

SC-900^{Q&As}

Microsoft Security Compliance and Identity Fundamentals

Pass Microsoft SC-900 Exam with 100% Guarantee

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

<https://www.pass2lead.com/sc-900.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Sentinel provides quick insights into data by using

	▼
Azure Logic Apps.	
Azure Monitor workbook templates.	
Azure Resource Graph Explorer.	
playbooks.	

Correct Answer:

Answer Area

Microsoft Sentinel provides quick insights into data by using

	▼
Azure Logic Apps.	
Azure Monitor workbook templates.	
Azure Resource Graph Explorer.	
playbooks.	

Box 1: Azure monitor workbook templates Create interactive reports by using workbooks After you onboard to Microsoft Sentinel, monitor your data by using the integration with Azure Monitor workbooks.

Workbooks display differently in Microsoft Sentinel than in Azure Monitor. But it may be useful for you to see how to create a workbook in Azure Monitor. Microsoft Sentinel allows you to create custom workbooks across your data. Microsoft Sentinel also comes with built-in workbook templates to allow you to quickly gain insights across your data as

soon as you connect a data source.

Reference: <https://learn.microsoft.com/en-us/azure/sentinel/overview>

QUESTION 2

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

- A. to control how often users must change their passwords
- B. to identify devices to which users can sign in without using multi-factor authentication (MFA)
- C. to encrypt a password by using globally recognized encryption standards
- D. to prevent users from using specific words in their passwords

Correct Answer: D

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization.

With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list.

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises>

QUESTION 3

You have a Microsoft 365 E5 tenant that uses a domain named contoso.com.

A user named User1 sends link-based, branded emails that are encrypted by using Microsoft Office 365 Advanced Message Encryption to the recipients shown in the following table.

Name	Email address
Recipient1	Recipient1@contoso.com
Recipient2	Recipient2@fabrikam.onmicrosoft.com
Recipient3	Recipient3@outlook.com
Recipient4	Recipient4@gmail.com

For which recipients can User1 revoke the emails?

- A. Recipient4 only

- B. Recipient1 only
- C. Recipient1, Recipient2, Recipient3, and Recipient4
- D. Recipient3 and Recipient4 only
- E. Recipient1 and Recipient2 only

Correct Answer: A

Reference: <https://docs.microsoft.com/en-us/microsoft-365/compliance/revoke-ome-encrypted-mail?view=o365-worldwide>

QUESTION 4

What do you use to provide real-time integration between Azure Sentinel and another security source?

- A. Azure AD Connect
- B. a Log Analytics workspace
- C. Azure Information Protection
- D. a connector

Correct Answer: D

To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc.

Reference: <https://docs.microsoft.com/en-us/azure/sentinel/overview>

QUESTION 5

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure. Which security methodology does this represent?

- A. threat modeling
- B. identity as the security perimeter
- C. defense in depth
- D. the shared responsibility model

Correct Answer: C

Reference:

<https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

[Latest SC-900 Dumps](#)

[SC-900 PDF Dumps](#)

[SC-900 Practice Test](#)