置いており、グローバル管理者ロールは過剰な権限です（最小限の権限ではありません）。
参考: Microsoft Purview のトレーニング可能な分類器

最新問題: **122**
10 年間の監査ログ保持アドオン ライセンスを備えた Microsoft Purview Audit (Premium) を使用する Microsoft 365 E5 サブスクリプションがあります。
サブスクリプションには、次の表に示す監査保持ポリシーが含まれています。

Name	Users	Record type	Activities	Duration	Priority
RP1	User1	SharePoint	Created site collection	1 Year	30
RP2	User1	SharePoint	None	3 Years	20
RP3	User1	SharePoint	Created site collection	3 Years	40
RP4	User1	SharePoint	Renamed site	6 Months	10

SharePoint Online 管理センターから、User1 は次の表に示すアクションを実行します。

Name	Description
Action1	Archives a site
Action2	Creates a site collection
Action3	Renames a site

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:

最新問題: **123**

ホットスポット

次のファイルを含む Microsoft SharePoint Online サイトがあります。

Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	*None*
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

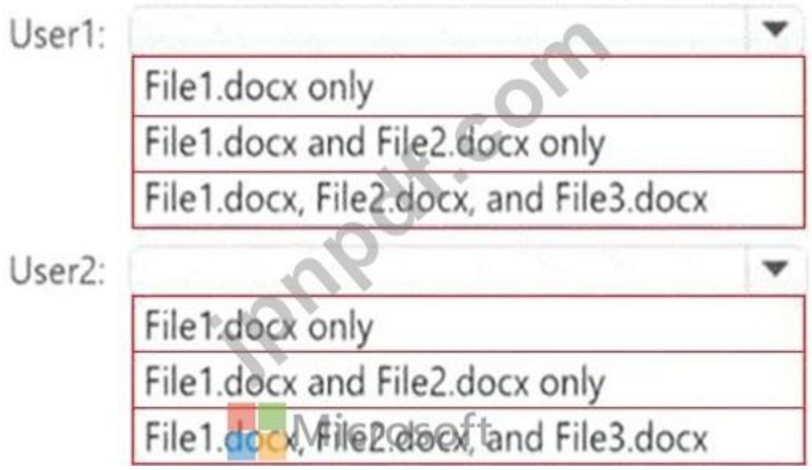
次の表に示すように、ユーザーにはサイトの役割が割り当てられます。

Name	Role
User1	Site owner
User2	Site member

User1 と User2 が開くことができるファイルはどれですか? 回答するには、回答領域で適切なオプションを選択してください。

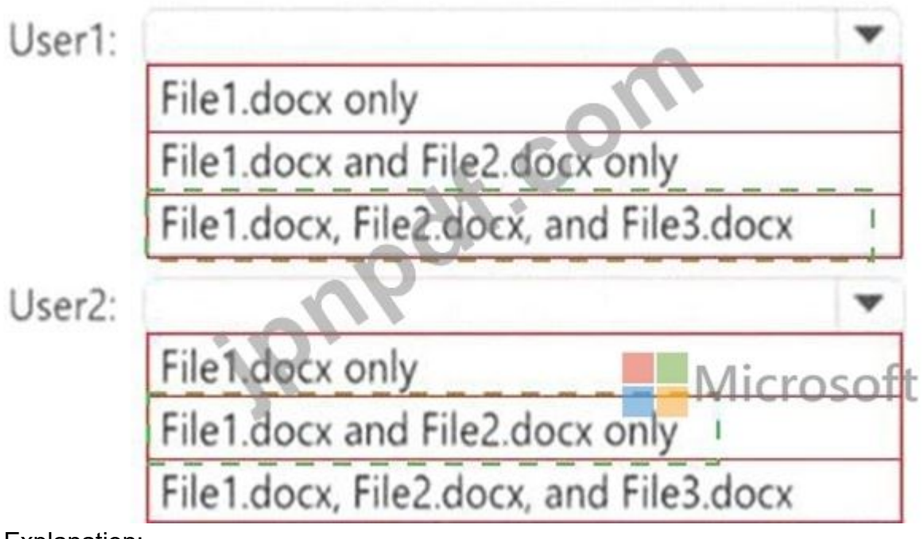
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

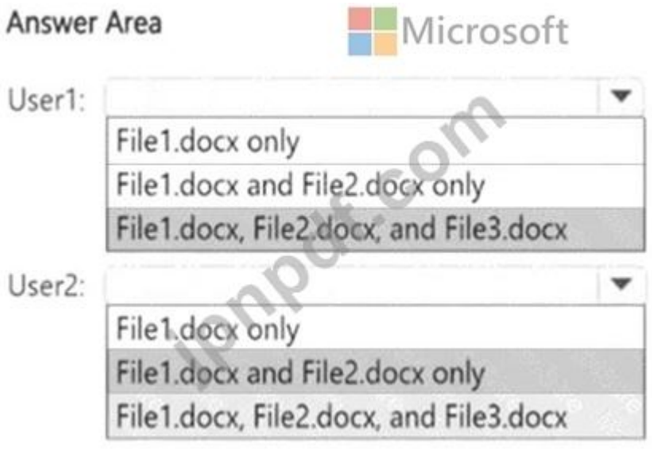


Answer:

Answer Area



Explanation:



最新問題: 124

100人のユーザーを含むMicrosoft 565サブスクリプションと、Group1という名前のMicrosoft 365グループがあります。すべてのユーザーはWindows 11デバイスを所有し、Microsoft SharePoint OnlineとExchange Onlineを使用しています。Group1のデフォルトラベルとして、「Label!」という機密ラベルが公開されています。Label1に、「Sublabel1」と「Sublabel2」という2つのサブラベルを追加します。Sublabel 1の設定がGroup 1にデフォルトで適用されるようにする必要があります。

何をすべきでしょうか?

A. サブラベルの順序を変更します。

B. Sublabel! のすべての設定を Label1 に複製します。

C. Label1 のポリシーを変更します。

D. Label1 のポリシーを削除し、Sublabel1 を公開します。

Answer: C (メーッセージを残す)

ステップ1 - シナリオ

100 人のユーザーと Microsoft 365 グループ (Group1) を含む Microsoft 365 E5 サブスクリプション。

機密ラベル (Label1) が Group1 の既定のラベルとして公開されます。

Label1 には、Sublabel1 と Sublabel2 の 2 つのサブラベルが含まれています。

要件: Sublabel1 の設定が Group1 にデフォルトで適用されていることを確認します。

ステップ2 - ラベル階層を理解する

Microsoft Purview Information Protection では、親ラベル (Label1) はコンテナーです。

サブラベル (Sublabel1、Sublabel2) は親名を継承しますが、異なる構成 (暗号化、透かし、アクセスなど) を表します。

ポリシー構成でデフォルトの公開オプションとして使用するサブラベルを指定しない限り、親ラベル自体にサブラベルの設定を自動的に適用することはできません。

ステップ3 - 「Label1のポリシーを変更する」が正しい理由

Sublabel1 をデフォルトで適用するには、Label1 の公開ポリシーを変更して、Sublabel1 がポリシー内のデフォルト ラベルになるようにする必要があります。

サブラベルの順序を変更するだけでは (オプション A)、デフォルトの割り当ては変更されません。

Sublabel1 の設定を Label1 に複製すると (オプション B)、サブラベルを持つ目的が達成されず、冗長性が追加されます。

Label1 のポリシーを削除し、Sublabel1 を公開すると (オプション D)、柔軟性が失われるため不要です。

ステップ4 - Microsoftリファレンス

Microsoft Docs: 「サブラベルを既定で適用する場合は、そのサブラベルをドキュメントと電子メールの既定のラベルとして選択するようにラベル ポリシーを構成します。」

最新問題: 125

Microsoft 365 E5 サブスクリプションをお持ちです。
プロジェクトに関連する機密データを管理するユーザーに対して、インサイダー リスク管理を実装する予定です。
ユーザー向けの保護ポリシーを作成する必要があります。ソリューションは以下の要件を満たす必要があります。
プロジェクトに参加していないユーザーへの影響を最小限に抑えます。
管理の手間を最小限に抑えます。
まず何をすべきでしょうか?
A. Microsoft Purview ポータルから、インサイダー リスク管理ポリシーを作成します。
B. Microsoft Entra 管理センターから、セキュリティ グループを作成します。
C. Microsoft Entra管理センターからユーザーリスクポリシーを作成します
D. Microsoft Purviewポータルから優先ユーザーグループを作成します
Answer: D (メーッセージを残す)
Microsoft Purview のインサイダー リスク管理ポリシーは、優先ユーザー グループに基づいてユーザーを対象とします。
特定のプロジェクト チームを監視する場合は、ポリシーがそのユーザーのみに影響するように、まずそれらのユーザーを優先ユーザー グループに定義する必要があります。
このアプローチ:
プロジェクトに参加していないユーザーへの影響を最小限に抑えます。
Entra ID で複数のセキュリティ グループを管理する必要がないため、管理の労力が軽減されます。
参照 :
Microsoft Learn: インサイダーリスク管理における優先ユーザーグループ
引用: 『リスク管理ポリシーを特定のユーザーに集中させるには、Microsoft Purview コンプライアンス ポータルで優先ユーザー グループを作成して管理します。」

最新問題: **126**
次の図に示すように、Alert2 という名前の Microsoft 365 アラートがあります。

Alertのステータスを管理する必要がありますか？Aletteをどのステータスに変更できますか？
A. ステータスを変更できません。
B. 却下のみ
C. 調査のみ
D. アクティブまたは調査中のみ
E. 調査中。アクティブ、または却下
Answer: E (メーッセージを残す)
ステップ1 - シナリオ
展示されているアラートの名前は Alert2 です。
現在のステータス = 解決済み。
タスクは、アラートをどのステータスに変更できるかを特定することです。

ステップ 2 - Microsoft 365 アラート ライフサイクル
Microsoft 365 のコンプライアンスおよびセキュリティアラートでは、調査と修復の状況に応じて、アラートが複数のステータス間を遷移することがあります。使用可能なステータスは次のとおりです。
アクティブ - アラートは新規であり、まだ対応されていません。
調査中 - アラートは確認中です。
解決済み - アラートが解決されました。
無視 – アラートは無視されるか、関連性がないと判断されます。
ステップ3 - ステータスが 解決済み」から変更される
アラートが 解決済み」状態の場合、管理者はアラートを再開または再分類できます。Microsoftのドキュメントによると、 解決済み」状態から以下の状態に変更できます。
アクティブ
調査中
解雇
これにより、必要に応じて調査を継続したり、誤検知を無視したりする柔軟性が得られます。
ステップ4 - Microsoftリファレンス
Microsoft Docsより：「トリアージプロセスの現在の段階に応じて、アラートのステータスをアクティブ、調査中、解決済み、却下の間で変更できます。」参考 :Microsoft 365セキュリティコンプライアンスセンターでアラートを管理する

最新問題**: 127**
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Member of security group
User1	Group1, Group2
User2	Group2
User3	Group1, Group3

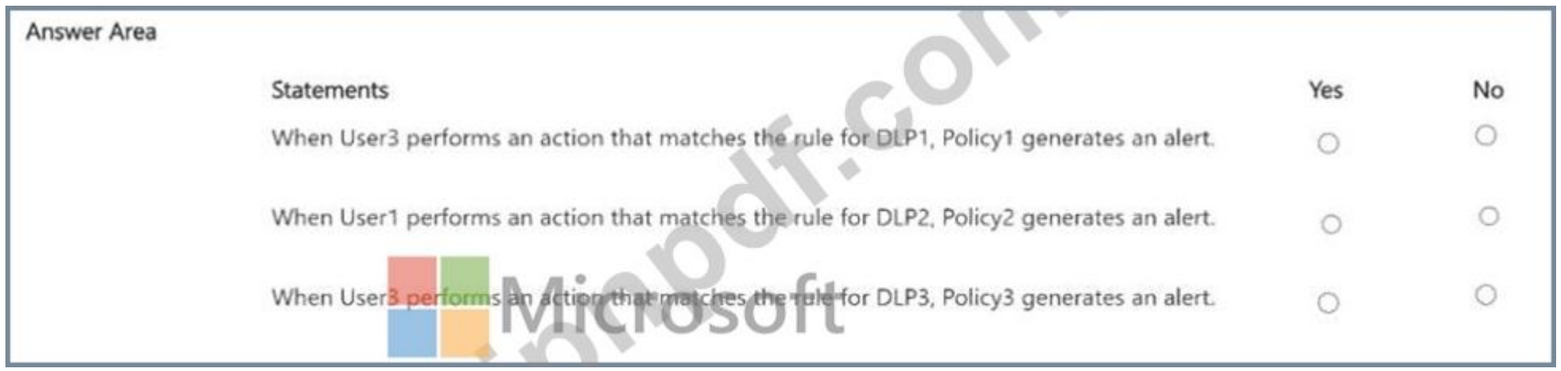
次の表に示すデータ損失防止 (DLP) ポリシーがあります。

Name	Location	Included	Number of DLP rules	Rule severity
DLP1	Devices	Group1	1	High
DLP2	Devices	Group2	1	Medium
DLP3	Devices	Group3	1	Medium

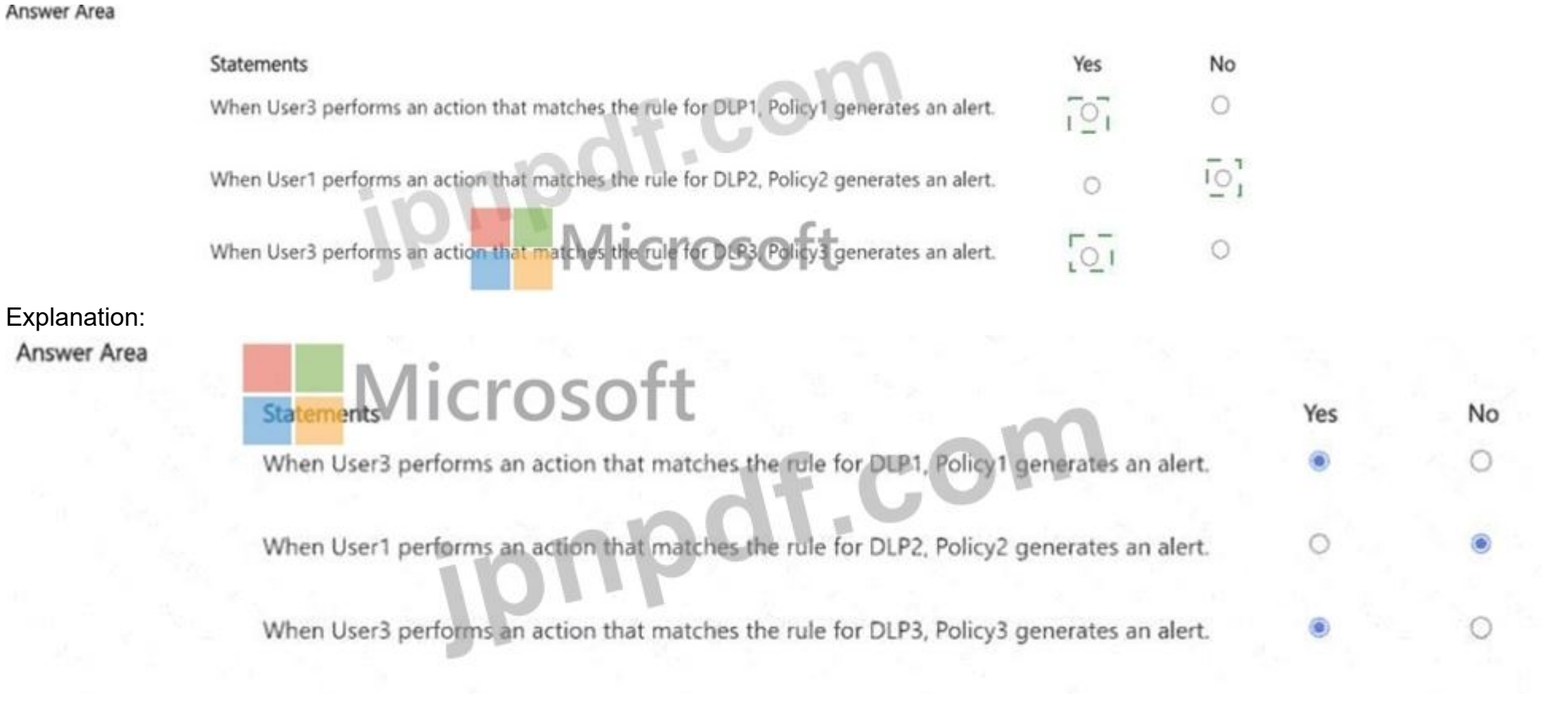
Insiderリスク管理から、User3をメンバーとして含むPriGroup1という優先ユーザーグループを構成します。次の表に示すInsiderリスクポリシーが適用されます。

Name	Policy template	Trigger	Group
Policy1	Data leaks	DLP1	Group1
Policy2	Data leaks	DLP2	Group2
Policy3	Data leaks by priority users	DLP3	PriGroup1

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

最新問題**: 128**

次の場所から 7 年後にコンテンツを削除するには、保持ポリシーを作成する必要があります。

* Exchange Online メール
* SharePoint Online サイト
* OneDriveアカウント
* Microsoft 365 グループ
* Teams チャネル メッセージ
* Teamsチャット

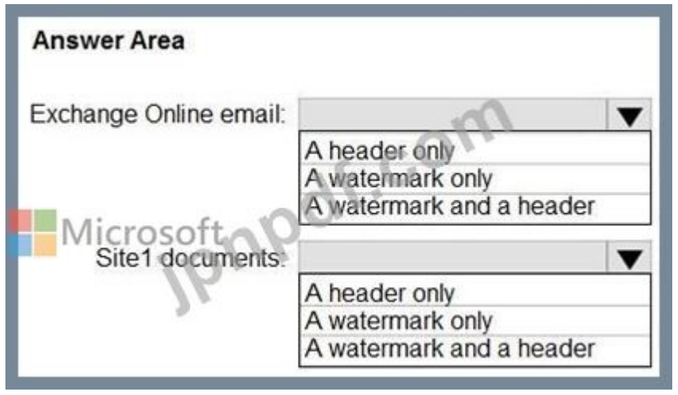
作成する必要がある保持ポリシーの最小数はいくつですか?

