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.pass4itsure.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

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 2

You have an Azure subscription.

You need to implement approval-based, time-bound role activation.

What should you use?

A. access reviews in Azure AD

B. Azure AD Privileged Identity Management (PIM)

C. Azure AD Identity Protection

D. Conditional access in Azure AD

Correct Answer: B

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

QUESTION 3

Which two cards are available in the Microsoft 365 Defender portal? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. Devices at risk

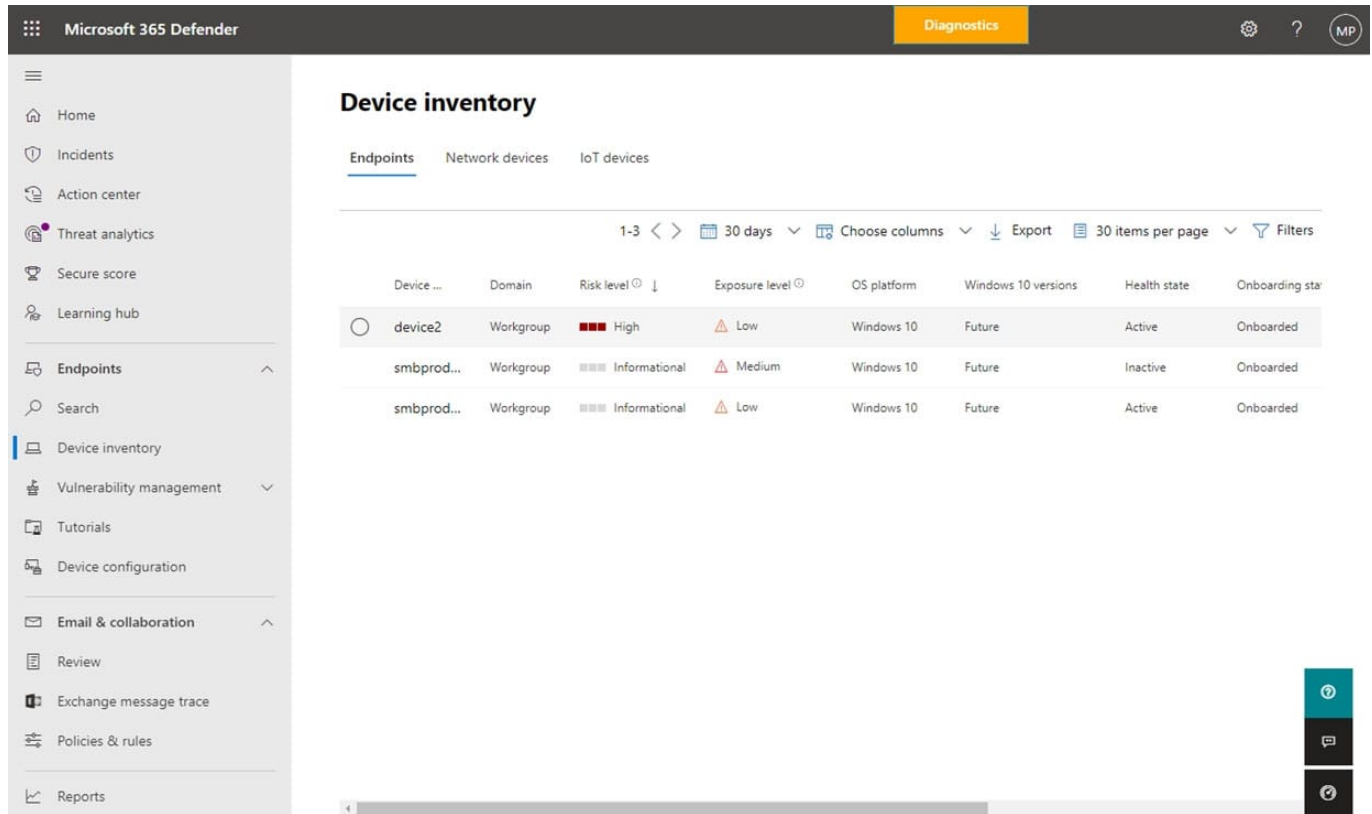B. Compliance Score

C. Service Health

D. User Management

E. Users at risk

Correct Answer: AE

A: The Devices at risk card includes a View details button. Selecting that button takes us to the Device inventory page, as shown in the following image

E: The Microsoft 365 Defender portal cards fall into these categories:

Identities- Monitor the identities in your organization and keep track of suspicious or risky behaviors. Here you can find the Users at risk card.

Data - Help track user activity that could lead to unauthorized data disclosure.

Devices - Get up-to-date information on alerts, breach activity, and other threats on your devices.

Apps - Gain insight into how cloud apps are being used in your organization.

Incorrect:

Not C: The Service Health card can be reached from the Microsoft 365 admin center.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-respond-mitigate-threats

QUESTION 4

HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Defender for Identity can identify advanced threats from

| | ∨ | signals. |

Azure Active Directory (Azure AD)
Azure AD Connect
on-premises Active Directory Domain Services (AD DS)

Correct Answer:

Answer Area

Microsoft Defender for Identity can identify advanced threats from

| | ∨ | signals. |

Azure Active Directory (Azure AD)
Azure AD Connect
on-premises Active Directory Domain Services (AD DS)

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Reference: https://docs.microsoft.com/en-us/defender-for-identity/what-is

QUESTION 5

What can be created in Active Directory Domain Services (AD DS)?

A. line-of-business (LOB) applications that require modern authentication

B. computer accounts

C. software as a service (SaaS) applications that require modern authentication

D. mobile devices

Correct Answer: B

What is computer account in Active Directory?

A computer account represents your desktop or laptop computer to the Active Directory.

Reference:

https://commons.lbl.gov/display/itfaq/Active+Directory

QUESTION 6

HOTSPOT

You have a Microsoft SharePoint Online site named Site1 and a sensitivity label named Sensitivity1.

Sensitivity1 adds a watermark and a header to content.

You create a policy to automatically apply Sensitivity1 to emails in Microsoft Exchange Online and Site1. How will Sensitivity1 mark matching emails and Site1 documents?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Exchange Online emails: [▼]

| A header only |
| A watermark only |
| A watermark and a header |

Site1 documents: [▼]

| A header only |
| A watermark only |
| A watermark and a header |

Correct Answer:

Exchange Online emails: [▼]

| **A header only** |
| A watermark only |
| A watermark and a header |

Site1 documents: [▼]

| A header only |
| A watermark only |
| **A watermark and a header** |

QUESTION 7

You have a Microsoft 365 tenant that uses trainable classifiers.

You are creating a custom trainable classifier.

You collect 300 sample file types from various geographical locations to use as seed content. Some of the file samples are encrypted.

You organize the files into categories as shown in the following table.

Category	Type	Language	Encryption status
Category1	.docx	French	Not encrypted
Category2	.xlsx	English	Encrypted
Category3	.pptx	German	Encrypted
Category4	.docx	English	Not encrypted
Category5	.mht	English	Not encrypted
Category6	.htm	English	Not encrypted

Which file categories can be used as seed content?

A. Category2, Category3, and Category5 only

B. Category1 and Category3 only

C. Category4 and Category6 only

D. Category4 and Category5 only

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/classifier-get-started-with?view=o365-worldwide
https://docs.microsoft.com/en-us/sharepoint/technical-reference/default-crawled-file-name-extensions-and-parsed-file-types

QUESTION 8

HOTSPOT

You have a Microsoft 365 tenant named contoso.com that contains two users named User1 and User2. The tenant uses Microsoft Office 365 Message Encryption (OME).

User1 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail1	User2@contoso.com	.docx	40 MB
Mail2	User4@outlook.com	.doc	3 MB
Mail3	User3@gmail.com	.xlsx	7 MB

User2 plans to send emails that contain attachments as shown in the following table.

Subject	To	Attachment type	Message size
Mail4	User1@contoso.com	.pptx	4 MB
Mail5	User4@outlook.com	.jpg	6 MB
Mail6	User3@gmail.com	.docx	3 MB

For which emails will the attachments be protected? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

User1:

Mail1 only
Mail3 only
Mail1 and Mail2 only
Mail2 and Mail3 only
Mail1, Mail2, and Mail3

User2:

Mail5 only
Mail6 only
Mail4 and Mail5 only
Mail4 and Mail6 only
Mail1, Mail2, and Mail3

Correct Answer:

User1:

Mail1 only
Mail3 only
Mail1 and Mail2 only
Mail2 and Mail3 only
Mail1, Mail2, and Mail3

User2:

Mail5 only
Mail6 only
Mail4 and Mail5 only
Mail4 and Mail6 only
Mail1, Mail2, and Mail3

Reference: https://support.microsoft.com/en-gb/office/introduction-to-irm-for-email-messages-bb643d33-4a3f-4ac7-9770-fd50d95f58dc?ui=en-usandrs=en-gbandad=gb#FileTypesforIRM
https://docs.microsoft.com/en-us/microsoft-365/compliance/ome?view=o365-worldwide https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/exchange-online-limits#message-limits-1

QUESTION 9

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

Correct Answer:

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

Box 1: No Advanced Audit helps organizations to conduct forensic and compliance investigations by increasing audit log retention.

