

DumpsCafe

Microsoft

SC-900



Microsoft Security Compliance and Identity Fundamentals

Version: Demo

[Total Questions: 10]

Web: www.dumpscafe.com

Email: support@dumpscafe.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpsafe.com

Support

If you have any questions about our product, please provide the following items:

- ➡ exam code
- ➡ screenshot of the question
- ➡ login id/email

please contact us at support@dumpsafe.com and our technical experts will provide support within 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

Question #:1

What feature supports email as a method of authenticating users?

- A. Microsoft Entra ID Protection
- B. Microsoft Entra Multi-Factor Authentication (MFA)
- C. self-service password reset (SSPR)
- D. Microsoft Entra Password Protection

Answer: B

Question #:2

What is an example of encryption at rest?

- A. encrypting communications by using a site-to-site VPN
- B. encrypting a virtual machine disk
- C. accessing a website by using an encrypted HTTPS connection
- D. sending an encrypted email

Answer: B

Question #:3

Which two tasks can you implement by using data loss prevention (DLP) policies in Microsoft 365? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Display policy tips to users who are about to violate your organization's policies.
- B. Enable disk encryption on endpoints.
- C. Protect documents in Microsoft OneDrive that contain sensitive information.
- D. Apply security baselines to devices.

Answer: A C

Question #:4

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input checked="" type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input checked="" type="radio"/>	<input type="radio"/>

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Sentinel uses workbooks to correlate alerts into incidents.	<input type="radio"/>	<input checked="" type="radio"/>
The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.	<input checked="" type="radio"/>	<input type="radio"/>

Question #:5

What should you use to ensure that the members of an Azure Active Directory group use multi-factor authentication (MFA) when they sign in?

- A. Azure Active Directory (Azure AD) Identity Protection
- B. a conditional access policy
- C. Azure role-based access control (Azure RBAC)
- D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Answer: B

Explanation

The recommended way to enable and use Azure AD Multi-Factor Authentication is with **Conditional Access policies**. Conditional Access lets you create and define policies that react to sign-in events and that request additional actions before a user is granted access to an application or service.

Question #:6

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements

You can use information barriers with Microsoft Exchange.

Yes

☐

No

☐

You can use information barriers with Microsoft SharePoint.

☐☐

You can use information barriers with Microsoft Teams.

☐☐

Answer:

Statements

You can use information barriers with Microsoft Exchange.

Yes

☐

No

☒

You can use information barriers with Microsoft SharePoint.

☒☐

You can use information barriers with Microsoft Teams.

☒☐

Statements

You can use information barriers with Microsoft Exchange.

Yes

☐

No

☒

You can use information barriers with Microsoft SharePoint.

☒☐

You can use information barriers with Microsoft Teams.

☒☐

Question #:7

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes**No**

Azure Active Directory (Azure AD) is deployed to an on-premises environment.

☐☐

Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.

☐☐

Azure Active Directory (Azure AD) is an identity and access management service.

☐☐

Answer:

Answer Area

Statements

Yes**No**

Azure Active Directory (Azure AD) is deployed to an on-premises environment.

☐☒

Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.

☒☐

Azure Active Directory (Azure AD) is an identity and access management service.

☒☐

Explanation

Answer Area

Statements

Yes**No**

Azure Active Directory (Azure AD) is deployed to an on-premises environment.

☐☒

Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.

☒☐

Azure Active Directory (Azure AD) is an identity and access management service.

☒☐

Box 1: No

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Box 2: Yes

Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.

Box 3: Yes

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Question #:8

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

NOTE: Each correct selection is worth one point.

Answer Area	Statements	Yes	No
	Azure AD Identity Protection generates risk detections once a user is authenticated.	<input type="radio"/>	<input type="radio"/>
	Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input type="radio"/>	<input type="radio"/>
	A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area	Statements	Yes	No
	Azure AD Identity Protection generates risk detections once a user is authenticated.	<input type="radio"/>	<input type="radio"/>
	Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input type="radio"/>	<input type="radio"/>
	A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	<input type="radio"/>	<input type="radio"/>

Answer Area	Statements	Yes	No
	Azure AD Identity Protection generates risk detections once a user is authenticated.	<input checked="" type="radio"/>	<input type="radio"/>
	Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	<input checked="" type="radio"/>	<input type="radio"/>
	A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	<input checked="" type="radio"/>	<input type="radio"/>

Question #:9

Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements

Yes

Conditional access policies always enforce the use of multi-factor authentication (MFA).

☐

Conditional access policies can be used to block access to an application based on the location of the user.

☐

Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.

☐

Answer:

Statements

Yes

Conditional access policies always enforce the use of multi-factor authentication (MFA).

☐

Conditional access policies can be used to block access to an application based on the location of the user.

☒

Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.

☐

Statements

Yes

Conditional access policies always enforce the use of multi-factor authentication (MFA).

☐

Conditional access policies can be used to block access to an application based on the location of the user.

☐

Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.

☐

Question #:10

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) can be used on which operating systems?

- A. Windows 10 and iOS only
- B. Windows 10 and Android only
- C. Windows 10, Android, and iOS
- D. Windows 10 only

Answer: A

DumpsCafe

About dumpsafe.com

dumpsafe.com was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: [All vendors](#)

Microsoft



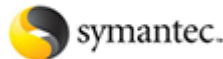
CITRIX



JUNIPER
NETWORKS



ORACLE



vmware

We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

- ➡ Sales: sales@dumpsafe.com
- ➡ Feedback: feedback@dumpsafe.com
- ➡ Support: support@dumpsafe.com

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.