A. 1

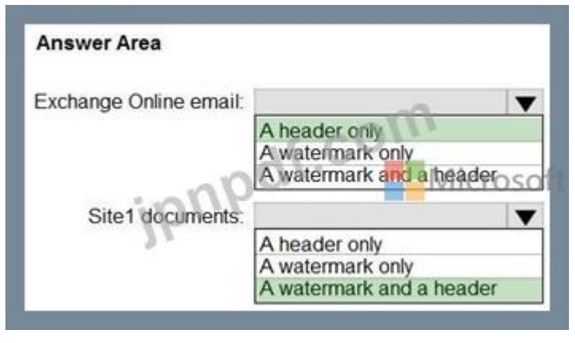
B. 2

C. 3
D. 4
Answer: B (メーッセージを残す**)**
以下のそれぞれについて保持ポリシーを設定できます
1.EXO、SPO、ODfB、M365 グループ
2.Teams チャネル メッセージ、Teams チャット
3.Teamsのプライベートチャンネルメッセージ

最新問題**: 129**
ホットスポットに関する質問
Site1 という名前の Microsoft SharePoint Online サイトと、Sensitivity1 という名前の機密ラベルがあります。Sensitivity1 は、コンテンツに透かしとヘッダーを追加します。
Microsoft Exchange Online および Site 内の電子メールに Sensitivity1 を自動的に適用するポリシーを作成します。
Sensitivity1 は一致する電子メールと Site1 ドキュメントをどのようにマークしますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題**: 130**
次の表に示すデバイスが含まれる Microsoft 36S ES サブスクリプションがあります。

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

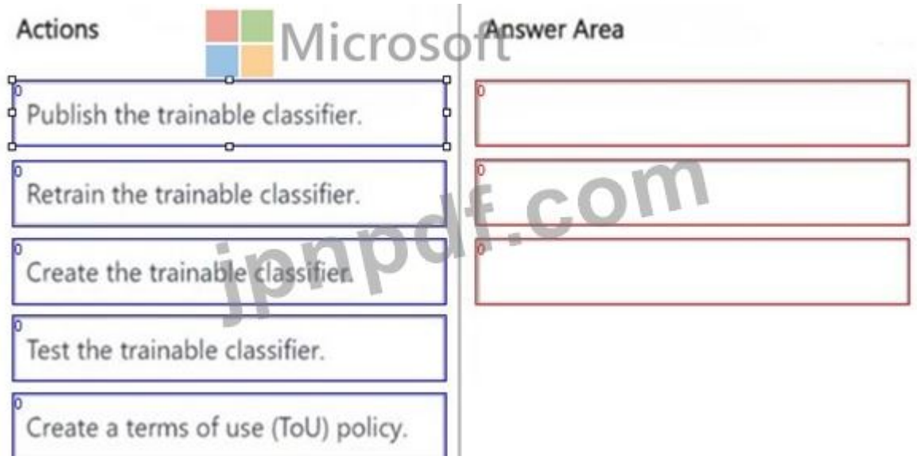
社内リスク管理を実施し、フォレンジック証拠を取得する予定です。フォレンジック証拠の収集をサポートするデバイスはどれですか？また、サポートされる各デバイスを準備するには何をする必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

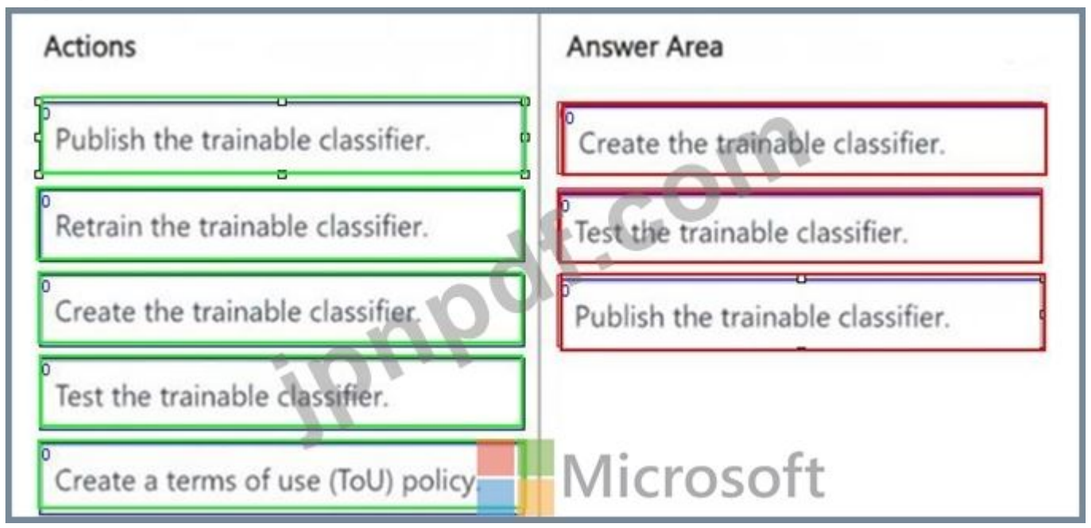
Explanation:

最新問題: 131

自動適用保持ラベル ポリシーの条件として使用できるトレーニング可能な分類子を作成する必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

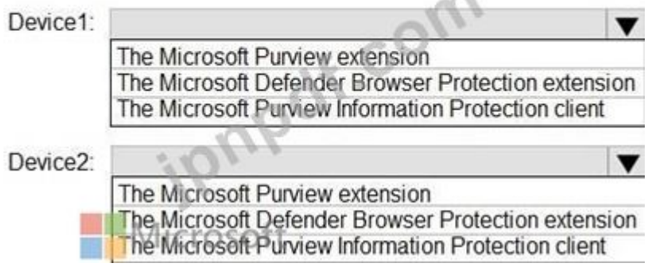


Answer:

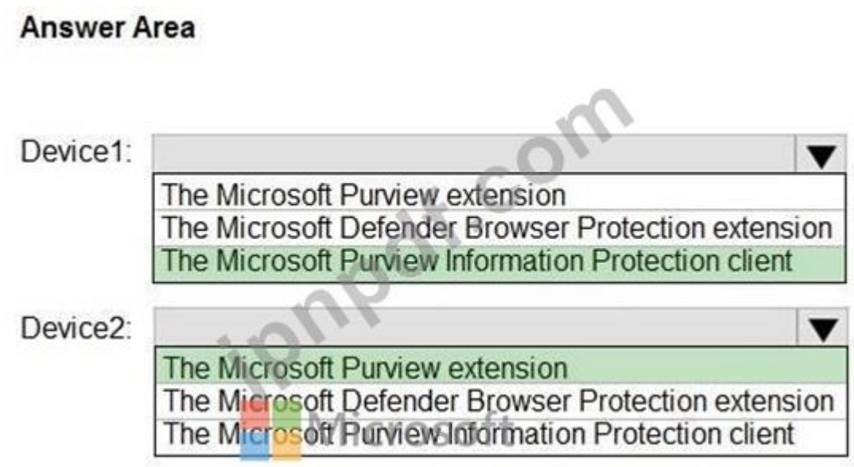


最新問題**: 132**
ホットスポットに関する質問
Microsoft 365 E5 サブスクリプションがあり、このサブスクリプションには Device1 と Device2 という 2 台の Windows デバイスが含まれています。Device1 の既定のブラウザーは Microsoft Edge に設定されています。Device2 の既定のブラウザーは Google Chrome に設定されています。
ユーザーがデフォルトのブラウザーを使用して USB デバイスにファイルをコピーするときに、Microsoft Purview インサイダー リスク管理が信号を収集できるようにする必要があります。
各デバイスに何を展開する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:



Explanation:

ボックス 1: Microsoft Purview 情報保護クライアント

デバイス1 では、デフォルトのブラウザが Microsoft Edge に設定されています。

Microsoft Edge に統合された Microsoft Purview Information Protection クライアントにより、組織はデータ セキュリティ ポリシーを適用し、ブラウザー内で機密情報を保護できるようになります。

具体的には、機密ラベルやデータ損失防止 (DLP) などの Microsoft Purview Information Protection 機能を Edge for Business で活用して、機密文書やデータへのアクセスと使用を制御できます。

ボックス2: Microsoft Purview拡張機能

デバイス2ではデフォルトのブラウザがGoogle Chromeに設定されています。

Windows デバイスに Google Chrome 用の Microsoft Purview 拡張機能をインストールすると、組織は Google Chrome ブラウザを使用しているときにクラウド サービスへのアクセスや機密アイテムのアップロードの試みを監視し、データ損失防止を通じて実際に保護アクションを実施できるようになります。

Microsoft Purview 拡張機能は Google Chrome で使用されますが、Microsoft Edge にはエンドポイント DLP 機能が組み込まれているため、必須ではありません。この拡張機能は、非ネイティブアプリケーション、特に Chrome などの DLP を明示的に拡張する必要があるブラウザにおけるデータ損失防止を強化します。

参照：

https://learn.microsoft.com/en-us/purview/dlp-chrome-get-started

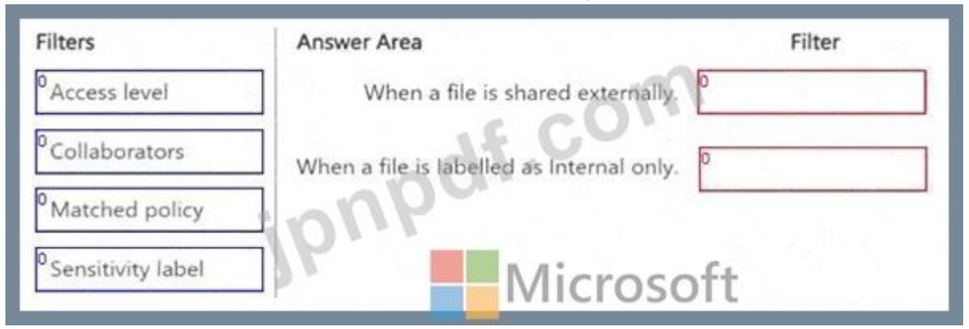
最新問題**: 133**

Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションがあります。

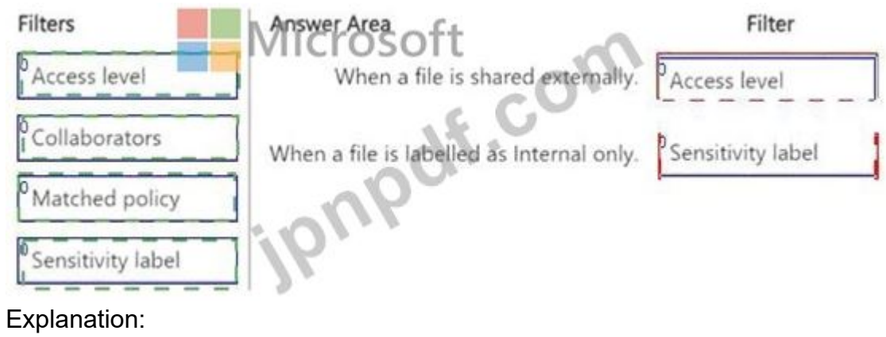
次の条件が満たされたときにトリガーされる Defender for Cloud Apps ファイル ポリシーを展開する予定です。

ファイルは外部と共有されています。

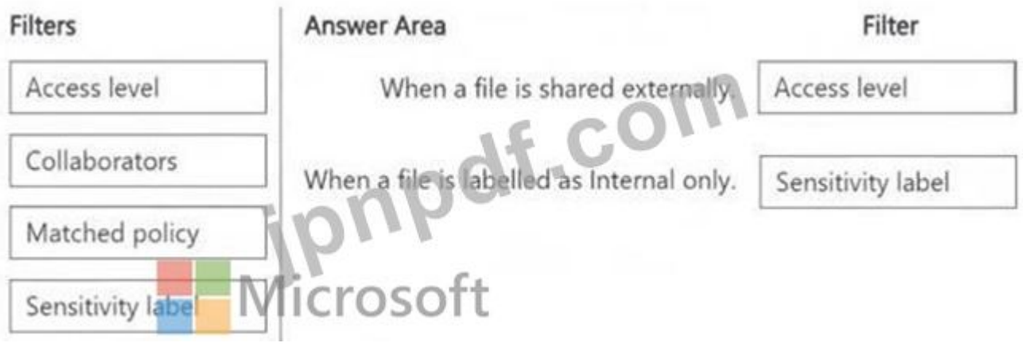
ファイルは内部専用としてラベル付けされています。
各条件にどのフィルターを使用すべきでしょうか？適切なフィルターを正しい条件にドラッグしてください。各フィルターは1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: **134**
次の図に示すように、Microsoft Entra テナント内のすべてのユーザーに公開されている Microsoft 365 機密ラベルがあります。

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

Answer Area

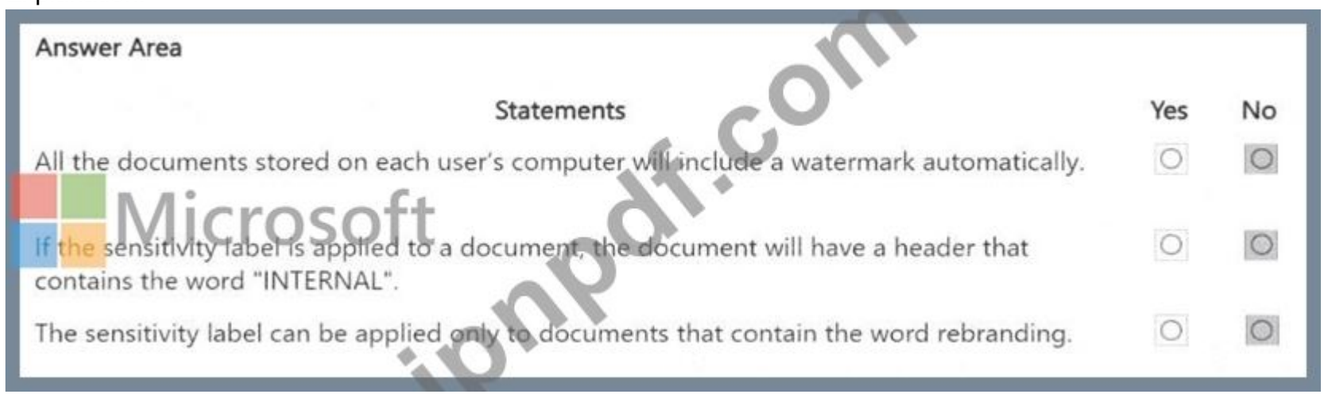
Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Answer:

Answer Area

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Explanation:



ステートメント 1 - いいえ。機密ラベルにはコンテンツのマーキング (透かし: INTERNAL) が含まれますが、これはラベルが手動または自動で適用されたドキュメントにのみ適用され、デフォルトではすべてのドキュメントに適用されるわけではありません。
ステートメント2 - いいえ。機密ラベルは透かしのみを指定し、ヘッダーは指定しません。ヘッダーマーキングが設定されている場合は、ラベル設定に明示的に表示されます。
ステートメント3 - いいえ。自動ラベル付けが「rebranding」という単語を含むドキュメントにのみラベルを適用するように設定されているという表示はありません。自動ラベル付けはオプション設定であり、明示的な設定が必要です。

最新問題**: 135**
次の表に示すファイルを含む Microsoft OneDrive フォルダーがあります。

Type	Number of files
.jpg	50
.docx	300
.txt	50
.zip	20

Microsoft Defender for Cloud Apps では、分類を自動的に適用するファイル ポリシーを作成します。
ポリシーを適用するとどのような効果がありますか?
A. このポリシーは.docxファイルと.txtファイルにのみ適用されます。ポリシーはファイルを直ちに分類します。
B. このポリシーは.docxファイルにのみ適用されます。このポリシーは1日あたり100件のファイルのみを分類します。
C. このポリシーはすべてのファイルに適用されます。このポリシーは1日あたり100件のファイルのみを分類します。
D. このポリシーは.docxファイルと.txtファイルにのみ適用されます。ポリシーは24時間以内にファイルを分類します。
Answer: B (メーッセージを残す**)**
https://docs.microsoft.com/ja-jp/cloud-app-security/azip-integration

最新問題**: 136**
ホットスポットに関する質問
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Purview Data Security Posture Management for AI (DSPM for AI) を展開します。
User1 が次のアクションを実行できることを確認する必要があります。
- 「推奨事項」ページから推奨事項を表示します。
- アクティビティ エクスプローラーを使用して、すべてのイベントのユーザー リスク レベルを表示します。
ソリューションは最小権限の原則に従う必要があります。
各アクションに対して User1 をどのロール グループに追加する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:
ボックス1 :インサイダーリスク管理調査員ロールは、インサイダーリスクケースに関連する推奨事項と、AIインサイトのためのMicrosoft Purview DSPMを閲覧する権限をユーザーに付与します。このロールは、不要な管理者権限を付与することなく、AI関連のリスク推奨事項を確認するためのアクセス権を付与するため、適切です。
ボックス2: Insider Risk Management Analysts ロールでは、ユーザーはアクティビティエクスプローラーを使用してユーザーのリスクレベルとイベントを分析できます。これは最小権限の原則に従っており、User1 はリスクレベルの表示と調査のみが可能で、インサイダーリスクポリシーに対する完全な管理権限は取得しません。

最新問題: **137**
Microsoft 365 サブスクリプションをお持ちです。
Microsoft Purview ポータルからコンテンツ検索を作成して実行します。
コンテンツ検索の結果をダウンロードする必要があります。
まず何を入手すべきでしょうか?
A. 証明書
B. パスワード
C. ピン
D. エクスポートキー
Answer: D (メーッセージを残す**)**
Microsoft Purview コンプライアンス ポータルでコンテンツ検索を実行し、検索結果をダウンロード/エクスポートする場合は、次の操作を行う必要があります。
コンテンツ検索ツールで結果のエクスポートを選択します。
Purview はエクスポート キーを生成します。
結果をダウンロードするには、eDiscovery エクスポート ツール (ClickOnce アプリケーション) を使用します。
エクスポート プロセスを認証するには、エクスポート キーが必要です。

証明書番号 このプロセスでは使用されません。
パスワード # エクスポートには必要ありません。
PIN 番号はここでは関係ありません。
エクスポート キー ## 検索結果をエクスポートするには必須です。
参照：
コンテンツ検索結果のエクスポート - Microsoft Learn

最新問題: **138**
Microsoft 365 サブスクリプションをお持ちです。
新しいトレーニング可能な分類子を作成します。
分類器をトレーニングする必要があります。
分類器をトレーニングするためにどのソースを使用できますか?
A. オンプレミスの Microsoft SharePoint Server サイト
B. Azure Files 共有
C. Microsoft SharePoint Online サイト
D. NFSファイル共有
Answer: A (メーッセージを残す**)**
参照：
https://learn.microsoft.com/en-us/purview/classifier-get-started-with

最新問題: **139**
次の表に示すデバイスが含まれる Microsoft 365 サブスクリプションがあります。

Name	Platform	Microsoft Purview	Microsoft Purview client
Device1	Windows 11	Not onboarded	Installed
Device2	Windows 10	Onboarded	Installed
Device3	macOS	Onboarded	Not installed

Microsoft Purview Insider Risk Management はどのデバイスからフォレンジック証拠をキャプチャできますか?
A. デバイスのみ
B. デバイス2のみ
C. デバイス1とデバイス2のみ
D. デバイス2とデバイス3のみ
E. デバイス1、デバイス2、デバイス3
Answer: (解答を表示する**)**
Microsoft Purview Insider Risk Management のフォレンジック証拠により、エンドポイントでのユーザー アクティビティのスクリーンショット/クリップをキャプチャできます。
法医学的証拠の捕捉の要件:
デバイスは Microsoft Purview (Defender for Endpoint 経由) にオンボードする必要があります。
Microsoft Purview クライアントをインストールする必要があります。
サポートされているプラットフォーム: Windows 10 および Windows 11 (macOS はフォレンジック証拠にはサポートされていません)。
次に各デバイスを確認します。

デバイス 1 (Windows 11) # クライアントはインストールされていますが、オンボードされていません ## 対象外です。
デバイス 2 (Windows 10) # オンボードされ、クライアントがインストールされました ## 対象です。
デバイス3 (macOS) # オンボードされていますが、クライアントがインストールされておらず、macOS はサポートされていません。## 対象外です。
したがって、Device2 のみが適格となります。
参照：
Microsoft Learn: インサイダーリスク管理におけるフォレンジック証拠
Microsoft Learn: インサイダーリスク管理フォレンジック証拠のためのデバイスオンボード

最新問題: **140**
Microsoft 36S ES サブスクリプションをお持ちです。
次の表に示す Microsoft Purview インサイダー リスク管理ポリシーを作成する必要があります。

Name	Description
Policy1	Monitors the printing of files by users that submitted their resignation
Policy2	Monitors the accidental sharing of data outside of an organization by users in a priority user group
Policy3	Monitors the downloading of files from Microsoft SharePoint Online to personal cloud storage services

各ポリシーにはどのポリシーテンプレートを使用すべきでしょうか？適切なポリシーテンプレートを適切なポリシーにドラッグしてください。各テンプレートは複数回使用される場合もあれば、まったく使用されない場合もあります。ペイン間の分割バーをドラッグするか、スクロールして表示する必要がある場合があります。

Answer:

Explanation:

最新問題: **141**

ホットスポットに関する質問

次の表に示す機密情報の種類 (SIT) が含まれる Microsoft 365 E5 サブスクリプションがあります。

Name	Primary element	Character proximity	Supporting elements	Additional checks
SIT1	Regular expression: `prd:\d{4}`	15	Keyword: product	*None*
SIT2	Regular expression: `(\d{10}\d{12})`	*None*	*None*	Exclude specific values: 111-111-1111
SIT3	Function: `Func_credit_card`	*None*	*None*	*None*

ユーザーは、次の表に示す電子メール メッセージを送信します。

Name	Content
Email1	The product code you requested for the bicycle is prd:1234.
Email2	The bank account number is 123456789012. Contact your account rep at 111-111-1111.
Email3	Please use my credit card that ends with 0023 and has an expiration date of 01/25.

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:
ボックス1: はい
Prd:1234はSIT1の正規表現と一致します。
ボックス2: はい
111-111-1111 は SIT2 の除外と一致します。
ただし、123456789012 は SIT2 の正規表現と一致します。
ボックス3: いいえ
Email3 にクレジットカード番号全体が含まれていません。
注記：
機密情報タイプ（SIT）では、機密項目を識別するための主要な要素として関数を使用できます。例えば、クレジットカード番号SITでは、Func_credit_card関数を使用してクレジットカード番号を検出します。
参照：
https://learn.microsoft.com/en-us/purview/sit-regex-validators-additional-checks#sensitive- information-type-regular-expression-validators
https://learn.microsoft.com/en-us/purview/sit-functions

最新問題**: 142**
ホットスポット
Microsoft 365 E5 サブスクリプションをお持ちです。
次の要件を満たすコンプライアンス ソリューションを実装する必要があります。
機密性の高い会社のデータの流出など、セキュリティに関連する主要なユーザー アクティビティのクリップをキャプチャします。
データ損失防止 (DLP) 機能とインサイダー リスク管理を統合します。
各要件には何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

Answer Area

主要なセキュリティ関連のユーザーアクティビティのクリップをキャプチャします
この要件は、リスクのあるユーザー行動（機密ファイルを USB にコピーする、クラウド ストレージにアップロードする、データを盗み出すなど）の証拠を記録して表面化させることを指します。
Microsoft Purview Insider Risk Management では、これはフォレンジック証拠を通じて実現され、ポリシーがトリガーされたときにエンドポイントでのユーザー アクティビティのスクリーンショット/クリップをキャプチャできます。
参照: Microsoft Learn - インサイダーリスクのフォレンジック証拠
DLP機能とインサイダーリスク管理を統合
Microsoft は、Purview Insider Risk の一部として Adaptive Protection を導入しました。
Adaptive Protection は、インサイダー リスク シグナルと DLP を併用し、ユーザーのリスク レベルに基づいて DLP コントロール (ブロック、制限、監視) を動的に調整します。
この統合により誤検知が減り、リスクの高いユーザーはより厳密に監視され、リスクの低いユーザーへの影響は軽減されます。
参照: Microsoft Learn - Microsoft Purview の Adaptive Protection
除外された他の選択肢:
適応スコープ: アクティビティをキャプチャするのではなく、グループを動的にターゲットとするポリシーを定義するために使用されます。
分類子/トレーニング可能な分類子: コンテンツの分類に使用され、流出キャプチャや DLP 統合には使用されません。
eDiscovery (プレミアム): インサイダーリスクではなく法的調査向け + DLP 統合。
記録管理: ライフサイクル保持。インサイダー リスクとは関係ありません。

最新問題**: 143**
Microsoft 365 E5 サブスクリプションをお持ちです。
次の表に示す時間にトリガーされる、Policy1 および Policy2 という名前の 2 つのアラート ポリシーを作成します。

Policy	Time (hh:mm:ss)
Policy1	10:00:00
Policy2	10:00:03
Policy1	10:00:04
Policy2	10:00:31
Policy1	10:01:01
Policy1	10:04:45

Microsoft Purview ポータルに追加されるアラートの数はいくつですか?

