Microsoft

MS-101

Microsoft 365 Mobility and Security

http://killexams.com/pass4sure/exam-detail/MS-101
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York. The company has the employees and devices shown in the following table.

<table>
<thead>
<tr>
<th>Location</th>
<th>Employees</th>
<th>Laptops</th>
<th>Desktops</th>
<th>Mobile devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Montreal</td>
<td>2,500</td>
<td>2,800</td>
<td>300</td>
<td>3,100</td>
</tr>
<tr>
<td>Seattle</td>
<td>1,000</td>
<td>1,100</td>
<td>200</td>
<td>1,500</td>
</tr>
<tr>
<td>New York</td>
<td>300</td>
<td>320</td>
<td>30</td>
<td>400</td>
</tr>
</tbody>
</table>

Contoso recently purchased a Microsoft 365 E5 subscription.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server1</td>
<td>Domain controller</td>
</tr>
<tr>
<td>Server2</td>
<td>Member server</td>
</tr>
<tr>
<td>Server3</td>
<td>Network Policy Server (NPS) server</td>
</tr>
<tr>
<td>Server4</td>
<td>Remote access server</td>
</tr>
<tr>
<td>Server5</td>
<td>Microsoft Azure AD Connect server</td>
</tr>
</tbody>
</table>

All servers run Windows Server 2016. All desktops and laptops run Windows 10 Enterprise and are joined to the domain. The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS. The domain is synced to Azure Active Directory (Azure AD) and includes the users shown in the following table.
The domain also includes a group named Group1.

Requirements -

Planned Changes -
Contoso plans to implement the following changes:
Implement Microsoft 365.
Manage devices by using Endpoint Manager.
Implement Azure Advanced Threat Protection (ATP).
Update computers in Seattle and Montreal with the fall Semi-Annual Channel feature update.
Update computers in the New York office with the spring Semi-Annual Channel feature update.

Technical Requirements -
Contoso identifies the following technical requirements:
When a Windows 10 device is joined to Azure AD, the device must enroll to Endpoint Manager automatically.
Dedicated support technicians must enroll all the Montreal office mobile devices in Endpoint Manager.
Each dedicated support technician must be assigned only a single Device Enrollment Manager (DEM) account.
User1 must be able to enroll all the New York office mobile devices in Endpoint Manager.
Azure ATP sensors must be installed and must NOT use port mirroring.
Whenever possible, the principle of least privilege must be used.
A Microsoft Store for Business must be created.

Compliance Requirements -
Contoso identifies the following compliance requirements:
Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Endpoint Manager and configured in accordance with the corporate policy.
Configure Windows Information Protection (WIP) for the Windows 10 devices. Question You need to meet the compliance requirements for the Windows 10 devices.
What should you create from the Endpoint Management admin center?

- A. a device compliance policy
- B. a device configuration profile
- C. an app protection policy
- D. an app configuration policy

Answer: C
Reference:

Question: 1 Section 10

Introductory Info Case Study -

Overview -
ADatum Corporation is an international financial services company that has 5,000 employees.
ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.
All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -
ADatum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.

<table>
<thead>
<tr>
<th>Name</th>
<th>Azure AD role</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td>None</td>
</tr>
<tr>
<td>User2</td>
<td>Application administrator</td>
</tr>
<tr>
<td>User3</td>
<td>Cloud application administrator</td>
</tr>
<tr>
<td>User4</td>
<td>Global administrator</td>
</tr>
<tr>
<td>User5</td>
<td>Intune administrator</td>
</tr>
</tbody>
</table>

The domain also includes a group named Group1.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com. Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors. A Datum uses and processes Personally Identifiable Information (PII).

Problem Statements -
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.

Requirements -

Business Goals -
A Datum wants 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 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data. Question Which report should the New York office auditors view?
  - A. DLP incidents
  - B. Top Senders and Recipients
  - C. DLP false positives and overrides
  - D. DLP policy matches

Answer: A

References:

Question: 2 Section 10

Introductory Info Case Study -

Overview -
A Datum Corporation is an international financial services company that has 5,000 employees.
A Datum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.
All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -
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.adatum.com.
Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.
A Datum uses and processes Personally Identifiable Information (PII).

Problem Statements -
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.

Requirements -

Business Goals -
ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.
ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -
ADatum 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 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data. Question You need to meet the technical requirement for the EU PII data.

What should you create?

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

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

Question: 3 Section 10

Introductory Info Case Study -

Overview -
ADatum Corporation is an international financial services company that has 5,000 employees.
ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.
All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -
ADatum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.
Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.
ADatum uses and processes Personally Identifiable Information (PII).

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

Requirements -

Business Goals -
ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.
ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -
ADatum 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 users user account. A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk. Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data. Question 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

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

Question: 4 Section 10

Introductory Info Case Study -

Overview -
ADatum Corporation is an international financial services company that has 5,000 employees. ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy. All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -
ADatum recently purchased a Microsoft 365 subscription. All user files are migrated to Microsoft 365. All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com. Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors. ADatum uses and processes Personally Identifiable Information (PII).

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

Requirements -

Business Goals -
ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where is operates. ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -
ADatum identifies the following technical requirements:
- 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 users user account.
- A security administrator requires a report that shown which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office uses. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

Question 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.
Introductory Info Case Study -

Overview -
ADatum Corporation is an international financial services company that has 5,000 employees.
ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy. All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

Existing Environment -

Current Infrastructure -
ADatum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com. Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.
ADatum uses and processes Personally Identifiable Information (PII).

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

Requirements -
ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.
ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -
ADatum 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 users' user account.
A security administrator requires a report that shows which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data. Question 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:
References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker
ADatum Corporation is an international financial services company that has 5,000 employees.
ADatum has six offices: a main office in New York and five branch offices in Germany, the United Kingdom, France, Spain, and Italy.
All the offices are connected to each other by using a WAN link. Each office connects directly to the Internet.

ADatum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2@uk.adatum.com.
Each office has a security information and event management (SIEM) appliance. The appliance comes from three different vendors.
ADatum uses and processes Personally Identifiable Information (PII).

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

Business Goals -
ADatum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.
ADatum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements -
ADatum 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 users user account.
A security administrator requires a report that shows which Microsoft 365 users signed in. Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign-in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive U.S. PII data to other New York office users. Email messages must be monitored to ensure compliance.
Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data. Question 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 area.

NOTE: Each correct selection is worth one point.

Hot Area:
From the Security & Compliance admin center, perform a search by using:

<table>
<thead>
<tr>
<th>Filter by:</th>
<th>Audit log</th>
<th>Data governance events</th>
<th>DLP policy matches</th>
<th>eDiscovery</th>
</tr>
</thead>
</table>

Answer:

References:
For More exams visit https://killexams.com/vendors-exam-list

Kill your exam at First Attempt....Guaranteed!