DUMPSARENA

Microsoft Security Compliance and Identity Fundamentals

Microsoft SC-900

Version Demo

Total Demo Questions: 10

Total Premium Questions: 165

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, New Update	68
Topic 2, Describe the Concepts of Security, Compliance, and Identity	24
Topic 3, Describe the Capabilities of Microsoft Identity and Access Management Solutions	25
Topic 4, Describe the Capabilities of Microsoft Security Solutions	25
Topic 5, Describe the Capabilities of Microsoft Compliance Solutions	23
Total	165

QUESTION NO: 1

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. All users must authenticate from a registered device.

B. Administrators must always use Azure Multi-Factor Authentication (MFA).

C. Azure Multi-Factor Authentication (MFA) registration is required for all users.

D. All users must authenticate by using passwordless sign-in.

E. All users must authenticate by using Windows Hello.

ANSWER: B C

Explanation:

Security defaults make it easy to protect your organization with the following preconfigured security settings:

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

QUESTION NO: 2 - (DRAG DROP)

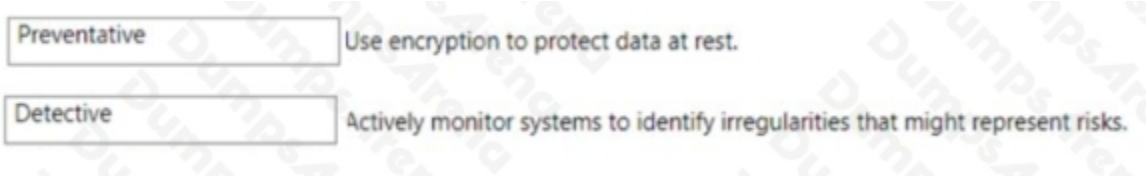
Match the types Of compliance score actions to the appropriate tasks.

To answer. drag the appropriate action type from the column on the left to its task on the right. Each type may be used once. more than once, or not at all.

NOTE: Each correct match is worth one point.

ANSWER:

Explanation:



QUESTION NO: 3

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. fingerprint

B. facial recognition

C. PIN

D. email verification

E. security question

ANSWER: A B C

Explanation:

Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

QUESTION NO: 4

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

ANSWER: C

Explanation:

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

QUESTION NO: 5

What is a use case for implementing information barrier policies in Microsoft 365?

A. to restrict unauthenticated access to Microsoft 365

B. to restrict Microsoft Teams chats between certain groups within an organization

C. to restrict Microsoft Exchange Online email between certain groups within an organization

D. to restrict data sharing to external email recipients

ANSWER: C

Explanation:

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers-policies?view=o365-worldwide

QUESTION NO: 6 - (HOTSPOT)

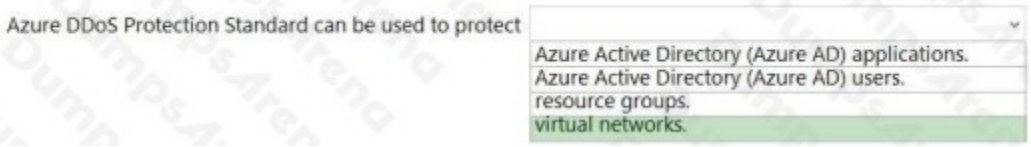
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:

ANSWER:

Answer Area



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

QUESTION NO: 7

What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?

A. automated remediation

B. automated investigation

C. advanced hunting

D. network protection

ANSWER: D

Explanation:

Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide

QUESTION NO: 8

What can you use to view the Microsoft Secure Score for Devices?

A. Microsoft Defender for Cloud Apps

B. Microsoft Defender for Endpoint

C. Microsoft Defender for Identity

D. Microsoft Defender for Office 365

ANSWER: B

Explanation:

Microsoft Secure Score for Devices

Applies to:

Some information relates to pre-released product which may be substantially modified before it's commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here.

To sign up for the Defender Vulnerability Management public preview or if you have any questions, contact us (mdvmtrial@microsoft.com).

Already have Microsoft Defender for Endpoint P2? Sign up for a free trial of the Defender Vulnerability Management Add-on.

Configuration score is now part of vulnerability management as Microsoft Secure Score for Devices.

Your score for devices is visible in the Defender Vulnerability Management dashboard of the Microsoft 365 Defender portal. A higher Microsoft Secure Score for Devices means your endpoints are more resilient from cybersecurity threat attacks. It reflects the collective security configuration state of your devices across the following categories:

Select a category to go to the Security recommendations page and view the relevant recommendations.

Turn on the Microsoft Secure Score connector

Forward Microsoft Defender for Endpoint signals, giving Microsoft Secure Score visibility into the device security posture. Forwarded data is stored and processed in the same location as your Microsoft Secure Score data.

Changes might take up to a few hours to reflect in the dashboard.

How it works

Microsoft Secure Score for Devices currently supports configurations set via Group Policy. Due to the current partial Intune support, configurations which might have been set through Intune might show up as misconfigured. Contact your IT Administrator to verify the actual configuration status in case your organization is using Intune for secure configuration management.

The data in the Microsoft Secure Score for Devices card is the product of meticulous and ongoing vulnerability discovery process. It is aggregated with configuration discovery assessments that continuously:

QUESTION NO: 9

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. Users at risk

B. Compliance Score

C. Devices at risk

D. Service Health

E. User Management

ANSWER: B C

QUESTION NO: 10 - (HOTSPOT)

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:

ANSWER:

Explanation:

Box 1: Yes

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes

Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Reference: https://docs.microsoft.com/en-us/azure/security-center/azure-defender https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction