SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 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:

1.

Identify unused personal data and empower users to make smart data handling decisions.

2.

Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.

3.

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

Correct Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal

guides and can help you:

Detect overexposed personal data so that users can secure it.

Spot and limit transfers of personal data across departments or regional borders.

Help users identify and reduce the amount of unused personal data that you store.

Incorrect:

Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the

day for uninterrupted, individual work.

Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export

content that\\'s responsive to your organization\\'s internal and external investigations.

Reference: https://docs.microsoft.com/en-us/privacy/priva/risk-management

QUESTION 2

You are designing an auditing solution for Azure landing zones that will contain the following components:

1.

SQL audit logs for Azure SQL databases

2.

Windows Security logs from Azure virtual machines

3.

Azure App Service audit logs from App Service web apps

You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:

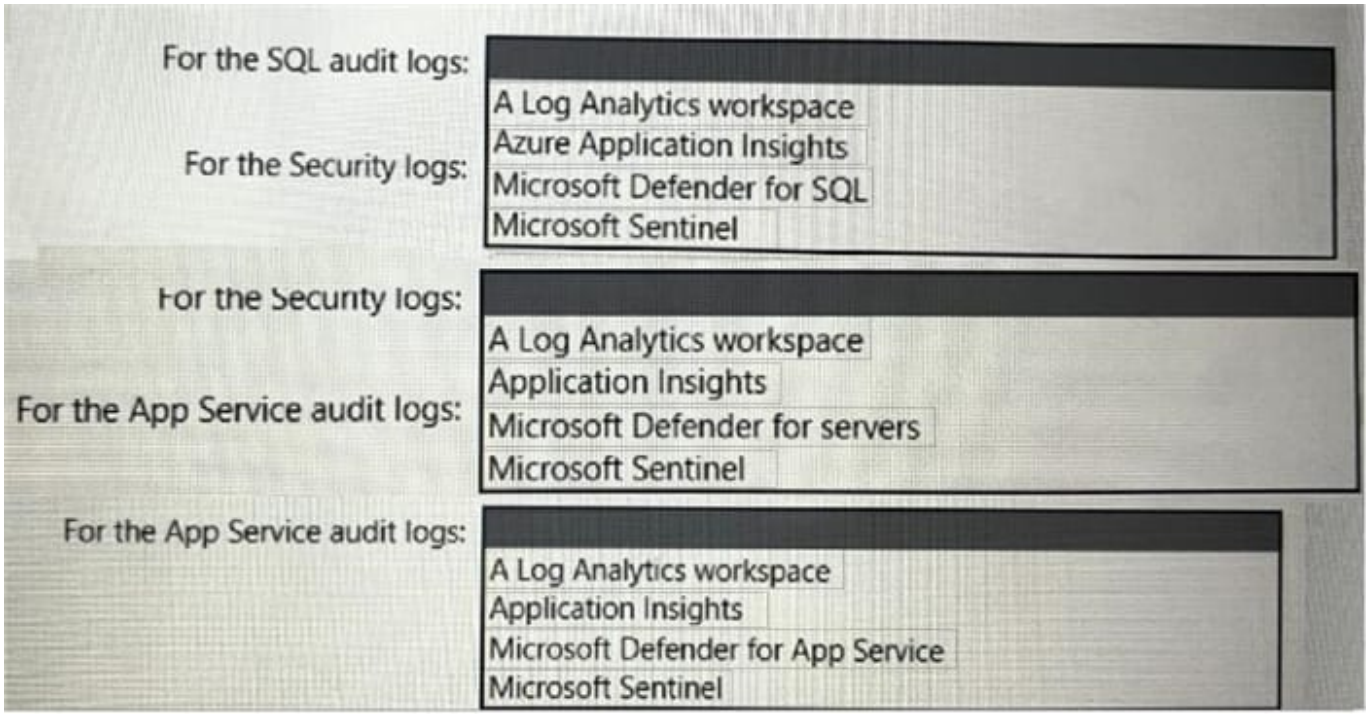
Log all privileged access.

Retain logs for at least 365 days.

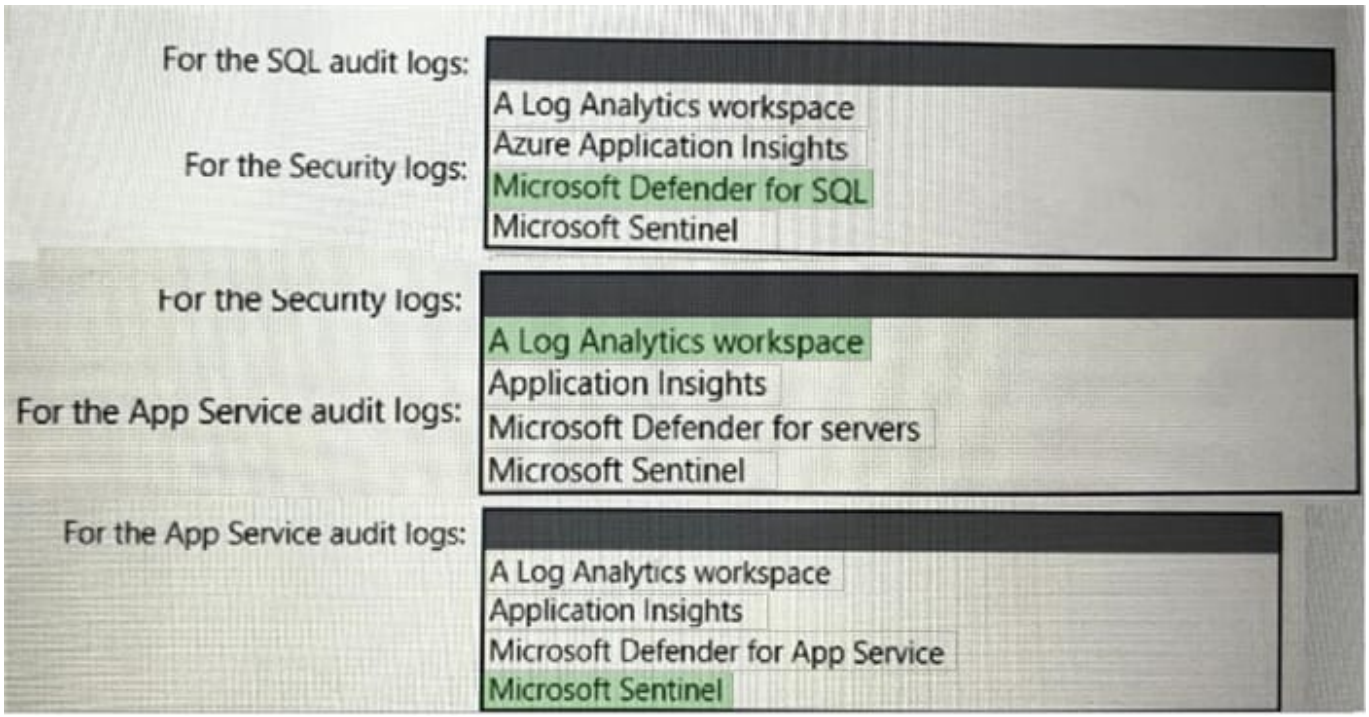
Minimize costs.

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.

Hot Area:



Correct Answer:



QUESTION 3

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions that allow traffic from the Front Door service tags.

Does this meet the goal?

