

EXAMGOOD

QUESTION & ANSWER

Exam Good provides update free of charge in one year!

Accurate study guides
High passing rate!

<http://www.examgood.com>

Exam : **SC-900**

Title : Microsoft Security
Compliance and Identity
Fundamentals

Version : DEMO

1.HOTSPOT

Select the answer that correctly completes the sentence.

<input type="checkbox"/>	Customer Lockbox	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
<input type="checkbox"/>	Information barriers	
<input type="checkbox"/>	Privileged Access Management (PAM)	
<input type="checkbox"/>	Sensitivity labels	

Answer:

<input type="checkbox"/>	Customer Lockbox	can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.
<input checked="" type="checkbox"/>	Information barriers	
<input type="checkbox"/>	Privileged Access Management (PAM)	
<input type="checkbox"/>	Sensitivity labels	

Explanation:

Text

Description automatically generated

2.HOTSPOT

Select the answer that correctly completes the sentence.

<input type="checkbox"/>	Azure Defender	provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.
<input type="checkbox"/>	The Microsoft 365 compliance center	
<input type="checkbox"/>	The Microsoft 365 security center	
<input type="checkbox"/>	Microsoft Endpoint Manager	

Answer:

<input type="checkbox"/>	Azure Defender	provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.
<input checked="" type="checkbox"/>	The Microsoft 365 compliance center	
<input type="checkbox"/>	The Microsoft 365 security center	
<input type="checkbox"/>	Microsoft Endpoint Manager	

Explanation:

Text

Description automatically generated

3.HOTSPOT

Select the answer that correctly completes the sentence.

<input type="checkbox"/>	Azure Active Directory (Azure AD) Privileged Identity Management (PIM)	can use conditional access policies to control sessions in real time.
<input type="checkbox"/>	Microsoft Defender for Cloud	
<input type="checkbox"/>	Microsoft Sentinel	
<input checked="" type="checkbox"/>	Microsoft Defender for Cloud Apps	

Answer:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Microsoft Defender for Cloud
Microsoft Sentinel
Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

4.Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

- A. conditional access policies
- B. Azure AD Identity Protection
- C. Azure AD Privileged Identity Management (PIM)
- D. authentication method policies

Answer: C

Explanation:

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources

Reference: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

5.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.

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	<input checked="" type="radio"/>	<input type="radio"/>
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Graphical user interface, text, application, email

Description automatically generated

Box 1: Yes

System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes

Box 3: Yes

If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure.