Prüfungsnummer:MS-101

Prüfungsname: Microsoft 365 Mobility and Security

Version:demo

Case Study: 1
A Datum
Case Study Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
A Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A Datum uses and processes Personally Identifiable Information (PII).
Problem Statements
Requirements
A Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A Datum warns to be fully compliant with all the relevant data privacy laws in the regions where

it operates.
A Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A Datum identifies the following technical requirements:
-Centrally perform log analysis for all offices.
-Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
-Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
-Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
-Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
-If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account. -A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
-Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Q1
You need to meet the technical requirement for the EU PII data.

What should you create?

A. a retention policy from the Security & Compliance admin center.
B. a retention policy from the Exchange admin center
C. a data loss prevention (DLP) policy from the Exchange admin center
D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

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

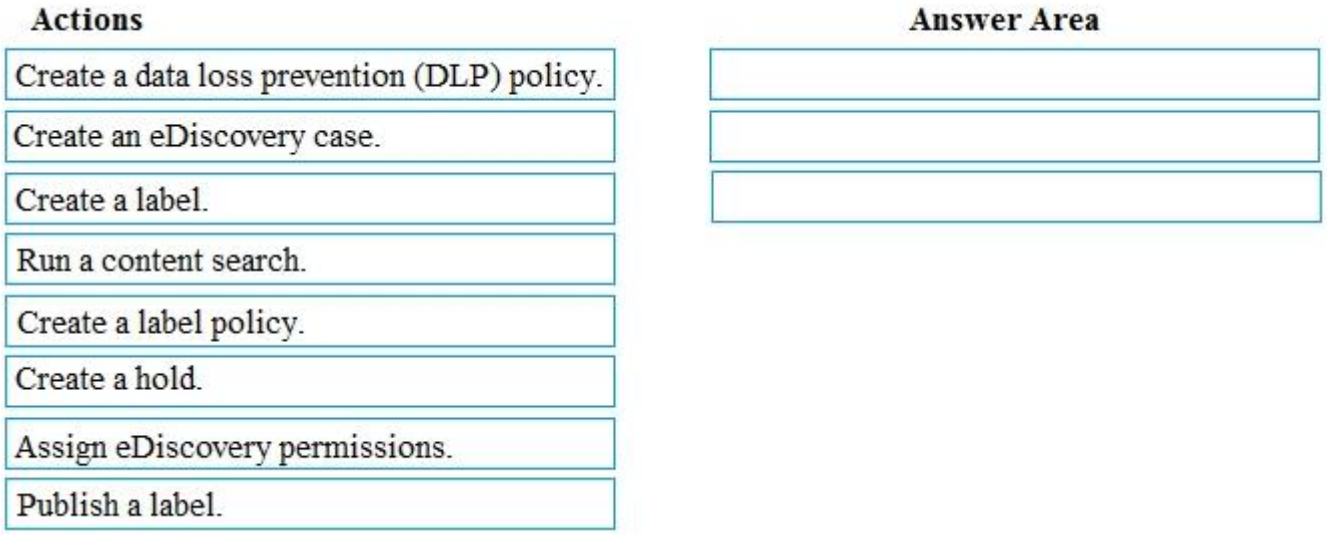
Q2
You need to meet the technical requirement for large-volume document retrieval. What should you create?

A. a data loss prevention (DLP) policy from the Security & Compliance admin center
B. an alert policy from the Security & Compliance admin center
C. a file policy from Microsoft Cloud App Security
D. an activity policy from Microsoft Cloud App Security

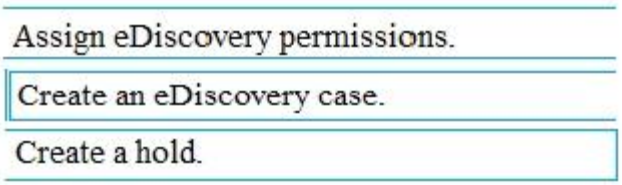
Answer: D

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts

Q3
DRAG DROP
You need to meet the requirement for the legal department Which three actions should you perform in sequence from the Security & Compliance admin center? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



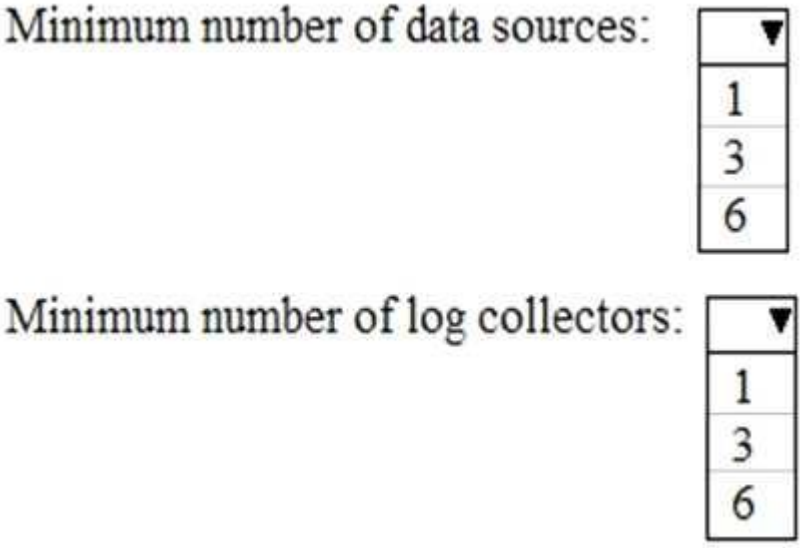
Answer:



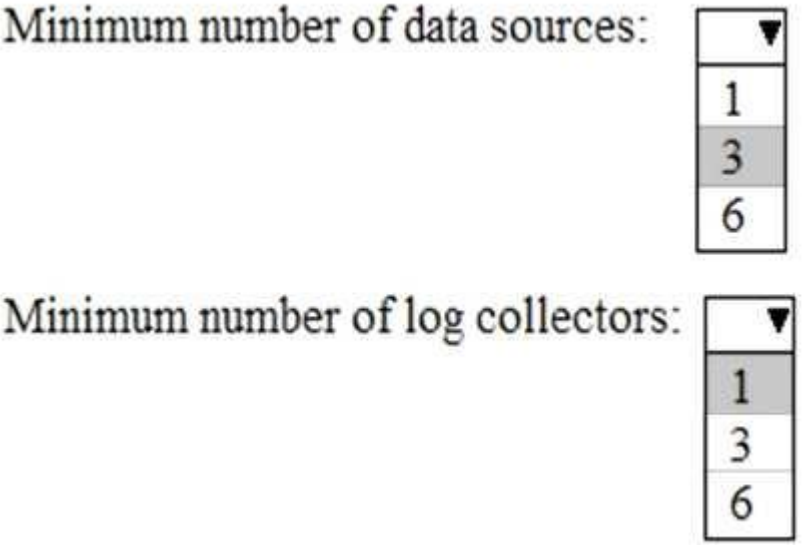
Explanation:

References:
https://www.sherweb.com/blog/edisHYPERLINK "https://www.sherweb.com/blog/ediscovery-office-365/"covery-office-365/

Q4
HOTSPOT
You need to meet the technical requirement for log analysis. What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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

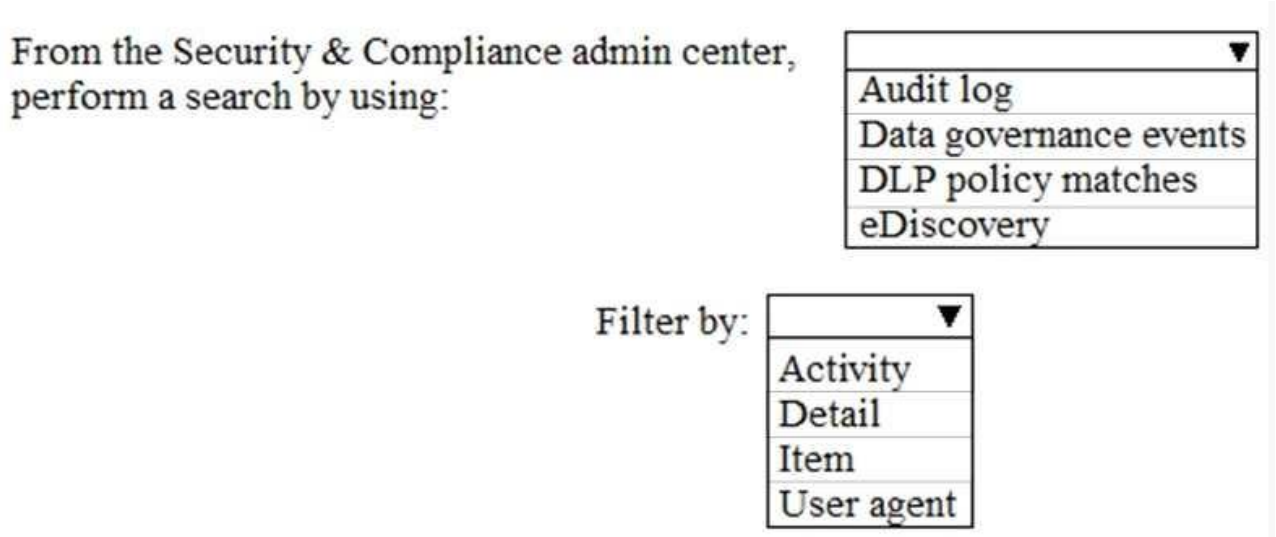
Q5
Which report should the New York office auditors view?