A. 2
B. 3
C. 4
D. 5
E. 6

Answer: D (メーッセージを残す)

Microsoft Purview では、複数のアラート ポリシーによってアラートがトリガーされると、冗長性を回避するために、短期間 (通常 5 分) 内の重複したアラートが抑制されることがあります。
ステップバイステップの分析:

Policy	Time Triggered (hh:mm:ss)	New Alert?
Policy1	10:00:00	Yes
Policy2	10:00:03	Yes
Policy1	10:00:04	No (Duplicate within 5 min)
Policy2	10:00:31	No (Duplicate within 5 min)
Policy1	10:01:01	Yes
Policy1	10:04:45	Yes

* 10:00:04 の Policy1 は無視されます。これは、Policy1 がすでに 10:00:00 にトリガーされており、5 分以内であるためです。
* 10:00:31 の Policy2 は無視されます。これは、Policy2 がすでに 10:00:03 にトリガーされており、5 分以内であるためです。
* 10:01:01 の Policy1 は、前の Policy1 アラートから 1 分以上経過しているため、新しいアラートです。
*10:04:45 の Policy1 は、前回の Policy1 アラートから 3 分以上経過しているため、新しいアラートです。

最新問題**: 144**
Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
ユーザーが Site1 上の機密情報を外部の受信者と共有するときにアラートを生成する Microsoft Purview インサイダー リスク管理ソリューションを展開する必要があります。
実行すべき 2 つのアクションはどれですか。それぞれの正解は解決策の一部を示しています。
注意: 正解ごとに 1 ポイントが加算されます。

A. 適応型保護を構成します。
B. データ損失防止 (DLP) ポリシーを作成します。
C. 分析をオンにします。
D. インサイダー リスク ポリシーを作成します。
E. インジケーターをオンにします。

Answer: D,E (メーッセージを残す)

最新問題: **145**

Microsoft 365 E5 サブスクリプションには、User1、User2、User3、User4 という 4 人のユーザーと、File1.docx というファイルが含まれています。

File1 には、次の図に示す権限を持つ機密ラベルを適用します。

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Explanation:

ステップ1 - Copilotでの要約
Microsoft 365 Copilot でファイルを要約するには:
ユーザーには少なくとも表示権限が必要です。
要約には編集、コピー、所有権は必要ありません。
展示物を見ると：
User1 (共同所有者) # には表示権限を含むフルアクセス権があります。
ユーザー2 (共同作成者) # には編集と表示の権限があります。
User3 (レビュー担当者) # には読み取り専用権限があります。
User4 (閲覧者) # には読み取り権限があります。
4人のユーザー全員がドキュメントを閲覧できます。そのため、CopilotはUser1、User2、User3、User4のFile1を要約できます。
ステップ2 - Copilotでリンクを使用してファイルを参照する
Copilot がリンクによってファイルを参照するには (つまり、生成されたコンテンツ内で引用または共有するには)、次の手順を実行します。
ユーザーには再共有やエクスポートなどの権限が必要です。
共同所有者のみがアクセスを管理し、リンクによる参照を許可する完全な権限を持ちます。
展示より:
ユーザー1 (共同所有者) # リンクで参照できます。
User2 (共同作成者)、User3 (レビュー担当者)、User4 (閲覧者) # 再共有またはリンクの権限はありません。
したがって、リンクによって File1 を参照できるのは User1 だけです。
参考: 機密ラベルと Microsoft 365 Copilot

最新問題**: 146**
Device1 という名前のデバイスが含まれる Microsoft 365 E5 サブスクリプションがあります。
デバイス 1 に対してエンドポイント データ損失防止 (エンドポイント DLP) を有効にする必要があります。

Microsoft Purview ポータルで最初に行うべきことは何ですか?
A. デバイスのオンボーディングをオンにします。
B. Microsoft Priva Privacy Risk Management を有効にします。
C. Microsoft Purview 情報バリア (IB) セグメントを作成します。
D. Microsoft Purview Information Protection スキャナー クラスターを追加します。
E. デバイス1をMicrosoft Purviewにオンボードします。
Answer: (解答を表示する**)**
エンドポイントDLPは、Microsoft Defender for Endpointとの統合を基盤としています。エンドポイントDLPを有効にする前に、Microsoft Purviewでデバイスオンボーディングを有効にして、デバイス（Device1など）を登録できるようにする必要があります。オンボーディング後、エンドポイントにDLPポリシーを割り当てることができます。
参考: エンドポイント DLP を使い始める

最新問題**: 147**
Microsoft 365 サブスクリプションをお持ちです。
新しいトレーニング可能な分類子を作成します。
分類器をトレーニングする必要があります。
分類器をトレーニングするためにどのソースを使用できますか?
A. オンプレミスの Microsoft SharePoint Server サイト
B. A2ure Files共有
C. Microsoft SharePoint Online サイト
D. NFSファイル共有
Answer: C (メッセージを残す**)**
Microsoft Purview のトレーニング可能な分類器には、分類器が認識すべき例としてラベル付けできるドキュメントソースが必要です。サポートされるソースには、SharePoint Online および Exchange Online のメールボックスが含まれます。オンプレミスの SharePoint Server サイト、Azure ファイル共有、NFS ファイル共有は、分類器のトレーニングではサポートされていません。
参考: Microsoft Purview のトレーニング可能な分類器

最新問題**: 148**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft 365 Copilot の使用状況レポートを確認する必要があります。
レポートはどこから確認すればよいですか?
A. Microsoft Purview ポータルの情報保護
B. Microsoft 365 管理センター
C. Microsoft Purview ポータルの AI 向け DSPM
D. Microsoft Defender ポータル
Answer: C (メッセージを残す**)**
Microsoft 365 Copilot の使用状況レポートを確認するには、Microsoft Purview ポータルで AI 向けデータ セキュリティ態勢管理 (DSPM for AI) を使用する必要があります。DSPM for AI は、Copilot の使用状況、リスク評価、Microsoft 365 内での AI のインタラクションに関連するデータ セキュリティ態勢など、AI 関連アクティビティに関する分析情報を提供します。

最新問題**: 149**
次の表に示すアダプティブ スコープを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Type	Query
Scope1	Users	FirstName starts with User
Scope2	SharePoint Online sites	SiteTitle starts with Site

次の表に示す保持ポリシーを作成します。

Name	Type	Location
RPolicy1	Adaptive	Scope1
RPolicy2	Adaptive	Scope2
RPolicy3	Static	Microsoft 365 groups

どの保持ポリシーが保存ロックをサポートしていますか?

A. RPolicy2のみ

B. RPolicy3on1y

C. RPolicy1 と RPolicy2 のみ

D. RPolicy1 と RPolicy3 のみ

E. RPolicy1、RPolicy2、およびRPolicy3

Answer: B (メーッセージを残す)

ステップ1 - 保存ロックの確認

* Microsoft 365 の保持ポリシーの保持ロックにより、ポリシーがロックされると、誰も (管理者を含む) それを無効にしたり、削除したり、制限を緩和したりすることができなくなります。

* 保持ロックは静的保持ポリシーでのみ使用でき、アダプティブ スコープではサポートされません。

参考: Microsoft 365 の保持ポリシーにおける保存ロック

Microsoft のドキュメントより:

保存ロックは、静的スコープで構成された保持ポリシーにのみ適用できます。適応型スコープは現在、保存ロックをサポートしていません。」ステップ2 - ケースデータの分析

* RPolicy1 # 適応スコープ (スコープ 1: ユーザー)。# 保持ロックには適格ではありません。

* RPolicy2 # 適応型スコープ (スコープ 2: SharePoint Online サイト)。# 保持ロックには対応していません。

* RPolicy3 # 静的スコープ (Microsoft 365 グループ)。# 保持ロックの対象です。

ステップ3 - 結論

RPolicy3 のみが Preservation Lock の対象となります。

最新問題**: 150**

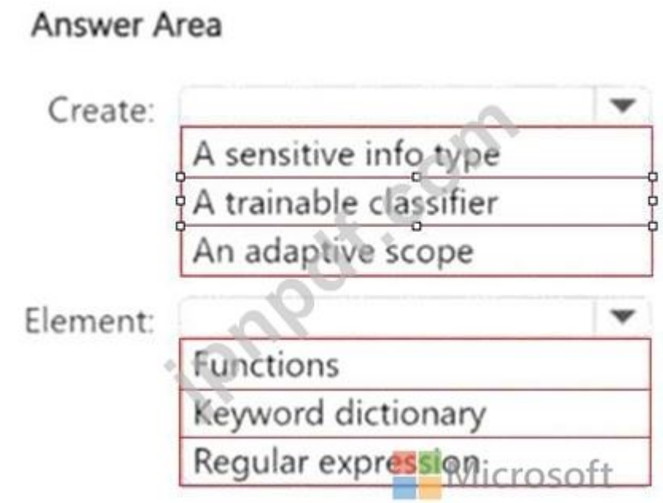
Microsoft 365 E5 サブスクリプションをお持ちです。

1,000 件の顧客名のリストが含まれる Customer.csv という名前のファイルがあります。

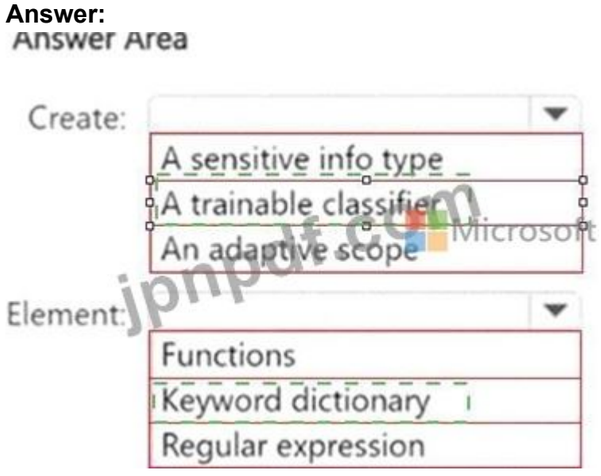
Customer.csv を使用して、Microsoft SharePoint Online ライブラリに保存されているドキュメントを分類する予定です。

Microsoft Purview ポータルで何を作成する必要がありますか? また、どのタイプの要素を選択する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

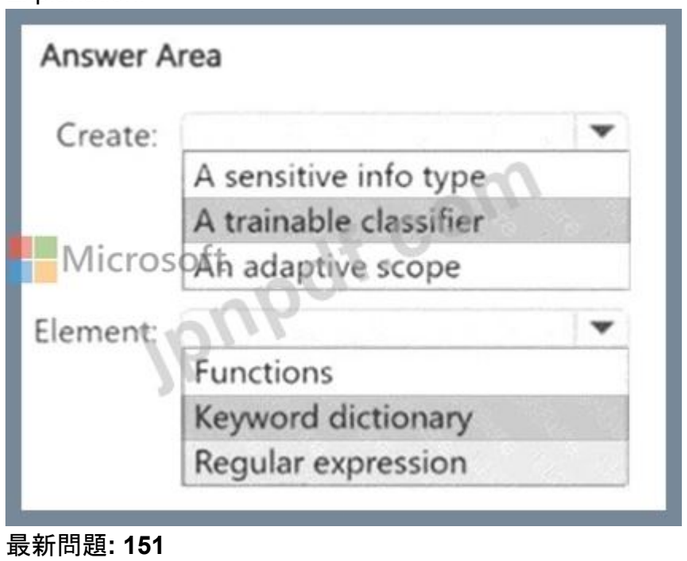
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: 151

次の図に示すように、場所に適用される Policy1 という名前の DLP ポリシーを作成します。

Policy1 には、Rule1 という名前の高度なデータ損失防止 (DLP) ルールが含まれています。

ルール 1 で使用できる 2 つの条件はどれですか。それぞれの正解は完全な解決策を示します。

注意: 正しい選択ごとに 1 ポイントが加算されます。

A. ドキュメントプロパティは

B. 添付ファイルのファイル拡張子は

C. ドキュメントサイズが等しいかそれより大きい

D. コンテンツは Microsoft 365 から共有されます

E. コンテンツに含まれる

Answer: D,E (メーッセージを残す)

Microsoft 365 で、高度なルールを使用してデータ損失防止 (DLP) ポリシーを作成しています。高度な DLP ルールでは、標準の DLP ルールよりも詳細な条件とアクションを設定できます。

高度なDLPで利用可能な条件

DLP ポリシーの条件に関する Microsoft Docs によると、次のようになります。

* # コンテンツに含まれるもの # 機密情報の種類、キーワード、または正確なデータの一致を検出するために使用されます。

これは最も一般的かつ基本的な DLP 条件の 1 つです。

* # コンテンツはMicrosoft 365から共有されています # コンテンツが外部または特定のドメイン/ユーザーと共有されているかどうかを検出するために使用されます。これは、最新の高度なDLP条件です。

他のものが正しくない理由:

* A. ドキュメントプロパティは # です。この条件は情報ガバナンス保持ポリシー/ラベル（DLPではない）に適用されます。DLPルールでは使用できません。
* B. 添付ファイルのファイル拡張子は # です。これは、Exchange メール フロー ルール (トランスポート ルール) ではサポートされていますが、高度な DLP ルールではサポートされていません。
* C. ドキュメント サイズが # 以上である。Exchange トランスポート ルールおよび特定の SharePoint 制限にも適用されますが、DLP ルールの条件としては使用できません。

最新問題: **152**

次の表に示すユーザーを含む Microsoft 36S サブスクリプションがあります。

Name	Email address	Distribution group
User1	user1@contoso.com	Finance
User2	user2@contoso.com	Sales

次の表に示すデータ損失防止 (DLP) ポリシーを作成します。

Name	Order	Apply policy to	Conditions	Actions	Exceptions	User notifications	Additional options
Policy1	0	Exchange email for the Finance distribution group	Content shared with people outside my organization. Content contains five or more credit card numbers.	Encrypt the message by using the Encrypt email messages option.	user4@fabrikam.com	Send an incident report to the administrator.	If there's a match for this rule, stop processing additional DLP policies and rules.
Policy2	1	All locations of Exchange email	Content shared with people outside my organization. Content contains five or more credit card numbers.	Restrict access or encrypt the content in Microsoft 365 locations. Block only people outside your organization.	*None*	Send an incident report to the administrator.	*None*

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
If User1 sends an email message that contains five credit card numbers to user4@fabrikam.com, the message will be encrypted.	○	○
If User1 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○
If User2 sends an email message that contains five credit card numbers to orders@adatum.com, the message will be encrypted and delivered.	○	○

Answer:

Explanation:

最新問題: **153**
Microsoft Purview を使用する Microsoft 365 E5 サブスクリプションがあります。
SIT1 という名前の機密情報の種類 (SIT) を作成します。
次の表に示す通信コンプライアンス ポリシーを作成する予定です。

Name	Template used
Policy1	Detect inappropriate text
Policy2	Detect inappropriate image
Policy3	Detect conflict of interest

SIT1 を条件として追加できるポリシーはどれですか?
A. ポリシー1のみ
B. ポリシー1とポリシー2のみ
C. ポリシー1とポリシー3のみ
D. ポリシー3のみ
E. ポリシー1、ポリシー2、およびポリシー3
Answer: C (メッセージを残す)

最新問題: **154**
最近、会社の開発者が Azure ストレージ アカウント キーをプレーン テキストで第三者に電子メールで送信していることがわかりました。Azure ストレージ アカウント キーを電子メールで送信する場合は、電子メールが暗号化されていることを確認する必要があります。
解決策: Exchange 電子メール、SharePoint サイト、OneDrive アカウント、Teams のチャットとチャネル メッセージが選択されたデータ損失防止 (DLP) ポリシーを作成します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: A (メッセージを残す)

最新問題: **155**
トレーニング可能な分類子に基づく機密情報タイプがあります。
トレーニング可能な分類器の結果に満足していません。
分類器を再トレーニングする必要があります。
Microsoft Purview ポータルでは何を使用すればよいですか?
A. データ分類からのコンテンツエクスプローラー

B. 情報保護からのラベル
C. 情報ガバナンスからのラベル
D. コンテンツ検索
Answer: A (メーッセージを残す**)**
Microsoft Purview のトレーニング可能な分類器は、サンプルドキュメントから学習します。最初の結果が満足のいくものでない場合、Purview コンプライアンス ポータルのデータ分類セクションにあるコンテンツ エクスプローラーでアイテムを確認し、再分類することで再トレーニングが行われます。これにより、ドキュメントを 関連あり」または 関連なし」とマークすることでフィードバックを提供し、分類器の精度を向上させることができます。
その他のオプションは再トレーニングをサポートしていません。
情報保護からのラベル # 分類子をトレーニングするのではなく、機密ラベルを構成および管理するために使用されます。
情報ガバナンスからのラベル # 分類子ではなく、保持ラベルに使用されます。
コンテンツ検索 # 分類子のトレーニングではなく、電子情報開示とコンテンツの検索に使用されます。
参考: Microsoft Purview のトレーニング可能な分類器

最新問題: **156**
ホットスポット
次のファイルを含む Microsoft SharePoint Online サイトがあります。

Name	Modified by	Data loss prevention (DLP) action
File1.docx	Manager1	None
File2.docx	Manager1	Matched by DLP
File3.docx	Manager1	Blocked by DLP

次の表に示すように、ユーザーにはサイトの役割が割り当てられます。

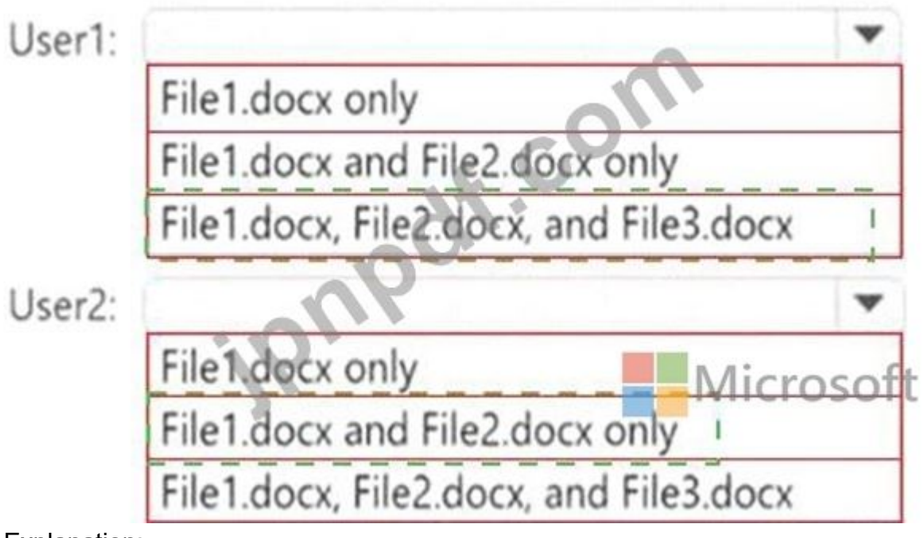
Name	Role
User1	Site owner
User2	Site member

User1 と User2 が開くことができるファイルはどれですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

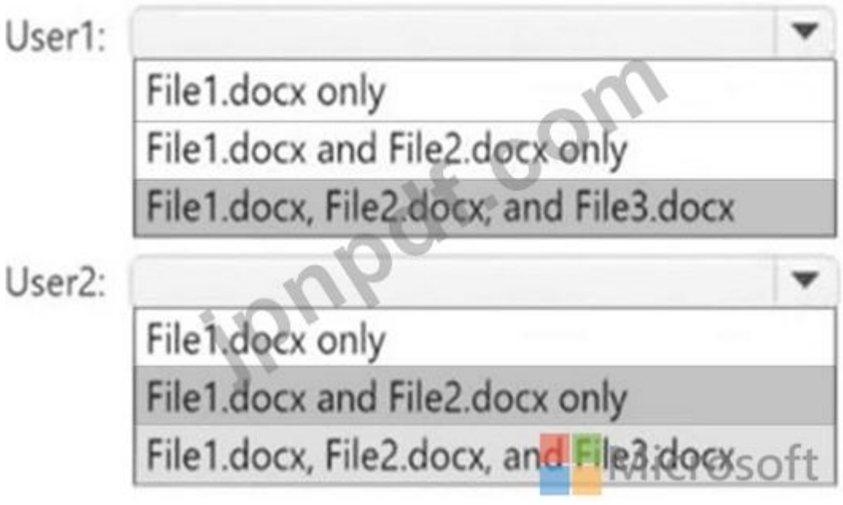
Answer:

Answer Area



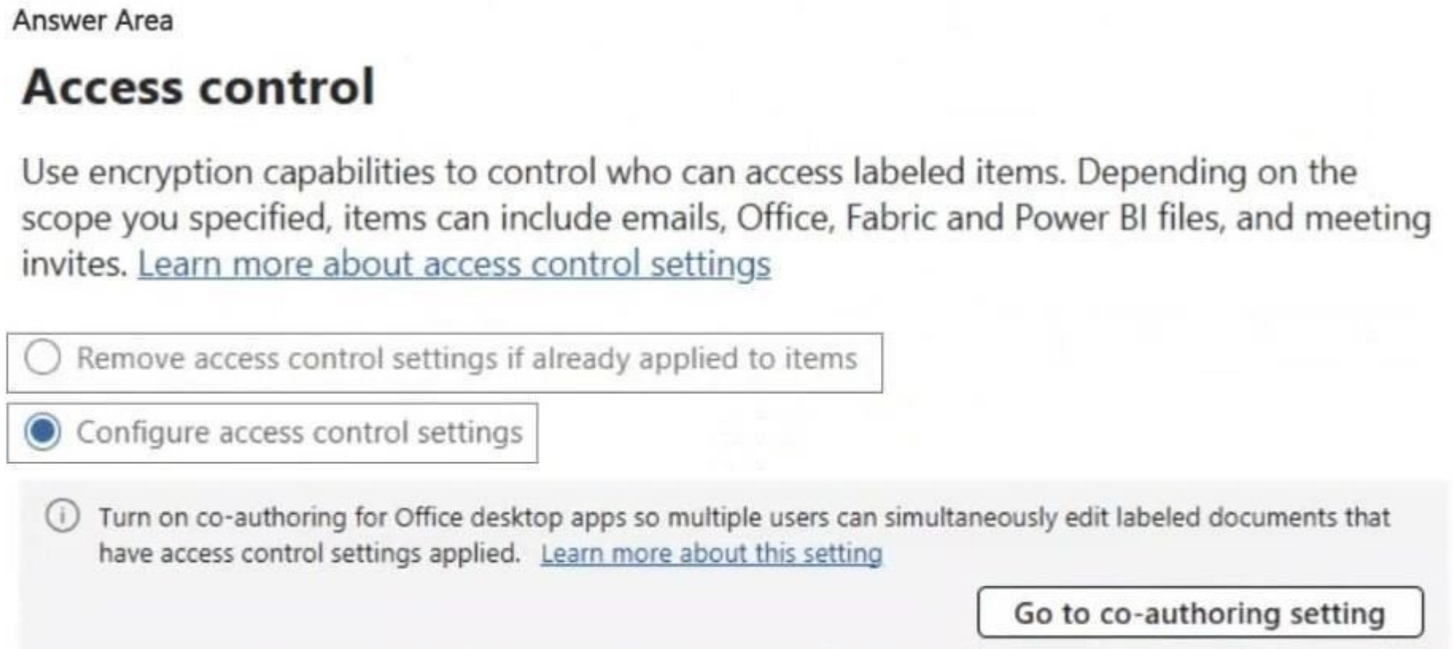
Explanation:

Answer Area



最新問題: **157**
ホットスポットに関する質問
label1 という名前の機密ラベルが含まれる Microsoft 365 E5 テナントがあります。
暗号化されたファイルの共同編集を有効にする予定です。
label1 が適用されたファイルが共同編集をサポートしていることを確認する必要があります。
どの 2 つの設定を変更する必要がありますか? 回答するには、回答領域で設定を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete
No data available			

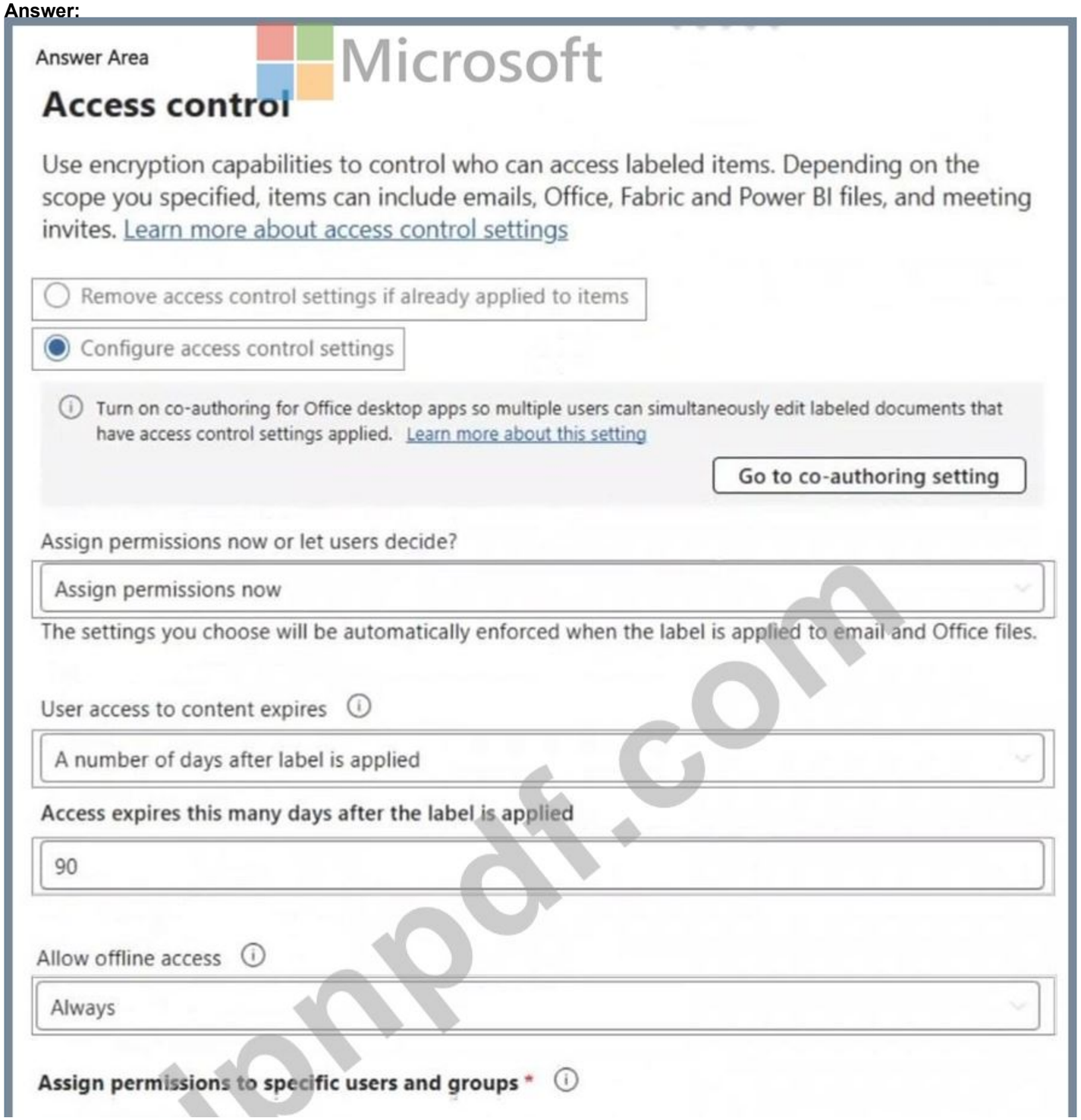
☑ Use dynamic watermarking ⓘ

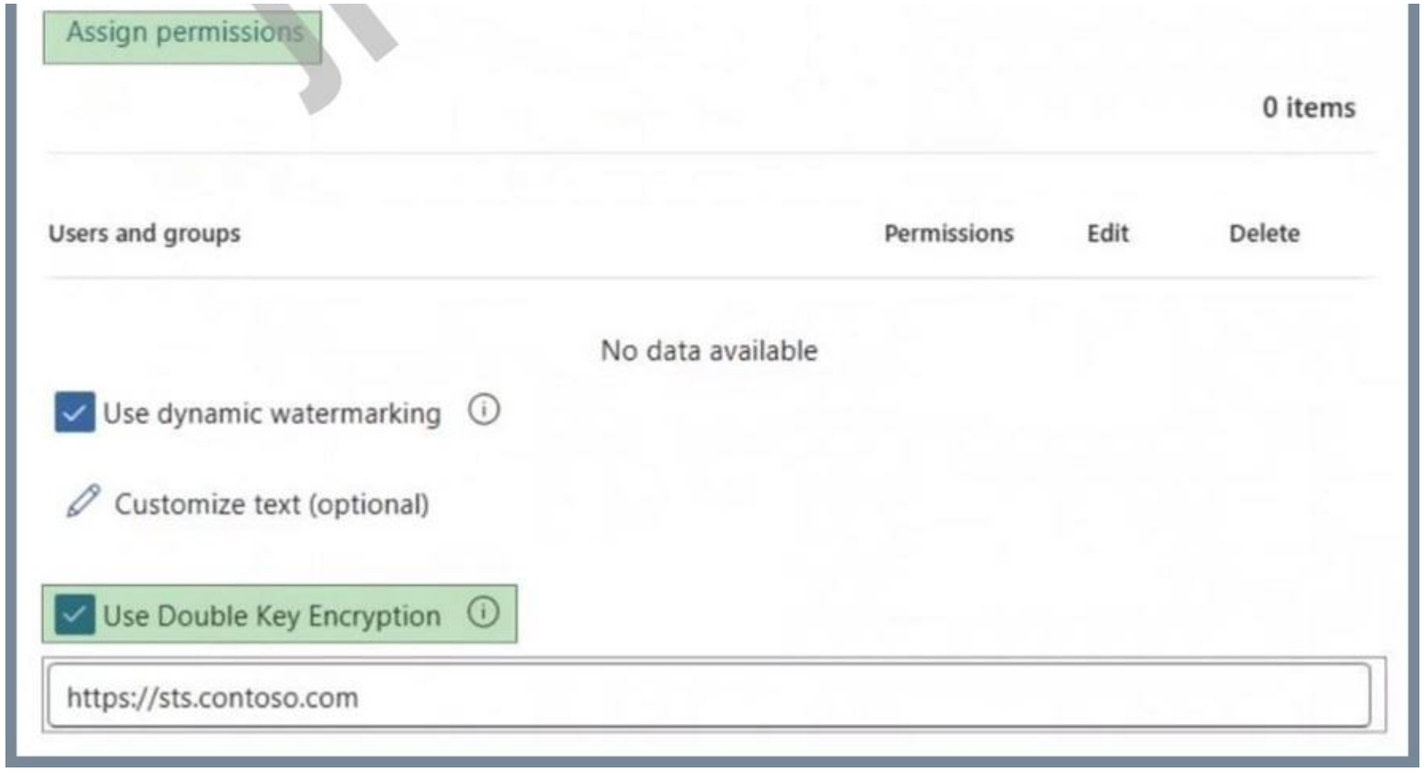
Customize text (optional)

☑ Use Double Key Encryption ⓘ

https://sts.contoso.com

Answer:



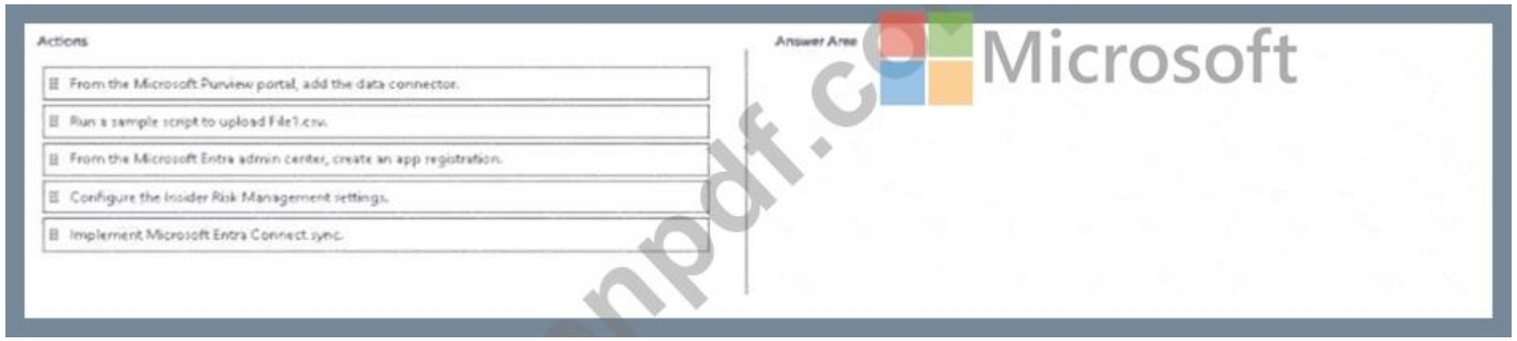


Explanation:
二重キー暗号化（DKE）により、Microsoft 365 サービスは暗号化されたコンテンツを処理できないため、共同編集ができなくなります。リアルタイムの共同作業を可能にするには、この設定を無効にする必要があります。
共同編集を行うには、ユーザーまたはグループに権限を明示的に割り当てる必要があります。権限が定義されていない場合、ユーザーはドキュメントにアクセスしたり、共同編集したりすることができません。

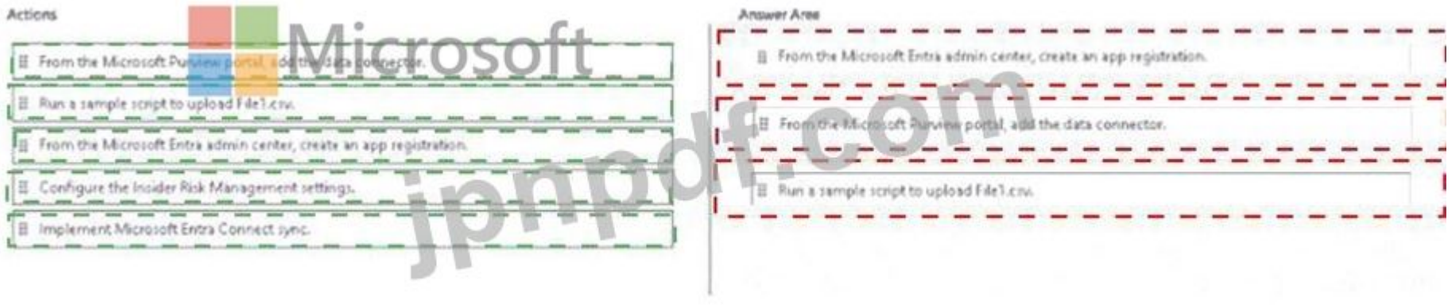
最新問題: **158**
100人のユーザーを含むMicrosoft 565サブスクリプションと、Group1という名前のMicrosoft 365グループがあります。すべてのユーザーはWindows 11デバイスを所有し、Microsoft SharePoint OnlineとExchange Onlineを使用しています。Group1のデフォルトラベルとして、「Label!」という機密ラベルが公開されています。Label1に、「Sublabel1」と「Sublabel2」という2つのサブラベルを追加します。Sublabel 1の設定がGroup 1にデフォルトで適用されるようにする必要があります。
何をすべきでしょうか?
A. Label1 のポリシーを削除し、Sublabel1 を公開します。
B. Label1 のポリシーを変更します。
C. Sublabel! のすべての設定を Label1 に複製します。
D. サブラベルの順序を変更します。
Answer: (解答を表示する**)**

最新問題: **159**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Purview Insider Risk Management を実装する予定です。

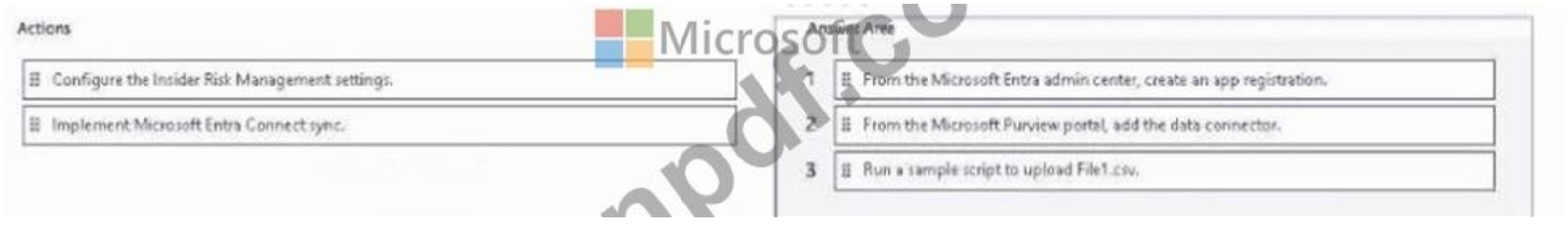
従業員の退職データが含まれる File1.csv という名前のファイルを取得します。
HR データ コネクタを実装し、コネクタを使用して File1.csv をアップロードする必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



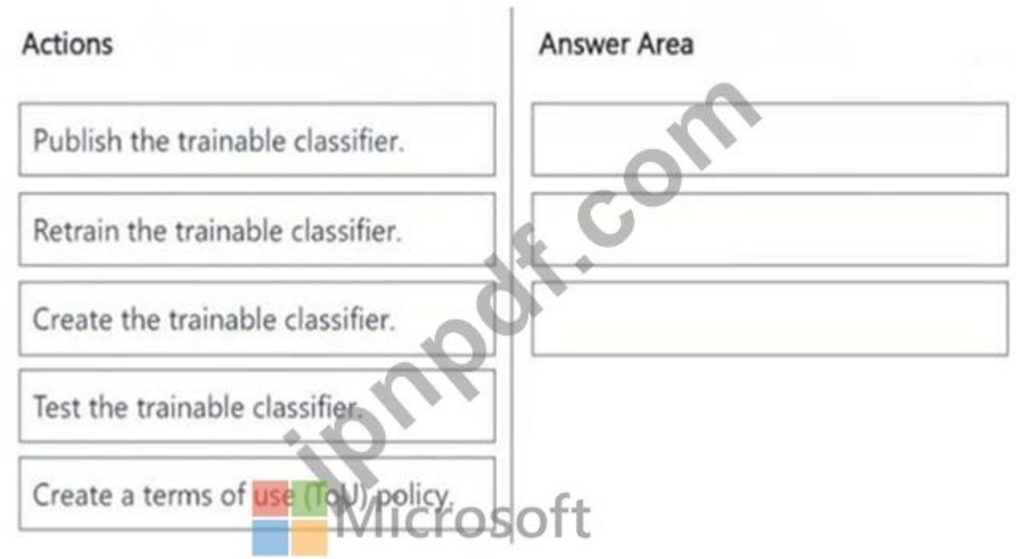
Answer:



Explanation:



最新問題: **160**
ドラッグアンドドロップの質問
自動適用保持ラベル ポリシーの条件として使用できるトレーニング可能な分類子を作成する必要があります。
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:

Explanation:

自動適用保持ラベル ポリシーで使用できるトレーニング可能な分類子を作成するには、次の主要な手順に従う必要があります。

1. 学習可能な分類器を作成する

これは分類子を定義し、識別するコンテンツの種類を指定する最初のステップです。

2. 学習可能な分類器をテストする

分類器を本番環境で使用する前に、サンプル ドキュメントに対してテストして、目的のデータが正しく分類されるかどうかを確認し、その精度を検証する必要があります。

3. トレーニング可能な分類器を公開する

テストが成功したら、Microsoft Purview の保持ラベルの自動適用などのポリシーで使用できるように分類子を公開する必要があります。

最新問題**: 161**

User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
添付ファイルを含むすべての電子メール メッセージが、Microsoft Purview Message Encryption を使用して自動的に暗号化されるようにする必要があります。
何を創造すべきでしょうか?
A. メールフロールール
B. 機密ラベル
C. データ損失防止 (DLP) ポリシー
D. 情報バリアセグメント
Answer: A (メーッセージを残す**)**
Microsoft Purview メッセージ暗号化のルールの定義
Microsoft Purview Message Encryption を有効にする方法の一つは、Exchange Online および Exchange Online Protection の管理者がメールフロールールを定義することです。これらのルールは、メールメッセージを暗号化する条件を決定します。ルールに暗号化アクションを設定すると、ルールの条件に一致するすべてのメッセージが送信される前に暗号化されます。
メールフロールールは柔軟性が高く、条件を組み合わせることで、単一のルールで特定のセキュリティ要件を満たすことができます。例えば、特定のキーワードを含み、外部の受信者宛てのメッセージをすべて暗号化するルールを作成できます。Microsoft Purview Message Encryptionは、暗号化されたメールの受信者からの返信も暗号化します。
参照：
https://learn.microsoft.com/en-us/purview/ome
最新問題**: 162**
Microsoft 36S ES サブスクリプションをお持ちです。
Microsoft Purview Data Security Posture Management for AI ポータルから、AI データ セキュリティに関する推奨事項を確認します。リスクの高いユーザーが機密データを AI Web サイトに貼り付けたりアップロードしたりできないようにするワンクリック ポリシーを作成する予定ですか? ポリシーはどのように構成しますか? 回答するには、回答領域で適切なオプションを選択します。注: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

この質問は、Microsoft Purview の AI 向けデータセキュリティ態勢管理ポータル内でワンクリックポリシーを作成する方法に関するものです。これらのポリシーは、機密データや AI ウェブサイトに関連するリスクを軽減するように設計されています。この特定のシナリオにおける正しい構成は、「まずテストする」を選択し、「デバイス、インスタンス、および SharePoint サイト」にポリシーを適用することです。この構成は、データ損失防止 (DLP) および同様のポリシーの導入に関する Microsoft の推奨プラクティスに基づいています。

ポリシーモード: 「まずはテストしてみましょう」

マイクロソフトは、新しいポリシーを適用する前に、その影響と有効性を評価するためにテストモードの使用を推奨しています。このアプローチにより、ユーザーのワークフローへの意図しない中断を防止できます。テストモードでは、ポリシーは指定されたアクティビティをブロックすることなく監視および監査します。アラートとレポートが生成されるため、管理者はポリシーの動作を確認し、必要な調整を行うことができます。これは「小規模から始めて拡張する」という原則に合致しており、機密データの転送をブロックするように設計されたポリシーが、正当なビジネス活動を意図せず妨げることがないようにします。

ポリシーの範囲: 「デバイス、インスタンス、および SharePoint サイト」

このポリシーは、ユーザーがAIウェブサイトに機密データを貼り付けたりアップロードしたりすることをブロックすることを目的としています。そのためには、あらゆる潜在的なデータ流出ポイントを網羅する包括的な適用範囲が必要です。

デバイス :これはユーザーのローカルデバイスを対象とし、マシン上で実行されているアプリケーションからのデータのアップロードや貼り付けを防止します。これはエンドポイントからのデータ制御に不可欠です。

インスタンス :これは、AIウェブサイトを含むSaaS（Software as a Service）インスタンスを指します。インスタンスにポリシーを適用することで、これらの外部サービスへのデータ転送が監視および制御されます。

SharePoint サイト :SharePoint に保存されているデータは、機密情報の一般的なソースです。ポリシーの適用範囲に SharePoint サイトを含めることで、これらの場所からデータが直接コピーされ、AI ウェブサイトにアップロードされることを防ぎ、包括的なセキュリティ体制を実現します。

「デバイス、インスタンス、SharePoint サイト」を選択すると、最も一般的なソースと宛先にわたるデータを監視 保護するようにポリシーが構成され、AIサービスへのデータ流出に対する強力な防御が実現します。この包括的なアプローチは、Microsoft 365 における最新のデータセキュリティ戦略の基盤となります。

この情報は、Microsoft Purview に関する Microsoft の公式ドキュメント、特にデータ損失防止 (DLP) ポリシーと AI 向けデータセキュリティ態勢管理に関するセクションで確認できます。「まずテスト」というベストプラクティスと、機密データの保護範囲の広範さが一貫して推奨されています。

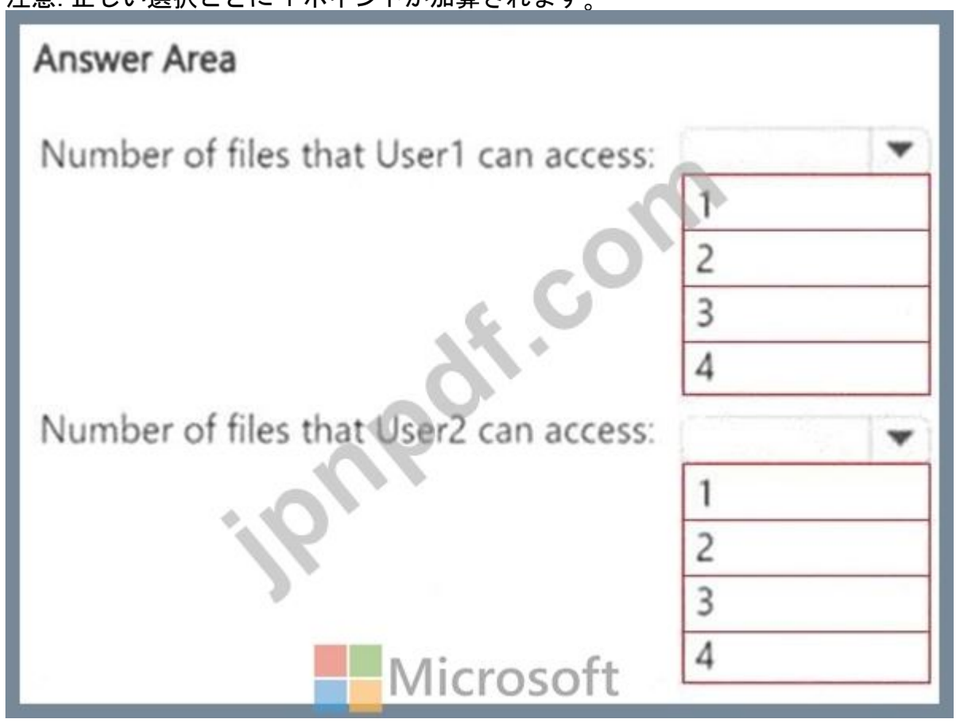
最新問題: **163**

Microsoft 365 ES サブスクリプションをお持ちです。

セキュリティ マネージャーは、データ損失防止 (DIP) ポリシーの一致が発生するたびに電子メール メッセージを受信します。

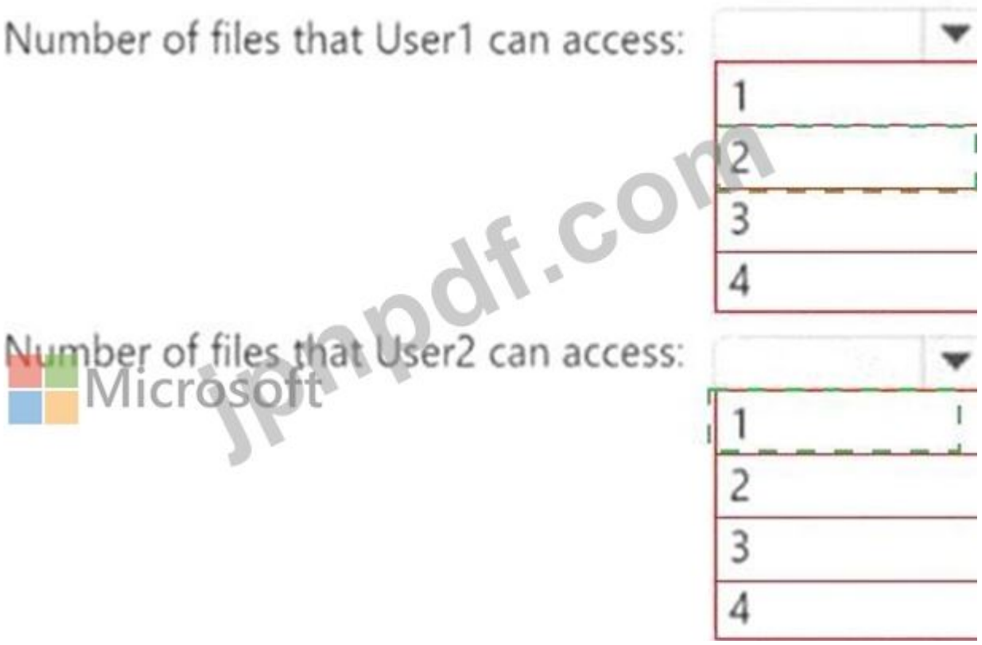
アラート通知を実用的なDLPイベントに限定する必要があります。どうすればよいでしょうか？
A. Microsoft Purview ポータルから、DLP ポリシーのポリシー ヒントの設定を変更します。
B. Microsoft Purview ポータルから、アラート ポリシーの一致したアクティビティのしきい値を変更します。
C. Microsoft Defender ポータルから、アラートにフィルターを適用します。
D. Microsoft Purview ポータルから、DLP ポリシーのユーザー オーバーライド設定を変更します。
Answer: B (メーッセージを残す)

最新問題**: 164**
ホットスポット
DLPpolicy1 をオンにした後、User1 と User2 は Site2 内のいくつのファイルにアクセスできますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Answer Area



Explanation:

コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

DLP ポリシーがファイル アクセスに与える影響を理解する

DLP ポリシー (DLPpolicy1) は Site2 に適用され、次の場合にアクセスを制限します。

コンテンツには SWIFT コードが含まれています。

インスタンス数は2以上です。
ファイル分析（$WIFTコード数に基づく）
コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

File Name	SWIFT Codes Count	DLP Policy Restricts Access?
File1.docx	1	□ No restriction (SWIFT codes < 2)
File2.bmp	4	□ Restricted (SWIFT codes ≥ 2)
File3.txt	3	□ Restricted (SWIFT codes ≥ 2)
File4.xlsx	7	□ Restricted (SWIFT codes ≥ 2)

アクセス可能なままのファイル（DLP によって制限されていないもの）:
File1.docx (SWIFT コードが 1 つだけ含まれています # 制限しきい値未満) DLP ポリシー適用後のユーザー アクセス:
コンピューターの AI によって生成されたコンテンツのスクリーンショットは不正確である可能性があります。

User	Role in Site2	Access Rights	Can Access Files?
User1	Site Owner	Full Access	File1.docx, plus override access to another file
User2	Site Visitor	Read-only	File1.docx only

ユーザー1 （サイト所有者）:
より高い権限を持ち、DLP 制限をオーバーライドできます (管理者の介入を通じて)。
2 つのファイルにアクセスできます (File1.docx + 別のファイルへのオーバーライド アクセス)。
ユーザー2 （サイト訪問者）:
読み取り専用アクセスがありますが、DLP により制限されたファイルへのアクセスがブロックされます。
他のファイルはすべて制限されているため、1 つのファイル (File1.docx) にのみアクセスできます。

最新問題: **165**
Microsoft 365 E5 テナントがあります。
新しいキーワード辞書を追加する必要があります。
何を創造すべきでしょうか?
A. 学習可能な分類器
B. 保持ポリシー
C. 機密ラベル
D. 機密情報の種類
Answer: D (メーッセージを残す**)**
Microsoft Purview データ損失防止 (DLP) に新しいキーワード辞書を追加するには、機密情報タイプ (SIT) を作成する必要があります。
機密情報タイプ（SIT）を使用すると、キーワード辞書、正規表現、メール、ドキュメント、その他のMicrosoft 365内の機密コンテンツを識別するための関数など、カスタム検出ルールを定義できます。キーワード辞書は、Microsoft PurviewがDLPポリシーのコンテンツを識別および分類するために使用できる、定義済みの単語/フレーズのリストです。
キーワード辞書を追加する手順:
1. Microsoft Purviewコンプライアンスポータルにアクセスする
2. データ分類 > 機密情報の種類に移動します
3. 新しい機密情報タイプを作成する
4. キーワード辞書を追加する

5. DLPポリシーに保存して使用する

最新問題**: 166**

Contoso と Fabrikam という2つの Microsoft 365 サブスクリプションがあります。これらのサブスクリプションには、次の表に示すユーザーが含まれています。

Name	Subscription	Email address
User1	Contoso	user1@contoso.com
User2	Contoso	user2@contoso.com
User3	Fabrikam	user3@fabrikam.com
User4	Fabrikam	user4@fabrikam.com

展示に示されているように、「Sensitivity!」という機密ラベルがあります。（展示」タブをクリック）次の表に示すファイルがあります。

Name	Sensitivity1
File1	Automatically applied by using an auto-labeling policy
File2	Applied by User2
File3	Applied by User1

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

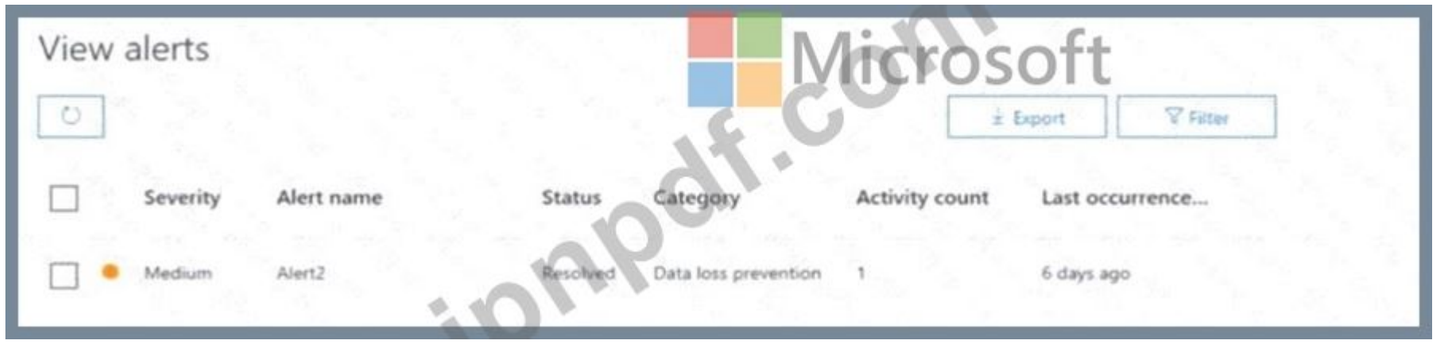
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

最新問題**: 167**
User1 という名前のユーザーを含む Microsoft Entra テナントにリンクされた Microsoft J65 サブスクリプションがあります。
Microsoft 365 監査ログを検索する権限を User1 に付与する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。User1 にはどのロールを割り当てる必要がありますか？
A. Microsoft Entra 管理センターのセキュリティ リーダー ロール
B. Exchange 管理センターのコンプライアンス管理の役割
C. Exchange 管理センターの監査ログの表示のみのロール
D. Microsoft Purview ポータルのレビュー担当者の役割
Answer: (解答を表示する**)**
ステップ1 - シナリオ
最小権限の原則に従いながら、User1 に Microsoft 365 監査ログを検索する権限を付与する必要があります。
ステップ2 - 監査ログを検索できるロール
監査ログ データは Exchange に保存されるため、Microsoft 365 の監査ログ検索は Exchange Online のロール グループに関連付けられています。
関連する役割は次のとおりです。
監査ログの表示のみ # 監査ログの検索と表示権限を付与しますが、監査の設定やその他のコンプライアンスアクションは実行できません。これは最も権限の低いロールです。
監査ログ # 監査のオン/オフを含む、より広範な権限を付与します。
コンプライアンス管理 # 監査ログ検索やその他多くのコンプライアンス機能を含む、最小権限に違反するより広範なロール グループ。
セキュリティ リーダー (Entra ID) # セキュリティ機能への読み取り専用アクセスを許可しますが、監査ログには許可しません。
レビュー担当者 (Purview) # 監査ログではなく、eDiscovery で使用されます。
ステップ3 - 表示専用監査ログ」が正しい理由
Microsoft のドキュメントによると:
監査ログを検索するには、ユーザーに Exchange Online の監査ログまたは表示専用監査ログの役割が割り当てられている必要があります。権限を最小限に抑えるには、表示専用監査ログを割り当てます。
リファレンス: 監査ログを検索するために必要な権限
ステップ4 - 他の選択肢の排除
A). セキュリティ リーダー ロール # Purview 監査ログではなく、Microsoft 365 Defender のセキュリティ関連情報の読み取りを許可します。
B). コンプライアンス管理ロール # 監査ログだけでなく、特権も含まれます。
C). 監査ログの表示のみのロール # 正しい、最小限の権限。
D). レビュー担当者の役割 # 監査ログではなく、電子情報開示ケースの場合。

最新問題**: 168**
次の図に示すように、Alert2 という名前の Microsoft 365 アラートがあります。



Alertのステータスを管理する必要がありますか？Aletteをどのステータスに変更できますか？

A. ステータスを変更できません。

B. 却下のみ

C. 調査のみ

D. アクティブまたは調査中のみ

E. 調査中。アクティブ、または却下

Answer: E (メーッセージを残す)

ステップ1 - シナリオ

展示されているアラートの名前は Alert2 です。

現在のステータス = 解決済み。

タスクは、アラートをどのステータスに変更できるかを特定することです。

ステップ 2 - Microsoft 365 アラート ライフサイクル

Microsoft 365 のコンプライアンスおよびセキュリティアラートでは、調査と修復の状況に応じて、アラートが複数のステータス間を遷移することがあります。使用可能なステータスは次のとおりです。

アクティブ - アラートは新規であり、まだ対応されていません。

調査中 - アラートは確認中です。

解決済み - アラートが解決されました。

無視 – アラートは無視されるか、関連性がないと判断されます。

ステップ3 - ステータスが 解決済み」から変更される

アラートが 解決済み」状態の場合、管理者はアラートを再開または再分類できます。Microsoftのドキュメントによると、 解決済み」状態から以下の状態に変更できます。

アクティブ

調査中

解雇

これにより、必要に応じて調査を継続したり、誤検知を無視したりする柔軟性が得られます。

ステップ4 - Microsoftリファレンス

Microsoft Docsより：「トリアージプロセスの現在の段階に応じて、アラートのステータスをアクティブ、調査中、解決済み、却下の間で変更できます。」参考 :Microsoft 365セキュリティコンプライアンスセンターでアラートを管理する

最新問題**: 169**

Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という 3 人のユーザーと Filetdocx というファイルが含まれています。

次の図に示すように、Label1 という名前の機密ラベルを作成します。

Label1 を File1 に適用します。
Microsoft 365 Copilot はどのユーザー向けに File1 を要約できますか?

A. ユーザー1のみ
B. ユーザーなし
C. ユーザー1とユーザー2のみ
D. ユーザー1、ユーザー2、ユーザー3
Answer: D (メーッセージを残す**)**

最新問題**: 170**
Site1 という名前の Microsoft SharePoint Online サイトと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Member of
User1	Members group of Site1
User2	Owners group of Site1
Admin1	SharePoint Administrator role

次の図に示すように、DLP1 という名前のデータ損失防止 (DLP) ポリシーがあります。

DLP1 を Site1 に適用します。
ユーザー1はサイト1にFile1というファイルをアップロードします。File1はDLP1ルールのいずれにも一致しません。ユーザー2はFile1を更新し、DLP1ルールに一致するデータを追加します。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

最新問題: **171**

次の表に示すような高度な DIP ルールを持つデータ損失防止 (DIP) ポリシーがあります。

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

コンテンツが複数の高度な DIP ルールに一致する場合にどのルールを適用するかを特定する必要があります。

どのルールを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

Answer:

Explanation:

参考文献付きの包括的で詳細な説明

複数の高度な DLP ルールがコンテンツに一致する場合、Microsoft 365 DLP は次の基準に基づいて評価します。

ルールの優先順位

数字が小さいほど優先度が高くなります (0 が最高)。

Rule2 (優先度 1)、Rule3 (優先度 2)、および Rule4 (優先度 3) のうち、Rule2 の優先度が最も高くなります。

競合解決（単一ルールと複数ルールの適用）

デフォルトでは、複数のルールが一致する場合、最も優先度の高いルールのみが適用されます。# そのため、最初のドロップダウンでは、正しい答えは 「ルール 2 のみが有効」です。

ただし、高度なDLPを設定することで、複数の一致ルールを同時に適用できます。この設定を有効にすると、ルール2、ルール3、ルール4のすべてが適用されます。# そのため、2番目のドロップダウンでは、ルール2、ルール3、ルール4のすべてが適用されます。

参考文献:

Microsoft Learn: DLP におけるルール処理の順序

Microsoft Learn: 高度な DLP ルールの優先順位

最新問題: **172**

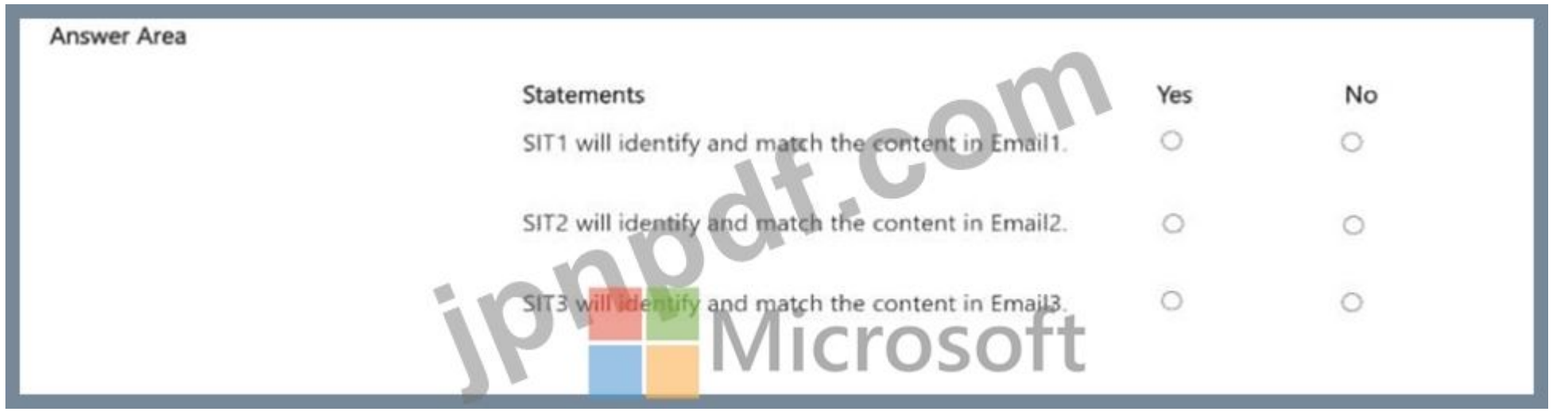
次の表に示す機密情報の種類 (SIT) が含まれる Microsoft 365 E5 サブスクリプションがあります。

Name	Primary element	Character proximity	Supporting elements	Additional checks
SIT1	Regular expression: `prd:\d{4}`	15	Keyword: `product`	*None*
SIT2	Regular expression: `(\d{10}|\d{12})`	*None*	*None*	Exclude specific values: `111-111-1111`
SIT3	Function: `Func_credit_card`	*None*	*None*	*None*

ユーザーは、次の表に示す電子メール メッセージを送信します。

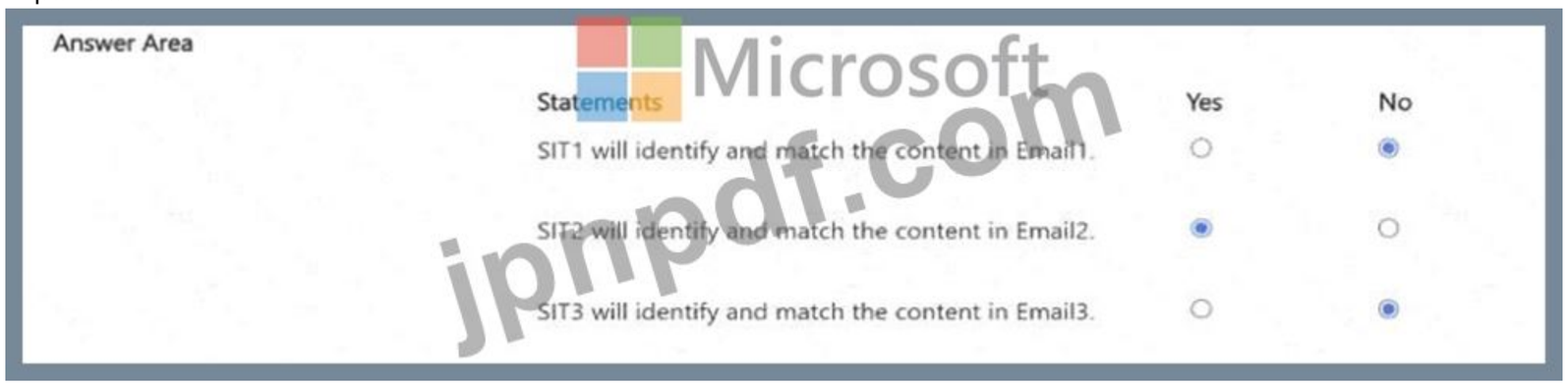
Name	Content
Email1	The product code you requested for the bicycle is prd:1234.
Email2	The bank account number is 123456789012. Contact your account rep at 111-111-1111.
Email3	Please use my credit card that ends with 0023 and has an expiration date of 01/25.

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。注：正しい選択は1つにつき1点です。



Answer:

Explanation:



最新問題: 173

Microsoft 365 サブスクリプションをお持ちです。監査が有効になっています。

User1 という名前のユーザーは、Group1 という名前の動的セキュリティ グループのメンバーです。

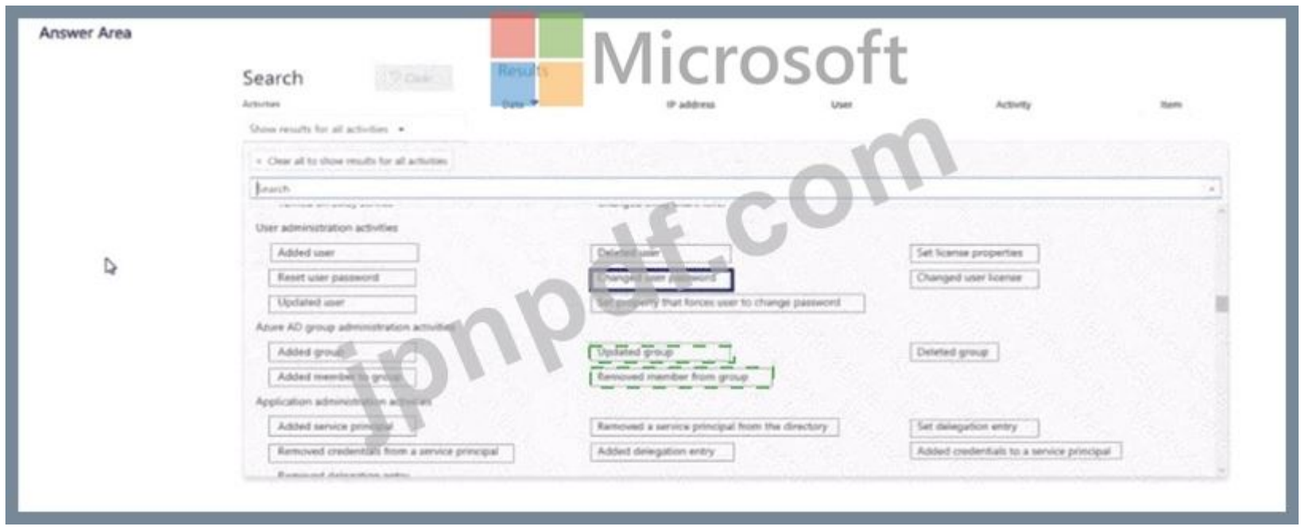
User1 が Group1 のメンバーではなくなったことがわかります。

User1 が Group1 から削除された理由を特定するには、監査ログを検索する必要があります。

検索ではどの 2 つのアクティビティを使用する必要がありますか? 回答するには、回答領域で適切なアクティビティを選択してください。

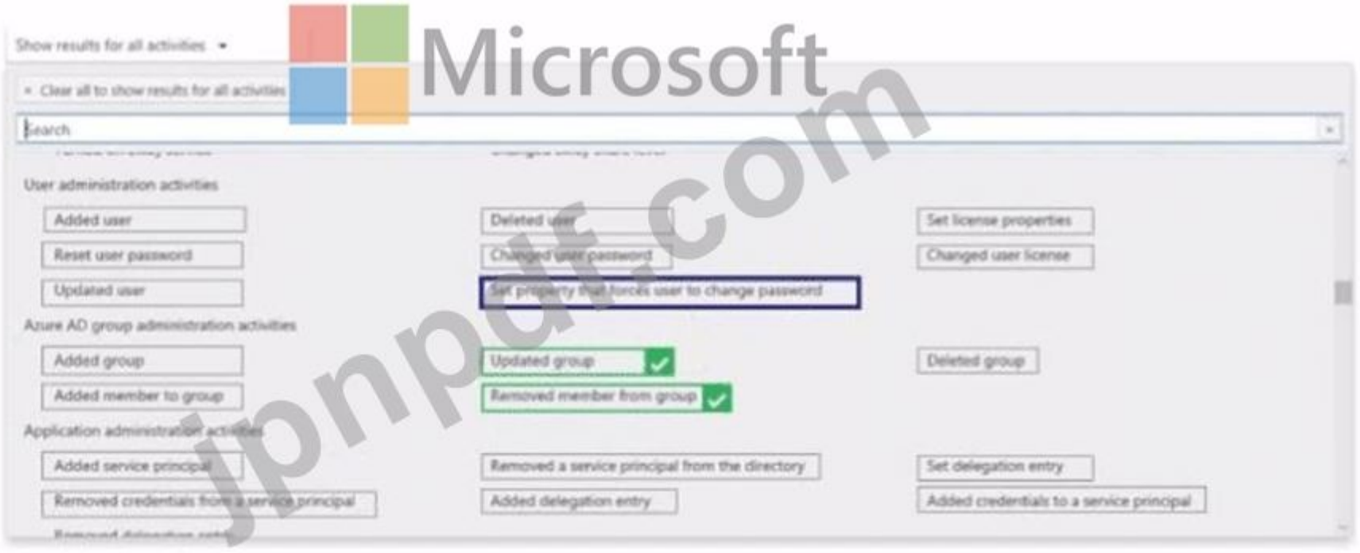
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:



Explanation:

Answer Area



ステップ1 - シナリオ
User1 という名前のユーザーは、動的セキュリティ グループ (Group1) のメンバーでした。
User1 はそのグループのメンバーではなくなりました。
監査ログを検索して、User1 が削除された理由を特定する必要があります。
ステップ2 - グループメンバーシップの変更がMicrosoft 365監査ログに記録される仕組み Microsoft 365監査ログには、Azure ADにおけるグループメンバーシップのアクティビティが記録されます。ユーザーがグループから消える際に最も関連性の高いアクティビティは次のとおりです。
グループからメンバーを削除しました - ユーザーがグループから削除されたことを直接示します。
更新されたグループ - グループのプロパティまたはメンバーシップルール（動的グループの場合）が変更されたときにログに記録されます。Group1 が動的グループの場合、メンバーシップルールの変更によって User1 が資格を失った可能性があり、これは 更新されたグループ」イベントとして表示されます。
ステップ3 - 他の選択肢はなぜダメなのか
削除されたユーザー / 削除されたグループ: 単なる削除ではなく、ユーザーまたはグループ オブジェクト全体が削除されたことを意味します。
ユーザー パスワードの変更、ユーザー パスワードのリセット、ライセンス プロパティの設定、ユーザー ライセンスの変更: これらはアカウント関連であり、グループ メンバーシップ関連ではありません。
グループにメンバーを追加しました: 反対のアクションです。
ステップ4 - Microsoftリファレンス
Microsoft のドキュメントより:
監査ログには、グループのメンバーが追加または削除されたときや、グループのプロパティまたはメンバーシップ ルールが更新されたときなどのイベントが含まれます。
参考: Microsoft Purview コンプライアンス ポータルで監査ログを検索する

最新問題**: 174**
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
すべてのユーザーに Microsoft 365 Copilot ライセンスが割り当てられます。
Microsoft Purview Data Security Posture Management for AI (DSPM for AI) を展開します。
ユーザー1がAIインタラクションイベントのプロンプトと応答を分析できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 をどの 2 つのロール グループに追加する必要がありますか? それぞれの正解はソリューションの一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。

A. セキュリティリーダー
B. コンテンツエクスプローラーリストビューアー
C. インサイダーリスク管理調査員
D. 情報保護アナリスト
E. コンテンツエクスプローラー コンテンツビューアー
Answer: D,E (メーッセージを残す**)**
コンテンツエクスプローラー コンテンツビューアー
Purview によって表示されたアイテムの完全なコンテンツ (AI インタラクションを含む) をユーザーが表示できるようにします。
■
メタデータだけでなく、実際のプロンプトと応答を分析するために必要です。
■
カウントのみを表示するリスト ビューアーよりも権限が高くなります。
■
情報保護アナリスト
ユーザーは、AIを含むデータ分類とデータ保護の洞察を調査できます。
■
関連するデータセキュリティの問題。
広範なセキュリティ権限なしで、Purview レベルの分析機能を提供します。
■

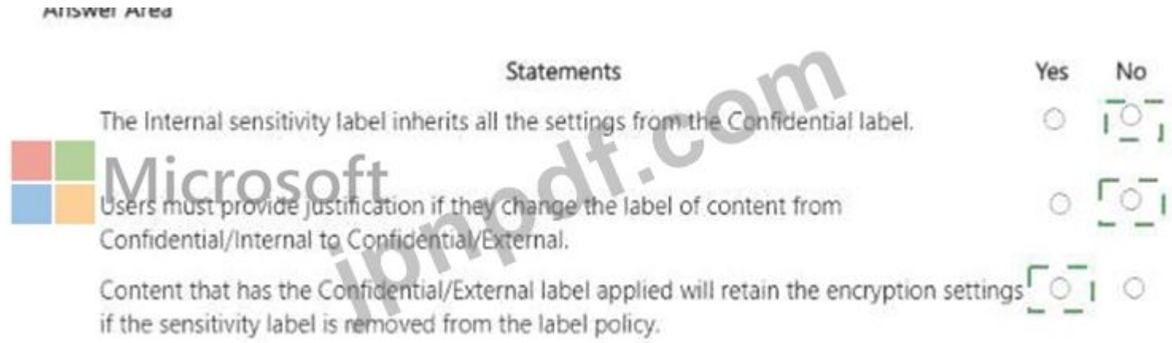
最新問題**: 175**
Windows クライアント コンピューターに適用されるデータ損失防止 (DLP) ソリューションを計画しています。
ユーザーが機密情報を含むファイルを USB ストレージ デバイスにコピーしようとする場合は、次の要件が満たされていることを確認する必要があります。
ユーザーが Group1 というグループのメンバーである場合、ユーザーにファイルのコピーを許可し、監査ログにイベントを記録する必要があります。
他のすべてのユーザーによるファイルのコピーをブロックする必要があります。
何を創造すべきでしょうか?
A. 1 つの DLP ルールを含む 1 つの DLP ポリシー
B. 2つのDLPルールを含む1つのDLPポリシー
C. それぞれ 1 つの DLP ルールを含む 2 つの DLP ポリシー
Answer: B (メーッセージを残す**)**
1 つのポリシーでは、監査とブロックの両方を選択することはできません。
ブロック ルールが適用され、group1 が除外されるすべてのユーザーに対するポリシーが 1 つと、group1 のみが含まれ、ルールが監査のみに設定されたポリシーが 1 つ必要です。

最新問題**: 176**
Microsoft 365 E5 テナントがあります。
「機密ラベル」展示に示されているように、機密ラベルがあります。（「機密ラベル」タブをクリックします。）

機密/外部の機密ラベルは、コンテンツに適用されたときにファイルと電子メールを暗号化するように構成されています。
機密ラベルは、 公開済み」展示に示されているとおりに公開されました。(公開済み」タブをクリックします。)

以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:



Explanation:

最新問題**: 177**

Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。

Site1 には、File1、File2、File3 という名前の 3 つのファイルが含まれています。

次の表に示すデータ損失防止 (DLP) ポリシーを作成します。

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

各ファイルに一致する DLP ルールを次の表に示します。

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

アクティビティ エクスプローラーに追加される DLP ポリシー一致イベントの数はいくつですか。また、DLP インシデント レポートに追加されるポリシー一致の数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

最新問題: **178**
機密情報の種類に使用される単語のリストを含む電子メールを受信します。
キーワード辞書のソースとして使用できるファイルを作成する必要があります。
リストはどの形式で保存すればよいですか?
A. 各単語の要素を持つJSONファイル
B. 各行に1つの単語が含まれるDOCXファイル
C. カンマで区切られた単語を含むCSVファイル
D. Dictionaryという名前のテーブルを含むACCDBデータベースファイル
Answer: C (メーッセージを残す)
正しい：
* カンマで区切られた単語を含むCSVファイル
* 各行に1つの単語が含まれるテキストファイル
正しくない：
* Dictionaryという名前のテーブルを含むACCDBデータベースファイル
* 各行に1つの単語が含まれるDOCXファイル
* 各単語の要素を持つJSONファイル
* タブで区切られた単語を含むTSVファイル
* 各単語のキーワードタグを含むXMLファイル
* 最初の行の各セルに1つの単語が含まれるXLSXファイル
注記：
Microsoft Purview Data Loss Prevention (DLP) で機密情報の種類に対するキーワード ディクショナリを作成するには、各キーワードが別々の行にあるプレーン テキスト (.txt) ファイル (または .CSV ファイル) を使用する必要があります。
フォーマット例（TXTファイル）:
機密
センシティブ
分類された
極秘
この形式はシンプルで効率的であり、キーワード辞書の Microsoft 365 DLP ポリシーと直接互換性があります。
キーワード辞書の使い方は？
1 行に 1 つのキーワードを含むテキスト ファイルを作成します。
「データ分類」> 「機密情報の種類」の Microsoft Purview にアップロードします。
DLP ポリシーで辞書を使用して、機密情報を識別して保護します。
手順:
Microsoft Purview ポータルを使用してキーワード辞書を作成する
カスタム辞書のキーワードを作成またはインポートするには、次の手順に従います。
1. Microsoft Purview ポータルの [情報保護] > [分類子] > [機密情報の種類] にサインインします。
2. 「+ 機密情報の種類を作成」を選択し、機密情報の種類の名前と説明を入力します。「次へ」を選択します。
3. [この機密情報の種類のパターンの定義] ページで、[+ パターンの作成] を選択します。
4. 「新しいパターン」ウィンドウで、信頼レベルを選択します。
5. 「プライマリ要素の追加」を選択し、「キーワード辞書」を選択します。
*-> 6. 「キーワード辞書の追加」フライアウトでは、次の操作を実行できます。

6a. TXT または CSV 形式の辞書ファイルをアップロードします。
6b. 既存の辞書から選択します。
または、キーワードを手動で入力して名前を付けて新しい辞書を作成します。
参照：
https://learn.microsoft.com/en-us/purview/sit-create-a-keyword-dictionary

最新問題**: 179**
Microsoft J65 ES サブスクリプションをお持ちです。
データ損失防止（DIP）違反を検出するMicrosoft Defender for Cloud Appsポリシーを作成する必要があります。どのようなポリシーを作成すればよいでしょうか？
A. ファイルポリシー
B. アクティビティポリシー
C. セッションポリシー
D. アクセスポリシー
Answer: A (メーッセージを残す**)**
質問は、データ損失防止 (DLP) 違反を検出する Microsoft Defender for Cloud Apps (MCAS/MDA) ポリシーの作成に関するものです。
Defender for Cloud Apps のポリシーの種類について理解する:
ファイルポリシー
クラウド アプリ (SharePoint、OneDrive、Box、Google Drive など) に保存されているファイルを監視および制御するために使用されます。
機密情報の種類 (クレジットカード、社会保障番号、SWIFT コードなど) を検出し、DLP 違反にフラグを立てることができます。
ガバナンス アクション (例: 検疫、共有の削除、ユーザーへの通知) を適用できます。
DLP違反検出を修正します。
活動方針
ユーザーのアクティビティ (ログイン試行、大量ダウンロード、疑わしい動作など) を監視します。
ファイル コンテンツの DLP には対応していません。
セッションポリシー
ユーザー セッション中のリアルタイムの監視/制御のために、条件付きアクセス アプリ制御を通じて適用されます。
アクション (ダウンロード、切り取り/貼り付け) を制御するために使用されますが、保存されたファイルの広範な DLP スキャンには使用されません。
アクセスポリシー
条件に基づいてアプリへのアクセスを制御します (例: 管理されていないデバイスへのアクセス)。
DLP コンテンツ検査用に設計されていません。
ファイルポリシーが正しい理由
要件は次のとおりです。
DLP違反を検出する」
つまり、ファイルの内容から機密情報をスキャンするということです。これは、Microsoft Defender for Cloud Apps のファイルポリシーでのみ可能です。
参考資料: Microsoft Defender for Cloud Apps のファイル ポリシー

最新問題**: 180**
Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
Site1 には、File1、File2、File3 という名前の 3 つのファイルが含まれています。
次の表に示すデータ損失防止 (DLP) ポリシーを作成します。

Name	Applied to	DLP rules
DLP1	Site1	Rule11, Rule12, Rule13
DLP2	Site1	Rule21, Rule22

各ファイルに一致する DLP ルールを次の表に示します。

Name	Matches
File1	Rule11, Rule12
File2	Rule21, Rule22
File3	Rule11, Rule22

アクティビティ エクスプローラーに追加される DLP ポリシー一致イベントの数はいくつですか。また、DLP インシデント レポートに追加されるポリシー一致の数はいくつですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

最新問題: **181**

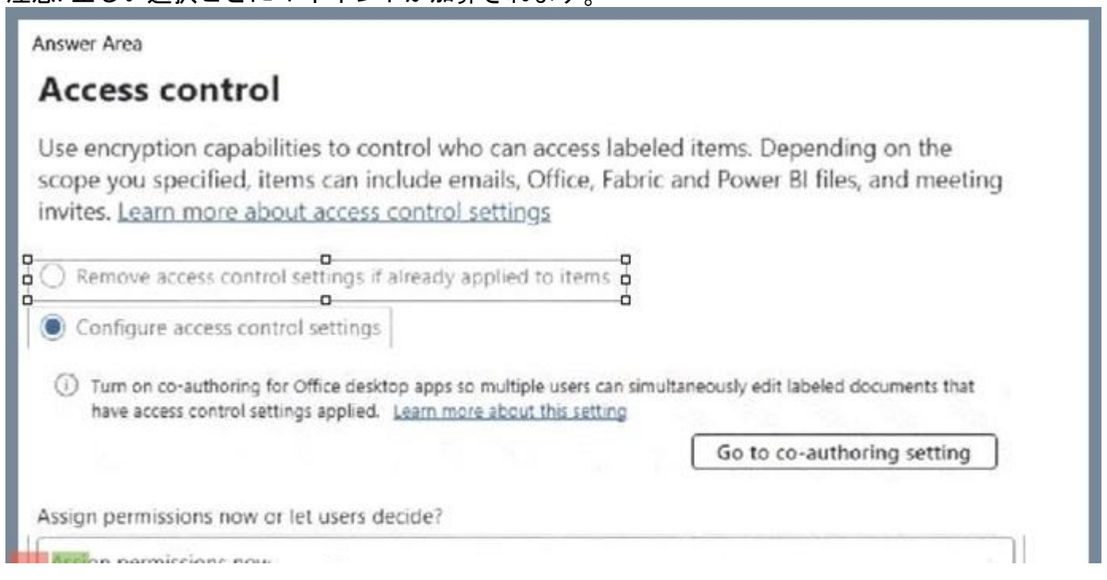
label1 という名前の機密ラベルが含まれる Microsoft 365 E5 テナントがあります。

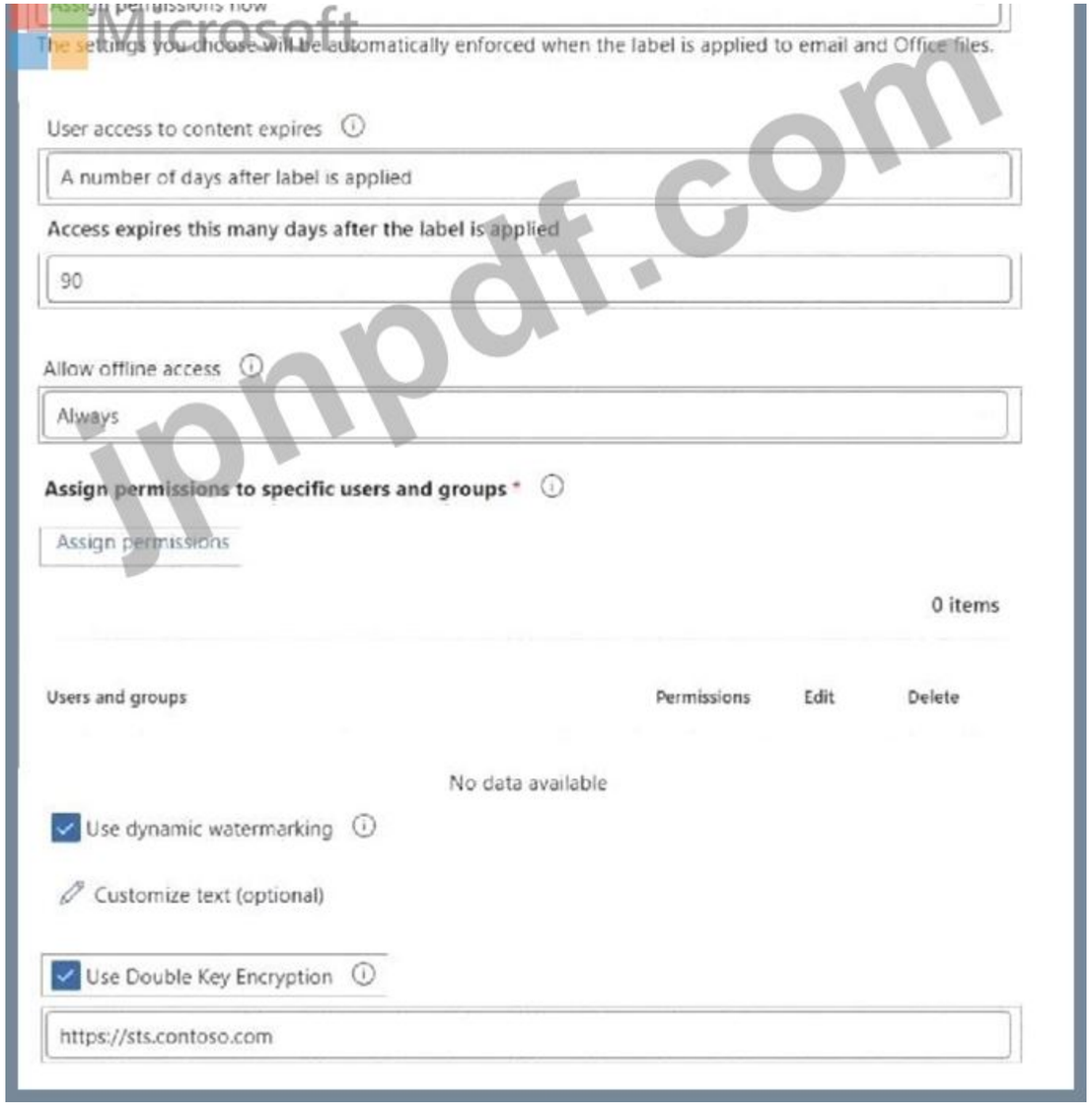
暗号化されたファイルの共同編集を有効にする予定です。

label1 が適用されたファイルが共同編集をサポートしていることを確認する必要があります。

どの 2 つの設定を変更する必要がありますか? 回答するには、回答領域で設定を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



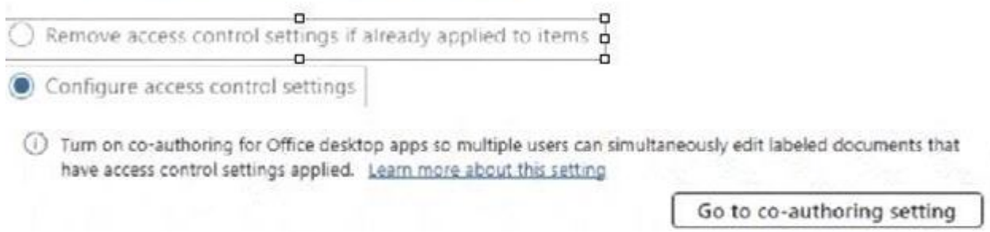


Answer:

Answer Area

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings



Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires ⓘ

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access ⓘ

Always

Assign permissions to specific users and groups * ⓘ

Assign permissions

0 items

Users and groups	Permissions	Edit	Delete
No data available			

☑ Use dynamic watermarking ⓘ

Customize text (optional)

☑ Use Double Key Encryption ⓘ

https://sts.contoso.com

Explanation:

Answer Area

Access control

Use encryption capabilities to control who can access labeled items. Depending on the scope you specified, items can include emails, Office, Fabric and Power BI files, and meeting invites. Learn more about access control settings

○ Remove access control settings if already applied to items

Configure access control settings

Turn on co-authoring for Office desktop apps so multiple users can simultaneously edit labeled documents that have access control settings applied. Learn more about this setting

Go to co-authoring setting

Assign permissions now or let users decide?

Assign permissions now

The settings you choose will be automatically enforced when the label is applied to email and Office files.

User access to content expires

A number of days after label is applied

Access expires this many days after the label is applied

90

Allow offline access

Always

Assign permissions to specific users and groups *

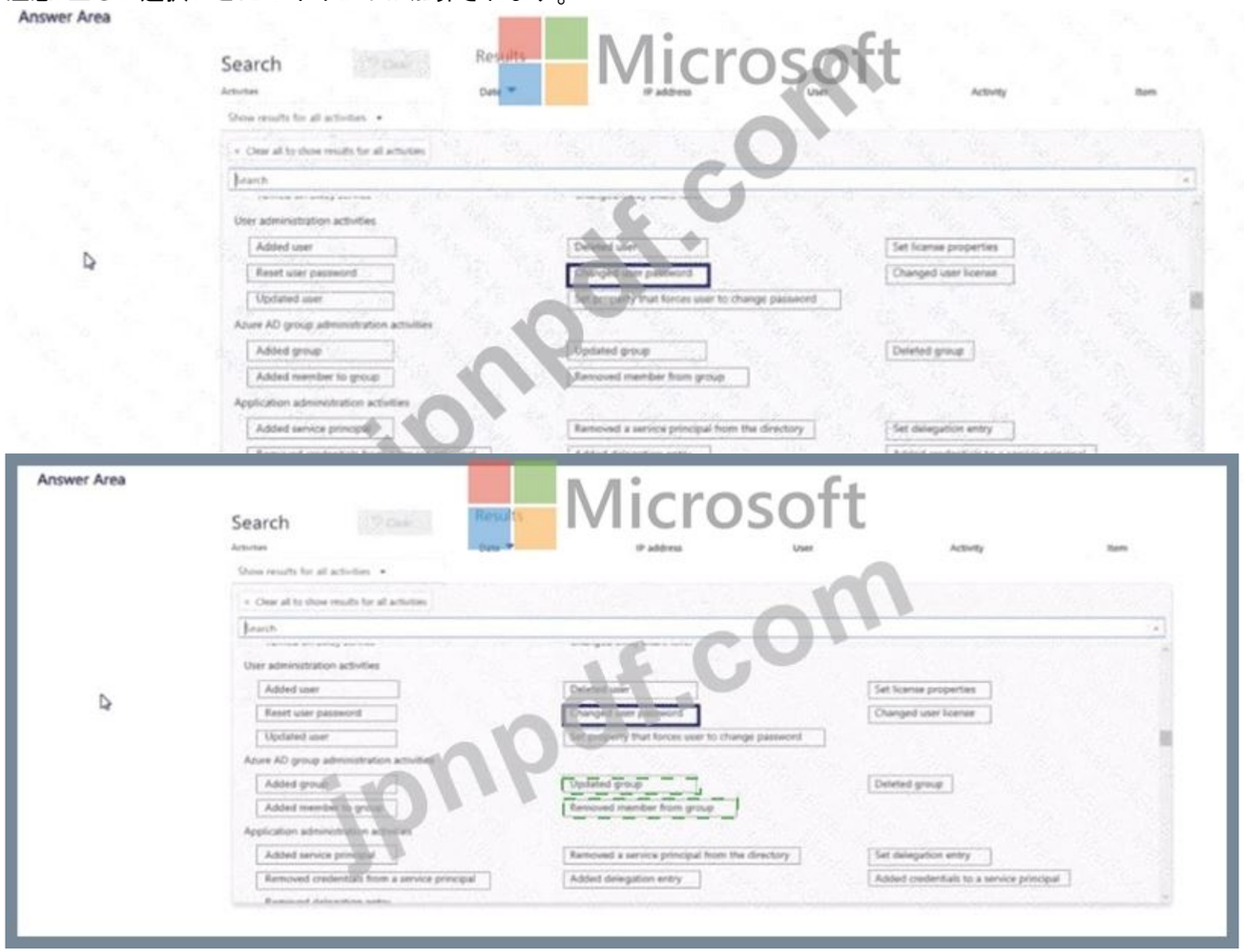
Assign permissions

0 items

Users and groups	Permissions	Edit	Delete
No data available			

最新問題: 182
Microsoft 365 サブスクリプションをお持ちです。監査が有効になっています。
User1 という名前のユーザーは、Group1 という名前の動的セキュリティ グループのメンバーです。
User1 が Group1 のメンバーではなくなったことがわかります。
User1 が Group1 から削除された理由を特定するには、監査ログを検索する必要があります。
検索ではどの 2 つのアクティビティを使用する必要がありますか? 回答するには、回答領域で適切なアクティビティを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

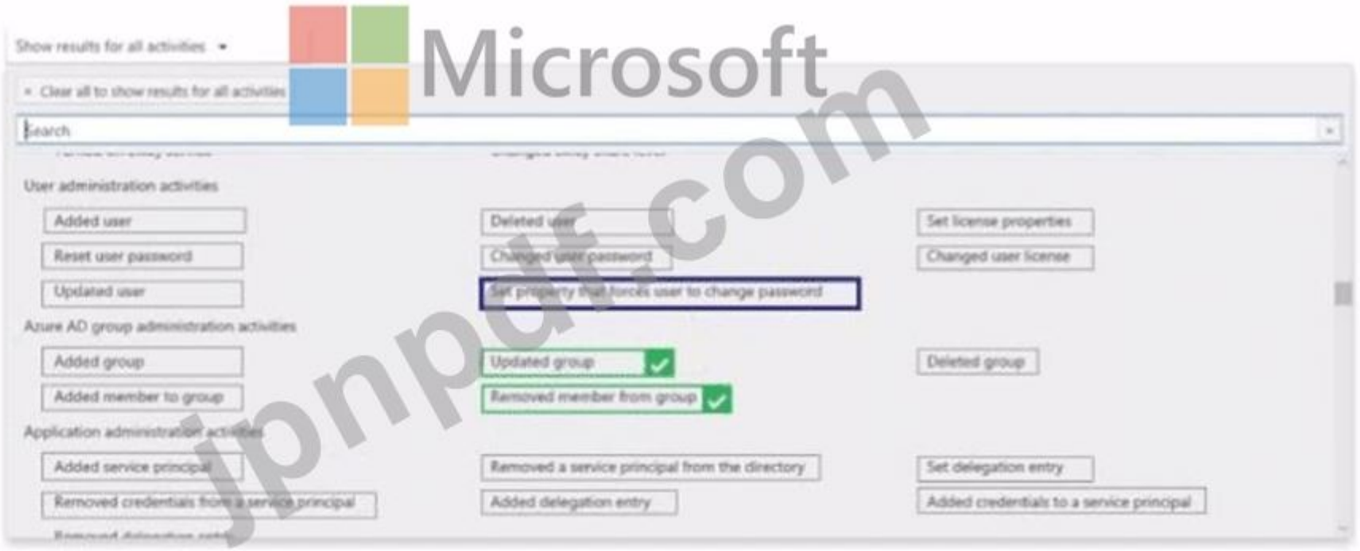
Answer Area



Answer Area

Explanation:

Answer Area



最新問題**: 183**

Microsoft Teams を使用し、次の表に示すユーザーを含む Microsoft 365 ES サブスクリプションがあります。

Name	Team membership
User1	Team1, Team2
User2	Team2

次の表に示す保持ポリシーがあります。

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	Microsoft Teams channel messages	All teams	7 years	When items are created	Delete items automatically
	Microsoft Teams chats	User1			
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats				

ユーザーは、次の表に示すアクションを実行します。

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

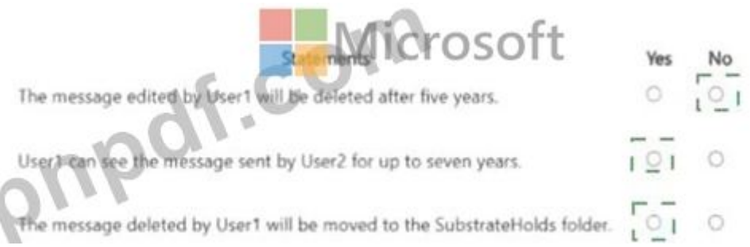
以下の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注: 正解ごとに1ポイント獲得

Answer Area

Answer:

Answer Area



Explanation:

Answer Area

最新問題: 184

Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、User1 というユーザーと、次の表に示す機密ラベルが含まれています。

Name	Authenticated users: View content(VIEW)	Authenticated users: Copy and extract content(EXTRACT)	Authenticated users: Export content(EXPORT)
Label1	Granted	Not granted	Not granted
Label2	Granted	Granted	Not granted
Label3	Granted	Not granted	Granted

ラベルを User1 に公開します。

サブスクリプションには、次の表に示すファイルが含まれています。

Name	Label
File1	Label1
File2	Label2
File3	Label3

Microsoft 365 Copilot は User1 のどのファイルを要約できますか?

A. ファイル2のみ

B. ファイル1、ファイル2、ファイル3

C. ファイル2とファイル3のみ

D. ファイル3のみ

Answer: A (メーッセージを残す)

最新問題: 185

ケーススタディ 1 - Contoso 社

概要

Contoso 社は、モントリオールに本社を置き、シアトル、ボストン、ヨハネスブルグに 3 つの支社を持つコンサルティング会社です。

既存の環境

Microsoft 365 環境

Contoso 社には Microsoft 365 E5 テナントがあります。このテナントには、次の表に示す管理ユーザーアカウントが含まれています。

Name	Role
Admin1	Global Reader
Admin2	Compliance Data Administrator
Admin3	Compliance Administrator
Admin4	Security Operator
Admin5	Security Administrator

ユーザーは次の場所にデータを保存します。
- SharePoint サイト
- OneDriveアカウント
- Exchangeメール
- Exchangeパブリックフォルダ
- Teamsチャット
- Teams チャネル メッセージ

研究部門のユーザーが文書を作成する際は、各文書に10桁のプロジェクトコードを追加する必要があります。999で始まるプロジェクトコードは機密情報です。

SharePoint Online 環境

Contoso には、Site1、Site2、Site3、Site4 という名前の 4 つの Microsoft SharePoint Online サイトがあります。

Site2 には、次の表に示すファイルが含まれています。

Name	Number of SWIFT codes in the file
File1.docx	1
File2.bmp	4
File3.txt	3
File4.xlsx	7

次の表に示すように、User1 と User2 という名前の 2 人のユーザーに Site2 のロールが割り当てられています。

User	Role
User1	Site owner
User2	Site visitor

Site3には、会社のプロジェクトに関連する文書が保存されています。文書はプロジェクトごとにフォルダ階層に整理されています。

Site4 には次の 2 つの保持ポリシーが適用されています。
- 名前: Site4RetentionPolicy1

ポリシーを適用する場所: サイト4

2年以上前のアイテムを削除

コンテンツを削除する基準: アイテムが作成された日時
- 名前: Site4RetentionPolicy2

ポリシーを適用する場所: サイト4

特定の期間アイテムを保管する: 4 年間

保存期間の開始基準: アイテムが作成された日時

保存期間の終了時: 何もしない

問題ステートメント

Contoso社の経営陣はデータ漏洩を懸念しています。研究部門の機密文書が漏洩するケースが複数回発生しました。
要件
計画された変更
Contoso では、次のデータ損失防止 (DLP) ポリシーを作成する予定です。
- 名前: DLPpolicy1
ポリシーを適用する場所: サイト2
条件：
コンテンツには、次のいずれかの機密情報タイプが含まれています: SWIFT コード
- インスタンス数: 2〜任意
アクション: コンテンツへのアクセスを制限する
技術要件
Contoso は次の技術要件を満たす必要があります。
- すべての管理ユーザーは DLP レポートを確認できる必要があります。
- 可能な限り、最小権限の原則を使用する必要があります。
- すべてのユーザーについて、Microsoft 365のデータは少なくとも
1年。
- 機密文書は、以下の方法で検出し保護する必要があります。
マイクロソフト365。
- クレジットカード番号を含むサイト1文書にはラベルを付ける必要がある
自動的に。
- すべての管理ユーザーはMicrosoft 365を作成できる必要があります
機密ラベル。
- プロジェクトが完了したら、サイト3にある関連する文書は
プロジェクトは10年間保持する必要があります。
ホットスポットに関する質問
SharePoint Online 環境のポリシーを確認しています。
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Answer Area

Explanation:
Site4 の保持ポリシーを理解する:
- Site4RetentionPolicy1 は、作成から2年以上経過したアイテムを削除します。ファイルが2021年1月1日に作成された場合、2023年1月1日以降に削除されます。
- Site4RetentionPolicy2は、ファイルの作成から4年間保存します。ファイルが1月1日に作成された場合、
2021 年の場合、2025 年 1 月 1 日まで保存されますが、その後は削除されません (ポリシーでは 「何もしない」とされています)。
ボックス 1 - はい。Site4RetentionPolicy2 により、ファイルは 4 年間保持されます。
ボックス 2 - はい。Site4RetentionPolicy2 はファイルを 4 年間 (2025 年 1 月 1 日まで) 保持します。
ボックス3 - いいえ。保存期間は4年間（2025年1月1日まで）です。それ以降はポリシーは 「何もしない」ため、ファイルは回復できなくなります。

最新問題: **186**
Microsoft 365 の 5 ポンドのサブスクリプションをお持ちです。
0ME1 という名前の Microsoft Purview Advanced Message Encryption ブランド テンプレートがあります。
OME1 を電子メールに適用するには、Microsoft Exchange Online メール フロー ルールを作成する必要があります。
ルールをどのように設定すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:

ステップ1 - 要件
OME1 という名前の Microsoft Purview Advanced Message Encryption (OME) ブランド テンプレートを適用するには、Exchange Online でメール フロー ルールを構成する必要があります。
ステップ2 - メールフロールールの条件
Exchange Online で、機密ラベル (分類) に基づいて暗号化をトリガーするには:
「次の場合にこのルールを適用: 送信者が... 分類を含む」という条件を使用します。
これにより、ルールは送信者が電子メールに特定の機密ラベル (分類) を適用したタイミングを検出できます。
ステップ3 - メールフロールールアクション
カスタム ブランド テンプレート (OME1 など) を適用するには、次のアクションを構成します。
「メッセージのセキュリティを変更します」。
これは、暗号化を適用し、ブランド化のために特定の OME テンプレートを割り当てることができるアクションです。

最新問題: **187**

Microsoft 365 E5 サブスクリプションをお持ちです。
データ損失防止 (DLP) 違反を検出する Microsoft Defender for Cloud Apps ポリシーを作成する必要があります。
何を創造すべきでしょうか?
A. アクセスポリシー
B. アクティビティポリシー
C. ファイルポリシー
D. セッションポリシー
Answer: C (メーッセージを残す)
Microsoft Defender for Cloud Apps でデータ損失防止 (DLP) ポリシーを作成するには、Microsoft Defender ポータルにアクセスし、[クラウド アプリ] > [ポリシー] > [ポリシー管理] に移動して、新しいファイル ポリシーを作成します。ファイル フィルターを選択し、コンテンツ検査用のデータ分類サービスを構成することで条件を定義します。次に、違反に対するアクション (アラートの作成など) を選択します。必要に応じて、ファイルを検疫に移動するなどのガバナンス アクションを実装します。必要に応じて、ポリシーの重大度を設定し、リスクの種類にリンクし、機密ラベルを使用して正確なファイル フィルター処理を実現することもできます。
参照：
https://learn.microsoft.com/en-us/training/modules/create-configure-data-loss-prevention-policys/3-integrate-data-loss-prevention-with-microsoft-cloud-app-security

最新問題: 188
次の表に示すように、RP1 という名前のアイテム保持ポリシーを含む Microsoft 365 E5 サブスクリプションがあります。

Setting	Value
Location	• Exchange email (All recipients) • SharePoint sites (All sites)
Retain items for a specific period	5 years (When items were created)
At the end of the retention period	Delete items automatically

RP1 に保存ロックをかけます。
RP1 を変更する必要があります。
どの 2 つの変更を実行できますか。それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. ポリシーに場所を追加します。
B. ポリシーを削除します。
C. ポリシーから場所を削除します。
D. ポリシーの保持期間を短縮します。
E. ポリシーを無効にします。
F. ポリシーの保持期間を延長します。
Answer: A,F (メーッセージを残す)
Microsoft Purview 保持ポリシーの保存ロックは、厳格なコンプライアンスを強制し、特定の変更を防止して、データがコンプライアンス要件に従って保持されるようにします。
保存ロックが適用されると、次のようになります。
1. ポリシーを無効化または削除することはできません。
2. ポリシーから場所を削除することはできません。
3. 保存期間を短縮することはできません。
4. ポリシーに場所を追加できます。
5. 保存期間を延長できます。

保持ポリシーを拡張して、対象となる場所（例Exchangeメールボックス、SharePointサイトなど）を追加できます。より厳格なコンプライアンスに準拠するため、保持期間を延長（例5年から10年に延長）することも可能です。

最新問題: **189**
ホットスポット
Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、Microsoft Purview にオンボードされ、次の表のように構成されたデバイスが含まれています。

Name	Operating system	Microsoft Purview browser extension
Device1	Windows 11	Installed
Device2	Windows 11	Not installed
Deivce3	macOS	Installed

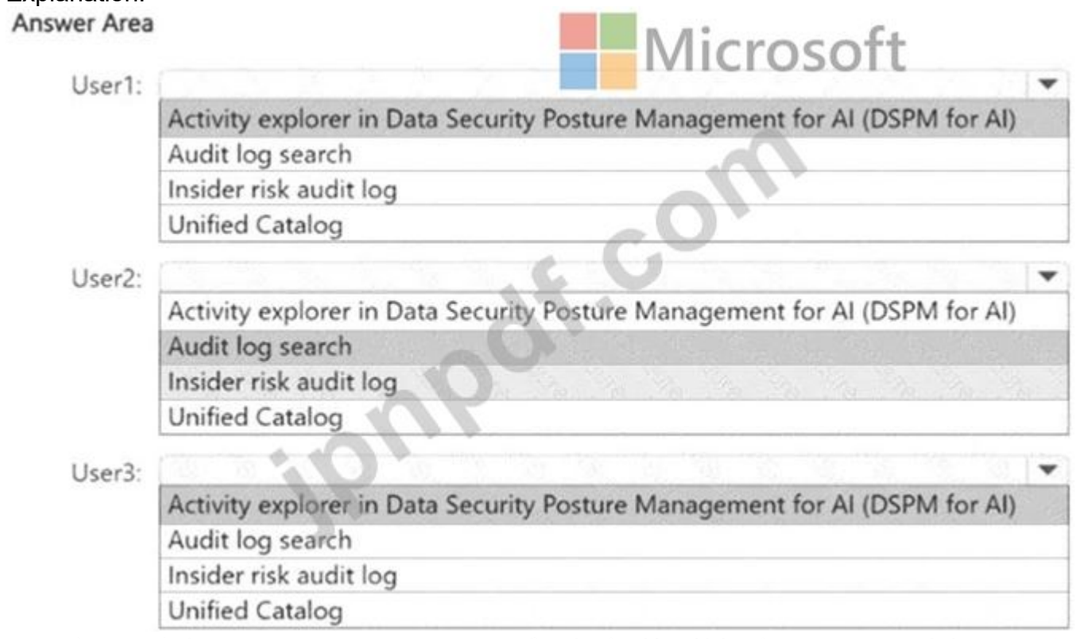
サブスクリプションには、次の表に示すユーザーが含まれます。

Name	Activity performed during the last seven days	On device
User1	Used a generative AI website to generate an image	Device1
User2	Asked Microsoft 365 Copilot to summarize a document	Device2
User3	Browsed sample content on a generative AI website	Device3

アクティビティを見直す必要があります。
各ユーザーには何を使用すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

Explanation:



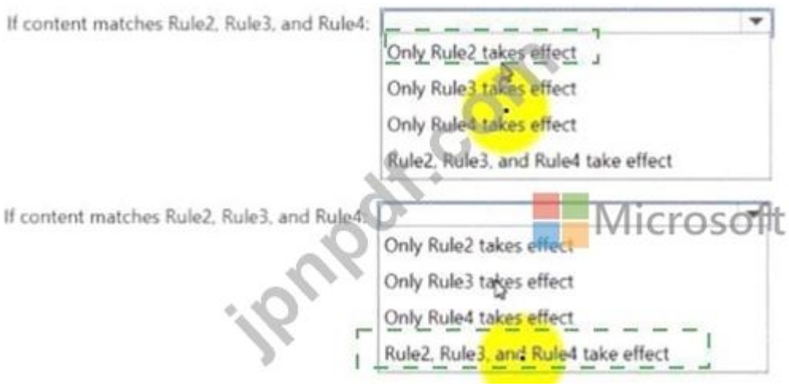
ユーザー 1: デバイス 1 に Microsoft Purview ブラウザー拡張機能がインストールされているため、ユーザー 1 が実行した AI 関連のアクティビティ (生成 AI Web サイトを使用して画像を生成する) を DSPM for AI のアクティビティ エクスプローラーで確認できます。
ユーザー2: デバイス2にはMicrosoft Purviewブラウザ拡張機能がインストールされていないため、DSPM for AIではAI関連のアクティビティを追跡できません。代わりに、Microsoft 365 Copilotの使用などのアクティビティを確認するには、監査ログ検索を使用してください。
ユーザー 3: デバイス 3 には Microsoft Purview ブラウザー拡張機能がインストールされているため、DSPM for AI のアクティビティ エクスプローラーを使用して AI 関連のアクティビティ (生成 AI Web サイトでのサンプル コンテンツの閲覧) を確認できます。

最新問題**: 190**
次の表に示すような高度な DIP ルールを持つデータ損失防止 (DIP) ポリシーがあります。

Name	Priority	Actions
Rule1	0	• Notify users with email and policy tips • User overrides: Off
Rule2	1	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off
Rule3	2	• Notify users with email and policy tips • Restrict access to the content • User overrides: On
Rule4	3	• Notify users with email and policy tips • Restrict access to the content • User overrides: Off

コンテンツが複数の高度な DIP ルールに一致する場合にどのルールを適用するかを特定する必要があります。
どのルールを特定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

Answer:

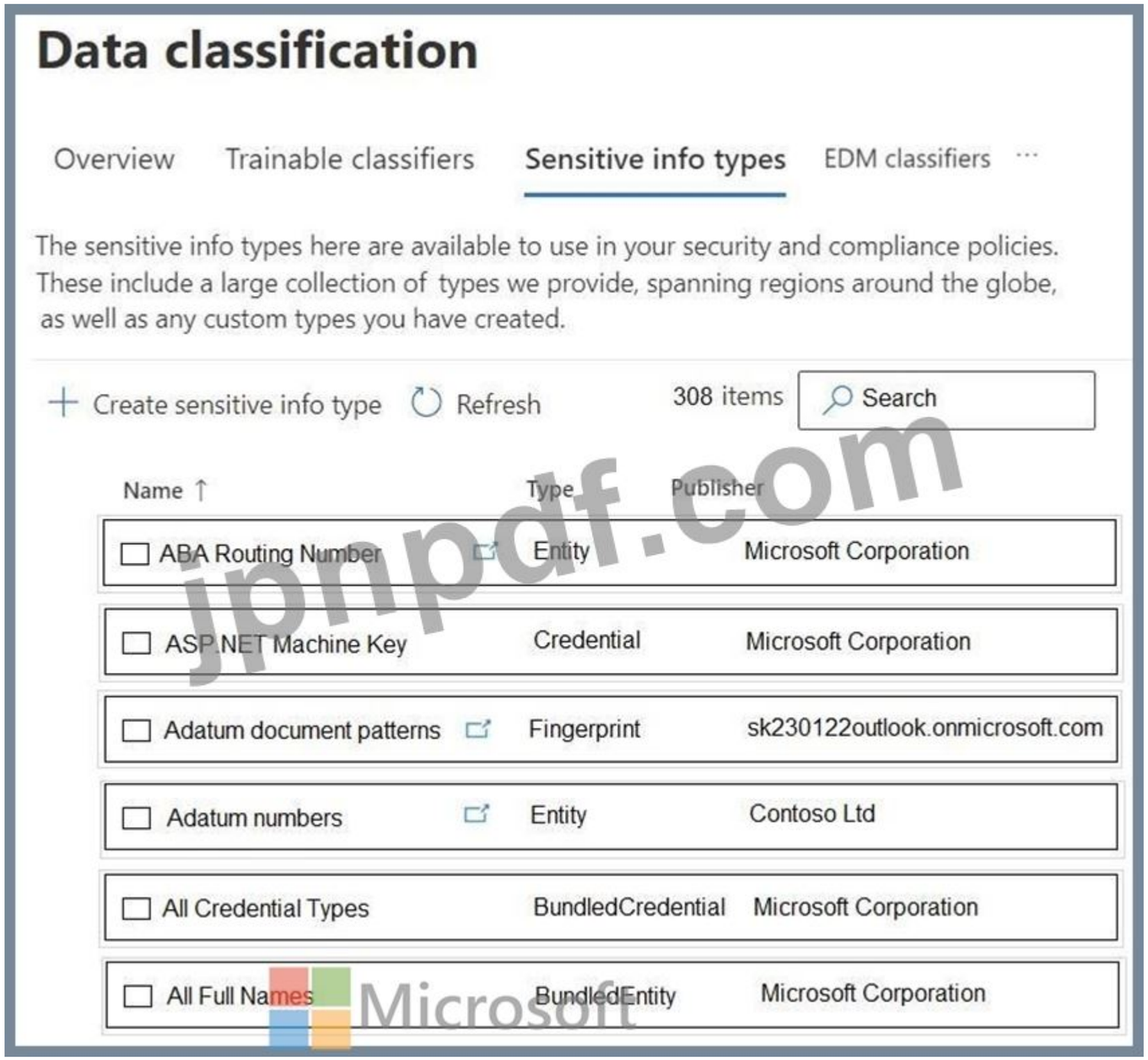


Explanation:

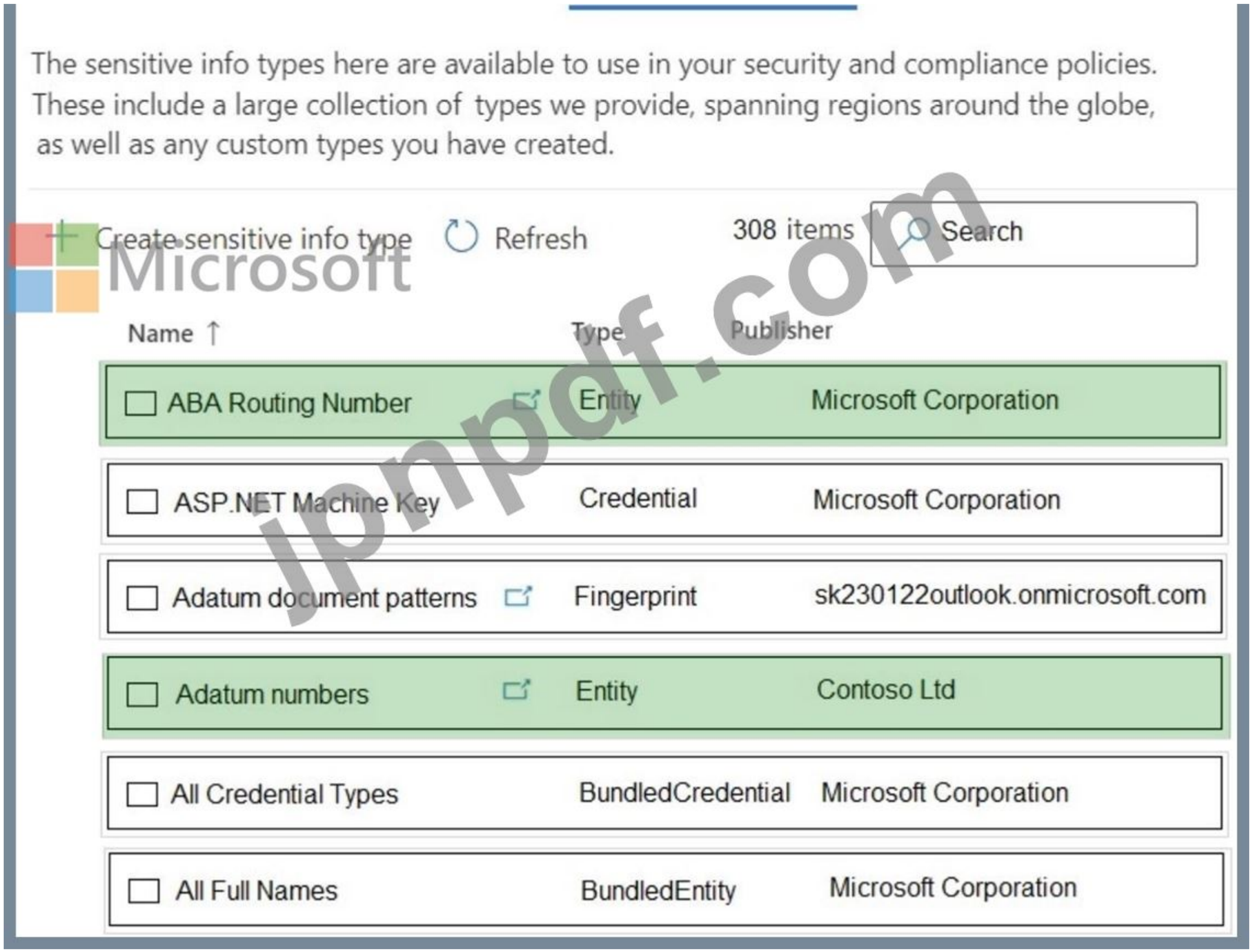
最新問題: **191**

Microsoftで参照される組織の製品コードを識別するためのカスタムトレーニング可能な分類子を作成しています
36S コンテンツ。シードコンテンツとして使用する 300 個のファイルを特定します。シードコンテンツはいつ保存する必要がありますか?
A. Microsoft Exchange Online 共有メールボックス
B. Azure ファイル共有
C. Microsoft SharePoint Online フォルダー
D. Microsoft OneDrive フォルダ
Answer: (解答を表示する**)**

最新問題**: 192**
ホットスポットに関する質問
Microsoft 365 365 E5 サブスクリプションをお持ちです。
Microsoft Purview ポータルを使用して、新しい機密情報の種類 (SIT) を作成する予定です。
新しい SIT を作成するには、既存の SIT をコピーして変更する必要があります。
コピーして変更できる 2 つの SIT は何ですか? 回答するには、回答領域で適切な SIT を選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ABAルーティングとAdatumは正しいです。繰り返し可能な標準化されたパターンのみをコピーできます。

参照：

https://learn.microsoft.com/en-us/purview/sit-common-scenarios

https://learn.microsoft.com/en-us/purview/sit-create-a-custom-sensitive-information-type

最新問題: **193**
Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには、Microsoft Purview にオンボードされた Windows デバイスが 500 台含まれています。
ユーザーがサードパーティの生成AIウェブサイトと機密情報を共有するのを防ぐ必要があります。どのMicrosoft Purviewソリューションを使用すべきでしょうか？
A. インサイダーリスク管理
B. 情報保護
C. データ損失防止
D. 情報障壁
Answer: C (メーッセージを残す**)**

最新問題: **194**
Microsoft 365 E5 サブスクリプションをお持ちです。
次の場所に対して静的保持ポリシーを作成する必要があります。
- Teamsチャット
- Exchangeメール
- SharePoint サイト
- Microsoft 365 グループ
- Teams チャネル メッセージ
必要な保持ポリシーの最小数はいくつですか?
A. 1
B. 2
C. 3
D. 4
E. 5
Answer: B (メーッセージを残す**)**
保持ポリシーを作成する際にTeamsまたはYammerの場所を選択した場合、他の場所は自動的に除外されます。つまり、TeamsまたはYammerの場所を含める必要があるかどうかによって、手順が異なります。
https://learn.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide&tabs=teams-retention#create-and-configure-a-retention-policy

最新問題: **195**
Microsoft 365 E5 サブスクリプションをお持ちです。
個人情報 (PII) を含む会社のデータがサードパーティの生成 AI ツールと共有されるのを防ぐために、Microsoft Purview Data Security Posture Management for AI (OSPM for AI) を展開する予定です。
計画された展開の前提条件を完了する必要があります。
どの 2 つの Microsoft Purview ソリューションを使用する必要がありますか? それぞれの正解はソリューションの一部を示しています。
注意: 正しい選択ごとに 1 ポイントが加算されます。
A. データ損失防止
B. 情報障壁
C. インサイダーリスク管理
D. コミュニケーションコンプライアンス
E. 監査
Answer: A,D (メーッセージを残す**)**
[A] DLP は、データへのアクセス方法、共有方法、送信方法を監視および制御することで、財務記録、個人を特定できる情報 (PII)、健康データ、知的財産などの機密情報を保護するのに役立ちます。

組織は次のような機密情報を管理しています。
財務データ
独自のデータ
クレジットカード番号
健康記録
社会保障番号
こうした機密データを保護し、過剰な共有によるリスクを軽減するためには、ユーザーが機密データを不適切な相手に不適切に共有することを防ぐ手段が必要です。この対策は、データ損失防止（DLP）と呼ばれます。
[D] Microsoft Purview Communication Compliance は、組織が規制コンプライアンス（SEC や FINRA など）や、機密情報、嫌がらせや脅迫的な表現、成人向けコンテンツの共有といった業務行為違反を検出するためのツールを提供します。Communication Compliance は、プライバシーを最優先に設計されています。ユーザー名は既定で仮名化され、ロールベースのアクセス制御が組み込まれています。また、管理者が調査員の参加をオプトインし、ユーザーレベルのプライバシーを確保するための監査ログも用意されています。
参照：
https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp
https://learn.microsoft.com/en-us/purview/communication-compliance

最新問題: **196**
次の表に示すように、Microsoft Defender for Endpoint にオンボードされたデバイスを持つ Microsoft 365 E5 テナントがあります。

Name	Type
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	macOS

Microsoft 365 エンドポイント データ損失防止 (エンドポイント DLP) の使用を開始する予定です。
エンドポイント DLP をサポートするデバイスはどれですか?
A. デバイス1のみ
B. デバイス1とデバイス2のみ
C. デバイス1とデバイス4のみ
D. デバイス1、デバイス2、デバイス4のみ
E. デバイス1、デバイス2、デバイス3、デバイス4
Answer: D (メーッセージを残す**)**
https://learn.microsoft.com/es-es/purview/endpoint-dlp-getting-started
https://learn.microsoft.com/en-us/purview/device-onboarding-macos-overview#始める前に