Box 2: No

Box 3: Yes Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/advanced-audit?view=o365-worldwide

QUESTION 10

HOTSPOT

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	○
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	○	○

Correct Answer:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	●	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	●
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	●	○

QUESTION 11

HOTSPOT

You use project codes that have a format of three alphabetical characters that represent the project type, followed by three digits, for example Abc123.

You need to create a new sensitive info type for the project codes. How should you configure the regular expression to detect the content? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

(\s)([aA]{3} / [abc]{3} / [alpha]{3} / [a-zA-Z]{3} ▼) \ (d{000-999} / d{123} / d{3} ▼) (\s)

Correct Answer:

(\s)([aA]{3} / [abc]{3} / [alpha]{3} / **[a-zA-Z]{3}** ▼) \ (**d{000-999}** / d{123} / d{3} ▼) (\s)

Reference: https://joannecklein.com/2018/08/07/build-and-use-custom-sensitive-information-types-in-office-365/

QUESTION 12

Which service includes the Attack simul-ation training feature?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Office 365

C. Microsoft Defender for Identity

D. Microsoft Defender for SQL

Correct Answer: B

Attack simulation training in Microsoft Defender for Office 365 Plan 2 or Microsoft 365 E5 lets you run benign cyberattack simulations in your organization. These simulations test your security policies and practices, as well as train your employees to increase their awareness and decrease their susceptibility to attacks.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training

QUESTION 13

HOTSPOT

You need to implement an information compliance policy to meet the following requirements:

Documents that contain passport numbers from the United States, Germany, Australia, and Japan must be identified automatically.

When a user attempts to send an email or an attachment that contains a passport number, the user must receive a tooltip in Microsoft Outlook.

Users must be blocked from using Microsoft SharePoint Online or OneDrive for Business to share a document that contains a passport number.

What is the minimum number of sensitivity labels and auto-labeling policies you should create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Sensitivity labels:

1
2
3
4

Auto-labeling policies:

1
2
3
4

Correct Answer:

Sensitivity labels:

1
2
3
4

Auto-labeling policies:

1
2
3
4

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

QUESTION 14

What should you use in the Microsoft 365 security center to view security trends and track the protection status of identities?

A. Attack simulator

B. Reports

C. Hunting

D. Incidents

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-and-insights-in-security-and-compliance?view=o365-worldwide

QUESTION 15

HOTSPOT You are implementing Microsoft Office 365 Message Encryption (OME) for a Microsoft 365 tenant named contoso.com. You need to meet the following requirements:

1.

All email to a domain named fabrikam.com must be encrypted automatically.

2.

Encrypted emails must expire seven days after they are sent.

What should you configure for each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

All email to a domain named fabrikam.com
must be encrypted automatically:

▼
A data connector in the Microsoft 365 compliance center
A data loss prevention (DLP) policy in the Microsoft 365 compliance center
A mail flow connector in the Exchange admin center
A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days
after they are sent:

▼
A custom branding template in Microsoft Exchange Online PowerShell
A label policy in the Microsoft 365 compliance center
A mail flow rule in the Exchange admin center
A sensitive info type in the Microsoft 365 compliance center

Correct Answer:

Answer Area

All email to a domain named fabrikam.com
must be encrypted automatically:

▼
A data connector in the Microsoft 365 compliance center
A data loss prevention (DLP) policy in the Microsoft 365 compliance center
A mail flow connector in the Exchange admin center
A mail flow rule in the Exchange admin center

Encrypted emails must expire seven days
after they are sent:

▼
A custom branding template in Microsoft Exchange Online PowerShell
A label policy in the Microsoft 365 compliance center
A mail flow rule in the Exchange admin center
A sensitive info type in the Microsoft 365 compliance center