Vendor: Microsoft

Exam Code:SC-900

Exam Name: Microsoft Security Compliance and Identity Fundamentals

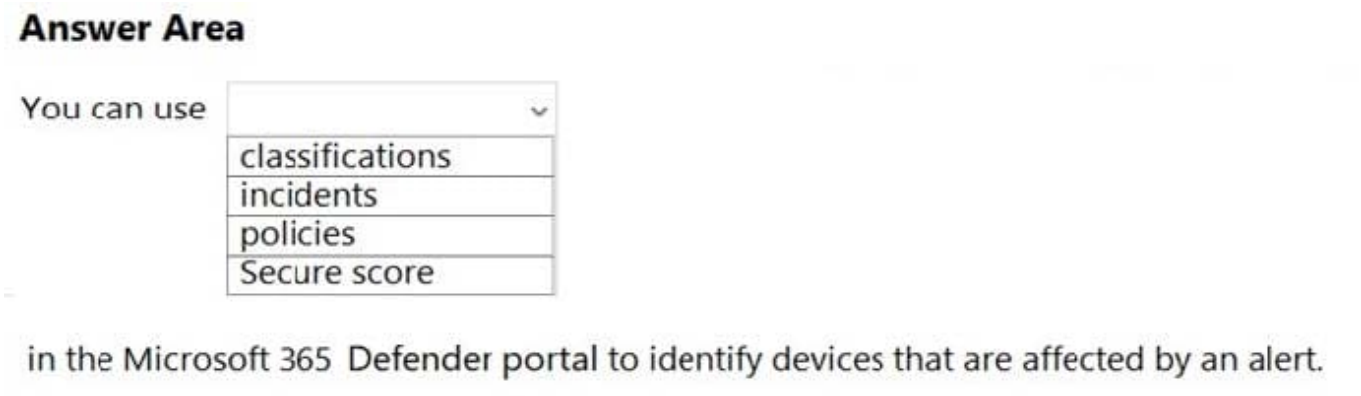
Version: Demo

QUESTION 1

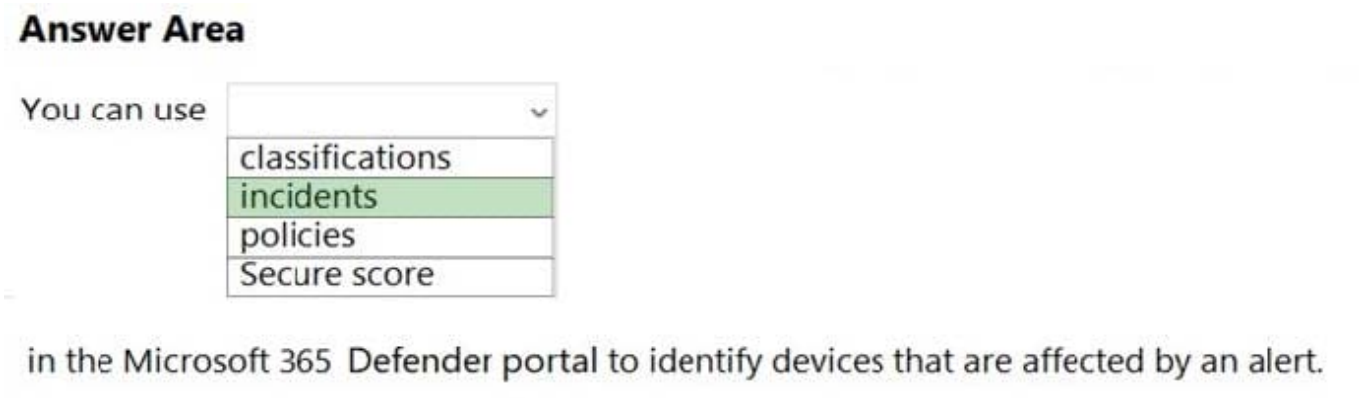
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

---

QUESTION 2

Which pillar of identity relates to tracking the resources accessed by a user?

A. authorization

B. auditing

C. administration

D. authentication

Correct Answer: B

Audit logs in Azure Active Directory

As an IT administrator, you want to know how your IT environment is doing. The information about your system\\'s health enables you to assess whether and how you need to respond to potential issues.

To support you with this goal, the Azure Active Directory portal gives you access to three activity logs:

Sign-ins

QUESTION 3

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:

Correct 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.	○	○

Reference: https://docs.microsoft.com/en-us/azure/governance/policy/overview

---

QUESTION 4

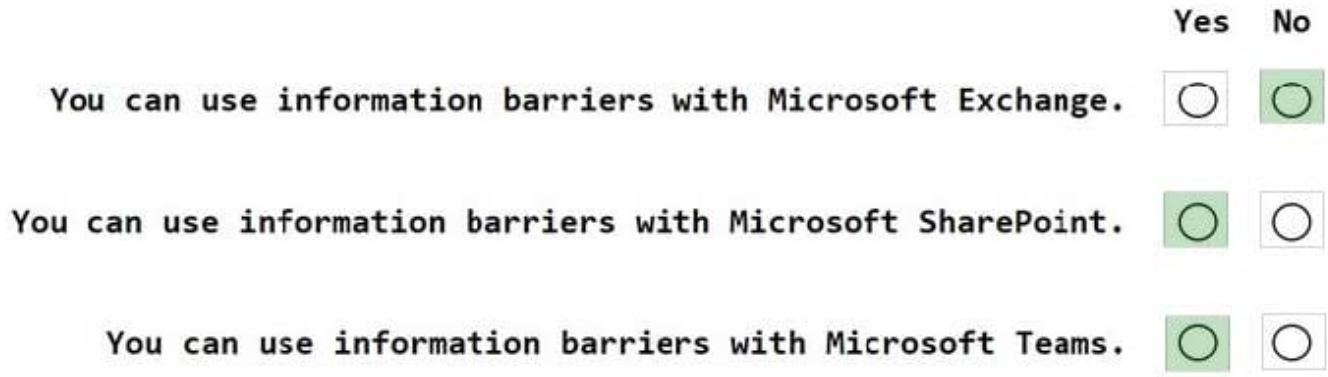
HOTSPOT

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:

	Yes	No
You can use information barriers with Microsoft Exchange.	○	○
You can use information barriers with Microsoft SharePoint.	○	○
You can use information barriers with Microsoft Teams.	○	○

Correct Answer:



Box 1: No

Information barriers and Exchange Online

IB policies aren\\'t available to restrict communication and collaboration between groups and users in email messages.

Box 2: Yes

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

Box 3: Yes

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

---

QUESTION 5

Each product group at your company must show a distinct product logo in encrypted emails instead of the standard Microsoft Office 365 logo. What should you do to create the branding templates?

A. Create a Transport rule.

B. Create an RMS template.

C. Run the Set-IRMConfiguration cmdlet.

D. Run the New-OMEConfiguration cmdlet.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/add-your-organization-brand-to-encrypted-messages?view=o365-worldwide

---

QUESTION 6

Which two Azure resources can a network security group (NSG) be associated with? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a network interface

B. an Azure App Service web app

C. a virtual network

D. a virtual network subnet

E. E. a resource group

Correct Answer: AD

Association of network security groups

You can associate a network security group with virtual machines, NICs, and subnets, depending on the deployment model you use.

Reference:

https://aviatrix.com/learn-center/cloud-security/create-network-security-groups-in-azure/

QUESTION 7

Which three forms of verification can be used with Azure AD Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.

NOTE: Each correct answer is worth one point.

A. security questions

B. the Microsoft Authenticator app

C. SMS messages

D. a smart card

E. Windows Hello for Business

Correct Answer: BCE

Available verification methods

When users sign in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. Users can access My Profile to edit or add verification methods.

The following additional forms of verification can be used with Azure AD Multi-Factor Authentication:

*

Microsoft Authenticator Authenticator Lite (in Outlook)

*

Windows Hello for Business FIDO2 security key OATH hardware token (preview) OATH software token

*

SMS Voice call

Reference: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

---

QUESTION 8

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
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Correct Answer:

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Box 1: Yes Box 2: Yes Box 3: No

The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

Reference:

https://docs.microsoft.com/en-us/security/zero-trust/

QUESTION 9

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove

users that no longer require membership in a group?

A. access reviews

B. managed identities

C. conditional access policies

D. Azure AD Identity Protection

Correct Answer: A

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

---

QUESTION 10

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

A. sensitivity label policies

B. Customer Lockbox

C. information Barriers

D. Privileged Access Management (PAM)

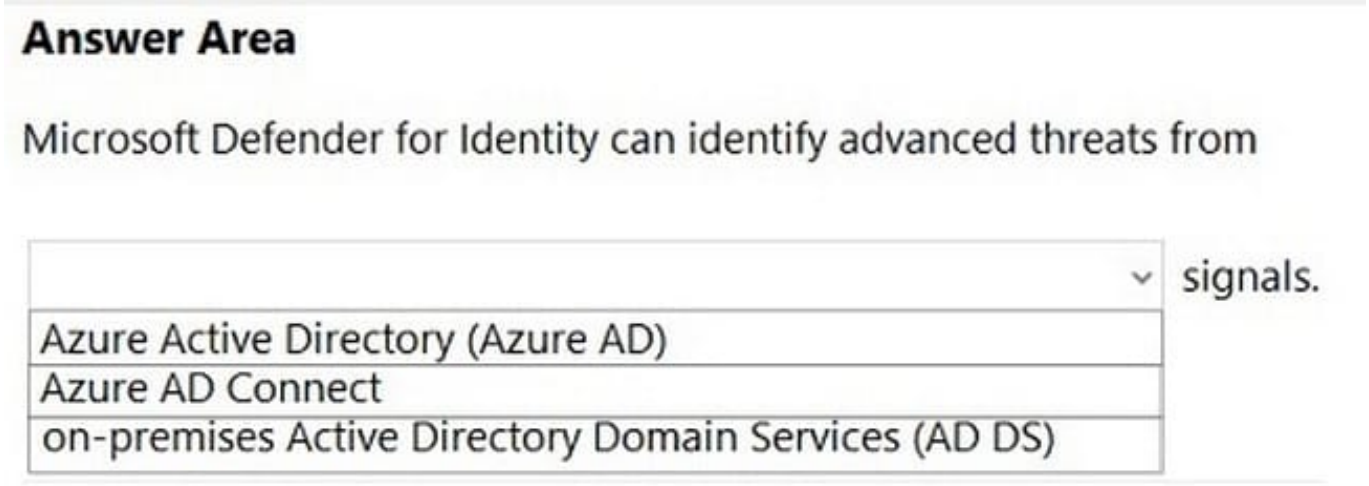
Correct Answer: C

QUESTION 11

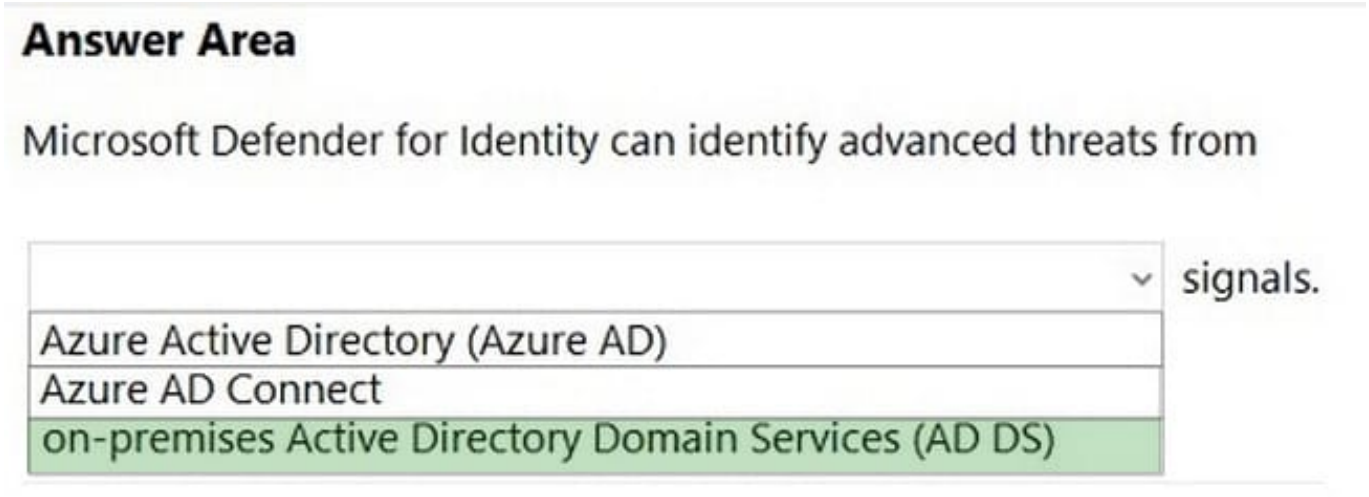
HOTSPOT

Select the answer that correctly completes the sentence.

Hot Area:



Correct Answer:



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 12

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 Area

Statements	Yes	No
Software tokens are an example of passwordless authentication	○	○
Windows Hello is an example of passwordless authentication	○	○
FIDO2 security keys are an example of passwordless authentication	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Software tokens are an example of passwordless authentication	○	●
Windows Hello is an example of passwordless authentication	●	○
FIDO2 security keys are an example of passwordless authentication	●	○

Box 1: No

Software tokens is a time-based one-time passcodes (TOTP) solution.

Microsoft Authenticator, which is a passwordless solution, uses software tokens though.

Note: Authentication methods in Azure Active Directory - OATH tokens

OATH TOTP (Time-based One Time Password) is an open standard that specifies how one-time password (OTP) codes are generated. OATH TOTP can be implemented using either software or hardware to generate the codes. Azure AD

doesn\\'t support OATH HOTP, a different code generation standard.

OATH software tokens

Software OATH tokens are typically applications such as the Microsoft Authenticator app and other authenticator apps. Azure AD generates the secret key, or seed, that\\'s input into the app and used to generate each OTP.

Box 2: Yes

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Azure Active Directory (Azure AD):

Windows Hello for Business

Microsoft Authenticator

FIDO2 security keys

Box 3: Yes

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-oath-tokens