QUESTIONS & ANSWERS
Kill your exam at first Attempt

KILL EXAMS

Microsoft

SC-900

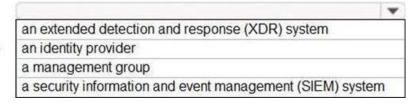*Microsoft Security, Compliance, and Identity Fundamentals*

Question: 70

HOTSPOT

Select the answer that correctly completes the sentence.
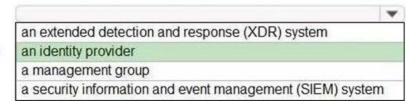
Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

an extended detection and response (XDR) system
an identity provider
a management group
a security information and event management (SIEM) system

Answer:

Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

an extended detection and response (XDR) system
an identity provider
a management group
a security information and event management (SIEM) system

Explanation:

Graphical user interface, text, application

Description automatically generated

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

Reference: https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

Question: 71

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
Azure Policy supports automatic remediation.	○	○
Azure Policy can be used to ensure that new resources adhere to corporate standards.	○	○
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	○	○

Answer:

Answer Area

Statements	Yes	No
Azure Policy supports automatic remediation.	●	○
Azure Policy can be used to ensure that new resources adhere to corporate standards.	●	○
Compliance evaluation in Azure Policy occurs only when a target resource is created or modified.	○	●

Explanation:

Graphical user interface, text, application, email

Description automatically generated

Question: 72

DRAG DROP

Match the Azure networking service to the appropriate description.

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

NOTE: Each correct match is worth one point.

Services	Answer Area	
Azure Bastion	Service	Provides Network Address Translation (NAT) services
Azure Firewall	Service	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines
Network security group (NSG)	Service	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Services

Azure Bastion

Azure Firewall

Network security group (NSG)

Answer Area

Azure Firewall	Provides Network Address Translation (NAT) services

Azure Bastion	Provides secure and seamless Remote Desktop connectivity to Azure virtual machines

Network security group (NSG)	Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Explanation:

Graphical user interface, application

Description automatically generated

Box 1: Azure Firewall

Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion

Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.
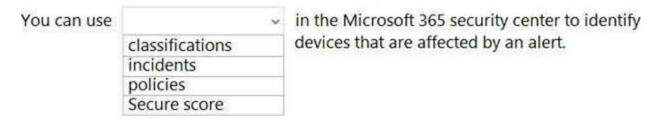
Box 3: Network security group (NSG)

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network.

Question: 73

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

You can use [classifications / incidents / policies / Secure score ▾] in the Microsoft 365 security center to identify devices that are affected by an alert.

Answer Area

You can use [▾] in the Microsoft 365 security center to identify devices that are affected by an alert.

classifications
incidents
policies
Secure score

(incidents highlighted)

Explanation:

Text, letter

Description automatically generated

Question: 74

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

[▾] is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

Answer:
Answer Area

[▾] is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Advisor
Azure Bastion
Azure Monitor
Azure Sentinel

(Azure Sentinel highlighted)

Explanation:

Text

Description automatically generated

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.

Question: 75

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Azure DDoS Protection
Standard can be used to protect

| Azure Active Directory (Azure AD) applications. |
| Azure Active Directory (Azure AD) users. |
| resource groups. |
| virtual networks. |

Answer:

Answer Area

Azure DDoS Protection
Standard can be used to protect

| Azure Active Directory (Azure AD) applications. |
| Azure Active Directory (Azure AD) users. |
| resource groups. |
| **virtual networks.** |

Explanation:

Graphical user interface, text

Description automatically generated

Question: 76

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

| Microsoft Cloud App Security |
| Microsoft Defender for Endpoint |
| Microsoft Defender for Identity |
| Microsoft Defender for Office 365 |

is a cloud-based solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced threats.

Answer:

Answer Area

| Microsoft Cloud App Security |
| Microsoft Defender for Endpoint |
| **Microsoft Defender for Identity** |
| Microsoft Defender for Office 365 |

is a cloud-based on that leverages on-premises Active Directory to identify, detect, and investigate advanced threats.
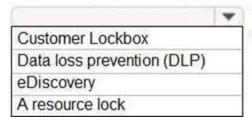
Explanation:

Graphical user interface, text

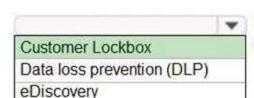Description automatically generated with medium confidence

HOTSPOT

Select the answer that correctly completes the sentence.

Answer Area

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Answer:
Answer Area

Customer Lockbox
Data loss prevention (DLP)
eDiscovery
A resource lock

is used to identify, hold, and export electronic information that might be used in an investigation.

Explanation:

Graphical user interface, application

Description automatically generated

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?
A. Microsoft Secure Score
B. Productivity Score
C. Secure score in Azure Security Center
D. Compliance score

Answer: D

Explanation:

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide

Question: 79

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
Sensitivity labels can be used to encrypt documents.	O	O
Sensitivity labels can add headers and footers to documents.	O	O
Sensitivity labels can apply watermarks to emails.	O	O

Answer:

Answer Area

Statements	Yes	No
Sensitivity labels can be used to encrypt documents.	O	O
Sensitivity labels can add headers and footers to documents.	O	O
Sensitivity labels can apply watermarks to emails.	O	O

Explanation:

Graphical user interface, text, application

Description automatically generated

Box 1: Yes

You can use sensitivity labels to provide protection settings that include encryption of emails and documents to prevent unauthorized people from accessing this data.

Box 2: Yes

You can use sensitivity labels to mark the content when you use Office apps, by adding watermarks, headers, or footers to documents that have the label applied.

Box 3: Yes

You can use sensitivity labels to mark the content when you use Office apps, by adding headers, or footers to email that have the label applied.

Question: 80

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

Answer: D

Explanation:

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

Kill your exam at First Attempt....Guaranteed!