Microsoft.SC-900.v2026-07-23.q205

試験コード:	SC-900
試験名称:	Microsoft Security Compliance and Identity Fundamentals
認定資格:	Microsoft
無料問題数:	205
バージョン:	v2026-07-23
アクセス数:	112
ページビュー数:	2050
https://www.jpnpdf.com/Microsoft.SC-900.v2026-07-23.q205-mondaishu.html	

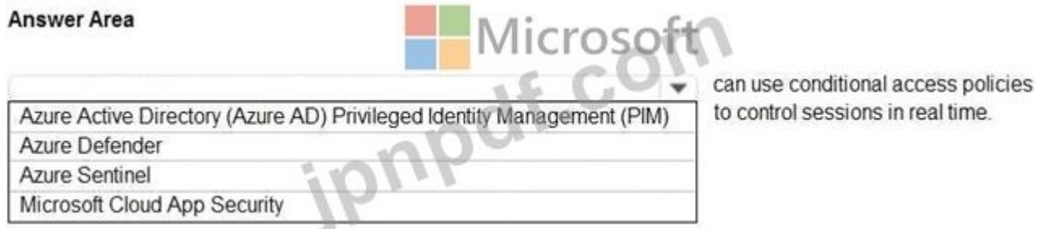
最新問題: **1**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

最新問題: **2**

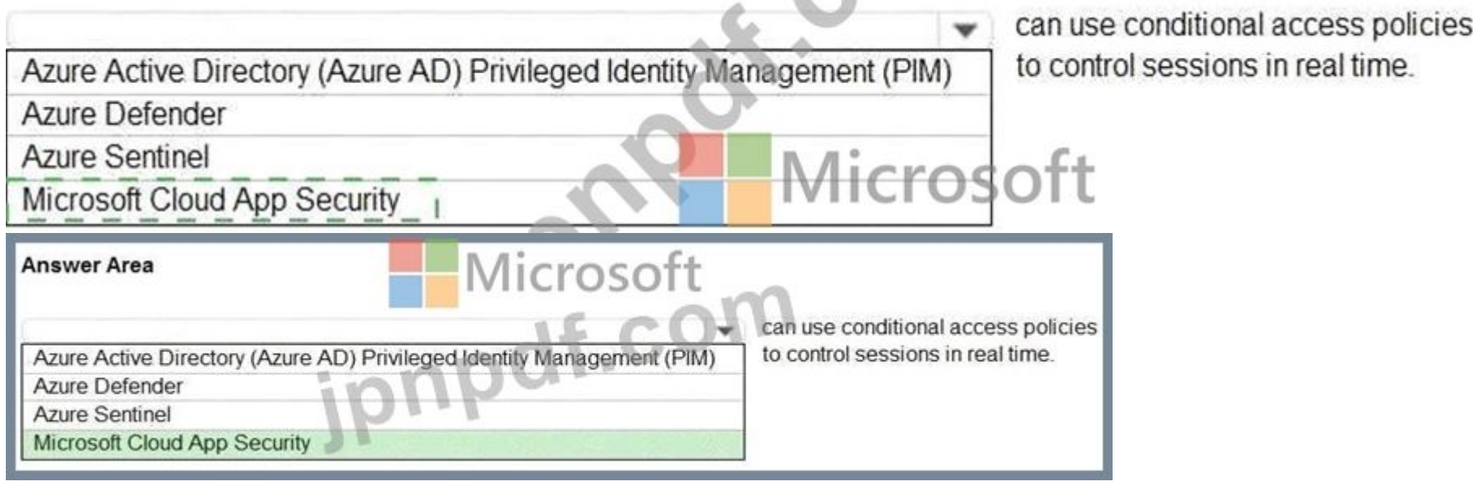
文を正しく完成させる選択肢を選びなさい。

Answer Area



Answer:

Answer Area



最新問題: **3**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:
アクセスおよびアプリケーション制御
Microsoft Defender for Cloud では、アクセス制御とアプリケーション制御としてグループ化された機能は、Azure 仮想マシンへのアクセス権限と実行権限の両方を制限することで、仮想マシンのセキュリティを強化するように設計されています。Microsoft のドキュメントでは、アダプティブ アプリケーション制御は 既知の安全なアプリケーションのみを許可することで、仮想マシン上で実行できるアプリケーションを制御できる」と説明されており、マルウェアやその他の不要なアプリケーションのブロックに直接役立ちます。同じ機能群であるジャストインタイム (JIT) VM アクセスは、 仮想マシンへの受信トラフィックをロックダウンし、承認されたユーザーに対して必要なポートのみを限られた時間だけ開くことで、攻撃への露出を軽減」し、ネットワーク攻撃対象領域を縮小します。これらの機能は、Defender for Cloud の推奨事項とポリシーに示されており、ネットワークのエッジとエンドポイント実行レイヤーで最小権限の原則を強制します。
それに対し、クラウドセキュリティ態勢管理 (CSPM) は継続的な評価とセキュリティスコアに基づく推奨事項を提供しますが、アプリケーションを積極的にブロックしたり、受信アクセスに時間制限を設けたりする制御機能ではありません。
コンテナセキュリティはコンテナイメージとランタイムを対象とし、脆弱性評価はソフトウェアの脆弱性を特定しますが、許可リストや時間制限付きアクセスを強制するものではありません。したがって、適切な補完項目はアクセスとアプリケーション制御であり、これには適応型アプリケーション制御とJIT VMアクセスが含まれ、不要なアプリケーションからVMを保護し、露出するネットワーク領域を最小限に抑えます。

最新問題: **4**
文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題: **5**
貴社は、セキュリティ情報およびイベント管理 (SIEM) ソリューションを含む、さまざまなセキュリティ製品を評価しています。SIEMソリューションの機能に関する情報を提供する必要があります。SIEMソリューションの機能とは何ですか？
A. ネットワークアクティビティをレビューし、どのアプリケーションやサービスが通信できるかについてのレポートを提供する機能
B. ログを確認し、悪意のある活動に関するレポートを提供する機能
C. ユーザーがAzureの利用限度額に達した際にアラートを発するアラートシステム

D. 自動インシデント修復
Answer: (解答を表示する**)**

最新問題**: 6**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	●	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	●	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	●	○

最新問題**: 7**
コンプライアンススコアのアクションの種類を、適切なタスクと一致させてください。

回答するには、左側の列から適切なアクションタイプを右側のタスクにドラッグしてください。各タイプは、1回、複数回、またはまったく使用しないことができます。
注：正解つにつき1ポイントが加算されます。

Answer:

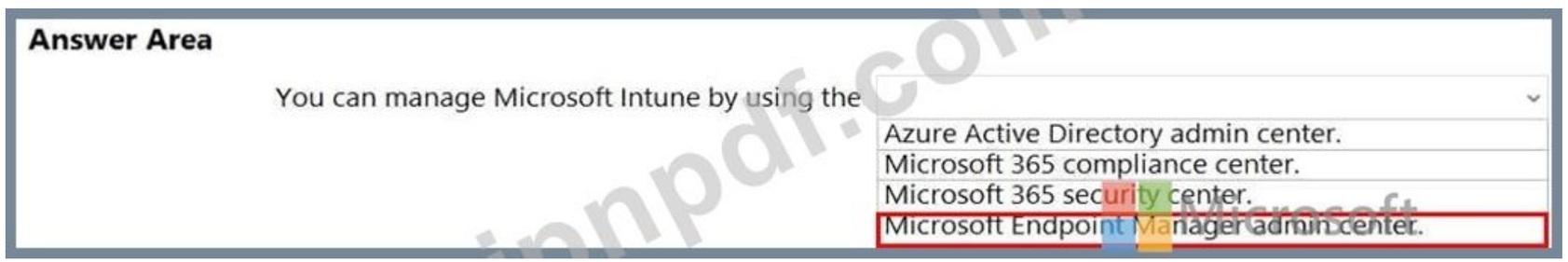
Explanation:

Microsoft Purview Compliance Manager では、改善策は、リスクをどのように軽減し、コンプライアンス スコアにどのように貢献するかを反映するように、制御タイプ別に分類されます。Microsoft の SCI ガイダンスでは、予防的制御とは、 保護を事前に適用することでセキュリティまたはコンプライアンス インシデントの発生を防ぐ たとえば、保存時および転送時のデータの暗号化、アクセス制限、構成ベースラインの適用など）」保護策であると説明しています。これは、 保存時のデータを暗号化して保護する」というタスクに直接対応しており、不正な開示が発生する前に阻止することを目的とした、古典的な予防メカニズムです。
また、このガイダンスでは、検出制御とは 異常またはコンプライアンス違反の活動を特定、記録、顕在化させ、調査および対処できるようにする措置（例えば、継続的な監視、アラート、監査ログ記録、および分析）」であると規定しています。これは、『リスクとなる可能性のある異常を特定するためにシステムを積極的に監視する」ことに相当します。なぜなら、その目的は、疑わしい行動や逸脱が発生した時点でそれを検出することだからです。
これに対し、是正措置は 問題が発見された後に問題を修復し、望ましい状態に戻す（例パッチ適用、インシデント対応、構成修正）」ために使用されます。記載されている2つのタスクには是正措置が記載されていないため、 是正」は選択されません。このマッピングは、コンプライアンス マネージャーが、リスク軽減効果に基づいてコンプライアンス スコアにポイントをもたらすアクションをどのように分類するかを示しています。

最新問題: **8**
文を正しく完成させる選択肢を選びなさい。

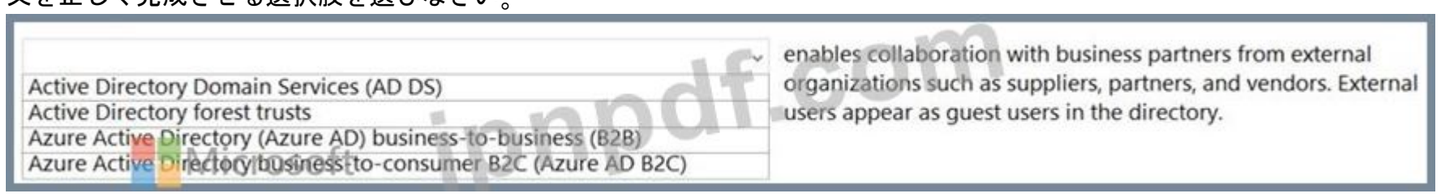
Answer Area

Answer:

