



# MICROSOFT SC-900 Exam Questions

**Total Questions: 200+**

**Demo Questions: 30**

**Version: Updated for 2025**

**Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner**

**For Access to the full set of Updated Questions – Visit:  
[MICROSOFT SC-900 Exam Questions](#) by Cert Empire**

## Question: 1

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

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	<input type="radio"/>	<input type="radio"/>
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	<input type="radio"/>	<input type="radio"/>
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	<input type="radio"/>	<input type="radio"/>

### Answer:

Yes

Yes

Yes

CertEmpire

### Explanation:

Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage. Yes. Microsoft Defender for Storage is a specific plan within Microsoft Defender for Cloud that uses advanced threat intelligence to detect malicious activities and potential threats against Azure Storage accounts. It analyzes telemetry data and alerts on suspicious activities such as malware uploads, access from anomalous locations, and unusual data exfiltration patterns.

Cloud Security Posture Management (CSPM) is available for all Azure subscriptions. Yes. The foundational Cloud Security Posture Management (CSPM) features of Microsoft Defender for Cloud are offered for free to all Azure subscriptions. This includes a secure score, security recommendations, and asset inventory, providing essential visibility into the security posture of Azure resources without any additional cost.

Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises. Yes. Microsoft Defender for Cloud is a hybrid cloud security solution. By using Azure Arc, it can extend its security posture management and threat protection capabilities to non-Azure environments, including on-premises servers and other public clouds like AWS and GCP. This allows for a unified security management experience across hybrid infrastructures.

**References:**

Microsoft Defender for Storage: Microsoft. (n.d.). Overview of Microsoft Defender for Storage. Microsoft Learn. Retrieved from

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction>

Supporting evidence: The "What are the benefits of Microsoft Defender for Storage?" section explicitly states it provides "threat detection" and alerts for "unusual and potentially harmful attempts to access or exploit your storage accounts."

Foundational CSPM: Microsoft. (n.d.). Foundational CSPM. Microsoft Learn. Retrieved from <https://docs.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management#what-is-foundational-cspm>

Supporting evidence: This document states, "Microsoft Defender for Cloud offers foundational multicloud CSPM capabilities for free. These capabilities are automatically enabled by default on any subscription or account that has onboarded to Defender for Cloud."

Hybrid Cloud Protection: Microsoft. (n.d.). Connect your non-Azure machines to Microsoft Defender for Cloud. Microsoft Learn. Retrieved from

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines>

Supporting evidence: The introduction clearly states, "You can protect your non-Azure virtual machines and physical servers by installing the Azure Arc agent and enabling Defender for Cloud's security capabilities."

CertEmpire

## Question: 2

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

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	<input type="radio"/>	<input type="radio"/>
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	<input type="radio"/>	<input type="radio"/>
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	<input type="radio"/>	<input type="radio"/>

### Answer:

Yes

Yes

No

### Explanation:

CertEmpire

Enabling MFA increases the score (Yes): Microsoft Secure Score is calculated based on the implementation of recommended security controls. Enabling multi-factor authentication (MFA) is one of the most impactful improvement actions you can take. Completing this action awards a significant number of points, thereby increasing your organization's Secure Score.

A higher score means lower risk (Yes): The Secure Score is a numerical representation of your organization's security posture. A higher score indicates that more security recommendations have been implemented, which helps to protect your organization from threats. Therefore, a higher score directly correlates with a reduced attack surface and a lower identified security risk.

Secure Score vs. Compliance (No): This statement incorrectly describes Microsoft Secure Score. The tool that measures progress against key regulations and standards (like GDPR, NIST, ISO) is Microsoft Purview Compliance Manager. While Secure Score helps improve security posture, which is a component of compliance, its primary function is not to track adherence to specific regulatory frameworks.

**References:**

Microsoft. (2024). Microsoft Secure Score. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score>.

This document states, "You're given points for... configuring recommended security features like MFA... The more improvement actions you take, the higher your score will be." It also explains that the score helps you "report on the current state of your organization's security posture."

Microsoft. (2024). Overview of improvement actions in Microsoft Secure Score. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score-improvement-actions>.

This source explicitly lists "Require MFA for administrative roles" and "Enable MFA for all users" as high-value improvement actions that contribute points to the total score.

Microsoft. (2024). Microsoft Purview Compliance Manager. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/compliance-manager>.

This document clarifies the distinction: "Compliance Manager helps you manage your organization's compliance requirements... It is not a measure of your security posture. For that, refer to Microsoft Secure Score."

CertEmpire

### Question: 3

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:

A, C

#### Explanation:

The Microsoft 365 Defender portal's home page is designed to provide security operations teams with an at-a-glance summary of the organization's security health. It features several informational cards that aggregate data from different services. Among the default cards are "Users at risk," which displays information on user accounts with high-risk levels as identified by Azure AD Identity Protection, and "Devices at risk," which shows devices with active alerts or vulnerabilities identified by Microsoft Defender for Endpoint. These cards help administrators quickly identify and prioritize potential threats.

#### Why Incorrect Options are Wrong:

- B. Compliance Score: This card is a primary feature of the Microsoft Purview compliance portal ([compliance.microsoft.com](https://compliance.microsoft.com)), not the Microsoft 365 Defender portal.
- D. Service Health: Service Health information is located in the Microsoft 365 admin center ([admin.microsoft.com](https://admin.microsoft.com)) and provides status updates on Microsoft services.
- E. User Management: This is a core administrative function performed in the Microsoft 365 admin center or the Microsoft Entra admin center, not a summary card in the Defender portal.

---

#### References:

1. Microsoft Learn. (2023). The Microsoft 365 Defender portal. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-portal>.  
Reference Details: In the section "Home," the documentation lists the available cards on the dashboard, explicitly mentioning "Users at risk" and "Devices at risk." It does not list Compliance Score, Service Health, or User Management as cards on this specific portal's home page.
2. Microsoft Learn. (2023). Microsoft Purview compliance portal. Microsoft Docs. Retrieved from

<https://learn.microsoft.com/en-us/purview/microsoft-365-compliance-center>.

Reference Details: The "Card dashboard" section describes the home page of the compliance portal, which includes the "Compliance Score" card. This confirms that this card belongs to a different portal.

CertEmpire

## Question: 4

HOTSPOT Select the answer that correctly completes the sentence.

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.

### Answer:

Microsoft Defender for Cloud Apps

### Explanation:

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that integrates with Azure Active Directory (Azure AD) Conditional Access to provide real-time session control. This feature, known as Conditional Access App Control, routes user sessions through a reverse proxy. This allows an organization to monitor and control user activities within a cloud app session in real time. For example, an administrator can create policies to block the download of sensitive documents, monitor specific user actions, or require step-up authentication based on in-session behavior. The other services listed serve different primary security functions.

### References:

Microsoft Learn, Microsoft Defender for Cloud Apps Documentation. "Protect with Microsoft Defender for Cloud Apps Conditional Access App Control." This document explicitly states, "In Microsoft Defender for Cloud Apps, you can create session policies to control sessions in real time... Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies."

Microsoft Learn, Microsoft Defender for Cloud Apps Documentation. "Session policies." This page details the functionality, explaining that "Defender for Cloud Apps session policies provide granular visibility into cloud apps and enable you to control actions in real-time based on the content of files."

Microsoft Learn, Microsoft Entra Documentation. "Conditional Access App Control." In the description of the "Use session controls" grant control, the documentation specifies that this control is "enforced by Microsoft Defender for Cloud Apps" to enable real-time monitoring and control of sessions.



## Question: 5

Which service includes the Attack simulation training feature?

- A. Microsoft Defender for Cloud Apps
- B. Microsoft Defender for Office 365
- C. Microsoft Defender for Identity
- D. Microsoft Defender for SQL

### Answer:

B

### Explanation:

Attack simulation training is a feature included in Microsoft Defender for Office 365 Plan 2. It enables organizations to run realistic, benign cyberattack simulations, such as credential harvesting or malware attachment phishing campaigns. The purpose is to identify vulnerable users and educate them on security best practices before a real attack occurs. This tool helps measure changes in employee security behavior and improve the organization's overall security posture against social engineering attacks, which are commonly delivered via email and other Office 365 services.

CertEmpire

### Why Incorrect Options are Wrong:

- A. Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that provides visibility, data control, and threat protection for cloud applications.
- C. Microsoft Defender for Identity is a cloud-based security solution that leverages on-premises Active Directory signals to identify, detect, and investigate advanced identity-based threats.
- D. Microsoft Defender for SQL is a feature within Microsoft Defender for Cloud that protects SQL databases by identifying vulnerabilities and detecting anomalous activities.

### References:

1. Microsoft Learn. (2023). Get started using Attack simulation training in Defender for Office 365. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-started>. (See the "What do you need to know before you begin?" section, which states, "Attack simulation training is available in subscriptions that include Microsoft Defender for Office 365 Plan 2.")
2. Microsoft Learn. (2023). SC-900: Describe the capabilities of Microsoft Defender for Office 365. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/training/modules/describe-capabilities-of-microsoft-defender-365/4-describe-microsoft-defender-office-365>. (This module covers the features of Defender for Office 365, including "Attack simulation training" as a key capability for proactive security.)

3. Microsoft. (2023). Microsoft 365 and Office 365 platform service description. Microsoft Docs. Retrieved from <https://learn.microsoft.com/en-us/office365/servicedescriptions/office-365-platform-service-description/microsoft-365-security-compliance-licensing-guidance>. (Under the "Microsoft Defender for Office 365 Plan 2" feature table, "Attack Simulation Training" is explicitly listed.)

CertEmpire

## Question: 6

HOTSPOT Select the answer that correctly completes the sentence.

You can use dynamic groups in Azure Active Directory (Azure AD) to automate the  lifecycle process.

### Answer:

access

### Explanation:

Dynamic groups in Azure Active Directory (Azure AD), now Microsoft Entra ID, automate the process of adding and removing members based on user or device attributes. The primary purpose of managing group membership is to control permissions and entitlements for resources such as applications, licenses, and data. By automating group composition, dynamic groups directly automate the provisioning and de-provisioning phases of the access lifecycle. For instance, when an employee joins the 'Sales' department (an attribute change), they can be automatically added to the 'Sales Team' group, granting them immediate access to necessary sales applications and files. This removes the need for manual administrative intervention to grant or revoke access as roles and attributes change. certEmpire

### References:

Microsoft Entra Documentation: Dynamic membership rules for groups in Microsoft Entra ID. Reference: Under the section "What are dynamic membership rules?", the documentation explains that dynamic groups add/remove members based on attributes. The provided use cases, such as creating a group for all users in a specific department or assigning licenses, are fundamentally about managing access. This automation is a core component of managing the access lifecycle.

Microsoft Entra Documentation: What is group-based licensing in Microsoft Entra ID?. Reference: This document provides a specific example of access lifecycle automation. It states, "you can assign one or more product licenses to a group. Microsoft Entra ID ensures that the licenses are assigned to all members of the group. Any new members who join the group are assigned the appropriate licenses. When they leave the group, those licenses are removed." This describes the automation of granting and revoking access to licensed software.

## Question: 7

You need to connect to an Azure virtual machine by using Azure Bastion. What should you use?

- A. an SSH client
- B. PowerShell remoting
- C. the Azure portal
- D. the Remote Desktop Connection client

### Answer:

C

### Explanation:

Azure Bastion is a fully managed platform-as-a-service (PaaS) that provides secure and seamless Remote Desktop Protocol (RDP) and Secure Shell (SSH) connectivity to your virtual machines directly through the Azure portal. When you connect via Azure Bastion, you select the target virtual machine in the portal, and the RDP or SSH session opens in a new browser tab. This method eliminates the need to expose virtual machines to the public internet via a public IP address or to use separate client software on your local computer.

### Why Incorrect Options are Wrong:

CertEmpire

- A. an SSH client: This is incorrect because the connection is initiated and brokered through the Azure portal's interface, not directly from a standalone SSH client on your local machine.
- B. PowerShell remoting: This is a management protocol (WinRM) and not the tool used to establish an interactive desktop or shell session through the Azure Bastion service.
- D. the Remote Desktop Connection client: This is incorrect because Azure Bastion provides an in-browser RDP session, removing the need for the local Remote Desktop client (mstsc.exe) and a public IP on the VM.

### References:

1. Microsoft Learn. "What is Azure Bastion?". Azure Bastion Documentation. "Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal... You connect to the VM directly from the Azure portal."
2. Microsoft Learn. "Tutorial: Connect to a virtual machine by using Azure Bastion". Azure Bastion Documentation. Under the "Connect" section, Step 1 explicitly states, "Sign in to the Azure portal." The subsequent steps detail navigating to the virtual machine and using the portal's "Connect" "Bastion" option.
3. Microsoft Learn. "About Azure Bastion configuration settings". Azure Bastion Documentation. Under the "SKUs" section, the feature matrix for the Basic and Standard SKUs shows that the primary connection method is "Connect to Azure VMs via RDP and SSH from the Azure portal."

## Question: 8

What is a characteristic of a sensitivity label in Microsoft 365?

- A. persistent
- B. encrypted
- C. restricted to predefined categories

### Answer:

A

### Explanation:

A primary characteristic of a sensitivity label is its persistence. When a label is applied to a document or email, it is embedded as clear-text metadata that travels with the content. This ensures that the classification and any associated protection settings (such as encryption or content markings) remain with the data, regardless of where it is stored, used, or shared. This persistence allows applications and services to read the label and enforce the appropriate policies consistently.

### Why Incorrect Options are Wrong:

- B. encrypted: Encryption is a protection that a sensitivity label can apply, but it is not an inherent characteristic of all labels. Some labels may only apply visual markings or no protection at all.
- C. restricted to predefined categories: Administrators can create and customize their own sensitivity labels and categories to match their organization's specific data classification schema; they are not limited to a fixed set of predefined categories.

### References:

1. Microsoft Learn, "Learn about sensitivity labels," Microsoft Purview documentation.  
Reference for Correct Answer (A): Under the section "What sensitivity labels are," the documentation states, "When you apply a sensitivity label to content, the label is stored in clear text in the metadata of that content. The label and its protection settings are persistent, and roam with the content..."  
Reference for Incorrect Answer (B): Under the section "What sensitivity labels can do," "Encrypt emails and documents" is listed as one of several possible actions, confirming it is an optional capability, not a universal characteristic.  
Reference for Incorrect Answer (C): The entire document details how administrators can "Create and configure sensitivity labels," which demonstrates that they are customizable and not restricted.
2. Microsoft Learn, "Get started with sensitivity labels," Microsoft Purview documentation.  
Reference for Correct Answer (A): In the introductory paragraph, it explains, "After a sensitivity

label is applied to an email, document, or site, any configured protection settings for that label are enforced on the content. The label also persists with the content..."

CertEmpire

## Question: 9

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.

[image could not be rendered]

### Answer:

Preventative

Detective

The screenshot shows a matching exercise interface. On the left, under the heading "Compliance score action", there are three rectangular boxes containing the text "Corrective", "Detective", and "Preventative" from top to bottom. On the right, under the heading "Answer Area", there are two rectangular boxes. The top box contains the text "Action" followed by "Use encryption to protect data at rest." The bottom box contains the text "Action" followed by "Actively monitor systems to identify irregularities that might represent risks." There are small circular icons between the two columns and above the answer area, indicating a drag-and-drop mechanism.

### Explanation:

The classification of security controls depends on their primary function in managing security risks.

- Preventative controls are proactive measures designed to stop a security incident from happening in the first place. Encryption is a classic example of a preventative control because it renders data unreadable to unauthorized parties, thereby preventing a data confidentiality breach even if the data is stolen.
- Detective controls are implemented to identify and report that an incident has occurred or is in progress. Actively monitoring systems for irregularities fits this description perfectly. Its goal is not to stop the initial event but to detect it so that a response can be initiated.

### References:

NIST Special Publication 800-53 Rev. 5, "Security and Privacy Controls for Information Systems and Organizations": This foundational document categorizes security controls.

It defines preventive controls as those that "avoid, deter, or impede" incidents. The control family

SC - System and Communications Protection, which includes SC-28 Protection of Information at Rest (encryption), falls under this category.

It defines detective controls as those that "detect incidents during or after their occurrence." The control family SI - System and Information Integrity, which includes SI-4 Information System Monitoring, is a primary example of detective controls. (See Section 2.3, "Control Structure").

Microsoft Cloud Adoption Framework for Azure, "Security controls": This official documentation outlines security best practices.

Under the "Data Protection" security control, it recommends, "Encrypt data at rest... to provide data-level protection," which is a preventative action.

Under the "Logging and threat detection" security control, it describes how services like Microsoft Sentinel "Collect and analyze data to detect potential threats," which is a detective function.

Purdue University, CERIAS (Center for Education and Research in Information Assurance and Security): Academic literature consistently uses this taxonomy.

In various publications on risk management, preventative controls are described as the first line of defense (e.g., locks, encryption), while detective controls are the second line used to discover breaches of the first line (e.g., alarms, monitoring logs). (See "A Brief Introduction to Information Security," CERIAS Tech Report 2004-13).

CertEmpire



## Question: 10

HOTSPOT Select the answer that correctly completes the sentence.

measures a company's progress in completing actions that help reduce risks

- Compliance score
- Microsoft Purview compliance portal reports
- The Trust Center
- Trust Documents

### Answer:

Compliance score

### Explanation:

The Compliance score in Microsoft Purview Compliance Manager is the specific metric used to measure and track an organization's progress in completing recommended improvement actions. This score is calculated based on the implementation of controls that align with data protection regulations and standards. A higher score indicates that more risk-reducing actions have been completed, providing a clear, at-a-glance understanding of the organization's compliance posture.

The Trust Center and Trust Documents are resources that provide information about Microsoft's own security and compliance practices, not a measure of a customer's progress. Microsoft Purview compliance portal reports are a broad category of outputs, whereas the compliance score is the precise measure in question.

### References:

Microsoft. (n.d.). Microsoft Purview Compliance Manager. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/compliance-manager>.

Reference Point: In the "Key features: what Compliance Manager provides" section, it states, "It provides a compliance score that helps you track your progress and prioritize actions based on their potential to reduce risk."

Microsoft. (n.d.). Understand your compliance score. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/compliance-score-calculation>.

Reference Point: The initial overview states, "Your compliance score measures your progress in completing recommended improvement actions within controls."

## Question: 11

You plan to move resources to the cloud. You are evaluating the use of Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) cloud models. You plan to manage only the data, user accounts, and user devices for a cloud-based app. Which cloud model will you use?

- A. IaaS
- B. SaaS
- C. PaaS

### Answer:

B

### Explanation:

The Software as a Service (SaaS) model is the correct choice. In this model, the cloud provider manages the entire technology stack, including the application, middleware, runtime, and underlying infrastructure. The customer's responsibility is limited to consuming the service and managing their own information, data, user accounts, and the devices used to access the application. This perfectly aligns with the scenario of managing only data, user accounts, and user devices for a cloud-based app.

CertEmpire

### Why Incorrect Options are Wrong:

- A. IaaS: Incorrect. With Infrastructure as a Service (IaaS), the customer is responsible for managing the operating system, middleware, runtime, and applications, which is significantly more responsibility than described in the scenario.
- C. PaaS: Incorrect. With Platform as a Service (PaaS), the customer is responsible for deploying and managing their own applications and data, which is more responsibility than just managing data and user accounts.

### References:

1. Microsoft Learn. (2024). Describe cloud service types. SC-900: Describe the concepts of security, compliance, and identity. Under the section "Compare cloud service types," the chart explicitly shows that for SaaS, the customer is responsible for "Information and data," "Devices (mobiles and PCs)," and "Accounts and identities."  
Reference: <https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/3-describe-iaas-paas-saas>
2. Microsoft Learn. (2024). Describe the shared responsibility model. SC-900: Describe the concepts of security, compliance, and identity. The "Division of responsibility" diagram clearly illustrates that in the SaaS model, the customer's responsibility is limited to data, endpoints

(devices), accounts, and access management.

Reference: <https://learn.microsoft.com/en-us/training/modules/describe-shared-responsibility-model/2-describe-shared-responsibility-model>

3. Microsoft Azure Documentation. (2023). Shared responsibility in the cloud. Microsoft Azure Security Fundamentals. The responsibility matrix diagram shows that for SaaS, the customer is always responsible for "Information and data," "Devices," and "Accounts and identities."

Reference: <https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>

CertEmpire

## Question: 12

You have an Azure subscription that contains a Log Analytics workspace. You need to onboard Microsoft Sentinel. What should you do first?

- A. Create a hunting query.
- B. Correlate alerts into incidents.
- C. Connect to your security sources.
- D. Create a custom detection rule.

### Answer:

C

### Explanation:

The foundational step for using Microsoft Sentinel is to ingest data for analysis. After enabling Microsoft Sentinel on a Log Analytics workspace, the immediate next action is to connect security sources (such as Microsoft Entra ID, Microsoft Defender XDR, or firewalls) using data connectors. Without data from these sources, Sentinel cannot perform its core functions of threat detection, investigation, or hunting, as there would be no information to analyze. All other activities, such as creating rules or hunting, are dependent on this initial data collection.

CertEmpire

### Why Incorrect Options are Wrong:

A. Create a hunting query.

Hunting queries are used to proactively search for threats within data that has already been ingested. This action requires data to be present in the workspace first.

B. Correlate alerts into incidents.

This is a feature of Sentinel that groups related alerts. Alerts are generated by analytics rules that run against data from connected sources, so data connection must precede this.

D. Create a custom detection rule.

Detection (or analytics) rules are created to analyze data from connected sources to identify threats. You must connect the data sources before you can create meaningful rules to analyze that data.

### References:

1. Microsoft Learn. "Quickstart: On-board Microsoft Sentinel." Microsoft Docs, 20 Sep 2023. In the "Next steps" section, after "Enable Microsoft Sentinel," the first recommended action is "Connect data sources." The document states, "Microsoft Sentinel ingests data from the services and apps you connect by using data connectors."
2. Microsoft Learn. "Connect data sources to Microsoft Sentinel." Microsoft Docs, 20 Sep 2023. The introduction explicitly states, "After you have enabled Microsoft Sentinel, the first step is to

connect your data sources." This confirms that connecting sources is the initial operational task.

3. Microsoft Learn. "Detect threats with built-in analytics rules in Microsoft Sentinel." Microsoft Docs, 20 Sep 2023. The overview section explains that analytics rules "search for specific events or sets of events across your connected data sources." This presupposes that data sources are already connected.

## Question: 13

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 DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	<input type="radio"/>	<input checked="" type="radio"/>
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	<input type="radio"/>	<input checked="" type="radio"/>
Azure DDoS Protection Standard protects against protocol attacks.	<input type="radio"/>	<input checked="" type="radio"/>

### Answer:

No

No

Yes

### Explanation:

Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks: No. Azure DDoS Protection is designed to mitigate availability threats by absorbing and scrubbing massive volumes of network traffic. A man-in-the-middle (MITM) attack is a confidentiality and integrity attack where an adversary secretly intercepts and potentially alters communications between two parties. This is a different class of threat that DDoS protection services are not designed to prevent.

Azure DDoS Protection Standard is enabled by default in an Azure subscription: No. Azure provides DDoS Protection Basic for free, which is automatically enabled for the entire Azure platform. However, DDoS Protection Standard is a premium, paid service with enhanced features that must be explicitly enabled on a specific virtual network (VNet). It is not enabled by default for a subscription.

Azure DDoS Protection Standard protects against protocol attacks: Yes. Azure DDoS Protection Standard is specifically designed to mitigate the three primary categories of DDoS attacks: volumetric attacks, protocol attacks, and application layer attacks. Protocol attacks, such as SYN floods, reflection attacks, and other L3/L4 protocol abuses, are a core threat vector that the service protects against.

**References:**

Microsoft. "What is Azure DDoS Protection?". Microsoft Learn, Azure Documentation. Accessed October 13, 2025.

Reference for Statement 1 & 3: Under the section "Azure DDoS Protection Tiers," the documentation describes the types of attacks mitigated, which include volumetric, protocol, and resource (application) layer attacks. It does not list MITM attacks as a covered threat.

Microsoft. "Azure DDoS Protection Standard features". Microsoft Learn, Azure Documentation. Accessed October 13, 2025.

Reference for Statement 3: The "Mitigation" section explicitly lists mitigations for "Protocol attacks" and provides examples such as "SYN, ACK, and TCP connection exhaustion" and "UDP reflection."

Microsoft. "Azure DDoS Protection Tiers". Microsoft Learn, Azure Documentation. Accessed October 13, 2025.

Reference for Statement 2: This document explicitly states, "DDoS Protection Basic is automatically enabled as part of your Azure subscription," and for DDoS Protection Standard, "You must manually enable DDoS Network Protection for your virtual networks."

## Question: 14

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.

Statements	Yes	No
Azure AD Identity Protection can add users to groups based on the users' risk level.	<input type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can detect whether user credentials were leaked to the public.	<input checked="" type="radio"/>	<input type="radio"/>
Azure AD Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	<input checked="" type="radio"/>	<input type="radio"/>

### Answer:

No

Yes

Yes

### Explanation:

Statement 1: No. Azure AD Identity Protection itself does not have a direct policy action to add users to a group. However, the risk level attribute it calculates (user.riskLevel) can be used as a property to create a dynamic membership rule for a group in Azure AD. Therefore, the action is performed by the Azure AD Dynamic Groups feature, which uses data from Identity Protection, but it is not a direct capability of Identity Protection policies.

Statement 2: Yes. This is a core feature of Azure AD Identity Protection. It works with researchers, law enforcement, and dark web monitoring teams to find publicly available lists of usernames and passwords. When a user's credentials are found on such a list, Identity Protection flags it as a "Leaked credentials" risk detection.

Statement 3: Yes. A primary function of Identity Protection is to automate responses to detected risks. You can configure a user risk policy or a sign-in risk policy that automatically requires a user to perform Multi-Factor Authentication (MFA) when their calculated risk level meets a specified threshold (e.g., medium or high). This helps ensure that even if a credential is compromised, the identity is protected.



**References:**

Statement 1 (Dynamic Groups):

Microsoft Entra ID Documentation. (n.d.). Dynamic membership rules for groups in Microsoft Entra ID. Microsoft Learn. Retrieved from

<https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership>.

This document lists user.riskLevel as a supported property for creating dynamic group rules, confirming that the capability exists within Azure AD but is configured under group properties, not Identity Protection policies.

Statement 2 (Leaked Credentials):

Microsoft Entra ID Documentation. (n.d.). What is risk? - Leaked credentials. Microsoft Learn.

Retrieved from <https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks#leaked-credentials>.

This official documentation explicitly describes the "Leaked credentials" risk detection type and how Identity Protection identifies it.

Statement 3 (MFA on Risk):

Microsoft Entra ID Documentation. (n.d.). Identity Protection policies - User risk policy. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies#user-risk-policy>.

This source details the configuration of the user risk policy, stating that administrators can set the "Access" control to "Allow access" and "Require multifactor authentication".

## Question: 15

What can you use to deploy Azure resources across multiple subscriptions in a consistent manner?

- A. Microsoft Sentinel
- B. Microsoft Defender for Cloud
- C. Azure Policy
- D. Azure Blueprints

### Answer:

D

### Explanation:

Azure Blueprints is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as role assignments, policy assignments, and Azure Resource Manager (ARM) templates. This service is specifically designed to help organizations set up governed and consistent environments at scale. A single blueprint can be versioned and assigned to multiple subscriptions, ensuring that each environment is provisioned with the same set of resources, configurations, and policies, thereby achieving consistency across the organization.

CertEmpire

### Why Incorrect Options are Wrong:

- A. Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution, used for threat detection and response, not resource deployment.
- B. Microsoft Defender for Cloud is a Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) that provides security recommendations and threat protection, not resource deployment.
- C. Azure Policy is used to enforce organizational standards and assess compliance. While it can trigger deployments for non-compliant resources, its primary purpose is governance, not the orchestrated deployment of a complete environment.

### References:

1. Microsoft Learn: "Overview of Azure Blueprints". Microsoft Docs. "Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. ....With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved."
2. Microsoft Learn: "What is Azure Policy?". Microsoft Docs. "Azure Policy is a service in Azure

that you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service level agreements." (This highlights its role in enforcement, not initial orchestrated deployment).

3. Microsoft Learn: "What is Microsoft Sentinel?". Microsoft Docs. "Microsoft Sentinel is a scalable, cloud-native solution that provides: Security information and event management (SIEM) and Security orchestration, automation, and response (SOAR)."

4. Microsoft Learn: "What is Microsoft Defender for Cloud?". Microsoft Docs. "Microsoft Defender for Cloud is a cloud security posture management (CSPM) and cloud workload protection platform (CWPP) that finds weak spots across your cloud configuration, helps strengthen the overall security posture of your environment, and can protect workloads across multicloud and hybrid environments from evolving threats."

## Question: 16

Which Microsoft Defender for Cloud metric displays the overall security health of an Azure subscription?

- A. resource health
- B. secure score
- C. the status of recommendations
- D. completed controls

### Answer:

B

### Explanation:

Microsoft Defender for Cloud's secure score is a numerical value that represents the overall security posture of a subscription. It aggregates findings from security recommendations into a single score, providing an at-a-glance view of the current security situation. A higher score indicates a lower identified risk level. This metric is calculated based on the ratio of healthy resources to the total resources, as evaluated against the enabled security recommendations.

### Why Incorrect Options are Wrong:

CertEmpire

- A. resource health: Azure Resource Health is a service that reports on the availability and operational health of Azure resources, not their security posture as defined by Defender for Cloud.
- C. the status of recommendations: The status of individual recommendations (e.g., healthy, unhealthy) provides the detailed data that is used to calculate the secure score, but it is not the single, aggregated metric for overall health.
- D. completed controls: Security controls are logical groups of related recommendations. While completing controls improves the secure score, the number of completed controls is a component, not the final overall metric itself.

### References:

1. Microsoft Learn. "Secure score in Microsoft Defender for Cloud." Microsoft Docs. Accessed May 20, 2024. In the "Introduction to secure score" section, it states, "Microsoft Defender for Cloud's secure score is a numerical value that represents your security posture."
2. Microsoft Learn. "Security controls and their recommendations." Microsoft Docs. Accessed May 20, 2024. This document explains that "Recommendations are grouped into security controls," clarifying that controls are a component of the overall score calculation.
3. Microsoft Learn. "Overview of Azure Resource Health." Microsoft Docs. Accessed May 20, 2024. The "What is Resource Health?" section clarifies its purpose: "Azure Resource Health helps

you diagnose and get support for service problems that affect your Azure resources," distinguishing it from security posture management.

CertEmpire

## Question: 17

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

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

### Answer:

C

### Explanation:

Microsoft 365 Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items on endpoint devices. According to official Microsoft documentation, Endpoint DLP is supported on devices running Windows 10 (build 1809 or later), Windows 11, and macOS (Catalina 10.15 or later). Devices must be onboarded into the Microsoft Purview compliance portal to be managed by Endpoint DLP policies. While Microsoft provides DLP capabilities for mobile devices, it is through different mechanisms like App Protection Policies in Intune, not Endpoint DLP.

### Why Incorrect Options are Wrong:

- A. This is incorrect because Endpoint DLP also supports macOS, not just Windows operating systems.
- B. This is incorrect because Endpoint DLP does not support Android. It supports macOS instead.
- D. This is incorrect because Android is not a supported operating system for Endpoint DLP.

### References:

1. Microsoft. (2024). Get started with Endpoint data loss prevention. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/endpoint-dlp-getting-started#prerequisites>. (Refer to the "Prerequisites" section, which lists supported operating systems as "Windows 10, Windows 11, and macOS Catalina 10.15 and higher").
2. Microsoft. (2024). Learn about Microsoft Purview Data Loss Prevention. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/dlp-learn-about-dlp#dlp-on-endpoints>. (Refer to the "DLP on endpoints" section, which states, "You can apply DLP policies to Windows 10/11 and macOS devices").

## Question: 18

What is a function of Conditional Access session controls?

- A. prompting multi-factor authentication (MFA)
- B. enable limited experiences, such as blocking download of sensitive information
- C. enforcing device compliance
- D. enforcing client app compliance

### Answer:

B

### Explanation:

Conditional Access session controls are applied after a user has been granted access to an application. Their function is to enforce restrictions within the user's session. For example, by integrating with Microsoft Defender for Cloud Apps, session controls can enable limited experiences, such as monitoring user activity in real-time, blocking the download of sensitive documents, or requiring a document to be labeled before download. This allows organizations to permit access while still controlling what happens to their data after sign-in.

### Why Incorrect Options are Wrong:

CertEmpire

- A. Prompting for multi-factor authentication (MFA) is a grant control, a condition required to gain access, not a control applied within the session.
- C. Enforcing device compliance is a grant control. It checks if the device meets organizational policy requirements before allowing access.
- D. Enforcing client app compliance (requiring an approved client app) is a grant control, ensuring the user connects from a managed application.

### References:

1. Microsoft Learn. (2023). Conditional Access: Session. "Within a Conditional Access policy, administrators can make use of session controls to enable limited experiences within a cloud application." The document lists "Use Conditional Access App Control" which enables features like "Block download (preview)".
2. Microsoft Learn. (2023). Conditional Access: Grant. This document explicitly lists "Require multifactor authentication," "Require device to be marked as compliant," and "Require approved client app" as Grant controls, which are evaluated to determine if a user can be granted access.

## Question: 19

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.

Statements	Yes	No
Device identity can be stored in Azure AD.	<input type="radio"/>	<input type="radio"/>
A single system-assigned managed identity can be used by multiple Azure resources.	<input type="radio"/>	<input type="radio"/>
If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.	<input type="radio"/>	<input type="radio"/>

### Answer:

Yes

No

No

### Explanation:

Device identity can be stored in Azure AD.

CertEmpire

- Yes. Azure Active Directory (Azure AD) is an identity provider that stores and manages various identity objects, including users, groups, applications, and devices. Registering a device with Azure AD creates a device identity, which is used to authenticate the device and apply security policies.

A single system-assigned managed identity can be used by multiple Azure resources.

- No. A system-assigned managed identity is created as part of an Azure resource and is tied directly to its lifecycle. It can only be used by the specific resource for which it was enabled and cannot be shared. If the parent resource is deleted, the system-assigned identity is automatically deleted as well.

If you delete an Azure resource that has a user-assigned managed identity, the managed identity is deleted automatically.

- No. A user-assigned managed identity is a standalone Azure resource with a lifecycle independent of any resource it is assigned to. Deleting a resource that uses a user-assigned identity does not delete the identity itself. It must be deleted separately. This design allows a single user-assigned identity to be assigned to multiple resources.



## References:

Microsoft Documentation. (2023). What is a device identity? Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/devices/overview>.

Reference: The "Introduction" section explicitly states, "A device identity is an object in Azure Active Directory (Azure AD)."

Microsoft Documentation. (2023). What are managed identities for Azure resources? Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>.

Reference: Under the "Managed identity types" section, it clarifies: "System-assigned: ...This identity's lifecycle is directly tied to the Azure resource. If the resource is deleted, Azure automatically cleans up the identity for you." and "User-assigned: ...The identity's lifecycle is managed separately from the lifecycle of the Azure resources that use it."

Microsoft Documentation. (2023). Managed identities for Azure resources frequently asked questions (FAQ). Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq>.

Reference: The FAQ section confirms, "The system-assigned managed identity is deleted when the resource is deleted." In contrast, it explains that a user-assigned identity is an independent resource, implying its separate lifecycle management.

## Question: 20

What are two reasons to deploy multiple virtual networks instead of using just one virtual network? Each correct answer presents a complete solution. NOTE; Each correct selection is worth one point.

- A. to separate the resources for budgeting
- B. to meet Governance policies
- C. to isolate the resources
- D. to connect multiple types of resources

### Answer:

B, C

### Explanation:

Deploying multiple Azure Virtual Networks (VNets) is a fundamental strategy for network segmentation and security. The primary reason is to create isolated environments for different workloads. For instance, a company might use separate VNets for its production, development, and testing environments. This isolation prevents resources in one network from communicating with resources in another by default, limiting the potential impact of a security breach. This practice is also a core component of meeting governance and compliance requirements. Many security policies and regulatory standards mandate the separation of duties and environments, which is directly achieved by using multiple, isolated VNets to enforce network boundaries and control traffic flow between them.

### Why Incorrect Options are Wrong:

A. to separate the resources for budgeting

Budgeting and cost management in Azure are typically handled at the subscription, resource group, or through tagging resources, not by creating separate VNets.

D. to connect multiple types of resources

A single virtual network is designed to connect various types of Azure resources (like VMs, databases, and App Services) that need to communicate with each other.

---

### References:

1. Microsoft Learn, "What is Azure Virtual Network?" - Under the "Why use an Azure virtual network?" section, the concept of isolation is highlighted as a key benefit. The document states, "Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure... VNet provides an isolated environment for your virtual machines and other resources."
2. Microsoft Cloud Adoption Framework for Azure, "Security - Network segmentation strategies" -

This document explicitly links network segmentation using multiple VNets to governance and isolation. It states, "Network segmentation is a central part of enterprise security governance... By isolating workloads into their own virtual networks, you can limit the effect of a security compromise to that network."

3. Microsoft Learn, "Azure landing zones - Network topology and connectivity" - This official guidance on enterprise-scale architecture describes the hub-spoke model, which uses multiple VNets (spokes) to isolate individual workloads. This design is a direct implementation of governance policies for network security and management.

CertEmpire

## Question: 21

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

- A. auditing
- B. authorization
- C. authentication
- D. administration

### Answer:

A

### Explanation:

Auditing is the identity pillar concerned with tracking and logging user and system activities. It answers the questions of who did what, from where, and when. This process involves collecting data on which resources were accessed by a user, providing a trail for security analysis, compliance verification, and incident investigation. The core function of auditing is to create a record of actions, which directly aligns with tracking resource access.

### Why Incorrect Options are Wrong:

CertEmpire

- B. authorization: This pillar determines what an authenticated user is permitted to do or access. It is about granting permissions, not tracking the subsequent access.
- C. authentication: This is the process of verifying a user's identity by validating their credentials. It answers "who are you?" but does not track actions after verification.
- D. administration: This pillar involves the management of identities, including their creation, modification, and deletion, as well as the assignment of roles and policies.

### References:

1. Microsoft Learn, "Describe the concepts of identity - SC-900," Module 1, Unit 3. The documentation outlines the four pillars of identity. It defines Auditing as the process of tracking who accesses which resources and when.
2. Microsoft Learn, "Describe authentication and authorization." This document distinguishes between Authentication (AuthN), which is the process of proving you are who you say you are, and Authorization (AuthZ), which is the act of granting an authenticated party permission to do something. This clarifies that neither is about tracking access.
3. Microsoft Learn, "Microsoft Entra audit logs." This resource states, "Microsoft Entra audit logs provide records of system activities for compliance. To access the audit log, select Audit logs in the Monitoring section of Microsoft Entra ID. An audit log has a default list view that shows... the activity." This directly supports the definition of auditing as tracking activity.

## Question: 22

HOTSPOT Select the answer that correctly completes the sentence.

**Answer Area**

When users sign in,  verifies their credentials to prove their identity.

- administration
- auditing
- authentication
- authorization

### Answer:

authentication

### Explanation:

Authentication is the security process that verifies a user's identity by validating the credentials they provide, such as a username and password, a biometric scan, or a security token. This process confirms that the user is who they claim to be. In contrast, authorization occurs after successful authentication and determines what resources or actions the verified user is permitted to access. Auditing is the process of reviewing logs of user activities, and administration involves the overall management of the system. Therefore, verifying credentials to prove identity is the specific function of authentication.

CertEmpire

### References:

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. *Communications of the ACM*, 18(9), 61. (Reprint from *Proceedings of the IEEE*, 63(9), 1278-1308). In Section I.A.3, the authors distinguish between authentication ("verifying the identity of a user") and authorization ("the question of which user is authorized to do what"). DOI: <https://doi.org/10.1145/361011.361062>

National Institute of Standards and Technology (NIST). (2017). *Digital Identity Guidelines*. (NIST Special Publication 800-63-3). In Section 4.1, "Authentication," the document states: "Authentication is the process of verifying the identity of a subject (e.g., user, process, or device) as a prerequisite to allowing access to resources in an information system."

DOI: <https://doi.org/10.6028/NIST.SP.800-63-3>

Abowd, G. D., & Mynatt, E. D. (2000). Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7(1), 29-58. The paper discusses security fundamentals, defining authentication as the challenge of "determining and verifying the identity of a person or entity."

DOI: <https://doi.org/10.1145/344949.344988>

## Question: 23

What can be created in Active Directory Domain Services (AD DS)?

- A. line-of-business (LOB) applications that require modern authentication
- B. mobile devices
- C. computer accounts
- D. software as a service (SaaS) applications that require modern authentication

### Answer:

C

### Explanation:

Active Directory Domain Services (AD DS) is a directory service for on-premises Windows domain networks. A primary function of AD DS is to store information about network objects and make this information available to users and administrators. One of the fundamental object types that can be created and managed within AD DS is a computer account. When a computer joins a domain, a computer account object is created in the directory. This object is used to authenticate and authorize the computer on the network and to apply configuration settings through Group Policy.

CertEmpire

### Why Incorrect Options are Wrong:

- A. line-of-business (LOB) applications that require modern authentication: Modern authentication (e.g., OAuth 2.0, OpenID Connect) is a feature of cloud identity providers like Microsoft Entra ID, not traditional on-premises AD DS.
- B. mobile devices: Mobile devices are typically managed through Mobile Device Management (MDM) solutions, such as Microsoft Intune, rather than being created as native objects directly within AD DS.
- D. software as a service (SaaS) applications that require modern authentication: Integrating SaaS applications for single sign-on using modern authentication is a core capability of Microsoft Entra ID, not on-premises AD DS.

### References:

1. Microsoft Learn. (2023). Active Directory Domain Services Overview. "AD DS provides a distributed database that stores and manages information about network resources and application-specific data from directory-enabled applications... Data stored in AD DS includes information about user accounts... groups, computers, printers, and other network resources." Section: What Is Active Directory Domain Services?
2. Microsoft Learn. (2023). Computer Objects. "Computer objects in Active Directory are used to uniquely identify and manage computers that are members of a domain... When you join a

computer to a domain, a computer account is created in Active Directory."

Section: Computer Objects in Active Directory.

3. Microsoft Learn. (2024). Compare Active Directory to Microsoft Entra ID. "Active Directory Domain Services... Core services: Domain join for Windows PCs... Microsoft Entra ID... Core services: Authentication for web and mobile apps, including Microsoft 365."

Section: Compare features and services.

4. Microsoft Learn. (2024). What is application management with Microsoft Entra ID?. "Microsoft Entra ID is an identity and access management (IAM) system. It provides a single place to manage users and applications... You can manage access to thousands of SaaS applications..."

Section: What are the benefits of application management?

## Question: 24

HOTSPOT Select the answer that correctly completes the sentence.

**Answer Area**

provides cloud workload protection for Azure and hybrid cloud resources.

- Microsoft Defender for Cloud
- Azure Monitor
- Microsoft cloud security benchmark
- Microsoft Secure Score

### Answer:

Microsoft Defender for Cloud

### Explanation:

Microsoft Defender for Cloud is a comprehensive solution that provides unified security management and advanced threat protection across hybrid cloud workloads. It fulfills two primary objectives: Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP). The CWP capabilities are specifically designed to protect various resources such as servers, containers, storage, databases, and other workloads in Azure and on-premises environments from evolving threats by using advanced analytics and threat intelligence.

CertEmpire

- Azure Monitor is a service for collecting, analyzing, and acting on telemetry data for performance and availability, not primarily for workload threat protection.
- Microsoft cloud security benchmark is a framework of security recommendations, not a service that provides active protection.
- Microsoft Secure Score is a feature within Defender for Cloud that measures security posture; it doesn't provide the protection itself.

### References:

Microsoft Learn. "What is Microsoft Defender for Cloud?" Microsoft Docs. "Microsoft Defender for Cloud is a cloud security posture management (CSPM) and cloud workload protection (CWP) solution that finds weak spots across your cloud configuration... and can protect workloads across multicloud and hybrid environments from evolving threats."

Microsoft Learn. "Introduction to cloud workload protection in Microsoft Defender for Cloud."

Microsoft Docs. "Defender for Cloud's integrated cloud workload protection platform (CWPP), brings advanced, intelligent protection of your Azure and hybrid resources and workloads."

Microsoft Learn. "Azure Monitor overview." Microsoft Docs. "Azure Monitor helps you maximize the availability and performance of your applications and services. It delivers a comprehensive



solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments."

CertEmpire

## Question: 25

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

er Area	Statements	Yes	No
	An external email address can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
	A notification to the Microsoft Authenticator app can be used to authenticate self-service password reset (SSPR).	<input type="radio"/>	<input type="radio"/>
	To perform self-service password reset (SSPR), a user must already be signed in and authenticated to Azure AD.	<input type="radio"/>	<input type="radio"/>

### Answer:

Yes

Yes

No

CertEmpire

### Explanation:

Azure Active Directory (Azure AD) Self-Service Password Reset (SSPR) allows users to reset their passwords without administrator intervention by verifying their identity using pre-registered authentication methods. An alternate email address and a notification to the Microsoft Authenticator app are both officially supported methods for this verification process.

The fundamental purpose of SSPR is to provide a recovery mechanism for users who are unable to sign in, typically because they have forgotten their password. Therefore, the process is initiated from the sign-in screen before the user is authenticated, making the third statement false.

### References:

Microsoft Learn Azure Active Directory Documentation: In the article "Authentication methods for Azure AD self-service password reset," the list of available methods explicitly includes Email and Mobile app notification.

Source: Microsoft. (2023, September 15). Authentication methods for Azure AD self-service password reset. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-authentication-methods> (Section: "Authentication methods").

Microsoft Learn Azure Active Directory Documentation: The "How it works: Azure AD self-service password reset" article details the user workflow, which begins when a user selects a "Can't

access your account" link on the sign-in page. This confirms the user is not authenticated when initiating SSPR.

Source: Microsoft. (2023, September 15). How it works: Azure AD self-service password reset. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#how-does-the-password-reset-process-work> (Section: "How does the password reset process work?").

CertEmpire

## Question: 26

HOTSPOT Select the answer that correctly completes the sentence.

**Answer Area**

When you enable security defaults in Azure AD, \_\_\_\_\_ will be enabled for all Azure AD users.

### Answer:

multi-factor authentication (MFA)

### Explanation:

When you enable security defaults in Azure Active Directory (Azure AD), a baseline set of identity security policies is enforced across your organization. The most significant of these policies is the requirement for all users to register for multi-factor authentication (MFA). Security defaults also require administrators to perform MFA, block legacy authentication protocols, and prompt users for MFA when a risky sign-in is detected. Azure AD Privileged Identity Management (PIM) and Azure AD Identity Protection are more advanced features that require Azure AD Premium licenses and are not enabled by the basic security defaults.

CertEmpire

### References:

Microsoft Entra documentation: "What are security defaults?".

Reference: In the section "What do security defaults provide?", the first policy listed is "Requiring all users to register for Azure AD Multi-Factor Authentication." This confirms that MFA registration is a universal requirement for all users when security defaults are enabled. The document further clarifies that MFA will be required for administrators and for users during risky sign-ins.

Microsoft Entra documentation: "Azure AD Multi-Factor Authentication versions and consumption plans".

Reference: This document contrasts the MFA capabilities provided by different licenses. It specifies that "Security defaults" are available for the "Microsoft Entra ID Free" tier and provide MFA enforcement. In contrast, features like "Identity Protection" and "Privileged Identity Management (PIM)" are listed under the "Microsoft Entra ID P2" tier, confirming they are separate, premium offerings.

## Question: 27

HOTSPOT Select the answer that correctly completes the sentence.

Answer Area

Microsoft Sentinel provides quick insights into data by using

Azure Logic Apps.  
 Azure Logic Apps.  
 Azure Monitor workbook templates.  
 Azure Resource Graph Explorer.  
 playbooks.

### Answer:

Azure Monitor workbook templates

### Explanation:

Microsoft Sentinel utilizes Azure Monitor workbook templates to provide rich, interactive dashboards and visualizations. These workbooks are specifically designed to offer security analysts immediate insights into the data collected from various sources. They allow for the creation of charts, graphs, and tables that help in monitoring security events, hunting for threats, and understanding an organization's security posture at a glance. Playbooks, built on Azure Logic Apps, are used for automating responses to alerts, while Azure Resource Graph Explorer is for querying Azure resource metadata, not analyzing security log data for insights.

CertEmpire

### References:

Microsoft Learn Visualize and monitor your data with Microsoft Sentinel workbooks: "After you've connected your data sources to Microsoft Sentinel, you can visualize and monitor the data using the Microsoft Sentinel adoption of Azure Monitor Workbooks... Microsoft Sentinel allows you to create custom workbooks from your data, and also comes with built-in workbook templates to allow you to quickly gain insights across your data as soon as you connect a data source."

Microsoft Learn Automate threat response with playbooks in Microsoft Sentinel: "A playbook is a collection of procedures that can be run from Microsoft Sentinel in response to an alert. A playbook can help automate and orchestrate your response..." (This distinguishes playbooks as an automation/response tool, not an insight/visualization tool).

Microsoft Learn What is Azure Resource Graph?: "Azure Resource Graph is an Azure service designed to extend Azure Resource Management by providing efficient and performant resource exploration... Use the Azure Resource Graph Explorer to query your Azure resource types and properties." (This confirms its purpose is for querying resource metadata, not security data insights).

## Question: 28

HOTSPOT Select the answer that correctly completes the sentence.

Answer Area

Insider risk management is configured from the



### Answer:

Microsoft Purview compliance portal

### Explanation:

Insider risk management is a compliance solution within the Microsoft Purview suite designed to help organizations detect, investigate, and act on malicious and inadvertent risks from within the organization. The configuration of policies, review of alerts, and overall management of this feature is performed exclusively within the Microsoft Purview compliance portal. This portal centralizes data governance and compliance tools. The Microsoft 365 admin center is for general tenant management, while the Microsoft 365 Defender and Defender for Cloud Apps portals are focused on security threat protection and cloud app security, respectively, not compliance-centric insider risk policy configuration.

### References:

Microsoft. (2024). Get started with insider risk management. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/purview/insider-risk-management-get-started>.

Reference Point: In the section "Step 1 (required): Enable permissions for insider risk management," the first instruction states, "Go to the Microsoft Purview compliance portal..." confirming this as the starting point for configuration.

Microsoft. (2024). Learn about the Microsoft Purview compliance portal. Microsoft Learn. Retrieved from

<https://learn.microsoft.com/en-us/purview/microsoft-purview-compliance-portal-overview>.

Reference Point: The article includes a table titled "Solutions in the compliance portal," which explicitly lists Insider risk management as a solution available and managed within this portal.

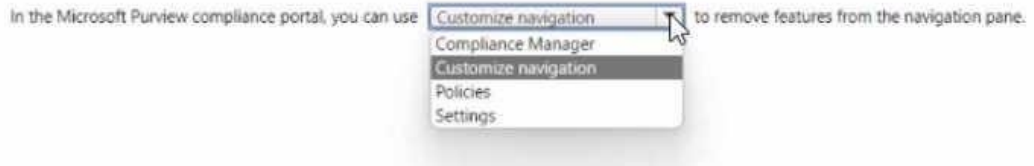
Microsoft. (2024). Microsoft 365 admin centers. Microsoft Learn. Retrieved from <https://learn.microsoft.com/en-us/microsoft-365/admin/manage/admin-centers?view=o365-worldwide>.

Reference Point: This document distinguishes between the portals, defining the Microsoft Purview compliance portal for "data protection and compliance" and the Microsoft 365 Defender portal for "security management," thereby differentiating their primary functions and confirming Purview as the correct location for a compliance tool.

## Question: 29

HOTSPOT Select the answer that correctly completes the sentence.

### Answer Area



### Answer:

Customize navigation

### Explanation:

In the Microsoft Purview compliance portal, the Customize navigation feature allows administrators to modify the left navigation pane. This functionality enables the hiding of features or solutions that an organization does not use, thereby simplifying the interface for users. Administrators can create custom navigation experiences and assign them to specific administrative roles, ensuring that users only see the tools relevant to their responsibilities. This helps streamline workflows and reduces clutter within the portal.

### References:

CertEmpire

Microsoft Learn. (2024). Customize the navigation pane in the Microsoft Purview portal. Microsoft Docs. Retrieved from the section "Customize the navigation pane," which states, "The global admin for your organization can customize the navigation pane in the Microsoft Purview portal for your organization."

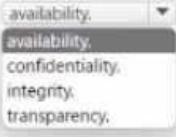
Microsoft Learn. (2024). Microsoft Purview compliance portal overview. Microsoft Docs. Retrieved from the section "Access the Microsoft Purview compliance portal," which describes the portal's layout and mentions the ability for customization to tailor the user experience.

## Question: 30

HOTSPOT Select the answer that correctly completes the sentence.

Answer Area

Ensuring that the data you retrieve is the same as the data you stored is an example of maintaining



### Answer:

integrity

### Explanation:

Integrity is the security principle that ensures data remains accurate, consistent, and trustworthy over its entire lifecycle. It guarantees that the data has not been subject to unauthorized modification, alteration, or destruction. The scenario described-retrieving the exact same data that was originally stored-is the fundamental definition of maintaining data integrity. In contrast, confidentiality prevents unauthorized disclosure, availability ensures data is accessible when needed, and transparency is not a core pillar of the foundational CIA security triad.

CertEmpire

### References:

National Institute of Standards and Technology (NIST). (2021). Glossary of Terms. Computer Security Resource Center.

Reference: Under the term "Integrity," the definition is provided as: "The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and in transit."

Saltzer, J. H., & Schroeder, M. D. (1975). The Protection of Information in Computer Systems. Communications of the ACM, 17(7), 38-49.

DOI: <https://doi.org/10.1145/361011.361062>

Reference: Section 1.A.2, "Integrity (preventing unauthorized modification of information)," clearly distinguishes integrity as the mechanism for ensuring information is not improperly altered.

Kaushik, S. (2012). Security, Privacy and Trust in Cloud Systems. IEEE.

DOI: <https://doi.org/10.1109/MCE.2012.2223594>

Reference: Section "Security," Paragraph 1, defines the three security goals: "Confidentiality, Integrity, and Availability (CIA). Integrity is the assurance that information is trustworthy and accurate."