A. DLP policy matches
B. DLP false positives and overrides
C. DLP incidents
D. Top Senders and Recipients

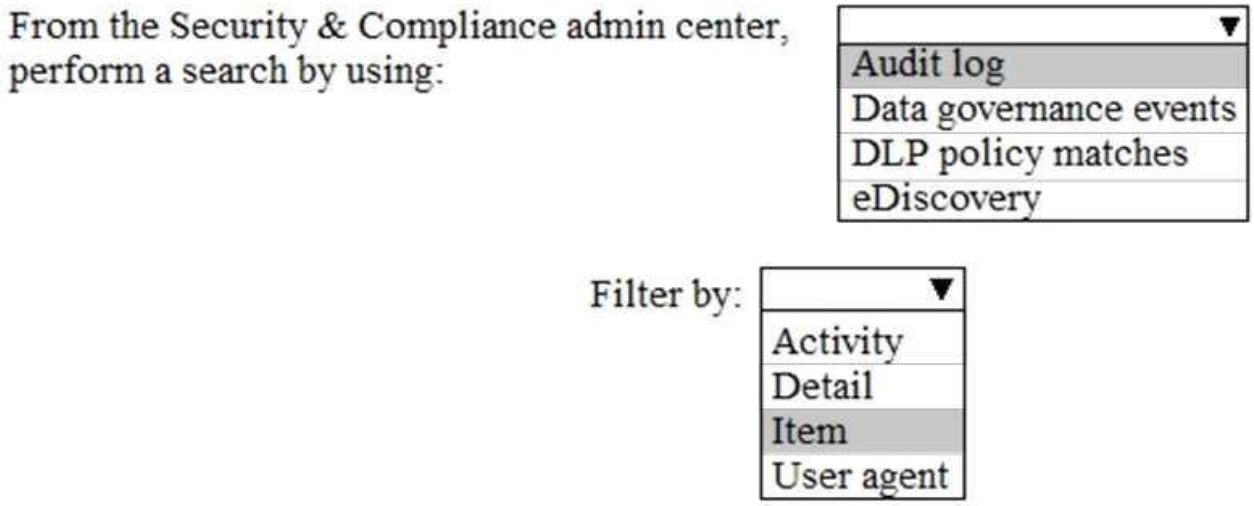
Answer: C

Explanation:
References:
https://docs.microsoft.comHYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies"/en-us/office365/sHYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies"ecuritycompliance/data-loss-prevention-policies

Q6
HOTSPOT
You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.



Answer:



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

Q7
You need to recommend a solution for the security administrator. The solution must meet the technical requirements.
What should you include in the recommendation?

A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
B. Microsoft Azure Active Directory (Azure AD) Identity Protection
C. Microsoft Azure Active Directory (Azure AD) conditional access policies
D. Microsoft Azure Active Directory (Azure AD) authentication methods

Answer: C

Explanation:
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks

Q8
You need to protect the U.S. PII data to meet the technical requirements.
What should you create?

A. a data loss prevention (DLP) policy that contains a domain exception
B. a Security & Compliance retention policy that detects content containing sensitive data
C. a Security & Compliance alert policy that contains an activity
D. a data loss prevention (DLP) policy that contains a user override

Answer: C

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

Case Study: 3
Mix Questions

Q9
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune. When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intuen.
Solution: You configure the Mobility (MDM and MAM) settings.
Does this meet the goal?

A. Yes
B. No

Answer: B

Q10
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune. When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intuen.
Solution: You create an Apple Configurator enrollment profile.
Does this meet the goal?

A. Yes
B. No

Answer: A

Q11
You are deploying Microsoft Intune.
You successfully enroll Windows 10 devices in Intune. When you try to enroll an iOS device in

Intune, you get an error. You need to ensure that you can enroll the iOS device in Intuen.
Solution: You configure the Apple MDM Push certificate.
Does this meet the goal?

A. Yes
B. No

Answer: B

Q12
You have a Microsoft 365 subscription.
You discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security & Compliance admin center, you create a threat management policy.
Does this meet the goal?

A. Yes
B. No

Answer: A