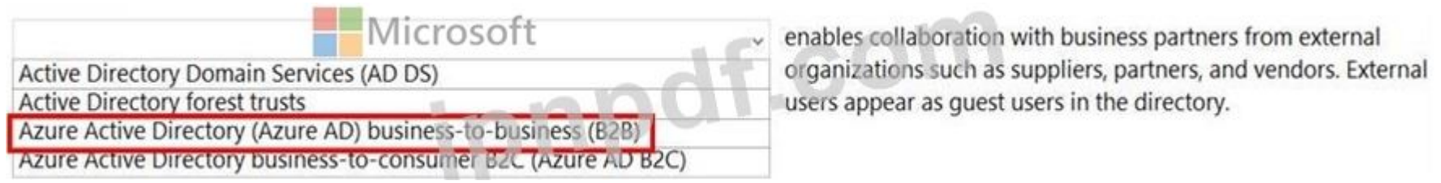


最新問題**: 9**

文を正しく完成させる選択肢を選びなさい。



Answer:



参照：

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

最新問題**: 10**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Answer:

Statements	Yes	No
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Explanation:

Statements	Yes	No
Users can apply sensitivity labels manually.	○	○
Multiple sensitivity labels can be applied to the same file.	○	○
A sensitivity label can apply a watermark to a Microsoft Word document.	○	○

Microsoft の機密ラベル (Microsoft Purview Information Protection) は、ユーザー主導のラベル付けをサポートしています。 ロユーザーは、ファイルやメールに機密ラベルを手動で適用できます」。また、組織は自動または推奨ラベル付けを構成することもできます。これは、ポリシーで許可されている場合、エンドユーザーが自分でラベルを選択できることを裏付けています。Microsoft は、アイテムのカーディナリティについても明確にしています。 ドキュメントまたはメールには、一度に 1 つの機密ラベルしか適用できません」。したがって、同じファイルに複数の機密ラベルを適用することはサポートされていません (ラベルは、特定のアイテムに対して相互に排他的です)。分類に加えて、ラベルは保護と視覚的なマーキングを強制できます。 機密ラベルを構成する際に、暗号化やコンテンツマーキング (ヘッダー、フッター、透かし) などの保護設定を追加できます」。Word、Excel、PowerPoint はこれらのコンテンツマーキングを尊重するため、ラベルは Word ドキュメントに自動的に透かしを刻印し、永続的な保護のためにラベルのメタデータを埋め込むことができます。Microsoft の SCI ドキュメントからのこれらの公式な記述を総合すると、正しい回答は次のようになります。はい (手動適用)、いいえ (ファイルごとに 1 つのラベルのみ)、はい (ラベルで透かしを適用可能)。

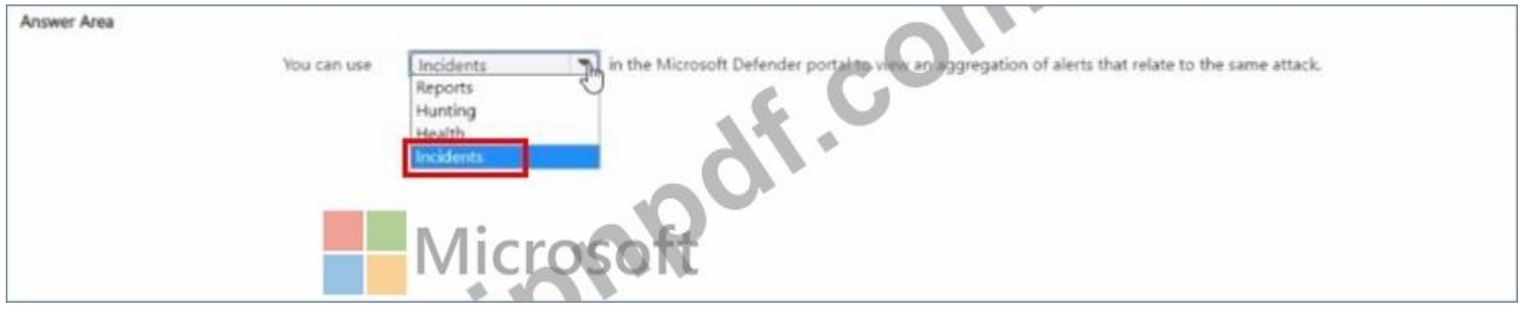
最新問題: **11**
文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題: **12**

文を正しく完成させる選択肢を選びなさい。

Answer:

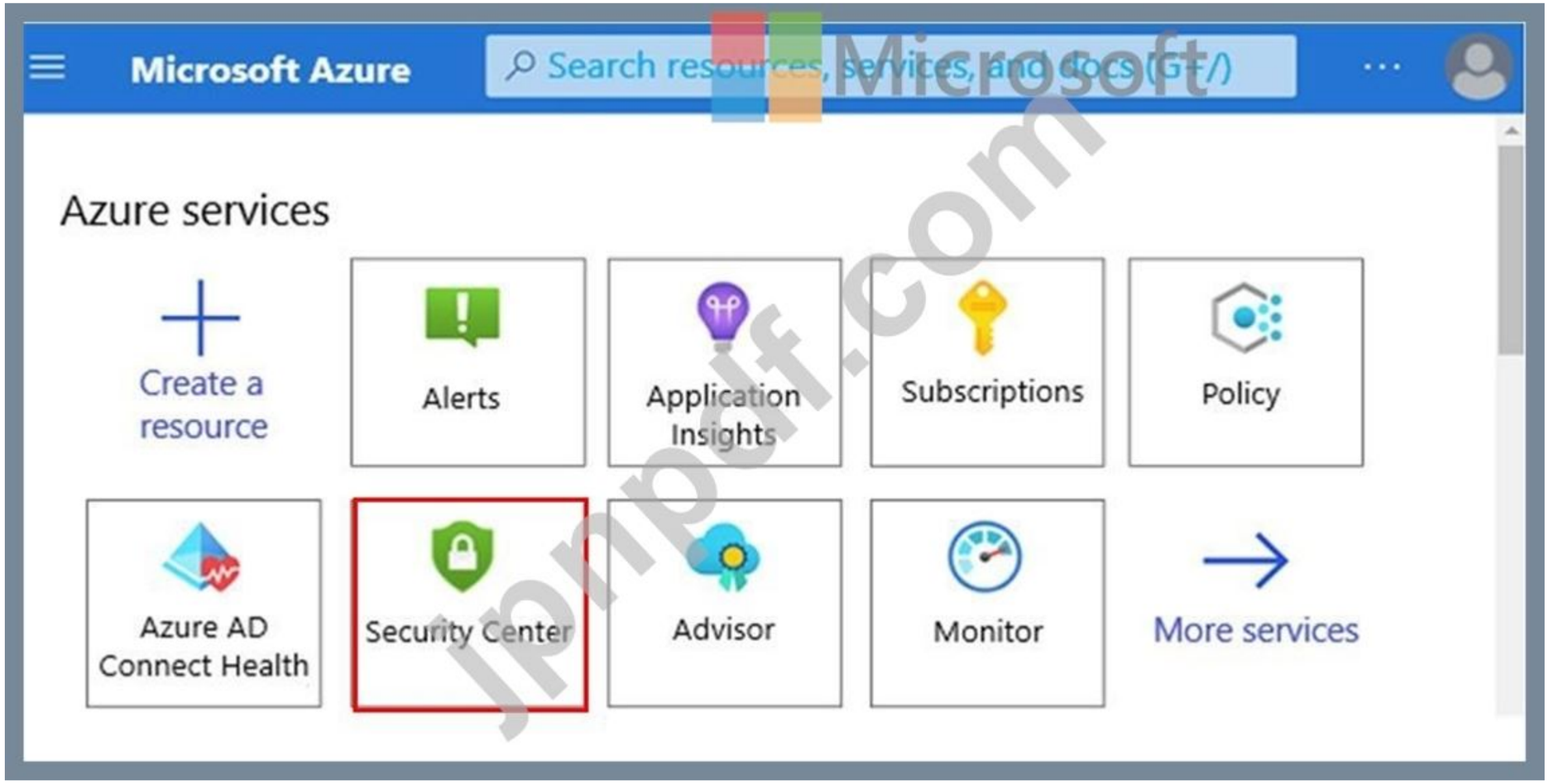


最新問題: **13**

Azureのセキュリティスコアを確認するには、どのサービスを使用すればよいですか？回答するには、回答欄で適切なサービスを選択してください。


Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Alerts
Application Insights
Subscriptions
Policy
Azure AD Connect Health
Security Center
Advisor
Monitor
More services
jpnpdf.com
Microsoft

Answer:



参照：
https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

最新問題: 14
以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Answer:

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	○	○
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.	○	○

Answer Area

Statements	Yes	No
Microsoft Sentinel uses logic apps to identify anomalies across resources.	○	●
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.	●	○

最新問題: **15**

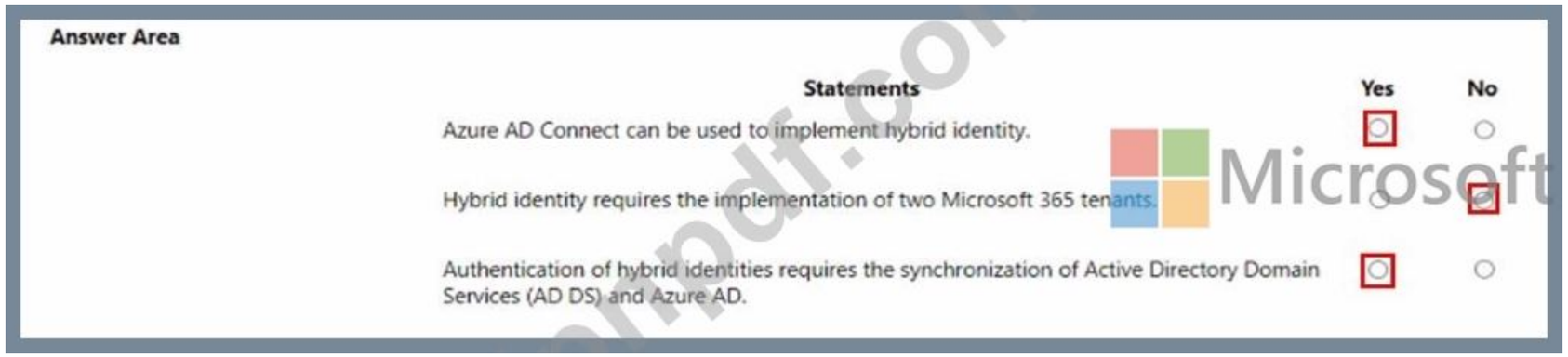
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:



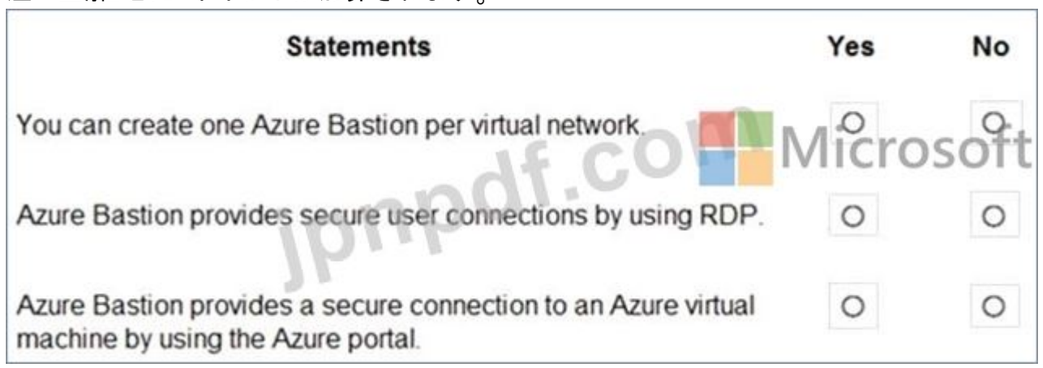
最新問題: **16**
Azure Firewall で保護できるリソースの種類はどれですか？正解はそれぞれ完全な解決策を示しています。
注：正解ごとに1ポイントが加算されます。
A. Azure仮想マシン
B. Azure Active Directory (Azure AD) ユーザー
C. Microsoft Exchange Online の受信トレイ
D. Azure仮想ネットワーク
E. Microsoft SharePoint Online サイト
Answer: (解答を表示する**)**
説明
ファイアウォールは仮想ネットワークを直接保護しているわけではないが、DDoS攻撃対策は仮想ネットワークにとって理想的だっただろう。

最新問題: **17**
文を正しく完成させる選択肢を選びなさい。

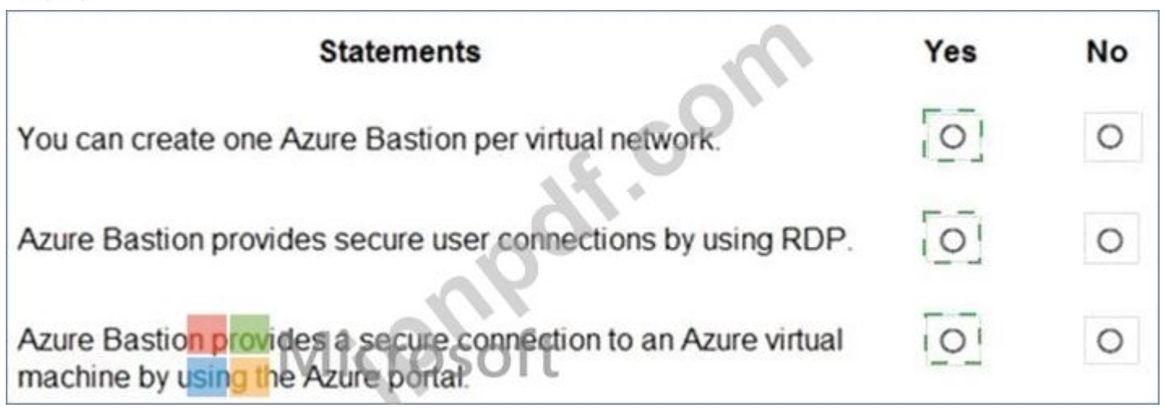
Answer:

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

最新問題: 18
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:

