

Microsoft.SC-900J.v2026-10-26.q101

試験コード：	SC-900J
試験名称：	Microsoft Security, Compliance, and Identity Fundamentals (SC-900日本語版)
認証ベンダー：	Microsoft
無料問題の数：	101
バージョン：	v2026-10-26
ページの閲覧量：	107
問題集の閲覧量：	1018
https://www.jpnsiken.com/shiken/Microsoft.SC-900J.v2026-10-26.q101.html	

質問: 1
文を正しく完成させる答えを選択してください。



正解:



Explanation:



Microsoft Purview Compliance Manager is designed to give organizations a continuous view of their compliance posture. In Microsoft's Security, Compliance, and Identity guidance, Compliance Manager is described as a capability that assesses your compliance posture against regulatory standards and data protection baselines and updates the compliance score as you implement or fail controls. The platform aggregates signals from assessments, controls, and improvement actions, then recalculates your compliance score as evidence is collected and actions are marked complete or tested. Because these evaluations are tied to live improvement actions and mapped controls (such as access, data protection, and governance controls), your organization's status isn't limited to a fixed reporting cycle; rather, it reflects ongoing progress and gaps across supported regulations and standards.

SCI study materials also emphasize that the score is not a one-time audit: it's a running indicator of risk reduction and control implementation. As you address recommendations, add or update evidence, or connect automated tests where available, the score and related dashboards refresh to show the latest compliance state. This makes Compliance Manager suitable for continuous assessment, enabling organizations to monitor posture, prioritize work, and demonstrate incremental improvements over time-hence, it assesses compliance data continually for an organization.

質問: 2

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	☐	☐
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	☐	☐
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	☐	☐

正解:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	☒	☐
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	☒	☐
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	☒	☐

Explanation:

Answer Area	Statements	Yes	No
	Azure Defender can detect vulnerabilities and threats for Azure Storage.	☒	☐
	Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	☒	☐
	Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	☒	☐

Box 1: Yes

Azure Defender provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more Box 2: Yes Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes

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

Reference:

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

質問: 3

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	☐	☐
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	☐	☐
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	☐	☐

正解:

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	☒	☐
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	☒	☐
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) Identity Protection can add users to groups based on the users' risk level.	☐	☒
Azure Active Directory (Azure AD) Identity Protection can detect whether user credentials were leaked to the public.	☒	☐
Azure Active Directory (Azure AD) Identity Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	☒	☐

Microsoft's Identity Protection provides risk-based detections and automated policies-not group management. Microsoft Learn explains that Identity Protection "uses detections to identify potential vulnerabilities affecting your organization's identities" and exposes user risk and sign-in risk for policy decisions. It does not support adding users to groups by "risk level"; group membership is handled by static or dynamic rules based on directory attributes, while risk is a transient signal surfaced to policies.

Identity Protection includes specific detections such as "Leaked credentials", where Microsoft's threat intelligence finds credentials "on the dark web or other dumps," and flags the affected account as risky. This directly confirms the ability to detect whether credentials have been exposed publicly.

For enforcement, Identity Protection policies and Conditional Access can require stronger authentication when risk is present. The documentation states that you can configure policies to "require multi-factor authentication for sign-ins assessed as risky" and use Conditional Access conditions like User risk or Sign-in risk with the grant control Require multi-factor authentication. Thus, Identity Protection signals can invoke MFA based on risk, but they do not place users into groups.

質問: 4

文を正しく完成させる答えを選択してください。

When using multi-factor authentication (MFA), a password is considered something you _____

are
have
know
share

正解:

When using multi-factor authentication (MFA), a password is considered something you _____

are
have
know
share

Explanation:

When using multi-factor authentication (MFA), a password is considered something you _____

are
have
know
share

In Microsoft's Security, Compliance, and Identity guidance, multi-factor authentication (MFA) is based on combining independent categories of credentials to verify a user. Microsoft describes the three factor types as:

something you know (knowledge), something you have (possession), and something you are (inherence). A password is explicitly categorized as "something you know," because it relies on a secret the user memorizes and types during sign-in. MFA improves security by requiring two or more of these distinct factors-e.g., a password (know) plus a phone approval or hardware token (have), or a biometric like Windows Hello (are). Using factors from different categories mitigates common attacks such as password spray, credential stuffing, and phishing, because compromising one factor (for example, the password) does not grant access without the second, unrelated factor. Microsoft recommends enabling MFA broadly and pairing passwords with stronger possession or inherence methods to achieve a measurable reduction in account compromise risk. Therefore, in the MFA model used by Microsoft Entra ID (Azure AD), a password is considered something you know.

質問: 5
文を正しく完成させる答えを選択してください。

Answer Area

▼

Archiving

Compressing

Deduplicating

Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key.



正解:

Answer Area

▼

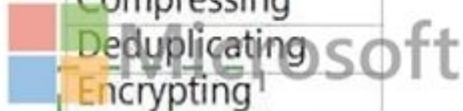
Archiving

Compressing

Deduplicating

Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key



Explanation:

Answer Area

▼

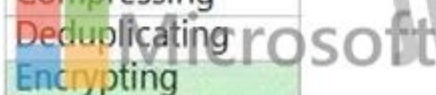
Archiving

Compressing

Deduplicating

Encrypting

a file makes the data in the file readable and usable to viewers that have the appropriate key



In Microsoft's Security, Compliance, and Identity guidance, encryption is described as the control that "converts data into a form that cannot be understood by anyone who does not possess the appropriate decryption key." In the Microsoft Purview Information Protection (sensitivity labels with encryption) documentation, Microsoft explains that when encryption is applied to a file, "only authorized users and services that present the correct keys and usage rights can open and use the content," and that access is enforced even if the file is moved outside the organization. Azure Rights Management (part of Microsoft Purview) further states that encryption "protects data at rest and in transit by using keys so that only permitted identities can decrypt and use the information." This aligns precisely with the sentence: encrypting a file makes the data readable and usable to viewers that have the appropriate key (and unreadable to those who do not). By contrast, archiving organizes or preserves data for long-term storage; compressing reduces file size without controlling

access; and deduplicating removes redundant copies to save space. None of these provide the key-based, identity-bound access control described in Microsoft SCI materials. Therefore, the correct completion is Encrypting.

質問: 6

文を正しく完成させる答えを選択してください。

In Azure Sentinel, you can automate common tasks by using

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

正解:

In Azure Sentinel, you can automate common tasks by using

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

Explanation:

In Azure Sentinel, you can automate common tasks by using

- deep investigation tools.
- hunting search-and-query tools.
- playbooks.
- workbooks.

In Microsoft Sentinel, automation is delivered through playbooks, which are built on Azure Logic Apps.

Microsoft's Sentinel documentation explains that playbooks "help automate and orchestrate your response to threats" and can be triggered by analytics alerts or incidents to run predefined actions. Typical automated tasks include "enriching alerts with data, blocking IP addresses, disabling users, or creating tickets," allowing security teams to standardize and speed up their response and remediation processes. Sentinel also uses automation rules to decide when a playbook should run (for example, on incident creation or update), enabling consistent handling of common SOC tasks. By contrast, the other options are not intended for automation: deep investigation tools are used to investigate incidents and entities; hunting search-and-query tools (built on KQL) are for proactive threat hunting rather than automating responses; and workbooks provide dashboards and visualizations for monitoring and reporting. Therefore, when the requirement is to automate common tasks-such as triggering actions across Microsoft 365 Defender, Azure, or third-party systems-the correct Sentinel capability is playbooks powered by Logic Apps. This aligns with the SCI guidance that emphasizes using Sentinel playbooks to "automate common workflows and response actions" and reduce manual effort while improving consistency and speed in security operations.

質問: 7

データ損失防止 (DLP) ポリシーを適用できる 3 つの場所はどれですか。それぞれの正解は完全なソリューションを示します。

注意: 正解ごとに 1 ポイントが付与されます。

- A. Microsoft Exchange Online メール
- B. Microsoft OneDrive アカウント
- C. Microsoft Exchange Online パブリック フォルダー
- D. Microsoft Teams のチャットとチャネル メッセージ
- E. Microsoft Viva Engage

正解: A,B,D (コメントを发表する)

Microsoft Purview Data Loss Prevention (DLP) defines supported service locations for policy enforcement. The Microsoft Learn/SCI materials state that DLP policies "help protect sensitive information across Microsoft 365 services" and can be scoped to common workloads. In the DLP overview, Microsoft explicitly lists the core cloud locations: "You can create DLP policies that protect content in Exchange Online, SharePoint Online, and OneDrive for Business." The Teams workload is also included: "DLP can monitor and take protective actions on Microsoft Teams chat and channel messages." These statements confirm that applying a DLP policy to Exchange Online email (A), OneDrive accounts (B), and Teams chat and channel messages (D) is supported. By contrast, Exchange Online public folders (C) are not listed among supported DLP locations in the SCI documentation, and Viva Engage (formerly Yammer) (E) is not a standard Microsoft Purview DLP location in the core list above (Viva Engage has separate governance and communication compliance controls). Therefore, from the supported locations enumerated in Microsoft's DLP guidance, the correct answers are Exchange Online email, OneDrive accounts, and Teams chat and channel messages.

質問: 8

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

eDiscovery (Standard) can be integrated with insider risk management.

eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders.

Yes

No

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

eDiscovery (Standard) can be integrated with insider risk management.

eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders.

Yes

No

Explanation:

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

eDiscovery (Standard) can be integrated with insider risk management.

eDiscovery (Standard) can be used to search Microsoft Exchange Online public folders.

Yes

No

In Microsoft Purview, eDiscovery (Standard) (formerly Core eDiscovery) provides case management, holds, searches, and export. Microsoft describes that eDiscovery (Standard) lets investigators "search across Microsoft 365 data sources and export the results," including options to export native files, email to PST, and CSV reports for further review. It uses the same Content search engine

and supports selecting locations such as **Exchange Online mailboxes, Microsoft 365 Groups, Teams, SharePoint sites, OneDrive accounts, and Exchange public folders," enabling organization-wide discovery that includes public folders.

Integration for end-to-end legal review from Microsoft Purview Insider Risk Management is specifically aligned to eDiscovery (Premium) (formerly Advanced eDiscovery). Insider Risk cases provide actions like

"Send to eDiscovery (Premium)" to create a review set and apply advanced processing, analytics, and review workflows. Those advanced integrations (review sets, analytics, legal hold communications) are not features of eDiscovery (Standard). Therefore: exporting results (Yes), Insider Risk integration (No, as it targets eDiscovery Premium), and searching Exchange Online public folders (Yes) are the correct evaluations based on the Microsoft Security, Compliance, and Identity study materials for Purview eDiscovery capabilities.

質問: 9

Azure Active Directory (Azure AD) ID保護を使用して実行できる3つのタスクはどれですか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. パートナー組織の外部アクセスを構成します。
- B. リスク検出をサードパーティのユーティリティにエクスポートします。
- C. IDベースのリスクの検出と修正を自動化します。
- D. ユーザー認証に関連するリスクを調査します。
- E. 機密ラベルを作成してデータに自動的に割り当てます。

正解: [\(正解を表示します\)](#)

Microsoft Entra ID Identity Protection is a risk-based conditional access capability that "automates the detection and remediation of identity-based risks" and enables admins to investigate risky users and sign-ins.

SCI guidance explains that Identity Protection evaluates signals such as user risk and sign-in risk, raises risk detections, and can automatically remediate by enforcing actions like password reset or blocking access via risk-based policies. The portal provides rich investigation experiences for risky users, risky sign-ins, and risk detections, allowing security teams to review evidence and confirm/dismiss risks. In addition, identity risk data can be exported through Azure Monitor/diagnostic settings and integrated with SIEM/SOAR tools, enabling "export of risk detections and security alerts to third-party solutions" for correlation and response.

Tasks such as configuring external access for partner organizations are handled by B2B collaboration features, and creating/assigning sensitivity labels belongs to Microsoft Purview Information Protection-not Identity Protection. Therefore, the tasks Identity Protection supports are: export risk detection (B), automate detection and remediation of identity-based risks (C), and investigate risks related to user authentication (D).

質問: 10

Microsoft 365コンプライアンスセンターの情報保護ソリューションを使用して何を保護できますか？

- A. ゼロデイエクспロイトによるコンピューター
- B. フィッシング詐欺のユーザー
- C. マルウェアとウイルスのファイル
- D. 機密データが許可されていないユーザーに公開されないようにする

正解: [D \(コメントを发表する\)](#)

Microsoft Purview Information Protection (in the Microsoft 365 compliance center) enables you to discover, classify, label, and protect sensitive information across emails, documents, and other data stores. Labels and policies can enforce encryption, access restrictions, and visual markings, helping prevent unauthorized disclosure of sensitive data-inside or outside your organization.

質問: 11

ソリューション カタログはどのポータルに含まれていますか？

- A. Microsoft 365 アプリ管理センター

- B. Microsoft 365 Defender ポータル
- C. Microsoft 365 管理センター
- D. Microsoft Purview コンプライアンス ポータル

正解: D (コメントを发表する)

In Microsoft's SCl materials, the Solutions catalog is described as part of the Microsoft Purview experience:
"The Microsoft Purview compliance portal is the home for solutions to manage your organization's data security and compliance needs." Within this portal, Microsoft states that "the Solutions catalog provides a single place to discover, learn about, and set up Microsoft Purview solutions." The catalog organizes capabilities across compliance domains, for example "Information Protection, Data Lifecycle Management, Data Loss Prevention, Insider Risk Management, eDiscovery, Audit, and Compliance Manager," and from the catalog "administrators can open setup guides and configuration wizards for each solution." This positioning makes the Purview compliance portal the correct portal when you are asked where the solution catalog lives.
By comparison, the Microsoft 365 admin center focuses on tenant administration and licensing, the Microsoft 365 Defender portal consolidates threat protection and security operations, and the Microsoft 365 Apps admin center targets Office app management and servicing. None of these are identified as the home of the Purview Solutions catalog. Therefore, the portal that contains the solution catalog is the Microsoft Purview compliance portal.

質問: 12

文を正しく完成させる答えを選択してください。



正解:



Explanation:

In Microsoft identity terminology, authentication is the step that proves who the user is when they attempt to sign in. Microsoft Learn defines it plainly: "Authentication is the process of proving the identity of a user, device, or service." By contrast, "Authorization is the process of determining what a user, device, or service can do." During sign-in to Microsoft Entra ID (formerly Azure AD), "the identity provider validates credentials and, upon successful authentication, issues tokens that applications use to grant access." Microsoft further explains the available methods: "Microsoft Entra ID supports multiple authentication methods, including passwords, multi-factor authentication, FIDO2 security keys, certificate-based authentication, and federated authentication." Auditing and administration are not the mechanisms that verify identity at sign-in. Auditing "records security- relevant events for investigation and compliance," while administration "refers to configuring and managing identities, access policies, and settings." Therefore, in the sentence "When users sign in, _____ verifies their credentials to prove their identity," the correct completion is authentication, because it is the control that validates the user's credentials and establishes identity before any authorization decisions are made.



質問: 13

条件付きアクセス セッション制御の機能とは何ですか？

- A. 多要素認証 (MFA) のプロンプト
- B. 機密情報のダウンロードをブロックするなど、限られたエクスペリエンスを有効にします
- C. デバイス コンプライアンスの適用
- D. クライアント アプリのコンプライアンスの適用

正解: (正解を表示します)

Conditional Access session controls enable user app access and sessions to be monitored and controlled in real time based on access and session policies. Based on this definition, the best answer for your question is B. enable limited experiences, such as blocking download of sensitive information.
<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session>

質問: 14

文を正しく完成させる答えを選択してください。

Answer Area

A user-assigned managed identity

A certificate

A service principal

A system-assigned managed identity

A user-assigned managed identity

is used when multiple Azure web apps must use the same identity.

Microsoft

正解:

Answer Area

A user-assigned managed identity

A certificate

A service principal

A system-assigned managed identity

A user-assigned managed identity

is used when multiple Azure web apps must use the same identity.

Microsoft

Explanation:

Answer Area

A user-assigned managed identity

is used when multiple Azure web apps must use the same identity.

Microsoft's identity guidance for Azure resources states there are two kinds of managed identities: system- assigned and user-assigned. The documentation describes that a system-assigned identity is scoped to a single resource and follows its lifecycle: "A system-assigned managed identity is created in Microsoft Entra ID and is tied to the lifecycle of that Azure service instance. When the resource is deleted, Azure automatically deletes the identity." By contrast, a user-assigned identity is reusable across resources: "A user-assigned managed identity is a standalone Azure resource... It can be assigned to one or more Azure service instances and is managed independently of the resources that use it." Because the scenario requires multiple Azure web apps to use the same identity, the only managed identity type that supports this sharing model is the user-assigned managed identity. This allows you to grant RBAC permissions once to the identity and then attach that same identity to several App Service instances, simplifying secretless access to Azure resources (Key Vault, Storage, SQL, etc.) and providing centralized lifecycle and rotation management. Certificates or generic service principals would reintroduce credential management, while a system-assigned identity cannot be shared across multiple apps. Therefore, a user- assigned managed identity is the correct choice.

質問: 15

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	☐	☐
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	☐	☐
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	☐	☐

正解:

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	☒	☐
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	☒	☐
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Azure Security Center.	☒	☐
The secure score in Azure Security Center can evaluate resources across multiple Azure subscriptions.	☒	☐
Enabling multi-factor authentication (MFA) increases an organization's secure score in Azure Security Center.	☒	☐

In Microsoft Defender for Cloud (formerly Azure Security Center), Secure score is defined as "a measurement of an organization's security posture; the higher the score, the lower the identified risk." Microsoft states that Defender for Cloud provides security recommendations that "help you harden your resources and increase your secure score." Among these recommendations is "Apply system updates" for virtual machines-Microsoft describes it as ensuring that "machines should have the latest security updates installed", and completing this action adds points to your secure score because it remediates a vulnerability class (missing patches).

Defender for Cloud also supports wide scope evaluation: you can "view and manage the secure score across subscriptions and management groups," allowing organizations with multiple Azure subscriptions to see an aggregated and per-scope score and track improvement actions consistently.

Identity protections are part of Defender for Cloud's recommendations as well. Under the Azure Security Benchmark controls, Defender for Cloud includes the recommendation that "MFA should be enabled on accounts with owner permissions on your subscription." Implementing this MFA control earns secure-score points because it mitigates high-impact identity risks.

Therefore, applying system updates (Yes), evaluating across multiple subscriptions (Yes), and enabling MFA (Yes) all increase or contribute to an organization's secure score in Azure Security Center/Defender for Cloud.

Azure Multi-Factor Authentication (MFA) で使用できる 3 つの認証方法はどれですか？それぞれの正解は完全な解決策を示します。注: 正しく選択するたびに 1 ポイントの価値があります。

- A. 電話
- B. テキスト メッセージ (SMS)
- C. 電子メールによる検証
- D. Microsoft Authenticator アプリ
- E. 秘密の質問

正解: ([正解を表示します](#))

Microsoft states that Azure AD Multi-Factor Authentication "adds a second form of verification" to sign-ins and supports multiple verification methods. The documented methods include Microsoft Authenticator app notifications or verification codes, text message (SMS) codes, and phone call verification. In Microsoft's description, users can approve a push notification in the Microsoft Authenticator app or enter a code from the app; they can receive a text message containing a verification code; or they can answer a phone call to complete the challenge. Email verification and security questions are not listed as supported MFA methods for Azure AD sign-ins and are not valid second factors in Azure AD MFA. Consequently, the correct methods from the options provided are Phone call, Text message (SMS), and Microsoft Authenticator app. These align with Azure AD's core MFA capabilities used in Conditional Access and per-user MFA to strengthen authentication beyond the password and to meet compliance and security requirements for strong user verification.

有効的な**SC-900J**問題集はJPNTTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-900J**試験問題集を提供します。JPNTTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

文を正しく完成させる答えを選択してください。

Answer Area

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

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

正解:

Answer Area

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

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

Explanation:

eDiscovery

In Microsoft Purview, eDiscovery is the purpose-built compliance solution for legal and investigative workflows. Microsoft's SCI materials describe eDiscovery as the tool that enables organizations to identify, preserve/hold, collect, review, and export potentially relevant content across Microsoft 365 services. Official guidance explains that eDiscovery (Standard) "provides search, hold, and export capabilities" for content in Exchange, SharePoint, OneDrive, Teams, and more. Another description states that eDiscovery (Premium) helps you "identify, preserve, collect, review, analyze, and export content" for legal matters and internal investigations. These capabilities are designed to support the eDiscovery lifecycle by allowing admins and case managers to: create cases, define custodians and non-custodial data sources, run targeted searches, apply legal holds to prevent data alteration or deletion, perform review and analytics, and export responsive data packages for counsel or regulators.

By contrast, Data Loss Prevention (DLP) protects sensitive information from accidental or inappropriate sharing; Customer Lockbox governs Microsoft engineer access to your data for support; and resource locks protect Azure resources from accidental deletion or modification. Therefore, the Microsoft SCI control that is explicitly used to identify, hold, and export electronic information for an investigation is Microsoft Purview eDiscovery.

質問: 18

特定の条件に基づいてコンテンツを自動的に暗号化するために使用できるMicrosoft365コンプライアンス機能はどれですか？

- A.** コンテンツ検索
- B.** 感度ラベル
- C.** 保持ポリシー
- D.** eDiscovery

正解: ([正解を表示します](#))

In Microsoft 365 compliance, sensitivity labels (Microsoft Purview Information Protection) are the feature designed to classify and automatically protect data. Microsoft states that sensitivity labels "let you classify and protect your organization's data" and that a label "can apply protection settings such as encryption" to files and emails. Labels can be deployed so that protection is applied without user action: Microsoft explains that labels "can be applied automatically, recommended, or by users," and that administrators can "auto-apply a sensitivity label to content in SharePoint, OneDrive, and Exchange based on conditions such as sensitive info types, keywords, or trainable classifiers." When a label with protection is applied, "encryption settings travel with the content" and enforce usage rights like who can open, print, or forward, even outside the organization.

By contrast, Content Search and eDiscovery are discovery/investigative tools and do not enforce protection.

Retention policies manage how long content is kept or deleted, but they don't encrypt content. Therefore, the Microsoft 365 compliance capability that encrypts content automatically based on specific conditions is sensitivity labels with auto-labeling policies in Microsoft Purview.

質問: 19

ユーザーがアクセスしたリソースの追跡に関連するアイデンティティの柱はどれですか？

- A.** 監査中
- B.** 認可
- C.** 認証
- D.** 管理

正解: ([正解を表示します](#))

Microsoft's identity model highlights four pillars: administration, authentication, authorization, and auditing.

In this model, auditing is the capability that records and reports identity-related activities, providing visibility into "who accessed what, when, from where, and how." SCI-aligned guidance explains that authentication verifies identity and authorization grants permissions, while auditing tracks and logs the resulting access to resources so organizations can investigate activity, satisfy compliance obligations, and detect anomalies.

Microsoft services such as Microsoft Entra ID (sign-in logs and audit logs), Access Reviews, Privileged Identity Management (PIM) reports, and Microsoft Purview Audit are explicitly positioned to capture user access events and administrative changes across cloud apps and services. This evidence enables security operations and compliance teams to monitor access patterns, prove regulatory adherence, and respond to incidents. Therefore, when the question focuses on tracking the resources accessed by a user, the pillar that directly addresses this requirement is auditing, not authentication (identity proof), authorization (permission assignment), or administration (lifecycle and configuration).

質問: 20

顧客のリストとそれに関連するクレジットカード番号を含む電子メールメッセージの送信をユーザーが制限するために使用できるMicrosoft365の機能はどれですか。

- A. 保持ポリシー
- B. データ損失防止 (DLP) ポリシー
- C. 条件付きアクセスポリシー
- D. 情報の障壁

正解: B ([コメントを發表する](#))

In Microsoft 365, Data Loss Prevention (DLP) policies are designed to "help you identify, monitor, and automatically protect sensitive information" across services such as Exchange Online, SharePoint Online, OneDrive, and Microsoft Teams. Microsoft's guidance explains that DLP uses sensitive information types- including built-in classifiers like Credit Card Number-to detect when content matches a defined pattern and then enforce protective actions. With DLP, you can create rules that trigger when email messages contain customer lists with credit card numbers, and choose actions to block the message, restrict access, or notify and educate users via policy tips and incident reports. Microsoft further notes that DLP "prevents the accidental sharing of sensitive information," can require user justification to override, and supports granular conditions (e.g., number of matches, recipients internal vs. external) to ensure that only risky transmissions are stopped. By applying a DLP policy to Exchange with the Credit Card Number sensitive info type, an organization can block or quarantine outbound mail that includes those numbers, thereby reducing regulatory and data- exposure risk. Other options listed-retention policies, conditional access, and information barriers-serve different purposes (data lifecycle, access/authentication conditions, and restricting communication between groups) and do not inspect message contents for sensitive data. Hence, DLP policies are the correct control to restrict sending emails that contain customer lists and associated credit card numbers.

質問: 21

従業員の履歴書であるドキュメントを識別するために、どのコンプライアンス機能を使用する必要がありますか？

- A. 事前にトレーニングされた分類器
- B. コンテンツエクスプローラー
- C. アクティビティエクスプローラー
- D. eDiscovery

正解: ([正解を表示します](#))

In Microsoft Purview Information Protection, pre-trained (Microsoft-provided) trainable classifiers are designed to automatically recognize specific categories of content by learning from examples rather than relying only on patterns or keywords. Microsoft's guidance explains that trainable classifiers "look for data by learning from examples," and that Microsoft supplies a catalog of "pre-trained classifiers that you can use immediately in your tenant." The documentation explicitly lists content types these classifiers can recognize, including "Resumes," along with other categories such as Source code, Threat and harassment, and more.

Because they're already trained by Microsoft, you can use them "to identify and classify items across SharePoint, OneDrive, and Exchange," and then take actions such as auto-labeling or enforcing DLP policies based on the classifier match.

By contrast, Content explorer is a reporting tool that lets you view where sensitive info types/labels were found; it doesn't identify resumes on its own. Activity explorer shows events like DLP policy matches over time. eDiscovery is used for legal hold, search, and review, not for semantic content identification. Therefore, to identify documents that are employee resumes, the correct Microsoft compliance feature is the pre-trained (Microsoft-provided) trainable classifier for Resumes.

質問: 22

ゼロトラストの指針となる原則を正確に説明している3つのステートメントはどれですか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. 物理的な場所で周囲を定義します。
- B. IDを主要なセキュリティ境界として使用します。

- C. 常にユーザーの権限を明示的に確認します。
- D. ユーザーシステムが侵害される可能性があることを常に想定してください。
- E. ネットワークを主要なセキュリティ境界として使用します。

正解: [\(正解を表示します\)](#)

Microsoft's Zero Trust guidance in the Security, Compliance, and Identity (SCI) materials frames three core principles: "Verify explicitly," "Use least-privilege access," and "Assume breach." The guidance explains that identity is the new control plane in cloud-based environments: identity becomes the primary security boundary, with access decisions evaluated continuously using signals such as user identity, device health, location, and risk. In Zero Trust, organizations must "verify explicitly"-that is, require strong authentication and explicit authorization for every access request, not just initial logon, and base decisions on the permissions and context presented. The model also directs organizations to "assume breach", operating with the expectation that an attacker may already be inside the environment and therefore applying containment practices such as micro-segmentation, telemetry, and rapid detection and response. Conversely, the traditional notion of defining the perimeter by physical locations or network boundaries is explicitly rejected; the documentation emphasizes that network location is no longer a reliable trust signal and should not be treated as the primary boundary. Therefore, the statements that align with Microsoft's Zero Trust principles are: Use identity as the primary security boundary (B), Always verify user permissions explicitly (C), and Always assume the user/system can be breached (D).

質問: 23

電子メール メッセージ、チャット メッセージ、チャンネルで送信される悪意のあるリンクから保護するには、何を使用できますか？

- A. Microsoft Defender for Identity
- B. エンドポイント向け Microsoft Defender
- C. クラウド アプリ向け Microsoft Defender
- D. Office 365 向け Microsoft Defender

正解: **D** ([コメントを発表する](#))

Microsoft Defender for Office 365 is the Microsoft 365 solution designed to protect users from threats delivered through email and collaboration workloads. SCI training material explains that Defender for Office

365 protects Exchange Online, Microsoft Teams, SharePoint Online, and OneDrive for Business by detecting and blocking malware, phishing, and other advanced attacks that use messages and shared content as the delivery channel.

A key capability is Safe Links, which specifically protects against malicious URLs. When a user receives an email, Teams chat message, or channel post that contains a hyperlink, Safe Links scans and rewrites that URL. At the moment the user clicks, the link is checked again; if it is identified as malicious or leads to a known phishing or malware-hosting site, access is blocked and a warning page is shown. This time-of-click protection is emphasized in Microsoft's security documentation as a primary defense against weaponized links in email and collaborative communications.

By comparison, Microsoft Defender for Identity focuses on detecting identity-related threats in on-premises Active Directory, Defender for Endpoint protects devices and endpoints, and Defender for Cloud Apps secures SaaS applications and shadow IT. None of these are the primary solution for blocking malicious links in email, chats, and channels. Therefore, the correct choice is Microsoft Defender for Office 365.

質問: 24

機械学習アルゴリズムを使用して機密項目を検出し、自動的に保護できる Microsoft Purview の機能は何ですか？

- A. 電子情報開示
- B. データ損失防止
- C. 情報リスク
- D. コミュニケーションコンプライアンス

正解: **B** ([コメントを発表する](#))

Microsoft Purview Data Loss Prevention (DLP) is designed to "detect and protect sensitive items" across Microsoft 365 locations, endpoints, and cloud apps. Microsoft explains that Purview DLP policies use sensitive information types, exact data match (EDM), and machine learning-based trainable classifiers to identify content, and then automatically apply protective actions such as

blocking or restricting sharing, notifying users with policy tips, auditing, or auto-quarantining/justifying activities. This fulfills the description "use machine learning algorithms to detect and automatically protect sensitive items." While eDiscovery focuses on legal hold and content discovery, and Communication compliance monitors communications for policy violations (ethics/regulatory scenarios), they are not positioned to broadly and automatically protect sensitive data across services. "Information risks" is not a distinct Purview solution category. Therefore, the Purview capability that leverages machine learning classifiers and automatically enforces protections on sensitive data is Data loss prevention (DLP).

質問: 25

文を正しく完成させる答えを選択してください。



正解:



Explanation:



In Microsoft's Security, Compliance, and Identity materials, Customer Lockbox is described as the feature that controls any Microsoft engineer access to your tenant content during support operations. Microsoft states that Customer Lockbox "ensures that Microsoft cannot access your content to perform a service operation without your explicit approval." It is specifically applicable to Microsoft 365 workloads that store customer data, including "Exchange Online, SharePoint Online, and OneDrive for Business." When a support case requires elevated access, "a lockbox request is created and routed to the customer for approval or rejection," and access is only granted if the organization's authorized admin approves the request within the defined window. The request contains who is requesting access, the reason, the scope, and the duration, and all actions are audited for compliance reporting. This capability aligns with Microsoft's zero standing access principles by making engineer access time-bound, least-privileged, and customer-approved. By contrast, Information barriers segregate communications between groups, Privileged Access Management (PAM) governs privileged tasks inside Microsoft 365, and Sensitivity labels classify and protect data. Therefore, the feature that "can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business" is Customer Lockbox.

質問: 26

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area**Microsoft****Statements**

Microsoft Sentinel uses logic apps to identify anomalies across resources.

Yes☐**No**☐

Microsoft Sentinel uses workbooks to correlate alerts into incidents.

☐☐

The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.

☐☐

正解:

Answer Area**Statements**

Microsoft Sentinel uses logic apps to identify anomalies across resources.

Yes☐**No**☒

Microsoft Sentinel uses workbooks to correlate alerts into incidents.

☐☒

The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.

☒☐

Explanation:

Answer Area**Microsoft****Statements**

Microsoft Sentinel uses logic apps to identify anomalies across resources.

Yes☐**No**☒

Microsoft Sentinel uses workbooks to correlate alerts into incidents.

☐☒

The hunting search-and-query tools of Microsoft Sentinel are based on the MITRE ATT&CK framework.

☒☐

In Microsoft Sentinel, Logic Apps are used as playbooks for automation and orchestration (SOAR)-to take actions after alerts/incidents occur (notify, enrich, remediate). They are not the component that detects or identifies anomalies; detections come from analytics rules, UEBA (user and entity behavior analytics), Fusion (ML-powered correlation), and anomaly rules. Workbooks are interactive dashboards and visualizations for monitoring and reporting; they don't correlate alerts. Correlation of alerts into incidents is handled by analytics rules (including alert grouping and Fusion) within Sentinel's detection pipeline. Finally, Sentinel's Hunting experience provides KQL-based queries and templates that are mapped to the MITRE ATT & CK tactics/techniques, enabling analysts to explore threats in a framework-aligned way. Thus, automation via Logic Apps # anomaly detection; Workbooks # incident correlation; Hunting tooling does align to MITRE ATT & CK.

質問: 27

リソースをクラウドに移動する予定です。

サービスとしてのインフラストラクチャ (IaaS) の使用を評価している、

サービスとしてのプラットフォーム (PaaS) およびサービスとしてのソフトウェア (SaaS) クラウド モデル。
クラウドベースのアプリのデータ、ユーザー アカウント、およびユーザー デバイスのみを管理する予定です。
どのクラウド モデルを使用しますか？

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

正解: [\(正解を表示します\)](#)

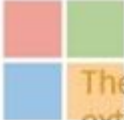
In Microsoft's cloud responsibility model, Software as a Service (SaaS) is the offering where the cloud provider operates the full application stack and the customer's responsibility is limited to data and access.

Microsoft's guidance explains that with SaaS, the provider manages the application, runtime, middleware, operating system, virtualization, servers, storage, and networking, while customers focus on "information and identities" and how users access the app. This aligns with your requirement to "manage only the data, user accounts, and user devices" for a cloud-based app. In contrast, PaaS still leaves you responsible for the application and data, and IaaS shifts even more components (OS, middleware, and apps) to you. Microsoft's shared responsibility descriptions consistently note that SaaS is chosen when organizations want to reduce operational overhead and concentrate on securing and governing their data and identities, leveraging provider controls for platform and infrastructure. Therefore, to meet the scenario of managing only data, user accounts, and devices while the provider runs the rest, SaaS is the correct cloud model.

質問: 28

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer 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.	☐	☐

正解:

Answer 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.	☐	☒

Explanation:

Answer 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.	☐	☒

Microsoft's Zero Trust guidance defines three core principles: "Verify explicitly, use least-privileged access, and assume breach." In Microsoft's SCI learning content and Zero Trust overview, the model is described as one that "treats every access attempt as though it originates from an open, untrusted network" and therefore requires explicit verification using all available signals (identity, device health, location, data sensitivity, and anomalies). This directly confirms the first statement as true: Verify explicitly is a guiding principle.

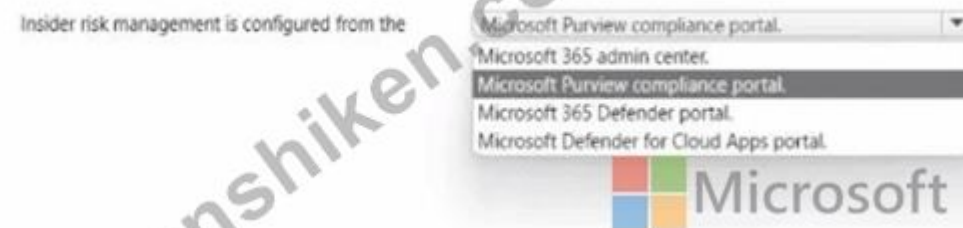
The same guidance states organizations must "assume breach"-designing controls so that if an attacker is already inside, blast radius is minimized through segmentation, Just-In-Time/Just-Enough-Access, continuous monitoring, and rapid detection and response. Microsoft's Zero Trust materials repeatedly explain to "assume attackers are present" and to "contain and remediate" through defense-in-depth controls, which validates the second statement as true.

Finally, Zero Trust rejects perimeter-based implicit trust. Microsoft clarifies that the model does not rely on a trusted internal network protected by a firewall; instead it "never trusts, always verifies," continuously enforcing policy regardless of network location (on-premises or internet). Therefore, the statement that Zero Trust assumes a firewall secures the internal network from external threats is false because Zero Trust presumes no inherent safety from being "inside" the network and requires continuous verification and least- privileged access everywhere.

質問: 29

HOTSPOT 文を正しく完成させる答えを選択してください。

Answer Area



正解:

Answer Area



In Microsoft's SCI guidance, Insider risk management is a Microsoft Purview capability surfaced and administered from the Microsoft Purview compliance portal. The official description states that Insider risk management "helps you minimize internal risks by enabling you to detect, investigate, and act on risky activities in your organization." Microsoft further clarifies access and configuration by directing admins to

"use the Microsoft Purview compliance portal to configure and manage insider risk policies, alerts, and investigations," and that you can "go to the Microsoft Purview compliance portal and select Insider risk management" to start. These statements place the feature squarely in the compliance plane-not the Microsoft

365 admin center (tenant-wide service management), not the Microsoft 365 Defender portal (threat protection and incident response), and not Microsoft Defender for Cloud Apps (app discovery and cloud app protection).

In the SCI learning path, Insider risk is consistently grouped with Microsoft Purview solutions (Information Protection, DLP, eDiscovery, and Audit), emphasizing compliance workflows, risk indicators, policy tuning, and case management. Therefore, the correct completion of the sentence "Insider risk management is configured from the" is the Microsoft Purview compliance portal, where administrators create policies, review alerts, investigate user activity timelines, and take appropriate remediation actions within a compliance- centric experience.

質問: 30
文を正しく完成させる答えを選択してください。

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.

正解:

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.

Explanation:

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.

In Microsoft's Security, Compliance, and Identity portfolio, Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) integrates directly with Microsoft Entra Conditional Access to provide Conditional Access App Control-Microsoft's real-time session control. Microsoft's documentation describes this capability as enabling organizations to "monitor and control user sessions in real time" and to "protect downloads, restrict uploads, block copy/paste and print, and apply access or session policies" for sanctioned and unsanctioned applications. The enforcement is achieved through a reverse-proxy session that is invoked by Conditional Access policy decisions, allowing continuous inspection and dynamic controls after authentication. By contrast, other options in the list do not offer real-time session enforcement via Conditional Access. Azure AD Privileged Identity Management (PIM) focuses on just-in-time role activation, approval workflows, and access reviews for privileged accounts-not session control of app usage. Microsoft Defender for Cloud provides cloud security posture management and workload protection across Azure, multicloud, and hybrid resources-again, not Conditional Access-based user session governance. Microsoft Sentinel is a SIEM /SOAR solution used for ingestion, detection, investigation, and response; it does not apply Conditional Access policies to control user sessions. Therefore, the service that can use Conditional Access policies to control sessions in real time is Microsoft Defender for Cloud Apps through Conditional Access App Control.

質問: 31
文を正しく完成させる答えを選択してください。

Microsoft

A domain controller
Active Directory Domain Services (AD DS)
Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

正解:

Microsoft

A domain controller
Active Directory Domain Services (AD DS)
Azure Active Directory (Azure AD) Privilege Identity Management (PIM)
Federation

provides single sign-on (SSO) capabilities across multiple identity providers.

有効的な**SC-900J**問題集はJPNTTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-900J**試験問題集を提供します。JPNTTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 32

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Microsoft

Statements

Yes

No

Compliance Manager tracks only customer-managed controls.	☐	☐
Compliance Manager provides predefined templates for creating assessments.	☐	☐
Compliance Manager can help you assess whether data adheres to specific data protection standards.	☐	☐

正解:

Answer Area

Microsoft

Statements

Yes

No

Compliance Manager tracks only customer-managed controls.	☐	☒
Compliance Manager provides predefined templates for creating assessments.	☒	☐
Compliance Manager can help you assess whether data adheres to specific data protection standards.	☐	☒

Explanation:

Compliance Manager tracks only customer-managed controls. No

Compliance Manager provides predefined templates for creating assessments. Yes Compliance Manager can help you assess whether data adheres to specific data protection standards. No

Microsoft Purview Compliance Manager is described as a feature that "helps you manage your organization's compliance requirements" by giving you assessments, improvement actions, and a compliance score that

"measures your progress in completing recommended actions" aligned to regulations and standards. The service does not track only customer-managed controls; Microsoft's documentation clarifies that Compliance Manager includes "Microsoft-managed controls and customer-managed controls," and it tracks both within each assessment to show overall posture. It also provides prebuilt (predefined) assessment templates for common regulations and industry standards so organizations can "create assessments from templates" such as GDPR, ISO/IEC 27001, and the Data Protection Baseline.

Importantly, Compliance Manager evaluates control implementation and improvement actions mapped to requirements; it does not scan or classify individual data to determine whether specific data items "adhere" to a standard. Instead, it helps you assess organizational compliance posture by tracking the status of controls, assigning actions, and recording evidence. Thus:

- * "Tracks only customer-managed controls" # No (it tracks Microsoft-managed and customer-managed).
- * "Provides predefined templates for creating assessments" # Yes (prebuilt templates are a core feature).
- * "Helps you assess whether data adheres to specific data protection standards" # No (it measures control /compliance posture, not data-level adherence).

Box 1: No

Compliance Manager tracks Microsoft managed controls, customer-managed controls, and shared controls.

Box 2: Yes

Box 3: Yes

Reference:

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

質問: 33

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	☐	☐
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	☐	☐
Azure DDoS Protection Standard protects against protocol attacks.	☐	☐



正解:

Answer Area

Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	☐	☒
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	☐	☒
Azure DDoS Protection Standard protects against protocol attacks.	☒	☐

Explanation:

Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks. = No Azure DDoS Protection Standard is enabled by default in an Azure subscription. = No Azure DDoS Protection Standard protects against protocol attacks. = Yes Microsoft's security guidance for Azure states that DDoS Protection is designed to defend internet-facing resources from distributed denial-of-service events at the network and transport layers (L3/L4). The documentation explains that DDoS Protection Standard provides "adaptive, real-time tuning and automatic attack mitigation for volumetric and protocol attacks (for example, SYN/ACK floods, UDP amplification, and other L3/L4 patterns)." It further clarifies that DDoS Protection is not intended to address attacks like man-in-the-middle (MITM), which are interception/alteration threats rather than traffic-exhaustion scenarios.

Regarding enablement, Microsoft notes that Azure DDoS Protection Standard is not enabled by default. The platform provides "basic DDoS protection for all Azure public IP addresses," but the Standard plan must be explicitly enabled on a virtual network and then applied to public IP resources in that VNet to gain its enhanced telemetry, mitigation policies, and cost-protection benefits. Putting this together: (1) MITM is out of scope for DDoS Protection Standard # No; (2) Standard is opt-in, not automatic # No; (3) Protection against protocol attacks is a primary capability of the Standard plan # Yes.

質問: 34

条件付きアクセス信号のタイプを適切な定義と一致させます。

答えるには、適切な条件付きアクセス信号の種類を左側の列から右側の定義にドラッグします。各信号タイプは、1 回使用することも、複数回使用することも、まったく使用しないこともできます。

注: 正しく一致するたびに 1 ポイントの価値があります。

Conditional access signals	Answer Area
Device	<input type="text"/>
Location	<input type="text"/>
Sign-in risk	<input type="text"/>
User risk	<input type="text"/>

The probability that an identity or account is compromised.

The probability that an authentication request isn't authorized by the identity owner.

Microsoft

正解:



Explanation:



In Microsoft Entra ID Protection, risk-based Conditional Access policies use signals such as User risk and Sign-in risk to evaluate potential threats during authentication and identity usage. These are core to adaptive access and identity protection features taught in Microsoft's SC-300 and SC-900 learning paths.

User risk:

Defined by Microsoft as: "The probability that a specific identity or account is compromised." User risk is assessed based on activities and behaviors that indicate the account may have been compromised-such as leaked credentials or atypical user activity over time.

Sign-in risk:

Defined as: "The probability that the authentication request is not performed by the legitimate identity owner." Sign-in risk is calculated at the time of authentication based on indicators such as unfamiliar locations, anonymous IP addresses, impossible travel, or malware-linked sign-ins.

These signals help automate access decisions, such as requiring MFA or blocking access, based on real-time risk assessments.

質問: 35

Azure AD 多要素認証 (MFA) を有効にする場合、認証にはいくつかの要素が必要ですか？

- A. 1
- B. 2
- C. 3
- D. 4

正解: ([正解を表示します](#))

In Microsoft's Security, Compliance, and Identity (SCI) learning content, Multi-Factor Authentication (MFA) is defined as requiring more than one verification method during sign-in. Microsoft states: "Multi-factor authentication (MFA) requires two or more verification methods" and Azure AD (Microsoft Entra ID) MFA

"works by requiring two or more of the following: something you know (password), something you have (trusted device or token), something you are (biometrics)." The SCI fundamentals also explain that MFA strengthens authentication beyond a single password by combining distinct factor types, noting that "strong authentication uses at least two different factors to verify identity." When you enable Azure AD MFA, a user must successfully present two factors from those categories to complete the authentication-commonly a password (something you know) plus a second factor such as Microsoft Authenticator approval, a FIDO2 security key, SMS/voice code, or Windows Hello (something you have/are). This is the core of Azure AD's risk-based and conditional access controls, which can require MFA based on conditions or risk signals. Therefore, the number of factors required after enabling Azure AD MFA is two, aligning with Microsoft's definition and implementation of multi-factor authentication in Entra ID.

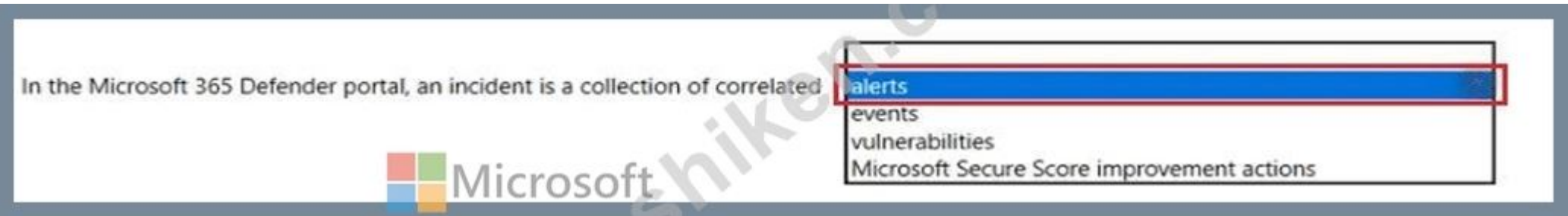
質問: 36
文を正しく完成させる答えを選択してください。



正解:



Explanation:



In Microsoft 365 Defender, security signals from across Microsoft 365 services are raised as alerts. Microsoft's documentation defines an incident as "a collection of correlated alerts" that represent the end-to-end story of an attack. The incident object aggregates the related signals, entities, and evidence so analysts can triage and remediate holistically rather than handling individual alerts in isolation. Microsoft further explains that incidents "group together related alerts, assets, users, and evidence" to reduce noise and provide context for investigation, and that automated correlation "helps SOCs focus on what matters most" by stitching alerts from Defender for Endpoint, Defender for Office 365, Defender for Identity, and Microsoft Defender for Cloud Apps into one case. Within an incident, analysts see a timeline, impacted assets and users, alert details, and recommended actions, and they can trigger response measures (for example, isolate device, block URL /file, or disable user). This contrasts with events (raw telemetry), vulnerabilities (exposure findings managed by Defender Vulnerability Management), and Microsoft Secure Score improvement actions (posture recommendations). Therefore, in the Microsoft 365 Defender portal, an incident is specifically a collection of correlated alerts, designed to streamline investigation and coordinated remediation across the Microsoft 365 security stack.

質問: 37
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	☐	☐
Network security groups (NSGs) can deny outbound traffic to the internet.	☐	☐
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	☐	☐

正解:

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	☐	☐
Network security groups (NSGs) can deny outbound traffic to the internet.	☐	☐
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	☐	☐

Explanation:

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	☐	☐
Network security groups (NSGs) can deny outbound traffic to the internet.	☐	☐
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	☐	☐

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

質問: 38

eDiscovery 保留に保存されているコンテンツを検索およびエクスポートするには何を作成する必要がありますか?

- A. Microsoft SharePoint Online サイト
- B. ケース
- C. Microsoft Exchange Online パブリック フォルダ
- D. Azure ファイル

正解: B ([コメントを发表する](#))

In Microsoft Purview eDiscovery, to search, preserve, analyze, and export content, you must first create a case. A case acts as a container for all eDiscovery activities, including placing users and content locations on litigation hold, running content searches, and exporting results for legal or compliance review.

SCI Extract: " Cases are used in Microsoft Purview eDiscovery (Standard and Premium) to manage, organize, and execute the various tasks associated with identifying and delivering content during an investigation or litigation. "

質問: 39

文を正しく完成させる答えを選択してください。



正解:



Explanation:

access and application control

In Microsoft Defender for Cloud, the capabilities grouped as access and application control are designed to harden Azure virtual machines by limiting both what can access a VM and what can run on it. Microsoft's documentation explains that Adaptive application controls "help you control which applications can run on your VMs by allowing only known-safe applications," which directly helps block malware and other unwanted applications. In the same family, Just-in-time (JIT) VM access "reduces exposure to attacks by locking down inbound traffic to your VMs and opening only the required ports, for approved users, for a limited time," thereby reducing the network attack surface. These capabilities are surfaced in Defender for Cloud recommendations and policies to enforce least privilege at the network edge and on the endpoint execution layer.

By contrast, Cloud Security Posture Management (CSPM) provides continuous assessment and secure-score- driven recommendations but isn't the control that actively blocks applications or time-bounds inbound access.

Container security targets container images and runtimes, and vulnerability assessment identifies software vulnerabilities but doesn't enforce allow-listing or time-bound access. Therefore, the correct completion is access and application control, which encompasses Adaptive application controls and JIT VM access to protect VMs from unwanted apps and minimize exposed network surface.

質問: 40

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☐	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☐
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	☐	☐

正解:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	☒	☐

Explanation:

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Hybrid identity refers to the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	☒	☐

Microsoft defines hybrid identity as enabling a common identity across on-premises and cloud by integrating your directory services. Microsoft Learn states: "Hybrid identity is achieved by integrating your on-premises Active Directory with Azure Active Directory." This integration is delivered through the synchronization and optional federation capabilities that connect AD DS to Azure AD so users can access both on-premises and cloud resources with one identity.

To implement this integration, Microsoft's tooling is explicit: "Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals." Azure AD Connect (now Microsoft Entra Connect) synchronizes users, groups, and optionally passwords or hashes to Azure AD, providing the foundation for hybrid scenarios such as single sign-on and seamless sign-in.

Regarding tenants, Microsoft's identity platform clarifies that "A Microsoft 365 organization is associated with a single Azure AD tenant." Therefore, a hybrid identity deployment does not require two Microsoft 365 tenants; it typically links a single Azure AD (Microsoft Entra ID) tenant with one or more on-premises AD DS forests. In summary, Azure AD Connect enables hybrid identity, hybrid identity is the synchronization

/integration of AD DS with Azure AD, and it does not necessitate multiple Microsoft 365 tenants.

質問: 41

文を正しく完成させる答えを選択してください。



正解:



Explanation:

Azure AD Identity Protection (now part of Microsoft Entra ID) is the Microsoft service that "automates the detection and remediation of identity-based risks." It continuously evaluates user risk and sign-in risk using signals such as leaked credentials, atypical travel, unfamiliar sign-in properties, and malware-linked IPs.

Microsoft documentation clarifies that Identity Protection "uses adaptive machine learning and heuristics to detect risky behaviors and sign-ins" and enables administrators to configure risk-based policies (for example, require MFA or block access) to automatically respond. It also provides rich investigations through risk reports so security teams can triage and remediate compromised identities. This distinctly differs from other Entra capabilities: Privileged Identity Management (PIM) governs just-in-time privileged access and role activation, while MFA is an authentication method enforced by policies. Because the service that specifically detects risk and applies automated protection based on risk is Azure AD Identity Protection, it is the correct completion for the sentence about identity risk detection and remediation.

質問: 42

文を正しく完成させる答えを選択してください。



正解:



Explanation:

authorization

In the context of Microsoft identity and access management, when users attempt to access an application or a service, authorization is what controls their level of access. This concept is clearly defined in Microsoft's Security, Compliance, and Identity (SCI) learning paths, particularly in SC-900 and SC-300 certifications.

From Microsoft SCI training materials:

"Authentication is the process of verifying the identity of a user, while authorization is the process of determining what resources a user can access and what actions they are permitted to perform."

In more detail:

Authentication confirms who you are (e.g., verifying credentials through Azure AD, MFA).

Authorization decides what you can do (e.g., access to files, roles, permissions in an app or service).

SCI documentation explains:

"Once authentication is successful, authorization policies are applied to determine whether the authenticated user is allowed to access the requested resource and at what level." This principle is implemented using role-based access control (RBAC) in Microsoft Azure and Microsoft 365 environments. For example, even if a user successfully logs into the Microsoft 365 portal (authentication), their ability to manage Exchange Online settings or view compliance data depends on their assigned roles (authorization).

質問: 43

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	☐	☐
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	☐	☐
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	☐	☐

正解:

Statements	Yes	No
Security defaults require an Azure Active Directory (Azure AD) Premium license.	☐	☒
Security defaults can be enabled for a single Azure Active Directory (Azure AD) user.	☐	☒
When Security defaults are enabled, all administrators must use multi-factor authentication (MFA).	☒	☐

Explanation:

Security defaults require an Azure Active Directory (Azure AD) Premium license. No Security defaults can be enabled for a single Azure Active Directory (Azure AD) user. No When Security defaults are enabled, all administrators must use multi-factor authentication (MFA). Yes Microsoft explains that Security defaults are baseline identity protections that are "available to all tenants at no additional cost" and are intended to "help protect your organization from common identity-related attacks." They are a tenant-wide setting: Microsoft states that security defaults are "either on or off for the entire tenant" and "can't be customized or targeted to specific users or groups." If you require per-user or granular targeting, Microsoft directs customers to use Conditional Access policies instead.

A core behavior of security defaults is enforcing MFA: "All users are required to register for Azure AD Multi- Factor Authentication," and "administrators are required to perform MFA." In addition, security defaults

"block legacy authentication" and apply other baseline requirements, but they do not enable premium features such as Azure AD Identity Protection or PIM. Summarizing the implications for the statements: no premium license is required; you cannot enable security defaults for just one user because the control is global; and when enabled, administrators must use MFA, with Microsoft recommending exclusion only for a break-glass account if necessary.

質問: 44

データ保護と規制基準に関連するリスクを軽減するのに役立つアクションの完了における組織の進捗状況を測定するスコアはどれですか？

- A. MicrosoftSecureスコア
- B. Productivity スコア
- C. Azure SecurityCenterでスコアを保護する
- D. コンプライアンススコア

正解: ([正解を表示します](#))

The Compliance score in Microsoft Purview Compliance Manager is a measurement tool that evaluates an organization's progress toward meeting data protection and regulatory compliance requirements. It is specifically designed to help organizations reduce risks related to data governance, privacy, and compliance with various standards such as GDPR, ISO 27001, NIST 800-53, and Microsoft Data Protection Baselines.

According to Microsoft's official documentation on Compliance Manager, the Compliance score "helps organizations track, improve, and demonstrate their compliance posture by providing a quantifiable measure of compliance with regulations and standards." Each action within Compliance Manager contributes a certain number of points to the overall score. These points are weighted based on risk, meaning that actions with a greater impact on reducing compliance risk contribute more significantly to the total score.

The score is not an absolute measure of legal compliance but rather an indicator of progress toward implementing recommended controls and risk-reducing actions. Microsoft emphasizes that Compliance score

"assists organizations in identifying areas of improvement, prioritizing compliance tasks, and maintaining an auditable record of their compliance activities." By contrast, Microsoft Secure Score measures security posture related to identity, device, and application protection, while Productivity Score evaluates collaboration and technology experience. Thus, the metric that specifically assesses data protection and regulatory compliance progress is the Compliance score in Microsoft Purview Compliance Manager.

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>

質問: 45

Azure サブスクリプションの全体的なセキュリティの正常性を表示する Microsoft Defender for Cloud メトリックはどれですか？

- A. リソースの状態
- B. セキュア スコア
- C. レコメンデーションのステータス
- D. 完了したコントロール

正解: ([正解を表示します](#))

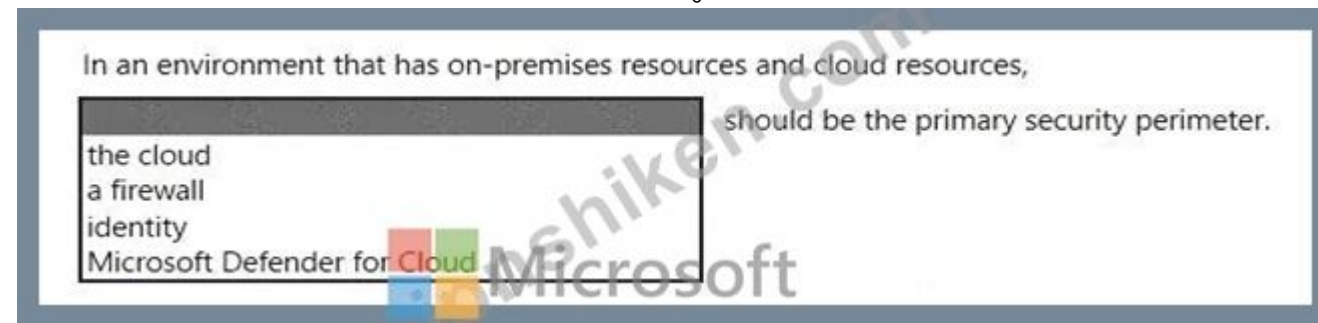
In Microsoft Defender for Cloud, the metric that represents the overall security health of your Azure subscription is secure score. Microsoft's documentation explains: "Secure score provides an aggregated view of your security posture across your subscriptions and resources. It's based on security recommendations; addressing those recommendations improves your score." Defender for Cloud calculates secure score by assessing controls and recommendations mapped to standards, then weighting them by risk and importance:

"Each recommendation contributes to the secure score. Completing remediation steps increases the score and reduces risk." This single percentage view lets security teams quickly gauge how well current configurations and protections align with Microsoft's security best practices and regulatory mappings. Other elements surfaced in Defender for Cloud-like "resource health," "status of recommendations," or "completed controls"

-are components and statuses that feed into or relate to the scoring model, but the overall subscription security health indicator presented and tracked over time is secure score.

質問: 46

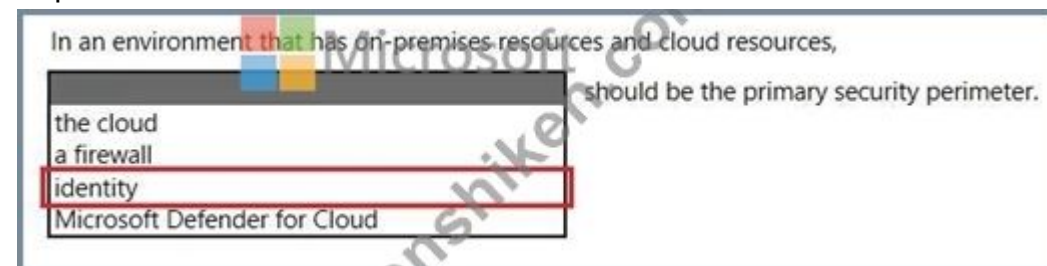
文を正しく完成させる答えを選択してください。



正解:



Explanation:



Microsoft's security guidance for hybrid and cloud environments adopts the Zero Trust approach, which explicitly positions identity as the primary boundary for access decisions. Microsoft states that in modern, distributed environments, "the traditional network perimeter is no longer sufficient" and that identity becomes the new security perimeter for protecting access to resources across on-premises and cloud. In Zero Trust, access is granted based on who the user or workload is, the risk of the sign-in, the device health, and the context of the session. Microsoft summarizes this shift as: "Identity is the control plane," emphasizing that authentication, authorization, and continuous evaluation of trust are enforced through identity-centric controls such as Conditional Access, multifactor authentication, Privileged Identity Management, device compliance, and session controls.

While tools like firewalls and services such as Microsoft Defender for Cloud remain important layers in a defense-in-depth strategy, they are not the primary perimeter in a hybrid model. Because users, devices, and applications operate from anywhere, identity is the consistent, verifiable layer through which policy is enforced for both on-premises and cloud resources. Therefore, in an environment that spans on-premises and cloud, Microsoft recommends treating identity as the primary security perimeter, applying continuous verification and least-privilege access through identity-driven policies.

有効的な**SC-900J**問題集はJPNTTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-900J**試験問題集を提供します。JPNTTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 47

Microsoft 365セキュリティセンターでセキュリティの傾向を表示し、IDの保護ステータスを追跡するには、何を使用する必要がありますか？

- A. 攻撃シミュレーター
- B. レポート
- C. ハンティング
- D. インシデント

正解: B (コメントを发表する)

In the Microsoft 365 security center/Microsoft 365 Defender portal, the Reports area is designed to provide organization-wide visibility into security posture and activity over time. Microsoft describes the Reports experience as enabling you to "view security trends and track the protection status across identities, endpoints, email & collaboration, and cloud apps." Within Reports, the Identity section aggregates signals from Microsoft Entra ID protection and related identity defenses so security teams can monitor trends such as risky sign-ins, user risk, MFA adoption/registration, and other identity protection metrics. These curated, read-only dashboards are aimed at measuring protection status and changes over time, helping you validate the impact of controls and prioritize remediation.

By contrast, Attack simulator is used to run user training simulations (e.g., phishing) and is not intended for posture trend reporting. Hunting (Advanced hunting) lets analysts query raw telemetry for investigations, not to provide summarized trend dashboards. Incidents correlates alerts into incident records for triage and response, rather than showing long-term trends and protection status views. Therefore, to view security trends and track the protection status of identities, the correct place is Reports in the Microsoft 365 security center /Microsoft 365 Defender portal.

質問: 48

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	☐	☐
Conditional access policies apply before first-factor authentication is complete.	☐	☐
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	☐	☐

正解:

Answer Area		
Statements	Yes	No
Conditional access policies can use the device state as a signal.	☒	☐
Conditional access policies apply before first-factor authentication is complete.	☐	☒
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	☐	☐

Explanation:

Answer Area Microsoft

Statements	Yes	No
Conditional access policies can use the device state as a signal.	☒	☐
Conditional access policies apply before first-factor authentication is complete.	☐	☒
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	☒	☐

Microsoft's Conditional Access (part of Microsoft Entra ID) evaluates multiple signals to make access decisions. The official description lists typical signals such as "user or group membership, IP location information, device state, application, and real-time risk." The device state element explicitly refers to conditions like "compliant or hybrid Azure AD joined devices," allowing policies that grant or block access- or require extra controls-based on whether a device meets compliance/registration requirements.

Regarding evaluation timing, Microsoft's guidance states that Conditional Access "policies are enforced after the first-factor authentication is completed." This means the engine needs the user's primary sign-in context (who the user is and how they authenticated) to evaluate the conditions and then decide whether to allow, block, or require additional controls. Therefore, the statement that policies apply before first factor is not correct.

Finally, Conditional Access includes grant controls such as "Require multi-factor authentication," and policies can be scoped to specific cloud apps or actions. As a result, you can target a particular application and require MFA when a user attempts to access it, satisfying application-specific risk mitigation while preserving user productivity.

質問: 49

安静時の暗号化の例は何ですか？

- A. サイト間VPNを使用した通信の暗号化
- B. 仮想マシンディスクの暗号化
- C. 暗号化されたHTTPS接続を使用してWebサイトにアクセスする
- D. 暗号化されたメールを送信する

正解: [\(正解を表示します\)](#)

In Microsoft's SCI guidance, encryption at rest is defined as protecting data when it is stored on a disk or other persistent media. Microsoft describes it as controls that "help safeguard your data to meet your organizational security and compliance commitments by encrypting data when it is persisted," distinguishing it from protections for data in transit. Within Azure and Microsoft 365, examples include Azure Disk Encryption for IaaS VMs (using BitLocker for Windows and DM-Crypt for Linux), server-side encryption for storage accounts, and Transparent Data Encryption for databases. A virtual machine's OS and data disks encrypted with BitLocker or DM-Crypt are canonical cases of at-rest encryption because the encryption keys protect the physical media; the data becomes unreadable if the disks are accessed outside the authorized context. By contrast, site-to-site VPN, HTTPS web sessions, and encrypted email protect data in transit-they secure network communications but do not encrypt the data where it is stored. Therefore, among the options provided, encrypting a virtual machine disk is the correct example of encryption at rest in Microsoft's security model.

質問: 50

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	☐	☐
Windows Hello for Business can use a PIN code as an authentication method.	☐	☐
Windows Hello for Business authentication information syncs across all the devices registered by a user.	☐	☐

正解:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	☐	☒
Windows Hello for Business can use a PIN code as an authentication method.	☒	☐
Windows Hello for Business authentication information syncs across all the devices registered by a user.	☐	☒

Explanation:

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	☐	☒
Windows Hello for Business can use a PIN code as an authentication method.	☒	☐
Windows Hello for Business authentication information syncs across all the devices registered by a user.	☐	☒

Microsoft describes Windows Hello for Business (WHfB) as replacing passwords with a device-bound credential: "Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or a PIN." WHfB authenticators are biometric gesture or PIN unlocking an asymmetric key stored on the device (typically in the TPM). Microsoft clarifies that the PIN is not a password and is "local to the device" and used to unlock the user's private key. Consequently, Yes-a PIN is a supported WHfB sign-in gesture.

Conversely, the Microsoft Authenticator app is a separate Azure AD (Microsoft Entra ID) authentication method (push notifications, TOTP, passwordless phone sign-in). It is not the WHfB credential; WHfB relies on keys/certificates on the device, not on the Authenticator app.

Finally, WHfB credentials are per-device: Microsoft states the credential is "tied to a device" and the private key never leaves the device, which means it does not roam/sync across a user's different devices. Each device enrolls and provisions its own WHfB key and gesture. These statements from Microsoft SCI documentation lead to the outcomes: No / Yes / No.

質問: 51

文を正しく完成させる答えを選択してください。



正解:



Explanation:

Answer Area

You can the default security rules of a network security group (NSG).



In Azure networking, each Network Security Group (NSG) is created with a built-in set of default security rules. Microsoft's documentation for NSGs explains: "Azure creates several default security rules within each network security group. You can't remove the default security rules, but you can override them by creating rules with a higher priority." The rule processing model is priority-based: "Security rules are processed in priority order, with lower numbers processed before higher numbers. Once a rule matches traffic, processing stops." Because the defaults have relatively low precedence (high priority numbers), an administrator can create an explicit allow or deny rule with a lower priority number to supersede the default behavior.

This is why the correct completion is override rather than copy or delete. You cannot delete the default rules; they remain present to provide baseline behavior (such as denying inbound traffic from the internet by default and allowing virtual network traffic). Instead, you override the defaults by adding your own NSG rules- using lower priority numbers-to achieve the desired access control outcome while preserving Azure's baseline protections and evaluation logic.

質問: 52

文を正しく完成させる答えを選択してください。

Answer Area

Microsoft Defender for Identity can identify advanced threats from [dropdown menu] signals.

Azure Active Directory (Azure AD)
Azure AD Connect
on-premises Active Directory Domain Services (AD DS)

正解:

Answer Area

Microsoft Defender for Identity can identify advanced threats from signals.

- Azure Active Directory (Azure AD)
- Azure AD Connect
- on-premises Active Directory Domain Services (AD DS)

Explanation:

Answer Area

Microsoft Defender for Identity can identify advanced threats from signals.

- Azure Active Directory (Azure AD)
- Azure AD Connect
- on-premises Active Directory Domain Services (AD DS)

Microsoft Defender for Identity (formerly Azure ATP) is designed to protect on-premises identity infrastructures by analyzing signals from Active Directory Domain Services (AD DS). In Microsoft's SCI guidance, Defender for Identity is described as a "cloud service that uses sensors installed on your domain controllers to monitor and analyze user activities and information across your on-premises Active Directory." The sensors "collect authentication, replication, and other security-relevant events and network traffic," enabling analytics to detect techniques such as Pass-the-Hash, Pass-the-Ticket, Golden Ticket, reconnaissance, lateral movement, and domain dominance. The product's purpose is to surface advanced threats, compromised identities, and malicious insider actions by continuously profiling and learning from AD DS behavior and security events.

While Defender for Identity integrates with other Microsoft security solutions (for example, Microsoft 365 Defender and Microsoft Defender for Cloud Apps) to enrich investigations, it does not rely on Azure Active Directory (Microsoft Entra ID) signals for its core detections, nor does it collect telemetry from Azure AD Connect itself. Instead, its foundational telemetry source is on-premises AD DS domain controllers via lightweight sensors, which provide the deep authentication and directory-service context required to identify sophisticated identity-based attacks in hybrid environments.

質問: 53

Windows Hello for Businessがサポートする3つの認証方法はどれですか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. 指紋
- B. 顔認識
- C. PIN
- D. メールによる確認
- E. セキュリティの質問

正解: A,B,C ([コメントを发表する](#))

documents: =

Microsoft's Windows Hello for Business replaces passwords with strong, two-factor authentication that is tied to the device and unlocked with a user gesture. The Microsoft Learn description states that Windows Hello for Business "replaces passwords with strong authentication" and that "users sign in using a gesture, such as a PIN, facial recognition, or fingerprint." It further clarifies that the credential is protected by the device's secure hardware and that the gesture (PIN or biometric) unlocks the private key used to authenticate. The guidance explains that "biometrics (face or fingerprint) or a PIN" are supported as the user's sign-in method, and that the PIN "is unique to the device" and does not roam, reducing attack surface.

By contrast, email verification and security questions are not authentication gestures for Windows Hello for Business. They are not listed as supported methods for unlocking the Hello for Business key or completing interactive sign-in to Windows. Therefore, the three supported Windows Hello for Business authentication methods from the options provided are fingerprint, facial recognition, and PIN. This aligns with Microsoft's documented model where the user enrolls a biometric (face or fingerprint) or creates a PIN, and subsequently uses that gesture to unlock the hardware-bound credential for secure sign-in and access to resources.

質問: 54

文を正しく完成させる答えを選択してください。

Active Directory Domain Services (AD DS)

Active Directory forest trusts

Azure Active Directory (Azure AD) business-to-business (B2B)

Azure Active Directory business-to-consumer B2C (Azure AD B2C)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

正解:

Active Directory Domain Services (AD DS)

Active Directory forest trusts

Azure Active Directory (Azure AD) business-to-business (B2B)

Azure Active Directory business-to-consumer B2C (Azure AD B2C)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Explanation:

Active Directory Domain Services (AD DS)

Active Directory forest trusts

Azure Active Directory (Azure AD) business-to-business (B. B)

Azure Active Directory business-to-consumer B2C (Azure AD B2C)

enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

In Microsoft's Security, Compliance, and Identity materials, Azure AD B2B collaboration is the feature designed for working with external organizations. Microsoft describes it as follows: "Azure AD B2B collaboration allows you to securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. Guest users sign in with their own work, school, or social identities, and appear as guest users in your directory." This directly matches the sentence in the prompt-enabling collaboration with suppliers, partners, and vendors while ensuring that external users appear as guest users in the tenant.

By contrast, Active Directory Domain Services (AD DS) is an on-premises directory service for Windows domain joined resources and does not provide cloud guest user collaboration. Active Directory forest trusts establish trust relationships between AD DS forests for resource access, not modern cloud guest access using Conditional Access, MFA, or entitlement processes. Azure AD B2C is for consumer/retail scenarios where you build customer-facing apps, managing their identities in a separate customer directory; it is not intended for partner collaboration within your enterprise tenant. Therefore, the capability that fits the statement- external partner collaboration with users appearing as guest accounts-is Azure AD B2B.

質問: 55

Microsoft 365の機密ラベルで何を指定できますか？

- A. ファイルを保存する必要がある期間
- B. メールメッセージをアーカイブするタイミング
- C. ファイルに追加する透かし
- D. ファイルを保存する場所

正解: [\(正解を表示します\)](#)

Sensitivity labels can apply content markings (headers, footers, and watermarks) to documents and emails, and can also enforce encryption and access controls. When configuring a label, you can specify the watermark text, size, and placement so that protected content is visibly marked according to your organization's policy.

質問: 56

Microsoft Cloud App Securityの3つの用途は何ですか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. シャドーITの使用を発見して管理する
- B. Azure仮想マシンへの安全な接続を提供する

- C. クラウド内のどこにでもホストされている機密情報を保護するため
- D. オンプレミスアプリケーションにパススルー認証を提供する
- E. 準拠していないアプリへのデータ漏洩を防ぎ、規制されたデータへのアクセスを制限する

正解: (正解を表示します)

Microsoft Cloud App Security (now Microsoft Defender for Cloud Apps) is Microsoft's CASB that

"discovers and controls shadow IT," integrates with identity and endpoint signals, and enforces data protection in SaaS and custom apps. SCI materials describe three core use cases relevant here:

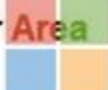
(1) Discovery and control of shadow IT by analyzing network logs and app usage, rating risk, and applying governance- matching A. (2) Protect sensitive information hosted anywhere in the cloud via policies such as DLP, information protection label awareness, and integration with apps through API connectors-matching C. (3) Prevent data leaks to noncompliant apps and limit access to regulated data using Conditional Access App Control and session controls that can block download, apply protections, or monitor in real time-matching E.

In contrast, secure connections to Azure virtual machines are provided by Azure Bastion, not the CASB (eliminating B), and pass-through authentication to on-premises apps is delivered by Azure AD features such as Azure AD Application Proxy or PTA (not Cloud App Security), eliminating D.

質問: 57

文を正しく完成させる答えを選択してください。

Answer Area

 Microsoft

Azure Active Directory (Azure AD) is

used for authentication and authorization.

an extended detection and response (XDR) system

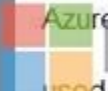
an identity provider

a management group

a security information and event management (SIEM) system

正解:

Answer Area

 Microsoft

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:

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

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>

質問: 58

Azure サブスクリプションをお持ちです。

承認ベースの、tiProme にバインドされたロールのアクティベーションを実装する必要があります。

何を使うべきでしょうか？

- A. Windows Hello for Business
- B. Azure Active Directory (Azure AD) ID 保護
- C. Azure Active Directory (Azure AD) のアクセス レビュー
- D. Azure Active Directory (Azure AD) 特権 ID 管理 (PIM)

正解: ([正解を表示します](#))

In Microsoft's Security, Compliance, and Identity guidance, Azure AD Privileged Identity Management (PIM) is the service used to manage, control, and monitor access to important resources in Azure and Microsoft 365. The documentation explains that PIM enables "just-in-time" and "time-bound" activation of privileged roles, requiring users to elevate only when needed and for a limited duration. PIM policies can require approval before a role is activated, enforce multifactor authentication, capture business justification, send notifications, and maintain detailed auditing and access review records. These controls are designed to reduce the risk associated with standing administrative privileges by ensuring that elevation is temporary, approved, and tracked.

By contrast, Windows Hello for Business provides strong, device-bound authentication; Azure AD Identity Protection focuses on detecting and remediating risky sign-ins and users; and Azure AD Access Reviews periodically reattest existing assignments but do not provide the on-demand, approval-based, time-limited activation of roles. Therefore, when the requirement is approval-based, time-bound role activation, Microsoft's prescribed capability is Azure AD PIM, which delivers just-in-time elevation with approvers, duration limits, and audit/logging to support least privilege and Zero Trust operational practices.

質問: 59

ネットワークセキュリティグループ (NSG) を関連付けることができる2つのAzureリソースはどれですか？それぞれの正解は完全な解決策を提示します。注：正しい選択はそれぞれ1ポイントの価値があります。

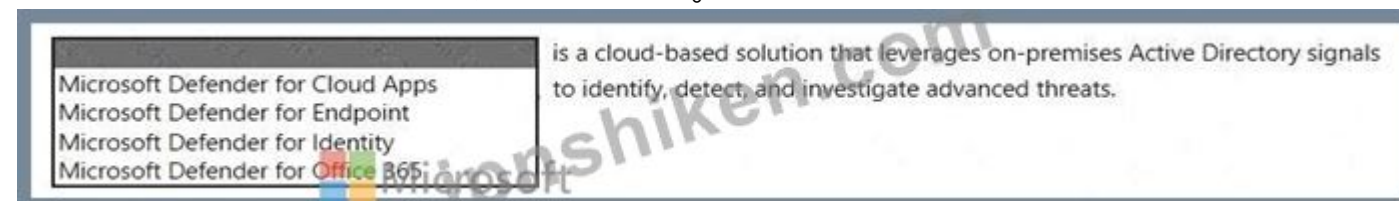
- A. ネットワークインターフェース
- B. Azure AppServiceWebアプリ
- C. 仮想ネットワーク
- D. 仮想ネットワークサブネット
- E. リソースグループ

正解: ([正解を表示します](#))

You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.

質問: 60

文を正しく完成させる答えを選択してください。



正解:

Microsoft Defender for Cloud Apps
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.

Explanation:

Microsoft Defender for Cloud Apps
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.

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) 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.

質問: 61

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Microsoft Entra Connect can be used to implement hybrid identity.	☐	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☐
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and a Microsoft Entra tenant.	☐	☐

正解:

Statements	Yes	No
Microsoft Entra Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and a Microsoft Entra tenant.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and a Microsoft Entra tenant.	☒	☐

Microsoft's hybrid identity guidance explains that Microsoft Entra Connect (formerly Azure AD Connect) is the tool used to synchronize identities from on-premises AD DS to a Microsoft Entra tenant, enabling hybrid identity. Microsoft states that hybrid identity is achieved by connecting your on-premises directory with your cloud directory so users have a single identity to access both environments. This does not require two Microsoft 365 tenants; rather, it requires one Microsoft Entra tenant integrated with your on-premises AD DS.

For authentication models-Password Hash Synchronization (PHS), Pass-through Authentication (PTA), or federation (AD FS)-Microsoft specifies that directory synchronization is required so that user objects exist in Entra ID and can authenticate to cloud services while maintaining a consistent identity. Thus, Entra Connect is used to implement the synchronization underpinning hybrid identity; two M365 tenants are unnecessary; and synchronization between AD DS and Entra ID is required for authenticating hybrid identities across Microsoft cloud services.

有効的な**SC-900J**問題集はJPNTTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-900J**試験問題集を提供します。JPNTTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 62

複数のリソースを含む Azure サブスクリプションがあります。

コンプライアンスを評価し、既存のリソースの標準を適用する必要があります。

何をえばいいのでしょうか？

- A. Anomaly Detector サービス
- B. マイクロソフト センチネル
- C. アズール ブループリント
- D. Azure ポリシー

正解: D ([コメントを发表する](#))

Microsoft describes Azure Policy as the built-in governance service that lets you "create, assign, and manage policies" to enforce organizational standards and "assess compliance at scale." It continuously evaluates existing resources for compliance and can take effect-enforcement actions such as deny, append, or modify during create/update operations. Azure Policy "helps you audit and enforce your standards" across subscriptions and resource groups, and its compliance dashboard shows overall and per-policy compliance states for all resources. By contrast, Azure Blueprints focuses on orchestrating deployments of artifacts (such as policy assignments, role assignments, and templates) for new environments; Microsoft guidance positions Policy as the engine that evaluates and enforces those standards on existing resources. Sentinel is a SIEM

/SOAR for security analytics, and Anomaly Detector is a Cognitive Service-not a governance/compliance enforcement tool. Therefore, to assess compliance and enforce standards for existing Azure resources, the prescribed control plane is Azure Policy with its evaluation cycle, initiative (policy set) support, and remediation tasks.

質問: 63

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	☐	☐
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).	☐	☐
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.	☐	☐

正解:

Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	☐	☒
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).	☒	☐
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
Microsoft Entra Permissions Management can be managed by using the Microsoft Purview compliance portal.	☐	☒
Microsoft Entra Permissions Management can be used to manage permissions in Amazon Web Services (AWS).	☒	☐
Microsoft Secure Score can be reviewed from Permissions Management in the Microsoft Entra admin center.	☐	☒

Microsoft Entra Permissions Management is Microsoft's cloud infrastructure entitlement management (CIEM) solution delivered in the Microsoft Entra admin center, not in the Microsoft Purview compliance portal. Microsoft guidance describes it as a CIEM service that provides "centralized visibility, right-sizing, and governance of permissions across clouds" and is accessed and administered from the Entra portal under Permissions Management. The Purview compliance portal is used for compliance solutions such as Compliance Manager, Information Protection, DLP, eDiscovery, and Insider Risk-not CIEM-so statement 1 is No.

Permissions Management supports multicloud environments. Microsoft documentation states that it

"discovers, monitors, and manages permissions for identities and resources across Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP)." It calculates a Permission Creep Index (PCI), surfaces excessive permissions, and recommends remediation across these clouds; therefore, using it to manage permissions in AWS is supported-statement 2 is Yes. Regarding secure scores: Permissions Management focuses on entitlements (e.g., effective permissions, PCI, right-sizing actions). Microsoft Secure Score (and Identity Secure Score) are separate posture metrics exposed in Microsoft 365 Defender and Microsoft Entra ID, respectively. The Permissions Management blade does not present Microsoft Secure Score; instead, it shows CIEM-specific insights and PCI. Consequently, the claim that Secure Score can be reviewed from Permissions Management in the Entra admin center is No.

質問: 64

Microsoft Cloud Adoption Framework for Azureでは、準備完了フェーズの前に対処される2つのフェーズはどれですか。それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. 計画
- B. 管理
- C. 採用
- D. 統治
- E. 戦略を定義する

正解: [\(正解を表示します\)](#)

In the Microsoft Cloud Adoption Framework (CAF) for Azure, the methodology is organized into sequential stages that guide an organization from initial intent through operations. Microsoft describes the flow as:

"Strategy # Plan # Ready # Adopt # Govern # Manage." The guidance explains that before building landing zones or preparing environments (Ready), organizations should complete the Strategy and Plan work.

Microsoft states that the framework "helps you create and align your business strategy, define business outcomes, and justify cloud adoption" in the Strategy stage; then, in Plan, you "translate that strategy into an actionable adoption plan, rationalize portfolios, and prepare a cloud adoption backlog." Only after these two stages does the Ready phase occur, where you "prepare your cloud environment (landing zone) to host the workloads." Additionally, CAF emphasizes that Govern and Manage are ongoing disciplines that operate alongside and after adoption rather than preceding Ready: "Govern and Manage provide iterative guardrails and operational baselines that evolve as you adopt more workloads." Therefore, the two phases addressed before the Ready phase are Define Strategy and Plan, aligning with Microsoft's prescribed order and intent of the Cloud Adoption Framework methodology.

質問: 65

複数のサブスクリプションに一貫した方法で Azure リソースをデプロイするには、何を使用できますか？

- A. Microsoft Sentinel
- B. Microsoft Defender for Cloud
- C. Azure ポリシー
- D. 紺碧の設計図

正解: **D** ([コメントを发表する](#))

Microsoft guidance describes Azure Blueprints as the native way to stamp out governed environments consistently across tenants and subscriptions. Microsoft states: "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." It further explains that "Blueprints make it possible to package artifacts, such as role assignments, policy assignments, ARM templates, and resource groups, into a single blueprint definition that can be assigned to your subscriptions." This is precisely what's required when you need to deploy Azure resources across multiple subscriptions in a consistent manner-you define a blueprint (with policies, RBAC, templates, and resource groups) and assign it to one or more subscriptions to get uniform, compliant deployments. While services like Microsoft Defender for Cloud and Azure Policy help assess and enforce security and compliance, Blueprints orchestrate multi-artifact deployment and governance at scale from day one of an environment's lifecycle, ensuring standardization and repeatability across subscriptions.

質問: 66

Azure Bastionはどのタイプのリソースに安全なアクセスを提供できますか？

- A. Azureファイル
- B. AzureSQLマネージドインスタンス
- C. Azure仮想マシン
- D. Azure App Service

正解: C ([コメントを發表する](#))

Azure Bastion is a managed PaaS service that provides secure and seamless RDP/SSH connectivity to your Azure virtual machines directly from the Azure portal over TLS/HTTPS. SCI and Azure security documentation summarize it as eliminating public IP exposure on VMs by using a fully managed bastion host deployed inside your virtual network. Users connect through their browser and the service brokers the RDP or SSH session, which "protects your VMs from exposing RDP/SSH to the Internet." Bastion does not provide access to Azure Files, SQL Managed Instance, or App Service; it is specifically built to secure management access to VMs without requiring a VPN or public endpoints. Therefore, the resource type Azure Bastion securely connects to is Azure virtual machines.

質問: 67

MicrosoftIntuneが管理するデバイスが企業リソースにアクセスするのを制限するために使用できるAzureActive Directory (Azure AD) 機能はどれですか？

- A. ネットワークセキュリティグループ (NSG)
- B. Azure ADの特権ID管理 (PIM)
- C. 条件付きアクセスポリシー
- D. リソースロック

正解: ([正解を表示します](#))

In Microsoft Entra ID (Azure AD), Conditional Access is the policy engine that evaluates signals about the user, device, app, and session to determine whether to grant access and under what conditions. Microsoft's guidance explains that Conditional Access is "the tool used by Azure AD to bring signals together, make decisions, and enforce organizational policies." In device-centric scenarios, Conditional Access integrates with Microsoft Intune device compliance so you can enforce controls such as "Require device to be marked as compliant" or "Require approved client app" before granting access to corporate resources like Microsoft 365 and Azure apps. This allows organizations to block or limit access from unmanaged or noncompliant devices, and to allow access only from devices that meet your compliance policies (encryption, OS version, jailbreak /root status, etc.).

By contrast, Network Security Groups (NSGs) filter traffic at the virtual network/subnet/NIC level and are not identity-aware; Privileged Identity Management (PIM) governs just-in-time elevation and access reviews for privileged roles; and resource locks prevent accidental deletion or modification of Azure resources. Therefore, the Azure AD feature specifically designed to restrict access by Intune-managed device state and enforce device-based access conditions to corporate resources is Conditional Access.

質問: 68

Active Directory ドメイン サービス (AD DS) では何を作成できますか？

- A. モデム認証を必要とする基幹業務 (106) アプリケーション
- B. Mob デバイス
- C. コンピュータアカウント
- D. モデム認証を必要とするサービスとしてのソフトウェア (SaaS) アプリケーション

正解: ([正解を表示します](#))

In Microsoft's identity platform, Active Directory Domain Services (AD DS) is the on-premises directory that maintains directory objects such as users, groups, and computers. Microsoft documentation describes AD DS as a service that "stores information about objects on the network and makes this information easy for administrators and users to find and use." It further explains that AD DS contains objects like "users, groups, computers, and other resources," and that administrators use tools such as Active Directory Users and Computers to create and manage these

objects. A key object type is the computer account; Microsoft states that "a computer that's joined to a domain has a corresponding computer account object in Active Directory" and that these accounts are created and managed within AD DS to enable secure authentication and authorization for domain-joined devices. By contrast, mobile devices are typically enrolled and managed through Microsoft Intune/Endpoint Manager and Azure AD device objects, not created in AD DS. Likewise, SaaS applications that require modern authentication integrate with Microsoft Entra ID (Azure AD) using OpenID Connect/OAuth 2.0-not with AD DS. Line-of-business apps that rely on modern authentication are also registered in Entra ID, while AD DS supports traditional Kerberos/NTLM for domain resources. Therefore, among the options provided, the object you can create in AD DS is computer accounts.

質問: 69
どの Microsoft Purview データ分類タイプが正規表現の使用をサポートしていますか？

- A. 完全データ一致 (EDM)
- B. 指紋分類器
- C. 機密情報の種類 (SIT)
- D. トレーニング可能な分類器

正解: (正解を表示します)
Sensitive Information Types (SITs) support regular expressions (regex), which allow for custom pattern matching to detect sensitive content like credit card numbers, social security numbers, or custom identifiers.
Regex is fundamental to the detection logic within SITs.
SCI Extract: "Sensitive information types use pattern matching techniques, including regular expressions, keyword matches, and checksums to identify sensitive data."

質問: 70
文を正しく完成させる答えを選択してください。

Microsoft

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services.

正解:

Microsoft

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services.

Microsoft

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services.

Reference:
<https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cloud-services-security-baseline>

質問: 71

文を正しく完成させる答えを選択してください。



正解:



Explanation:



In Microsoft's Security, Compliance, and Identity learning content for Microsoft Defender for Cloud, the service is described as providing ongoing posture management and threat protection. The official description states that Defender for Cloud "continuously assesses your resources to identify security misconfigurations and weaknesses" and "continuously discovers and evaluates resources" across your subscriptions. The recommendations and secure-score updates are produced as the platform "continuously analyzes your environment using security policies and analytics," surfacing issues the moment they're detected and mapping them to remediation guidance. This continuous assessment model underpins Defender for Cloud's cloud security posture management (CSPM) capability and ensures that newly created or modified resources are evaluated without waiting for a scheduled job. By design, there is no fixed interval (such as hourly, every 15 minutes, or daily) required to trigger assessments-policy-driven evaluation and data collection run as changes occur and signals are received. Therefore, the sentence "Microsoft Defender for Cloud assesses Azure resources _____ for security issues" is correctly completed with continuously, reflecting Microsoft's emphasis on persistent, real-time security posture evaluation rather than periodic scans.

質問: 72

Microsoft 365で情報バリアポリシーを実装するためのユースケースは何ですか？

- A. 認証されていないアクセスをMicrosoft365に制限する
- B. 組織内の特定のグループ間のMicrosoft Teamsチャットを制限する
- C. 組織内の特定のグループ間でMicrosoft Exchange Onlineの電子メールを制限する
- D. データ共有を外部の電子メール受信者に制限します

正解: [\(正解を表示します\)](#)

Microsoft 365 Information Barriers are compliance policies used "to prevent certain segments of users from communicating or collaborating with each other." In Microsoft's guidance, IB policies are designed for scenarios like insider trading restrictions, M&A deal rooms, or research-sales separation, where it's necessary to block chats, calls, and collaboration between defined user segments. The documentation explains that when IB policies are in place, "users in the blocked segments cannot search, discover, or communicate with each other in Microsoft Teams," and IB v2 extends these controls to additional collaboration workloads such as SharePoint and OneDrive. By contrast, email restrictions in Exchange Online are addressed through mail flow rules or other Exchange features, not information barriers, and restricting unauthenticated access or external sharing is handled by identity access controls and sharing settings, not IB. Therefore, the specific use case is restricting Microsoft Teams chats (and related collaboration) between certain groups within an organization.

質問: 73

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☐	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☐
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure AD.	☐	☐

正解:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure AD.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	☒	☐
Hybrid identity requires the implementation of two Microsoft 365 tenants.	☐	☒
Authentication of hybrid identities requires the synchronization of Active Directory Domain Services (AD DS) and Azure AD.	☒	☐

In Microsoft's hybrid identity model, organizations keep their authoritative identities in Active Directory Domain Services (AD DS) and surface those identities in Microsoft Entra ID (Azure AD). Microsoft guidance explains that hybrid identity is implemented by synchronizing on-premises directory objects (users, groups, and selected attributes) into Azure AD using Azure AD Connect or Cloud Sync. Azure AD Connect is explicitly documented as the Microsoft tool that establishes and maintains synchronization between AD DS and Azure AD and is therefore used to implement hybrid identity-hence statement 1 is Yes. Hybrid identity does not require two Microsoft 365 tenants; the standard design is one Azure AD tenant connected to one or more on-premises AD forests, so statement 2 is No. For users to authenticate to Microsoft cloud resources with their on-premises identity, Azure AD must have a corresponding cloud identity object, which is achieved by directory synchronization; sign-in can then be handled by cloud authentication (Password Hash Synchronization or Pass-through Authentication) or by federation (e.g., AD FS). Because these sign-in options

depend on synchronized identities being present in Azure AD, statement 3 is Yes. This aligns with SCI guidance that hybrid identity = synchronized identities + a chosen authentication method (PHS/PTA or federation).

質問: 74

Log Analytics ワークスペースを含む Azure サブスクリプションがあります。

Microsoft Sentinel をオンボードする必要があります。

最初に何をすべきですか？

- A. ハンティング クエリを作成します。
- B. アラートをインシデントに関連付けます。
- C. セキュリティ ソースに接続します。
- D. カスタム検出ルールを作成します。

正解: ([正解を表示します](#))

Onboarding Microsoft Sentinel starts by enabling Sentinel on an existing Log Analytics workspace and then connecting data sources so analytics can operate on ingested security data. Microsoft's Sentinel onboarding guidance emphasizes that after you add Sentinel to a workspace, you must "connect Microsoft services, non- Microsoft solutions, and custom sources" using built-in data connectors. Microsoft also states that "you need data in your workspace before you can use Microsoft Sentinel's analytics, hunting, and investigation capabilities." Features such as custom analytics rules, hunting queries, and incident correlation depend on ingested telemetry from sources like Microsoft Entra ID sign-in logs, Microsoft 365, Defender products, firewalls, and other appliances. Because the question already gives you a Log Analytics workspace (the prerequisite for enabling Sentinel), the first action in the onboarding workflow that unlocks Sentinel's value is to connect your security sources. Only after data is flowing should you proceed to create analytics rules, hunting queries, and incident processes. Therefore, the correct first step to onboard Microsoft Sentinel is connect to your security sources.

質問: 75

文を正しく完成させる答えを選択してください。



正解:

Assessments



Explanation:

Assessments

In Microsoft Purview Compliance Manager, assessments are the core components used to track compliance with groupings of controls from specific regulations, standards, or requirements.

According to official Microsoft Security, Compliance, and Identity (SCI) learning content, particularly within the SC-400 and SC-900 certification tracks, the role of assessments is explicitly defined as:

"Assessments in Compliance Manager help you track, implement, and improve compliance with requirements from standards and regulations. Each assessment maps to a specific regulation or control framework, such as ISO 27001, NIST, GDPR, or HIPAA, and includes a set of controls and recommended improvement actions." Further extracted content from SCI documentation confirms: "An assessment is used to measure your compliance posture against a particular regulation or standard. It includes control mappings and provides insight into what's in place and what still needs to be addressed to meet the compliance goals." The other options in the dropdown - Templates, Improvement actions, and Solutions - serve different functions:

Templates provide a blueprint for creating assessments.

Improvement actions are actionable steps generated within assessments.

Solutions in Microsoft Purview refer to bundled capabilities like Insider Risk Management, Information Protection, etc.

Therefore, to track compliance with groupings of controls from a specific regulation or requirement, the correct and Microsoft-verified term is " Assessments. "

質問: 76

文を正しく完成させる答えを選択してください。



正解:



Explanation:

Compliance score

In Microsoft Purview Compliance Manager, the Compliance score is the metric that measures an organization's progress in completing improvement actions that help reduce compliance and data-protection risk. Microsoft describes this score as a quantifiable indicator of your compliance posture across regulatory standards and data-protection baselines. Each recommended improvement action in Compliance Manager is assigned points; completing, testing, and attesting to those actions increases your score. Points are weighted by risk, so implementing controls with greater impact on reducing risk contributes more to the overall score. Microsoft also clarifies that the Compliance score is an operational progress indicator, not a certification or a legal determination of compliance, but it enables organizations to track, prioritize, and demonstrate the implementation of controls across frameworks such as GDPR, ISO/IEC 27001, NIST 800-53, and Microsoft Data Protection Baselines.

By contrast, Microsoft Purview compliance portal reports provide reporting and insights (for example, DLP, Insider Risk, Audit) but do not calculate a unified risk-reduction progress metric. The Trust Center is Microsoft's public site for transparency about security, privacy, and compliance commitments, and Trust Documents (auditor reports, certifications, and white papers) supply evidence and reference materials. Neither of these provide an in-product, points-based measure of progress-Compliance score does.

有効的な**SC-900J**問題集はJPNTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-900J**試験問題集を提供します。JPNTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 77

文を完成させます。

Answer Area

Microsoft provides the as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services.

Microsoft

正解:

Answer Area

Microsoft provides the as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services.

Microsoft

Explanation:

Answer Area

Microsoft provides the as a public site for publishing audit reports and other compliance-related information associated with Microsoft cloud services.

Microsoft

In Microsoft's Security, Compliance, and Identity guidance, the Microsoft Service Trust Portal (STP) is identified as the public destination where Microsoft publishes independent audit reports, compliance certifications, assessment reports, and trust-related documentation for Microsoft cloud services. The documentation explains that the STP provides customers with access to materials such as SOC 1/SOC 2 reports, ISO/IEC certifications, audit summaries, and compliance guides, enabling organizations to evaluate Microsoft's controls and map them to their own regulatory requirements. The STP is expressly positioned for transparency and due diligence, allowing customers and auditors to review Microsoft's compliance posture and understand how Microsoft manages security, privacy, and compliance across its cloud platforms.

By contrast, the Microsoft Purview compliance portal is a tenant-admin portal used to configure and manage compliance solutions (e.g., DLP, Information Protection, eDiscovery, Insider Risk, Compliance Manager) within your organization-not a public repository of Microsoft's audit artifacts. The Microsoft Purview governance portal focuses on data governance and cataloging scenarios. The Azure EA portal is used for Enterprise Agreement billing and usage management. Therefore, the public site for publishing audit reports and other compliance-related information for Microsoft cloud services is the Microsoft Service Trust Portal.

質問: 78

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	☐	☐
Federation provides single sign-on (SSO) with multiple identity providers.	☐	☐
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	☐	☐

正解:

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	☒	☐
Federation provides single sign-on (SSO) with multiple identity providers.	☒	☐
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
GitHub is a cloud-based identity provider.	☒	☐
Federation provides single sign-on (SSO) with multiple identity providers.	☒	☐
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	☐	☒

Microsoft's identity guidance classifies social identity services (e.g., GitHub, Google, Facebook) as cloud-based identity providers that can be used for external identities with Microsoft Entra ID. In this model, GitHub functions as an IdP using OAuth/OpenID Connect to authenticate users and issue tokens that applications or Entra ID can accept. Federation in Microsoft terms is the trust relationship that allows SSO across organizational boundaries and with multiple identity providers, such as Active Directory Federation Services (AD FS), SAML, or OpenID Connect providers, so users can authenticate once and access multiple apps without repeated sign-ins.

Crucially, SCI materials distinguish roles: an identity provider primarily handles authentication (proving who the user is and issuing claims/tokens). Authorization-deciding what the user can do-is enforced by the application or resource (often using roles/claims from the IdP). Auditing spans multiple planes: the IdP provides sign-in and audit logs, while applications and other services maintain their own activity logs.

Therefore, it is incorrect to say a central IdP "manages all modern authentication services" including authorization and auditing; those responsibilities are shared across the identity platform and the relying applications/resources.

質問: 79

Microsoft Purview Compliance Manager でコンプライアンス スコアを評価しています。
コンプライアンス スコア アクションのサブカテゴリを適切なアクションと一致させます。
答えるには、適切なアクション サブカテゴリを左側の列から右側のアクションにドラッグします。各アクション サブカテゴリは、1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。
注: 正しく一致するたびに 1 ポイントの価値があります。

Action Subcategories

Corrective

Detective

Preventative

Answer Area

Encrypt data at rest.

Perform a system access audit.

Make configuration changes in response to a security incident.

正解:

Action Subcategories

Corrective

Detective

Preventative

Answer Area

Preventative

Detective

Corrective

Encrypt data at rest.

Perform a system access audit.

Make configuration changes in response to a security incident.

Explanation:

Action Subcategories

Corrective

Detective

Preventative

Answer Area

Preventative

Detective

Corrective

Encrypt data at rest.

Perform a system access audit.

Make configuration changes in response to a security incident.

Microsoft Purview Compliance Manager organizes improvement actions into control action subcategories that mirror core security control types used throughout Microsoft Learn's SCI content: preventative, detective, and corrective. In the SC-900 security fundamentals guidance, Microsoft describes these control types as follows:
"Preventive controls are intended to deter or stop an attack from occurring (for example, encryption and access controls). Detective controls are used to discover and detect attacks that are in progress or have occurred (for example, logging, auditing, and monitoring). Corrective controls are used to limit the damage caused by an incident and to return systems to normal operations (for example, configuration changes, incident response, and recovery activities)." Applying those definitions to Compliance Manager actions: Encrypt data at rest is a preventative control because it deters exposure by protecting data before an event. Perform a system access audit is a detective action because auditing and reviewing access logs are used to discover and detect misuse or anomalies. Make configuration changes in response to a security incident is a corrective action because it remediates and restores the environment after detection, aligning with Compliance Manager's corrective action guidance.

These mappings reflect how Compliance Manager measures completion of improvement actions that reduce compliance risk through the right mix of preventative, detective, and corrective controls.

質問: 80

文を正しく完成させる答えを選択してください。

Answer Area

Microsoft

Single sign-on (SSO) configured between multiple identity providers is an example of

federation.
federation.
integration.
password hash synchronization.
pass-through authentication.

正解:

Answer Area

Microsoft

Single sign-on (SSO) configured between multiple identity providers is an example of

federation.
federation.
integration.
password hash synchronization.
pass-through authentication.

Explanation:

Answer Area

Single sign-on (SSO) configured between multiple identity providers is an example of

federation.

In Microsoft identity and access management terminology, federation refers to the establishment of a trust relationship between identity providers, which enables single sign-on (SSO) across different organizations or platforms.

According to the Microsoft Security, Compliance, and Identity (SCI) learning path, particularly in the SC-900 and SC-300 certifications, the following definition is provided:

"Federation is a means of establishing trust between two identity systems. This trust allows users from one domain to access resources in another domain without needing to authenticate again, typically using SAML, WS-Federation, or OAuth protocols." This concept is essential in cross-organization SSO scenarios, such as enabling users from one enterprise (or identity provider) to authenticate with services hosted in another, using existing credentials.

SCI documentation further states:

"Single sign-on (SSO) between multiple identity providers is enabled through federation protocols, which delegate authentication and allow token-based identity propagation across systems." The other options are not accurate in this context:

Integration is a vague term and not specific to SSO configuration.

Password hash synchronization and pass-through authentication are Azure AD authentication methods used for hybrid identity with on-premises AD, not for federating with external identity providers.

Therefore, SSO configured between multiple identity providers is best classified as an example of federation.

質問: 81

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	☐	☐
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	☐	☐
Azure Active Directory (Azure AD) is an identity and access management service.	☐	☐

正解:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	☐	☒
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	☒	☐
Azure Active Directory (Azure AD) is an identity and access management service.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	☐	☒
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	☐	☒
Azure Active Directory (Azure AD) is an identity and access management service.	☒	☐

Microsoft's SCI/Learn content describes Azure AD (now Microsoft Entra ID) as a cloud service, not something you install on-premises. The docs state Azure AD is a "cloud-based identity and access management service" that "helps your employees sign in and access resources." This clarifies the third statement (IAM service) as Yes, and the first statement (on-premises deployment) as No, because the native on-prem directory is Windows Server Active Directory, whereas Azure AD runs in Microsoft's cloud and can be synchronized with on-prem AD via tools like Azure AD Connect. Microsoft also explains licensing/availability: the service comes in several editions, and the free/Office 365 tier is included with many suites. The documentation explicitly notes that Azure AD is "included with subscriptions such as Microsoft 365" (formerly Office 365) and provides tenant-wide identity for those services. Therefore, stating that Azure AD is provided as part of a Microsoft 365 subscription is Yes.

In summary: Azure AD/Entra ID is a cloud identity and access management platform; it's not deployed on-premises, and Microsoft 365 subscriptions include an Azure AD tenant/edition to manage users, groups, apps, and access policies.

文を正しく完成させる答えを選択してください。

▼

Azure Defender

The Microsoft 365 compliance center

The Microsoft 365 security center

Microsoft Endpoint Manager

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.



正解:

▼

Azure Defender

The Microsoft 365 compliance center

The Microsoft 365 security center

Microsoft Endpoint Manager

provides a central location for managing information protection, information governance, and data loss prevention (DLP) policies.



Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-> worldwide MIP capabilities are included with Microsoft 365 Compliance and give you the tools to know your data, protect your data, and prevent data loss.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide>

質問: 83

文を正しく完成させる答えを選択してください。

Answer Area



▼

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

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.

正解:

Answer Area



▼

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

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.

Explanation:

Answer Area

▼

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

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.



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

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/overview>

質問: 84

コンプライアンスマネージャーの評価とは何ですか？

- A. 特定の規制、標準、またはポリシーからのコントロールのグループ。
- B. 組織が企業標準に準拠するのに役立つ推奨ガイダンス。
- C. 会社の文書で許可されていない単語の辞書。
- D. 複数のポリシーを含むポリシーイニシアチブ。

正解: (正解を表示します)

Microsoft Purview Compliance Manager is a feature in the Microsoft Purview compliance portal that helps you manage your organization's compliance requirements with greater ease and convenience. Compliance Manager can help you throughout your compliance journey, from taking inventory of your data protection risks to managing the complexities of implementing controls, staying current with regulations and certifications, and reporting to auditors.

Watch the video below to learn how Compliance Manager can help simplify how your organization manages compliance:

Compliance Manager helps simplify compliance and reduce risk by providing:

- * Pre-built assessments for common industry and regional standards and regulations, or custom assessments to meet your unique compliance needs (available assessments depend on your licensing agreement; learn more).
- * Workflow capabilities to help you efficiently complete your risk assessments through a single tool.
- * Detailed step-by-step guidance on suggested improvement actions to help you comply with the standards and regulations that are most relevant for your organization. For actions that are managed by Microsoft, you'll see implementation details and audit results.
- * A risk-based compliance score to help you understand your compliance posture by measuring your progress in completing improvement actions.

質問: 85

セキュリティ評価を実行し、脆弱性が見つかったときに自動的にアラートを生成するソリューションはどれですか？

- A. クラウド セキュリティ体制管理 (CSPM)
- B. DevSecOps
- C. クラウド ワークロード保護プラットフォーム (CWPP)
- D. セキュリティ情報およびイベント管理 (SIEM)

正解: A (コメントを発表する)

In Microsoft's cloud security terminology, Cloud Security Posture Management (CSPM) is the solution specifically designed to perform continuous security assessments of cloud resources and generate alerts when misconfigurations or vulnerabilities are detected. In Microsoft Defender for Cloud, the CSPM capabilities continuously analyze Azure, multi-cloud, and hybrid resources against built-in security benchmarks and regulatory standards. The platform evaluates configurations, detects insecure settings, missing protections, and exposure paths, then raises security recommendations and alerts so administrators can remediate issues that increase risk.

Microsoft's security and SCI learning content describes CSPM as providing "continuous assessment, visibility, and guidance to improve the security posture of your cloud environment," including automatic alerting when high-risk issues or vulnerabilities are found. These assessments are mapped to standards and best practices, helping organizations reduce risk proactively instead of waiting for an active attack.

By contrast, DevSecOps is a practice or methodology, not a specific product. A Cloud Workload Protection Platform (CWPP) focuses on runtime protection of workloads such as VMs, containers, and PaaS services. A SIEM solution (like Microsoft Sentinel) ingests and correlates logs and alerts from many sources but does not itself perform the core security posture assessments of cloud configurations. Therefore, the SCI domain clearly aligns this function with CSPM.

質問: 86

攻撃シミュレーショントレーニング機能はどのサービスに含まれていますか？

A. クラウド アプリ向け Microsoft Defender

B. Bマイクロソフトは、攻撃シミュレーショントレーニングをMicrosoft Defender for Office 365 (MDO) のメールおよびコラボレーション保護ワークロードに位置付けています。公式製品ガイドン
スでは、このトレーニングは 組織内で現実的な攻撃シナリオを実行し、脆弱なユーザーを特定し、フィッシングやその他のソーシャルエンジニアリングの手法を認識 報告できるようユーザーをト
レーニングできる」組み込み機能であると説明されています。さらにマイクロソフトは、攻撃シミュレーショントレーニングは 編集可能なフィッシングペイロード、認証情報収集および添付ファイ
ルのシナリオ、ランディングページ、ユーザートレーニング、詳細なレポートを提供する」ため、セキュリティチームは侵害率を測定し、ユーザーの回復力を長期的に向上させることができると述べ
ています。サービスの範囲は明確です。

攻撃シミュレーショントレーニングはMicrosoft Defender for Office 365 プラン2の機能です」と記載されており、Microsoft 365 E5やOffice 365 E5など、MDO P2を含むスイートに含まれていま
す。Microsoft 365 Defenderポータルでは、 「メールとコラボレーション」→ 攻撃シミュレーショントレーニング」からアクセスできます。管理者はここでシミュレーションの作成、グループのター
ゲット設定、トレーニングの割り当て、再犯者、回復カスコア、シミュレーション結果などの指標の確認を行うことができます。この機能は、設計上、Microsoft Defender for Cloud Apps クラウドア
プリのセキュリティとCASB機能)、Microsoft Defender for Identity オンプレミスのAD ID脅威検出)、Defender for SQLIには含まれていません。そのため、Microsoft SCIドキュメントでは、攻撃シ
ミュレーショントレーニングをホストする適切なサービスはMicrosoft Defender for Office 365 プラン2)であるとされています。

C. Microsoft Defender for Identity

D. Microsoft Defender for SQL

E. Office 365 向け Microsoft Defender

正解: ([正解を表示します](#))

質問: 87

Azure Key Vault を使用して実行できる 2 つのアクションはどれですか。それぞれの正解は完全なソリューションを示します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

A. Azure Resource Manager (ARM) テンプレートを保存します。

B. Azure DDoS Protection を実装します。

C. ネットワーク セキュリティ グループ (NSG) を実装します。

D. キーを保存します。

E. 秘密を保存します。

正解: ([正解を表示します](#))

Microsoft's official description of Azure Key Vault in the Security, Compliance, and Identity learning materials states that Key Vault is "a cloud service for securely storing and accessing secrets." The
same guidance clarifies that "a secret is anything you want to tightly control, such as API keys, passwords, or connection strings." In addition to secrets, Key Vault provides key management: "Azure
Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services." It further explains that organizations can "generate, import, rotate, disable, and delete keys" and
use them for operations such as

"encrypt and decrypt, sign and verify, wrap and unwrap." These excerpts confirm that Key Vault's core capabilities include the secure storage and lifecycle management of secrets and cryptographic
keys.

By contrast, the SCI content makes clear that infrastructure features like Azure DDoS Protection and Network Security Groups (NSGs) are networking/security controls delivered by Azure networking services, not Key Vault. Likewise, ARM templates are deployment artifacts stored in repositories such as Azure Repos or GitHub; Key Vault does not store or manage template files. Therefore, the two correct actions you can perform with Azure Key Vault-aligned with Microsoft's documentation-are to store (and manage) keys and store (and manage) secrets.

質問: 88

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	☐	☐
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	☐	☐
Hunting provides you with the ability to identify security threats before an alert is triggered.	☐	☐

正解:

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	☒	☐
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	☒	☐
Hunting provides you with the ability to identify security threats before an alert is triggered.	☒	☐

Explanation:

Answer Area

Statements	Yes	No
Microsoft Sentinel data connectors support only Microsoft services.	☐	☒
You can use Azure Monitor workbooks to monitor data collected by Microsoft Sentinel.	☒	☐
Hunting provides you with the ability to identify security threats before an alert is triggered.	☒	☐

Microsoft states that Microsoft Sentinel includes connectors for both Microsoft and non-Microsoft sources. The product overview explains that Sentinel "comes with built-in connectors" for services such as Microsoft 365, Defender, and Azure sources, and also built-in connectors for non-Microsoft solutions like firewalls and other security products. Therefore, the claim that data connectors support only Microsoft services is false. For visualization and monitoring, the documentation clarifies that "Microsoft Sentinel uses Azure Monitor workbooks to provide rich visualizations of your data." Workbooks are the native dashboarding framework in Sentinel and can be customized to monitor logs, incidents, and telemetry that Sentinel ingests. Hence, using Azure Monitor Workbooks to monitor data collected by Sentinel is true.

Regarding threat hunting, Microsoft describes the Hunting capability as a proactive feature: "Hunting lets you proactively hunt for security threats," using Kusto Query Language queries and analytic patterns to find indicators of compromise before alerts are generated. Analysts can run, save, and schedule hunts to uncover suspicious activity that hasn't yet raised an alert, making the statement about identifying threats before an alert is triggered true.

質問: **89**

AzureBastionを使用してAzure仮想マシンに接続する必要があります。何をすべきですか？

- A. SSHクライアント
- B. PowerShellリモーティング
- C. Azureポータル
- D. リモートデスクトップ接続クライアント

正解: **C** ([コメントを发表する](#))

Microsoft states that Azure Bastion is a fully managed PaaS service that provides "secure and seamless RDP

/SSH connectivity to your virtual machines directly in the Azure portal over SSL" and "eliminates the need to expose public IP addresses on your VMs." With Bastion, users open the VM blade in the Azure portal and launch an in-browser RDP or SSH session; no separate RDP or SSH client is required because the session is proxied through Bastion using HTTPS/TLS. The platform is designed to be agentless and browser-based, providing connectivity without VPN or jump hosts and enforcing least-exposure by keeping management ports off the internet. While traditional tools such as Remote Desktop Connection or an SSH client are common for direct access, Bastion's prescribed access method in Microsoft guidance is to initiate the session from the Azure portal. PowerShell remoting is unrelated to Bastion's web-based brokering. Therefore, to connect to an Azure virtual machine by using Azure Bastion, you use the Azure portal.

質問: **90**

Azure サブスクリプションをお持ちです。

承認ベースの期限付きロールのアクティブ化を実装する必要があります。

何をえばいいのでしょうか？

- A. Microsoft Entra ID 保護
- B. Microsoft Entra 条件付きアクセス
- C. Microsoft Entra 特権管理
- D. Microsoft Entra Access レビュー

正解: **C** ([コメントを发表する](#))

Microsoft documents describe Microsoft Entra Privileged Identity Management (PIM) as the service that delivers approval-based, time-limited elevation to privileged roles. Official guidance states:

"Privileged Identity Management (PIM) enables you to manage, control, and monitor access to important resources in Microsoft Entra ID, Azure, and Microsoft 365." PIM specifically supports just-in-time and time-bound activations: "PIM provides just-in-time privileged access to Microsoft Entra roles and Azure resources" and

"allows you to make access time-bound by setting start and end dates." It also supports approval workflows:

"You can require approval to activate privileged roles, and designate approvers to receive and approve requests." Additional controls include "require multi-factor authentication to activate, provide a justification, and ticket number," and auditing: "PIM records all activations and changes for review and alerting." By contrast, Microsoft Entra ID Protection focuses on risk detections and automated remediation, not role elevation workflows. Conditional Access enforces access policies at sign-in and session but does not provide approval-based role activation. Access Reviews help you "review and attest to continued access" but do not supply just-in-time elevation. Therefore, the Microsoft Purview/Entra feature that implements approval-based, time-bound role activation is Microsoft Entra Privileged Identity Management (PIM).

質問: **91**

Azureファイアウォールを使用して保護できる2種類のリソースはどれですか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. Azure仮想マシン
- B. Azure Active Directory (Azure AD) ユーザー
- C. Microsoft ExchangeOnlineの受信トレイ
- D. Azure virtual networks
- E. Microsoft SharePointOnlineサイト

正解: A,D (コメントを发表する)

Azure Firewall is a managed, cloud-based network security service designed to secure traffic inside and across Azure Virtual Networks. Microsoft describes Azure Firewall as a stateful firewall that "protects Azure Virtual Network resources" by enforcing network and application rules, central logging, and threat intelligence-based filtering. Because it is deployed into a VNet/subnet (often as the hub in a hub-and-spoke), it directly governs East/West and North/South flows to workloads such as Azure virtual machines and platform services reachable through the VNet, using DNAT/SNAT and rule collections. Microsoft guidance highlights capabilities to "centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks," and to filter traffic for peered VNets, branch connections (VPN /ExpressRoute), and internet traffic. These capabilities explicitly map to protecting Azure virtual networks and the VMs and subnets inside them. In contrast, Azure AD users, Exchange Online inboxes, and SharePoint Online sites are SaaS/identity resources protected by Microsoft Entra controls, Exchange/SharePoint security, and Purview/Defender for Office 365-not by a VNet firewall. Therefore, the Azure Firewall-protectable resource types among the options are Azure virtual machines and Azure virtual networks.

有効的な**SC-900J**問題集はJPNTTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTTest.comは今最新**SC-900J**試験問題集を提供します。JPNTTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 92

Software as a Service (SaaS)クラウドサービスモデルのセキュリティを評価する場合、顧客は何に責任がありますか？

- A. ネットワーク制御
- B. オペレーティングシステム
- C. アプリケーション
- D. アカウントとID

正解: (正解を表示します)

質問: 93

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

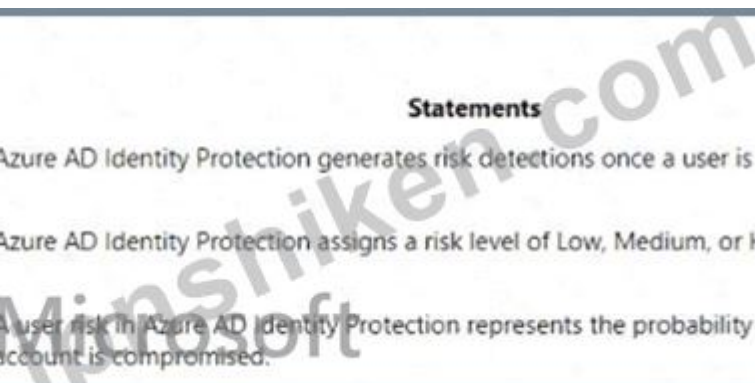
Answer Area

Statements	Yes	No
Azure AD Identity Protection generates risk detections once a user is authenticated.	☐	☐
Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	☐	☐
A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	☐	☐

正解:

Answer Area		Statements	Yes	No
		Azure AD Identity Protection generates risk detections once a user is authenticated.	☐	☐
		Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	☐	☐
		A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	☐	☐

Explanation:

Answer Area		Statements	Yes	No
		Azure AD Identity Protection generates risk detections once a user is authenticated.	☒	☐
		Azure AD Identity Protection assigns a risk level of Low, Medium, or High to each risk event.	☒	☐
		A user risk in Azure AD Identity Protection represents the probability that a given identity or account is compromised.	☒	☐

Microsoft describes Identity Protection as a capability that "detects risky users and risky sign-ins using real- time and offline detections and allows you to configure automated responses." Microsoft is explicit that detections aren't limited to after authentication; rather, signals are evaluated during sign-in and also by offline analytics, where "some detections are offline and can take up to 48 hours to appear." Therefore, saying it only "generates risk detections once a user is authenticated" is incorrect.

For risk scoring, Microsoft states that Identity Protection "assigns a risk level to each detection," and that "risk levels are Low, Medium, or High," which are then used by user-risk and sign-in-risk policies to drive remediation (for example, requiring password change or MFA).

Microsoft also defines the two core risk concepts: "User risk represents the probability that a given identity or account is compromised," while "Sign-in risk represents the probability that a given authentication request isn't authorized by the identity owner." These definitions underpin Conditional Access and Identity Protection policies that can require additional verification or block access based on the assessed risk.

Taken together, the documentation confirms: detections are not restricted to post-authentication (No), detections carry Low/Medium/High levels (Yes), and user risk is the probability the identity is compromised (Yes).

質問: 94

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Control is a key privacy principle of Microsoft.	☐	☐
Transparency is a key privacy principle of Microsoft.	☐	☐
Shared responsibility is a key privacy principle of Microsoft.	☐	☐

正解:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	☒	☐
Transparency is a key privacy principle of Microsoft.	☒	☐
Shared responsibility is a key privacy principle of Microsoft.	☐	☒

Explanation:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	☒	☐
Transparency is a key privacy principle of Microsoft.	☒	☐
Shared responsibility is a key privacy principle of Microsoft.	☐	☒

Microsoft sets out clear privacy principles for Microsoft 365 and Microsoft cloud services. In Microsoft's privacy commitments, Microsoft states that customers control their data: "You control your data." Microsoft also pledges transparency about data practices: "We are transparent about data collection and use." These two commitments are among the core privacy principles articulated across Microsoft 365 privacy and Microsoft Purview documentation, which emphasize customer choice, clear explanations of data processing, and admin capabilities to access, export, and delete data. Additional Microsoft privacy principles often listed alongside these include security of your data, strong legal protections, no content-based targeting, and benefits to you, but the key point for this question is that Control and Transparency are explicitly called out as privacy principles.

By contrast, shared responsibility is not a privacy principle; it is a cloud security model used in Azure

/Microsoft cloud guidance. That model explains that security is a shared responsibility between Microsoft (for the cloud infrastructure) and the customer (for their data, identities, endpoints, and configurations). It describes how duties are divided for protecting services and workloads, not a privacy promise to end users.

Therefore, the correct selections are Yes for Control and Transparency, and No for Shared responsibility.

質問: 95

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Digitally signing a document requires a private key.	☐	☐
Verifying the authenticity of a digitally signed document requires the public key of the signer.	☐	☐
Verifying the authenticity of a digitally signed document requires the private key of the singer.	☐	☐

正解:

Statements	Yes	No
Digitally signing a document requires a private key.	☒	☐
Verifying the authenticity of a digitally signed document requires the public key of the signer.	☒	☐
Verifying the authenticity of a digitally signed document requires the private key of the singer.	☐	☒

Explanation:

Microsoft's security and compliance learning content explains that digital signatures are built on public key (asymmetric) cryptography. In this model, each identity has a key pair: a private key that is kept secret and a public key that can be shared. The signing operation is performed with the private key to produce a signature bound to the content and the signer's identity. Verification is then performed by anyone who has access to the corresponding public key, which mathematically validates the signature and confirms both integrity (the content wasn't altered) and authenticity (it was signed by the holder of the private key). SCI materials (covering Microsoft Purview Information Protection, Azure Key Vault/PKI concepts, and identity fundamentals) emphasize that the private key must never be disclosed or required for verification; only the public key is used to validate signatures and certificates. This is the same principle used across Microsoft 365 for certificate-based trust, code signing, and document signing: sign with the private key; verify with the public key. Therefore, statements one and two are true, and the statement claiming verification requires the private key is false.

質問: 96

次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

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

正解:

Statements	Yes	No
Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage.	☒	☐
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	☒	☐
Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises.	☒	☐

Explanation:

Microsoft Defender for Cloud can detect vulnerabilities and threats for Azure Storage. Yes Cloud Security Posture Management (CSPM) is available for all Azure subscriptions. Yes Microsoft Defender for Cloud can evaluate the security of workloads deployed to Azure or on-premises. Yes Microsoft Defender for Cloud provides both workload protection and posture management. For Azure Storage, the Defender plan (Microsoft Defender for Storage) offers threat detection such as anomalous access, malware scanning, and sensitive-data threat alerts, while the CSPM guidance in Defender for Cloud flags misconfigurations that create vulnerabilities (for example, public blob access, weak TLS settings). CSPM capabilities-secure score, recommendations, and baseline assessments-are available to all Azure subscriptions (foundational CSPM), giving every tenant visibility into security posture without requiring a premium add-on for basic posture features. Beyond Azure, Defender for Cloud supports hybrid and multicloud: using Azure Arc and the Defender for Servers plan, it can onboard and assess on-premises servers and resources in other clouds, applying recommendations, security assessments, and threat protections across those environments. Collectively, these capabilities confirm that Defender for Cloud can detect storage- related threats and posture weaknesses, CSPM is broadly available to Azure subscriptions, and the service evaluates workloads running in Azure or on-premises.

質問: 97

文を正しく完成させる答えを選択してください。

An Azure resource can use a system-assigned

Azure Active Directory (Azure AD) joined device

managed identity

service principal

user identity

to access Azure services.

正解:

An Azure resource can use a system-assigned

Azure Active Directory (Azure AD) joined device

managed identity

service principal

user identity

to access Azure services.

Explanation:

An Azure resource can use a system-assigned

Azure Active Directory (Azure AD) joined device

managed identity

service principal

user identity

to access Azure services.

In Microsoft Entra ID (formerly Azure AD), Managed Identities for Azure resources are the built-in way for an Azure resource to authenticate to other Azure services without storing credentials. Microsoft's documentation states: "Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory." It further distinguishes the two

types and clarifies the one used here: "A system-assigned managed identity is enabled directly on an Azure service instance. When enabled, Azure creates an identity for the instance in Azure AD." Microsoft also emphasizes the lifecycle binding:

"This identity is tied to the lifecycle of that service instance and is deleted when the resource is deleted." Once enabled, the resource can call Azure services by requesting tokens: "You can use this identity to obtain Azure AD tokens for authentication to services that support Azure AD authentication." Because the prompt explicitly says "system-assigned", the correct completion is managed identity. The other options do not match Microsoft's definition: a user identity refers to a human user; a service principal is the underlying object applications use but isn't what Azure terms "system-assigned"; and an Azure AD-joined device pertains to device registration, not resource-to-service authentication. Therefore, the sentence correctly reads: "An Azure resource can use a system-assigned managed identity to access Azure services."

質問: 98

文を正しく完成させる答えを選択してください。

Answer Area



Microsoft Defender for Cloud provides cloud workload protection for Azure and hybrid cloud resources.

Microsoft Defender for Cloud

Azure Monitor

Microsoft cloud security benchmark

Microsoft Secure Score

正解:

Answer Area



Microsoft Defender for Cloud provides cloud workload protection for Azure and hybrid cloud resources.

Microsoft Defender for Cloud

Azure Monitor

Microsoft cloud security benchmark

Microsoft Secure Score

Explanation:

Answer Area



Microsoft Defender for Cloud provides cloud workload protection for Azure and hybrid cloud resources.

In Microsoft's security portfolio, Microsoft Defender for Cloud is the service that provides cloud workload protection for Azure and hybrid cloud resources. Microsoft describes it as a "cloud-native application protection platform (CNAPP) that helps strengthen the security posture of your cloud resources and protect workloads across multicloud and hybrid environments." The service delivers Cloud Security Posture Management (CSPM) and Cloud Workload Protection (CWP) by continuously assessing configurations and protecting workloads such as virtual machines, containers, databases, and storage. Documentation further states that Defender for Cloud "provides threat protection for workloads running in Azure, on-premises, and in other clouds," giving a single pane to harden resources, detect active threats, and remediate.

By contrast, Azure Monitor focuses on telemetry and observability; the Microsoft cloud security benchmark is a set of prescriptive best practices; and Microsoft Secure Score is an aggregate metric reflecting security posture. None of those deliver the workload protection and active defense capabilities (e.g., recommendations, hardening, and threat detection for servers, containers, and PaaS services) that Defender for Cloud offers.

Therefore, the sentence correctly completes as: Microsoft Defender for Cloud provides cloud workload protection for Azure and hybrid cloud resources.

質問: 99

Microsoft Secure Score for Devices が含まれるサービスはどれですか?

- A. Microsoft Defender for Endpoint
- B. Microsoft Defender for Identity

- C. Microsoft Defender for IoT
- D. Microsoft Defender for Office 365

正解: ([正解を表示します](#))

質問: 100

文を正しく完成させる答えを選択してください。



正解:



Explanation:

In Microsoft Sentinel, playbooks are the feature that integrates with Azure Logic Apps to automate response.

Microsoft's documentation describes them as "collections of procedures that can be run from Microsoft Sentinel in response to an alert" and clarifies that "playbooks are built on Azure Logic Apps" providing a workflow engine and a gallery of connectors to other Microsoft and third-party services. Playbooks can be triggered automatically from analytics rules or manually from incidents and alerts, enabling orchestration such as assigning owners, creating tickets, disabling accounts, blocking IPs, or posting to collaboration channels.

The platform emphasizes that the Logic Apps foundation gives security teams a visual designer, managed connectors, and run history to track execution and outcomes. In short, Sentinel uses playbooks to "automate and orchestrate responses to alerts and incidents", reducing mean-time-to-respond and standardizing actions across your SOC. Other Sentinel components serve different purposes: analytic rules detect threats, hunting queries aid proactive investigation, and workbooks provide dashboards and visualizations. Therefore, the correct completion is: Microsoft Sentinel playbooks use Azure Logic Apps to automate and orchestrate responses to alerts.

質問: 101

Azure Sentinel と別のセキュリティ ソースの間のリアルタイム統合を提供するには何を使用しますか？

- A. Azure AD コネクト
- B. Log Analytics ワークスペース
- C. Azure 情報保護
- D. データコネクタ

正解: ([正解を表示します](#))

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>

有効的な**SC-900J**問題集はJPNTest.com提供され、**SC-900J**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-900J**試験問題集を提供します。JPNTest.com SC-900J試験問題集はもう更新されました。ここで**SC-900J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SC-900J-mondaishu> 273問、30%ディスカウント、特別な割引コード: **JPNshiken**」