Prüfungsnummer:MS-102-deutsch

Prüfungsname: Microsoft 365 Administrator

Version:demo

https://www.itpruefungsfragen.de/

Achtung: Aktuelle englische Version zu MS-102 bei uns ist gratis!!

1.Sie haben einen Microsoft 365 E5-Abonnement, das Microsoft Defender für Cloud Apps verwendet.

Sie müssen benachrichtigt werden, wenn ein einzelner Benutzer in einem Zeitraum von 60 Sekunden mehr als 50 Dateien herunterlädt.

Was sollten Sie konfigurieren?

A.Eine Dateirichtlinie
B.Eine Richtlinie zur Anomalieerkennung
C.Eine Sitzungsrichtlinie
D.Eine Aktivitätsrichtlinie

Korrekte Antwort: D

Erläuterungen:

Mit Aktivitätsrichtlinien können Sie eine Vielzahl von automatisierten Prozessen mithilfe der APIs des App-Anbieters erzwingen. Mit diesen Richtlinien können Sie bestimmte Aktivitäten überwachen, die von verschiedenen Benutzern durchgeführt werden, oder unerwartet hohe Raten eines bestimmten Aktivitätstyps verfolgen.

Wir sollten eine Aktivitätsrichtlinie erstellen und wie nachstehend gezeigt konfigurieren.

Aktivitätsrichtlinie erstellen

Richtlinienvorlage *

Keine Vorlage

Richtlinienname *

Richtlinie1

Schweregrad der Ric... * | Kategorie *

Bedrohungserkennung

Beschreibung

Filter für die Richtlinie erstellen

Aktion ausführen bei:

- Einzelne Aktivität
  Jede Aktivität, die den Filtern entspricht
- Wiederholte Aktivität:
  Wiederholte Aktivität eines einzelnen Benutzers

Mindestanzahl wiederholter Aktivitäten: 50

Im Zeitrahmen: 1 Minuten

- [ ] In einer einzelnen App
- [ ] Nur eindeutige Zieldateien oder -ordner pro Benutzer zählen

"Aktivitäten" entspricht allen folgenden Kriterien

Aktivitätstyp | ist gleich | Herunterladen

+ Filter hinzufügen

Warnungen

- [x] Warnung für jedes mit dem Schweregrad der Richtlinie übereinstimmende Ereignis erstellen

Als Standardeinstellungen speichern | Standardeinstellungen wiederherstellen

- [x] Warnung als E-Mail senden

admin1@contoso.com ×

Grenzwert für tägliche Warnungen pro Richtlinie: 5

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Aktivitätsrichtlinien

2.Sie haben ein Microsoft 365 E5-Abonnement und einen On-Premises Server mit dem Namen Server1, auf dem Windows Server ausgeführt wird.

Sie planen, Cloud Discovery in Microsoft Defender für Cloud Apps zu implementieren.

Sie müssen einen Protokollsammler auf Server1 bereitstellen.

Was sollten Sie zuerst auf Server1 installieren?

A.Den Azure Monitor-Agent
B.Docker
C.Den Azure Connected Machine-Agent
D.Einen Microsoft Defender for Identity-Sensor

Korrekte Antwort: B

Erläuterungen:

Mit Protokollsammlern können Sie den Protokollupload aus Ihrem Netzwerk komfortabel automatisieren. Der Protokollsammler wird in Ihrem Netzwerk ausgeführt und empfängt Protokolle über Syslog oder FTP. Jedes Protokoll wird automatisch verarbeitet, komprimiert und an das Portal übermittelt. FTP-Protokolle werden in Microsoft Defender for Cloud Apps hochgeladen, nachdem die Datei die FTP-Übertragung an den Protokollsammler abgeschlossen hat. Der Protokollsammler schreibt für Syslog die empfangenen Protokolle auf den Datenträger. Dann lädt der Collector die Datei in Defender für Cloud Apps hoch, wenn die Dateigröße größer als 40 KB ist.

Nachdem ein Protokoll in Defender für Cloud-Apps hochgeladen wurde, wird es in ein Sicherungsverzeichnis verschoben. Im Sicherungsverzeichnis werden die letzten 20 Protokolle gespeichert. Wenn neue Protokolle eintreffen, werden die älteren gelöscht. Immer wenn der Speicherplatz des Protokollsammlers voll ist, löscht der Protokollsammler neue Protokolle, bis er über mehr freien Speicherplatz verfügt (dies sollte nicht passieren, wenn die Voraussetzungen ordnungsgemäß erfüllt sind). Wenn dies passiert, erhalten Sie eine Warnung auf der Registerkarte Protokollsammler in den Einstellungen Protokolle automatisch hochladen.

Der Protokollsammler unterstützt den Containerbereitstellungsmodus. Es wird als Docker-Image unter Windows, Ubuntu lokal, Ubuntu in Azure, RHEL lokal oder CentOS ausgeführt.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Konfigurieren des automatischen Uploads von Protokollen für kontinuierliche Berichte

3.Sie haben ein Microsoft 365 E5-Abonnement, das die in der folgenden Tabelle aufgeführten Benutzer enthält:

Name	Microsoft 365-Rollengruppe
Admin1	Content Explorer List Viewer Content Explorer Content Viewer
Admin2	Sicherheitsadministrator Content Explorer List Viewer

Sie haben die in der folgenden Tabelle gelisteten Bezeichnungen in Microsoft 365 erstellt:

Name	Typ
Label1	Vertraulichkeit
Label2	Aufbewahrung

Dem Inhalt in Microsoft 365 sind die in der folgenden Tabelle gezeigten Bezeichnungen zugewiesen:

Name	Type	Bezeichnung
Datei1	Datei in SharePoint Online	Label1
Mail1	E-Mail-Nachricht in Exchange Online	Label2

Wählen Sie für jede der folgenden Aussagen "Ja", wenn die Aussage wahr ist. Andernfalls wählen Sie "Nein".

(Für jede korrekte Markierung erhalten Sie einen Punkt.)

Abbildung

Aussagen	Ja	Nein
Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen.	◯	◯
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen.	◯	◯
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist.	◯	◯

A.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Ja
B.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Nein
C.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Ja
D.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Ja
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Ja
E.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Ja
F.Admin1 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalt von Datei1 mithilfe des Inhalts-Explorers anzeigen: Nein
Admin2 kann den Inhalts-Explorer verwenden, um zu überprüfen, ob Label2 Mail1 zugewiesen ist: Nein

Korrekte Antwort: C

Erläuterungen:

Um Zugriff auf die Registerkarte „Inhalts-Explorer“ zu erhalten, muss einem Konto die Mitgliedschaft in einer dieser Rollen oder Rollengruppen zugewiesen werden.

Microsoft 365-Rollengruppen

Globaler Administrator
Compliance-Administrator
Sicherheitsadministrator
Compliancedatenadministrator
Die Mitgliedschaft in diesen Rollengruppen erlaubt Ihnen nicht, die Liste der Elemente im Inhalts-Explorer oder den Inhalt der Elemente im Inhalts-Explorer anzuzeigen.

Der Zugriff auf den Inhalts-Explorer ist hochgradig eingeschränkt, da Sie damit den Inhalt überprüfter Dateien lesen können.

Es gibt zwei Rollen, die Zugriff auf den Inhalts-Explorer gewähren, und diese werden über das Microsoft Purview-Complianceportal gewährt:

Content Explorer List viewer: Durch die Mitgliedschaft in dieser Rollengruppe können Sie jedes Element und dessen Speicherort in der Listenansicht anzeigen. Die Rolle data classification list viewer wurde dieser Rollengruppe bereits zugewiesen.