A. Yes

B. No

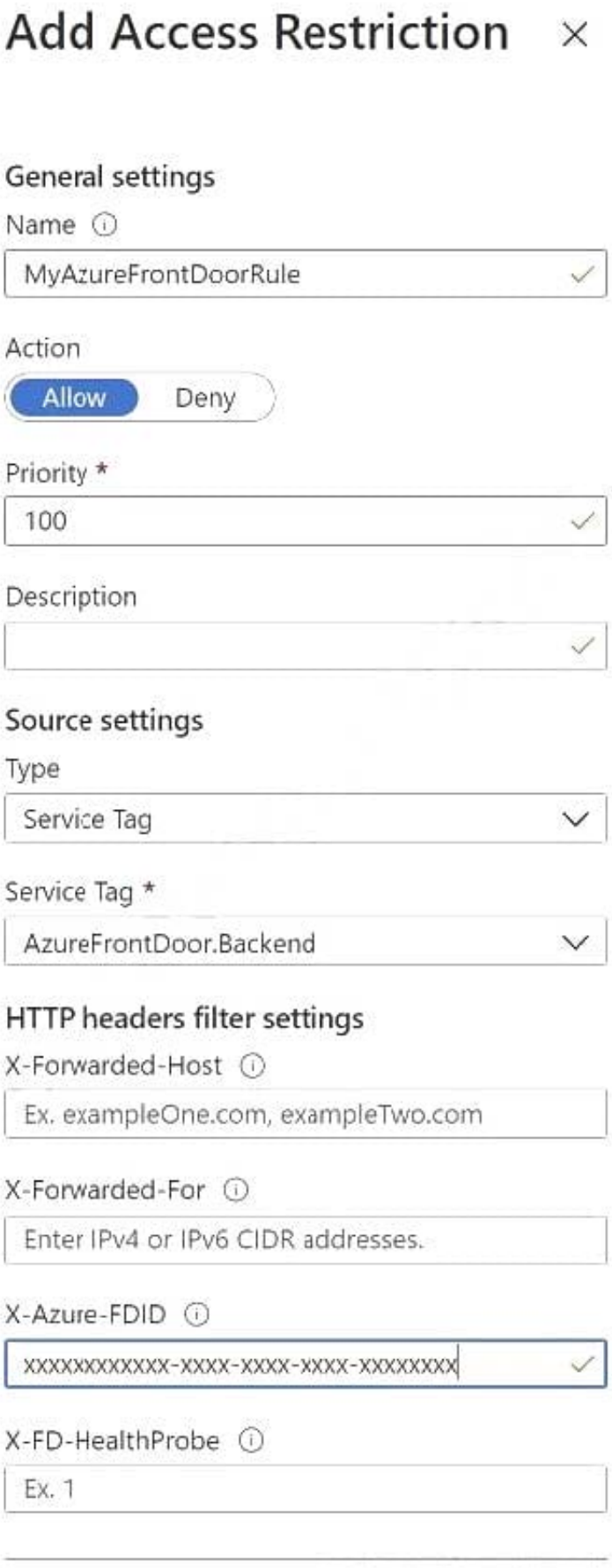
Correct Answer: B

Correct Solution: You recommend access restrictions based on HTTP headers that have the Front Door ID.

Restrict access to a specific Azure Front Door instance.

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front

Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.


Add Access Restriction
General settings
Name
MyAzureFrontDoorRule
Action
Allow
Deny
Priority *
100
Description
Source settings
Type
Service Tag
Service Tag *
AzureFrontDoor.Backend
HTTP headers filter settings
X-Forwarded-Host
Ex. exampleOne.com, exampleTwo.com
X-Forwarded-For
Enter IPv4 or IPv6 CIDR addresses.
X-Azure-FDID
xxxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx
X-FD-HealthProbe
Ex. 1

Reference: https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules

QUESTION 4

Your company is moving all on-premises workloads to Azure and Microsoft 365.

You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

1.

Minimizes manual intervention by security operation analysts

2.

Supports triaging alerts within Microsoft Teams channels What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. KQLworkbooks

Correct Answer: B

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.

A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to

specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Incorrect:

Not A: Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more. The query uses schema entities that are organized in a hierarchy similar to

SQL\\'s: databases, tables, and columns.

Not D: Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive

experiences.

Workbooks allow users to visualize the active alerts related to their resources.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

QUESTION 5

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

A. Azure Firewall

B. Azure Web Application Firewall (WAF)

C. Microsoft Defender for Cloud alerts

D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)

E. Microsoft Sentinel

Correct Answer: AB

This question is to increase secure score. Here is a long reference page from Microsoft of security recommendations that can increase your secure score. Sentinel and PIM are not on it. The explanation makes a great point about alerts not being preventive, which is a key aspect of the required solution.

https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls