KillTest

質量更高　服務更好



練習題

https://www.killtest.net

一年免費更新服務

Exam : **SC-100**

Title : Microsoft Cybersecurity Architect

Version : DEMO

1.Your company has a Microsoft 365 ES subscription.
The Chief Compliance Officer plans to enhance privacy management in the working environment.
You need to recommend a solution to enhance the privacy management.
The solution must meet the following requirements:
⇨ Identify unused personal data and empower users to make smart data handling decisions.
⇨ Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
⇨ Provide users with recommendations to mitigate privacy risks.
What should you include in the recommendation?
A. communication compliance in insider risk management
B. Microsoft Viva Insights
C. Privacy Risk Management in Microsoft Priva
D. Advanced eDiscovery
Answer: C

2.You have an Azure subscription that has Microsoft Defender for Cloud enabled.
Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.
You need to recommend a solution to evaluate and remediate the alerts by using workflow automation.
The solution must minimize development effort.
What should you include in the recommendation?
A. Azure Monitor webhooks
B. Azure Event Hubs
C. Azure Functions apps
D. Azure Logics Apps
Answer: D

3.Your company is moving a big data solution to Azure.
The company plans to use the following storage workloads:
⇨ Azure Storage blob containers
⇨ Azure Data Lake Storage Gen2
Azure Storage file shares
⇨ Azure Disk Storage
Which two storage workloads support authentication by using Azure Active Directory (Azure AD)? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. Azure Storage file shares
B. Azure Disk Storage
C. Azure Storage blob containers
D. Azure Data Lake Storage Gen2
Answer: CD

4.HOTSPOT
Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII).
The company plans to use Microsoft Information Protection for the PII data store in Azure.
You need to recommend a solution to discover PII data at risk in the Azure resources.
What should you include in the recommendation? To answer, select the appropriate options in the

answer area. NOTE: Each correct selection is worth one point.

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- Azure Purview
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

Answer:

Answer Area

To connect the Azure data sources to Microsoft Information Protection:

- **Azure Purview**
- Endpoint data loss prevention
- Microsoft Defender for Cloud Apps
- Microsoft Information Protection

To triage security alerts related to resources that contain PII data:

- Azure Monitor
- Endpoint data loss prevention
- **Microsoft Defender for Cloud**
- Microsoft Defender for Cloud Apps

Explanation:

Box 1: Azure Purview

Microsoft Purview is a unified data governance service that helps you manage and govern your on-premises, multi-cloud, and software-as-a-service (SaaS) data.

Microsoft Purview allows you to:
Create a holistic, up-to-date map of your data landscape with automated data discovery, sensitive data classification, and end-to-end data lineage.
Enable data curators to manage and secure your data estate.
Empower data consumers to find valuable, trustworthy data.
Box 2: Microsoft Defender for Cloud
Microsoft Purview provides rich insights into the sensitivity of your data. This makes it valuable to security teams using Microsoft Defender for Cloud to manage the organization's security posture and protect against threats to their workloads. Data resources remain a popular target for malicious actors, making it crucial for security teams to identify, prioritize, and secure sensitive data resources across their cloud environments. The integration with Microsoft Purview expands visibility into the data layer, enabling security teams to prioritize resources that contain sensitive data.
References:
https://docs.microsoft.com/en-us/azure/purview/overview
https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

5.You have a Microsoft 365 E5 subscription and an Azure subscription.
You are designing a Microsoft deployment.
You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events.
What should you recommend using in Microsoft Sentinel?
A. notebooks
B. playbooks
C. workbooks
D. threat intelligence
Answer: C