Content Explorer Content viewer: Durch die Mitgliedschaft in dieser Rollengruppe können Sie die Inhalte aller Elemente in der Liste anzeigen. Die Rolle data classification content viewer wurde dieser Rollengruppe bereits zugewiesen.

Das Konto, das Sie für den Zugriff auf den Inhalts-Explorer verwenden, muss einer oder beiden Rollengruppen angehören. Dies sind unabhängige Rollengruppen, die nicht kumulativ sind. Wenn Sie beispielsweise einem Konto die Möglichkeit geben möchten, nur die Elemente und deren Speicherorte anzuzeigen, erteilen Sie Inhalts-Explorer-Listenanzeige-Rechte. Wenn Sie möchten, dass dasselbe Konto auch in der Lage ist, die Inhalte der Elemente in der Liste anzuzeigen, erteilen Sie zusätzlich Inhalts-Explorer-Inhaltsanzeige-Rechte.

Sie können auch eine oder beide Rollen einer benutzerdefinierten Rollengruppe zuweisen, um den Zugriff auf den Inhalts-Explorer anzupassen.

Ein globaler Administrator kann die erforderliche Rollengruppenmitgliedschaften „Inhalts-Explorer-Listenanzeige“ und „Inhalts-Explorer-Inhaltsanzeige“ zuweisen.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Erste Schritte mit dem Inhalts-Explorer

4.Sie haben ein Microsoft 365 E5-Abonnement, das die Geräteverwaltung durch Microsoft Intune nutzt.

Sie kaufen fünf neue Android-Geräte und fünf neue macOS-Geräte.

Sie müssen die neuen Geräte in Microsoft Intune registrieren.

Womit sollten Sie die einzelnen Gerätetypen registrieren?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung

A.Android: Die Einstellungen-App
MacOS: Die Einstellungen-App
B.Android: Die Einstellungen-App
MacOS: Die Intune-Unternehmensportal-App
C.Android: Einen Browser und den URL https://compliance.microsoft.com
MacOS: Die Intune-Unternehmensportal-App
D.Android: Die Intune-Unternehmensportal-App
MacOS: Die Intune-Unternehmensportal-App
E.Android: Einen Browser und den URL https://manage.microsoft.com
MacOS: Einen Browser und den URL https://manage.microsoft.com
F.Android: Einen Browser und den URL https://manage.microsoft.com
MacOS: Einen Browser und den URL https://compliance.microsoft.com

Korrekte Antwort: D

Erläuterungen:

Mit der Geräteregistrierung können Sie von Ihrem mobilen Gerät aus auf die internen Ressourcen Ihrer Geschäfts- oder Bildungseinrichtung (z. B. Apps, WLAN und E-Mail) zugreifen. Bei einer Geräteregistrierung geschieht Folgendes:

Ihr Gerät wird bei Microsoft Intune, einem Anbieter für die Verwaltung mobiler Geräte, und bei Ihrer Organisation registriert. Durch diesen Schritt wird sichergestellt, dass Sie befugt sind, auf E-Mails, Apps und das WLAN Ihrer Organisation zuzugreifen.
Die Geräteverwaltungsrichtlinien Ihrer Organisation werden auf Ihr Gerät angewendet. Richtlinien können Anforderungen für Geräteschlüssel und Verschlüsselung umfassen. Der Zweck dieser Anforderungen ist, Ihr Gerät und die Daten Ihrer Organisation vor nicht autorisiertem Zugriff zu schützen.
Sie können die Unternehmensportal-App verwenden, um Geräte zu registrieren, auf denen Folgendes ausgeführt wird:

Windows 10/11
Windows 10 Mobile
Windows 8.1
Android OS
iOS
macOS
ie Unternehmensportal-App ist für Windows 10/11-, iOS-, macOS- und Android-Geräte verfügbar. Sie ist nahtlos in die Plattform Ihres Geräts integriert. Die Websiteversion ist über jedes Gerät zugänglich und stellt Ihnen unabhängig vom Gerät dieselbe universelle Benutzeroberfläche zu Verfügung.

Um auf die Unternehmensportal-Website zuzugreifen, öffnen Sie auf einem beliebigen Gerät den URL https://portal.manage.microsoft.com/ (es muss kein registriertes Gerät sein) und melden Sie sich mit Ihrem Geschäfts- oder Schulkonto an.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Was ist die Geräteregistrierung?

5.Sie haben ein Microsoft 365 E5-Abonnement, das die in der folgenden Tabelle aufgeführten Geräte enthält:

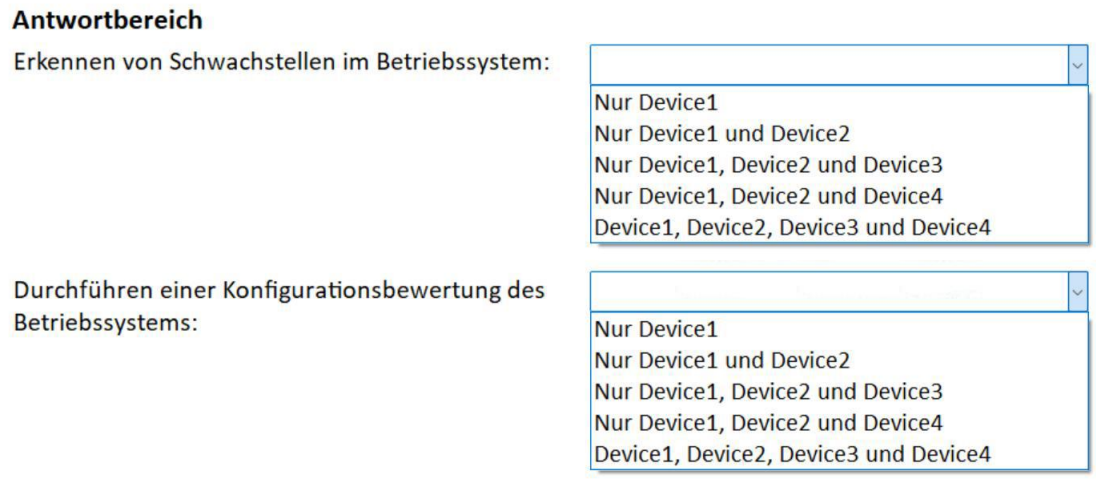
Name	Plattform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

Alle Geräte sind in Microsoft Defender for Endpoint integriert.

Sie planen, Microsoft Defender Vulnerability Management zu verwenden, um die folgenden Anforderungen zu erfüllen:
Erkennen von Schwachstellen im Betriebssystem.
Durchführen einer Konfigurationsbewertung des Betriebssystems.
Welche Geräte unterstützen die jeweilige Anforderung?

(Wählen Sie zum Beantworten der Frage die entsprechenden Optionen im Antwortbereich aus. Für jede richtige Auswahl erhalten Sie einen Punkt.)

Abbildung



A.Erkennen von Schwachstellen im Betriebssystem: Nur Device1
Durchführen einer Konfigurationsbewertung des Betriebssystems: Nur Device1
B.Erkennen von Schwachstellen im Betriebssystem: Nur Device1
Durchführen einer Konfigurationsbewertung des Betriebssystems: Nur Device1 und Device2
C.Erkennen von Schwachstellen im Betriebssystem: Nur Device1, Device2 und Device3
Durchführen einer Konfigurationsbewertung des Betriebssystems: Device1, Device2, Device3 und Device4
D.Erkennen von Schwachstellen im Betriebssystem: Nur Device1, Device2 und Device4
Durchführen einer Konfigurationsbewertung des Betriebssystems: Nur Device1, Device2 und Device4
E.Erkennen von Schwachstellen im Betriebssystem: Device1, Device2, Device3 und Device4
Durchführen einer Konfigurationsbewertung des Betriebssystems: Nur Device1 und Device2
F.Erkennen von Schwachstellen im Betriebssystem: Device1, Device2, Device3 und Device4
Durchführen einer Konfigurationsbewertung des Betriebssystems: Device1, Device2, Device3 und Device4

Korrekte Antwort: E

Erläuterungen:

In der folgenden Tabelle sind die unterstützten Betriebssysteme für die Schwachstellenerkennung und die Konfigurationsbewertung durch Microsoft Defender aufgeführt.

Unterstütztes Betriebssystem oder unterstützte Plattform	Sicherheitsrisiken des Betriebssystems	Sicherheitsrisiken für Softwareprodukte	Bewertung der Betriebssystemkonfiguration	Bewertung der Konfiguration von Sicherheitskontrollen	Bewertung der Softwareproduktkonfiguration
Windows 7	Ja	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 8.1	Ja	Ja	Ja	Ja	Ja
Windows 10, Versionen 1607-1703	Ja	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Windows 10, Version 1709 oder höher	Ja	Ja	Ja	Ja	Ja
Windows 11	Ja	Ja	Ja	Ja	Ja
Windows Server 2008 R2	Ja	Ja	Ja	Ja	Ja
Windows Server 2012 R2	Ja	Ja	Ja	Ja	Ja
Windows Server 2016	Ja	Ja	Ja	Ja	Ja
Windows Server 2019	Ja	Ja	Ja	Ja	Ja
Windows Server 2022	Ja	Ja	Ja	Ja	Ja
Android 6.0 oder höher	Ja	Ja	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
iOS 12.0 oder höher	Ja	Ja	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Unterstützte Betriebssysteme, Plattformen und Funktionen

6.Sie haben ein Microsoft 365 E5-Abonnement, das die in der folgenden Tabelle aufgeführten Geräte enthält:

Name	Gruppe
Device1	GeräteGruppe1
Device2	GeräteGruppe2

Um 08:00 Uhr erstellen Sie eine Vorfallsbenachrichtigungsregel mit der folgenden Konfiguration:
Name: Benachrichtigung1
Benachrichtigungseinstellungen
Bei Warnungsschweregrad benachrichtigen: Niedrig
Umfang der Gerätegruppe: Alle (3)
Details: Erste Benachrichtigung pro Vorfall
Empfänger: Benutzer1@contoso.com, Benutzer2@contoso.com
Um 08:02 Uhr erstellen Sie eine Vorfallsbenachrichtigungsregel mit der folgenden Konfiguration:
Name: Benachrichtigung2
Benachrichtigungseinstellungen
Bei Warnungsschweregrad benachrichtigen: Niedrig, Mittel
Umfang der Gerätegruppe: DeviceGroup1, DeviceGroup2
Empfänger: Benutzer1@contoso.com
In Microsoft 365 Defender werden die folgenden Warnungen protokolliert:

Zeit	Warnungsname	Schweregrad	Betroffene Ressourcen
08:05	Aktivität1	Niedrig	Device1
08:07	Aktivität1	Niedrig	Device1
08:08	Aktivität1	Mittel	Device1
08:15	Aktivität2	Mittel	Device2
08:16	Aktivität2	Mittel	Device2
08:20	Aktivität1	Hoch	Device1
08:30	Aktivität3	Mittel	Device2
08:35	Aktivität1	Hoch	Device2

Wählen Sie für jede der folgenden Aussagen "Ja", wenn die Aussage wahr ist. Andernfalls wählen Sie "Nein".

(Für jede korrekte Markierung erhalten Sie einen Punkt.)

Abbildung

Aussagen	Ja	Nein
Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr.	○	○
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr.	○	○
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr.	○	○

A.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Ja
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Ja
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Ja
B.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Ja
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Ja
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Nein
C.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Ja
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Nein
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Ja
D.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Nein
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Ja
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Nein
E.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Nein
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Ja
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Ja
F.Benutzer1@contoso.com erhält zwei Benachrichtigungs-E-Mails für den Vorfall um 08:05 Uhr: Nein
Benutzer2@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:07 Uhr: Nein
Benutzer1@contoso.com erhält eine Benachrichtigungs-E-Mail für den Vorfall um 08:20 Uhr: Nein

Korrekte Antwort: B

Erläuterungen:

Benutzer1 erhält für den Vorfall um 08:05 Uhr eine E-Mail-Benachrichtigung durch Benachrichtigung1 und eine zweite E-Mail-Benachrichtigung durch Benachrichtigung2.

Sowohl Benachrichtigung1 als auch Benachrichtigung2 schließen den Schweregrad Niedrig und Device1 ein und senden Benachrichtigungen an Benutzer1.

Benutzer2 erhält für den Vorfall um 08:07 Uhr eine einzelne E-Mail-Benachrichtigung durch Benachrichtigung1. Sowohl Benachrichtigung1 als auch Benachrichtigung2 schließen den Schweregrad Niedrig und Device1 ein. Benachrichtigung2 sendet jedoch keine E-Mail-Benachrichtigungen an Benutzer2.

Für den Vorfall um 08:20 Uhr erhält keiner der beiden Benutzer eine E-Mail-Benachrichtigung, da keine der beiden E-Mail-Benachrichtigungen den Schweregrad "Hoch" einschließt.

7.Sie haben ein Microsoft 365-Abonnement, das Microsoft Defender for Cloud Apps verwendet.

Sie konfigurieren eine Sitzungssteuerungsrichtlinie, um Downloads von SharePoint Online-Sites zu blockieren.

Benutzer berichten, dass sie weiterhin Dateien von SharePoint Online-Sites herunterladen können.

Sie müssen sicherstellen, dass das Herunterladen von Dateien blockiert wird, Benutzern jedoch weiterhin das Durchsuchen von SharePoint Online-Websites ermöglicht wird.

Was sollten Sie konfigurieren?

A.Eine Zugriffsrichtlinie
B.Eine Richtlinie zur Verhinderung von Datenverlust (DLP)
C.Eine Aktivitätsrichtlinie
D.Eine Richtlinie für bedingten Zugriff

Korrekte Antwort: D

Erläuterungen:

Wir müssen eine Richtlinie für bedingten ZUgriff erstellen, die die App-Steuerung durch Microsoft Defender for Cloud Apps für Sitzungen mit SharePoint Online ermöglicht.

Die App-Steuerung für bedingten Zugriff verwendet eine Reverseproxyarchitektur und ist in Ihren IdP integriert. Bei der Integration mit bedingtem Azure AD-Zugriff können Sie Apps mit nur wenigen Klicks so konfigurieren, dass sie mit der App-Steuerung für

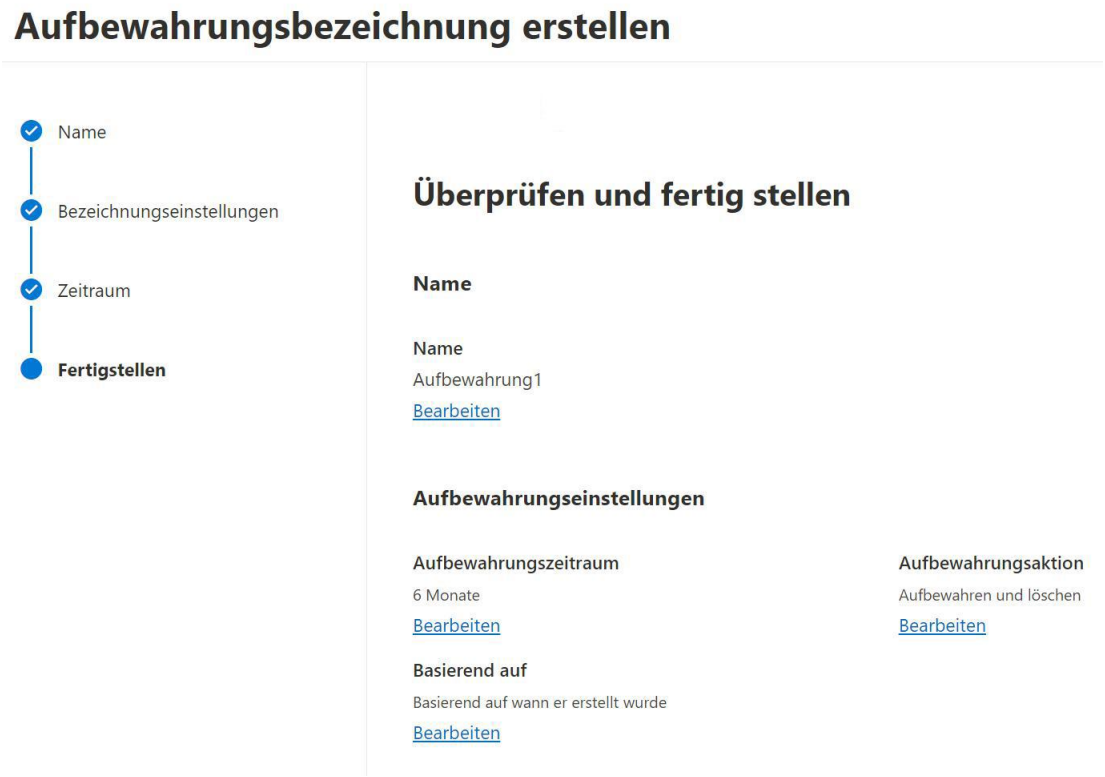
bedingten Zugriff funktionieren, sodass Sie den Zugriff und die Sitzungssteuerung für die Apps Ihrer organization einfach und selektiv erzwingen können, basierend auf jeder Bedingung in bedingtem Zugriff. Die Bedingungen definieren , wer (Benutzer oder Benutzergruppe) und was (welche Cloud-Apps) und wo (welche Standorte und Netzwerke) eine Richtlinie für bedingten Zugriff angewendet wird. Nachdem Sie die Bedingungen festgelegt haben, können Sie Benutzer an Defender für Cloud-Apps weiterleiten, wo Sie Daten mit der App-Steuerung für bedingten Zugriff schützen können, indem Sie Zugriffs- und Sitzungssteuerungen anwenden.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Schützen von Apps mit der App-Steuerung für bedingten Zugriff von Microsoft Defender for Cloud Apps

8.Sie haben ein Microsoft 365-Abonnement.

Sie erstellen eine Aufbewahrungsbezeichnung mit dem Namen Aufbewahrung1. Ihre Konfiguration wird in der folgenden Abbildung gezeigt:



Sie wenden Aufbewahrung1 auf alle Microsoft OneDrive-Inhalte an.

Am 1. Januar 2023 speichert ein Benutzer eine Datei mit dem Namen Datei1 in OneDrive. Am 10. Januar 2023 ändert der Benutzer Datei1. Am 1. Februar 2023 löscht der Benutzer Datei1.

Wann wird Datei1 dauerhaft und unwiederbringlich von OneDrive entfernt?

A.1. Februar 2023
B.1. Juli 2023
C.10. Juli 2023
D.1. August 2023

Korrekte Antwort: B

Erläuterungen:

Die Aufbewahrungsbezeichnung stellt die Aufbewahrung von Dateien für einen Zeitraum von 6 Monaten, beginnend mit dem Datum, an dem die Datei erstellt wurde, sicher. Nach Ablauf der 6 Monate, wird die Datei gelöscht. Datei1 wurde am 1. Januar 2023 erstellt und wird 6 Monate später, am 1. Juli 2023, gelöscht.

Der folgende Microsoft Learn-Artikel enthält weitere Informationen zum Thema:

Informationen zu Aufbewahrungsrichtlinien und Aufbewahrungsbezeichnungen