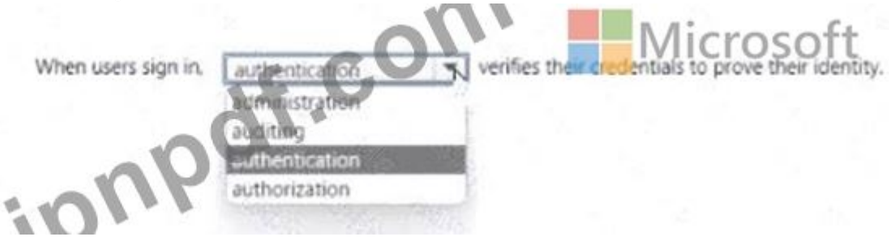


Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

最新問題: **19**

文を正しく完成させる選択肢を選びなさい。

Answer Area



Answer:

最新問題: **20**

文を正しく完成させる選択肢を選びなさい。

Answer:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication

- is stored on an external device.
- is stored on a local device only.
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

最新問題: **21**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	●	○

参照：

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

最新問題: **22**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Answer:

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

参照：
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune
https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

最新問題: **23**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	○
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	○	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

Answer:

最新問題: 24

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

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

Answer:

参照：

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

最新問題: 25

文を正しく完成させる選択肢を選びなさい。

Answer:

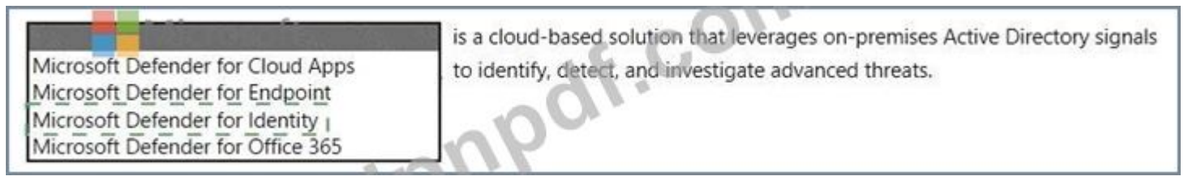
参照：

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

最新問題: 26

文を正しく完成させる選択肢を選びなさい。

Answer:



Explanation:

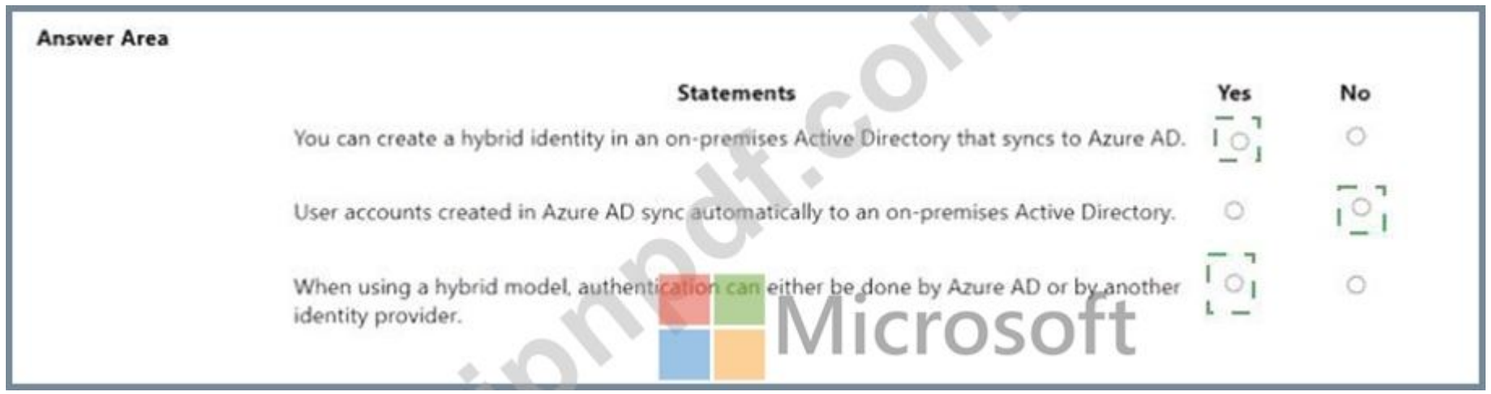
Microsoft Defender for Identity（旧称Azure Advanced Threat Protection、Azure ATP）は、オンプレミスの Active Directory シグナルを活用して、組織を標的とした高度な脅威、侵害された ID、および悪意のある内部犯行を特定、検出、調査するクラウドベースのセキュリティ ソリューションです。

最新問題: **27**
攻撃シミュレーション訓練機能が含まれているサービスは何ですか？
A. Microsoft Defender for Identity
B. Microsoft Defender for Office 365
C. Microsoft Defender for SQL
D. B
E. Microsoft Defender for Cloud Apps
Answer: (解答を表示する)

最新問題: **28**
あなたはAzureサブスクリプションをお持ちです。
承認制で時間制限のある役割有効化を実装する必要があります。
何を使うべきでしょうか？
A. Azure Active Directory（Azure AD）ID保護
B. Azure Active Directory（Azure AD）でのアクセスレビュー
C. Azure Active Directory（Azure AD）特権ID管理（PIM）
D. Windows Hello for Business
Answer: (解答を表示する)

最新問題: **29**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:



Explanation:

Microsoft は、ハイブリッド ID をオンプレミスの Active Directory と Microsoft Entra ID (Azure AD) を統合し、クラウドとオンプレミスのアプリケーション全体で単一の ID を実現するために 「オンプレミスの ID が Azure AD に同期される」ものと説明しています。このモデルでは、ディレクトリ オブジェクト (ユーザー、グループ、および選択された属性) は、Azure AD Connect または Cloud Sync を使用してオンプレミス AD から Azure AD に流れます。これは、ハイブリッド環境におけるプロビジョニングの標準的な方向です。Microsoft はさらに、特定の書き戻し機能 (パスワードの書き戻し、デバイスまたはグループの書き戻しシナリオなど) はサポートされていますが、クラウドで作成されたユーザーはオンプレミス AD に自動的に同期されないと説明しています。特定の限定的な書き戻し機能を展開しない限り、アカウント プロビジョニングはオンプレミスで権限を持ち続けます。つまり、「Azure AD から AD DS へのユーザー アカウントの作成」はデフォルトでは行われません。認証に関して、Microsoft は、ハイブリッド ID はクラウド認証 (パスワード ハッシュ同期またはパススルー認証) をサポートしており、Azure AD がサインインを実行するか、別の ID プロバイダー (AD FS やサードパーティの IdP など) とのフェデレーションをサポートし、そのプロバイダーが資格情報を検証して Azure AD にトークンを発行すると述べています。これらの記述は、ハイブリッド ID に関する Microsoft の SCI ガイダンスと一致しています。オンプレミスからクラウドへの同期は標準ですが、自動的な逆方向のユーザー同期は標準ではなく、認証は選択したサインイン方法に応じて Azure AD またはフェデレーションされた IdP によって処理されます。

最新問題: **30**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
You can add a resource lock to an Azure subscription.	○	○
You can add only one resource lock to an Azure resource.	○	○
You can delete a resource group containing resources that have resource locks.	○	○

Answer:
説明
グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます

Statements	Yes	No
You can add a resource lock to an Azure subscription.	○	○
You can add only one resource lock to an Azure resource.	○	○
You can delete a resource group containing resources that have resource locks.	○	○

最新問題: **31**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

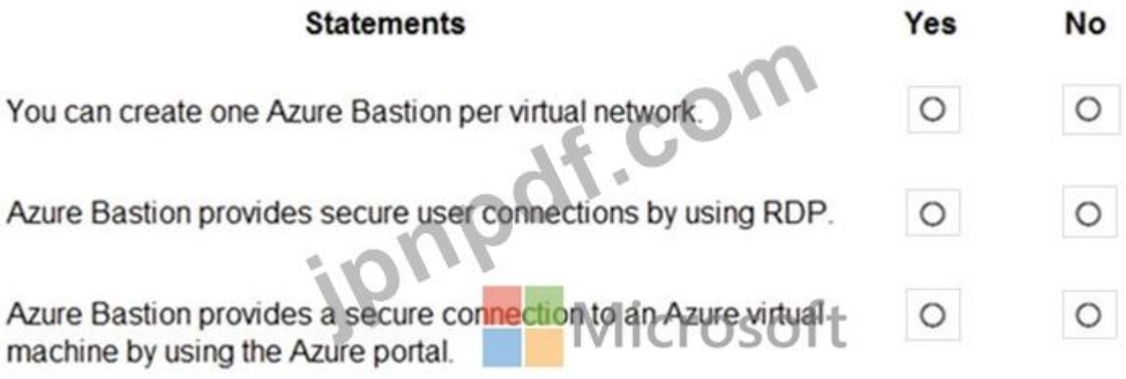
Answer Area

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.	○	○

Answer:

参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

最新問題: 32
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



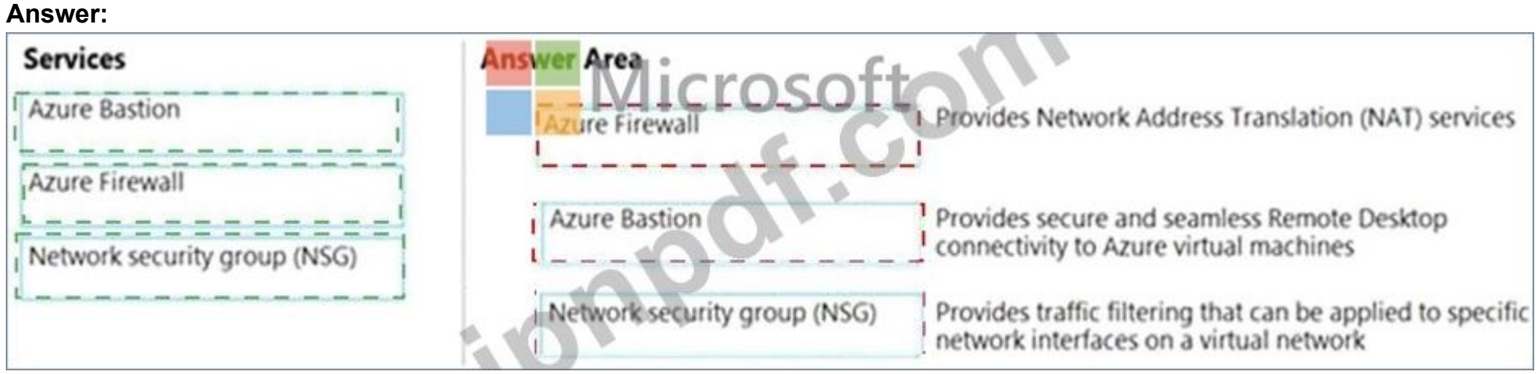
Answer:

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

参照：
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal

最新問題: **33**
Azureのネットワークサービスを適切な説明と一致させてください。
回答するには、左側の列から該当するサービスを右側の説明欄にドラッグしてください。各サービスは、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：正解つにつき1ポイントが加算されます。

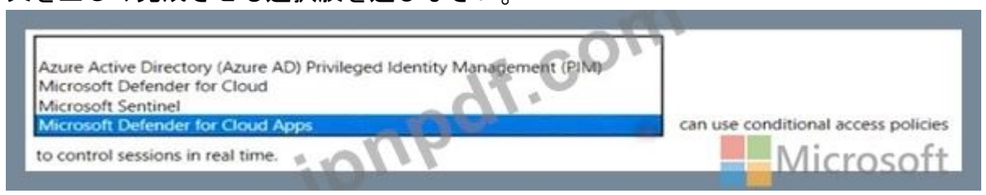
Answer:



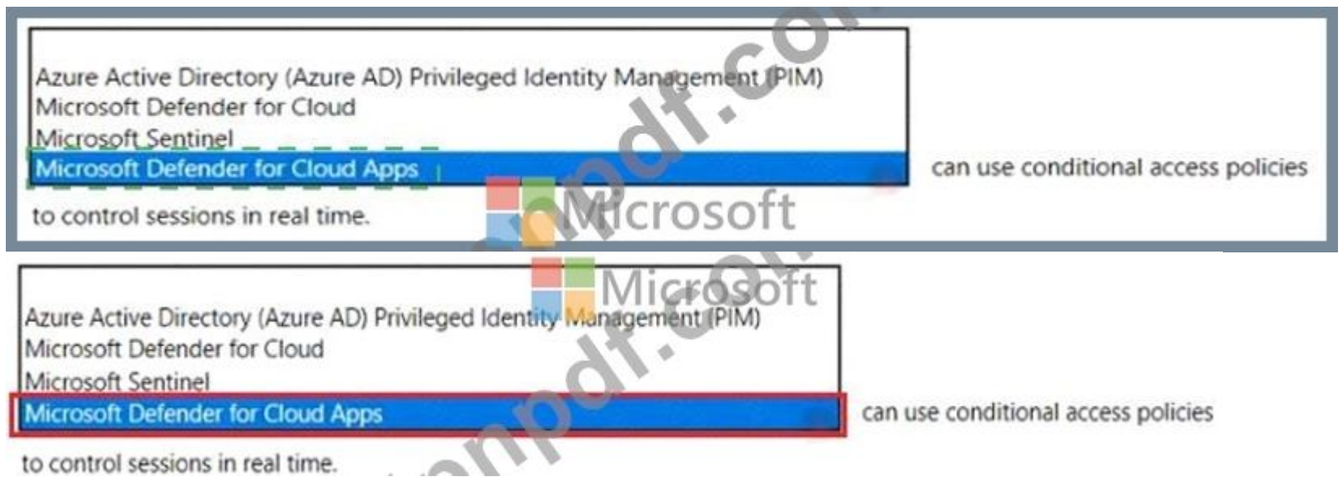
Explanation:

MicrosoftのAzureネットワークサービスには、プロンプト内の記述に直接対応する明確な役割があります。
Azure Firewallは、ステートフルなクラウドネイティブのネットワークセキュリティサービスであり、トラフィックフローの制御と変換のために、送信元NAT（SNAT）と宛先NAT（DNAT）を明示的にサポートしています。Microsoftの説明によると、Azure Firewallは「受信トラフィックと送信トラフィックのネットワークアドレス変換（SNAT/DNAT）とフィルタリングを提供する」ため、NATサービスに最適です。
Azure Bastionは、仮想マシンにパブリックIPアドレスを公開することなく、Azureポータルから TLS経由で仮想マシンへの安全かつシームレスなRDPおよびSSH接続を直接提供するように設計されています。これは、Azure仮想マシンへの安全なリモートデスクトップ接続と完全に一致します。
ネットワークセキュリティグループ（NSG）は、Azureに組み込まれたトラフィックフィルタリングの仕組みです。Microsoftは、NSGには「複数の種類のAzureリソースへの受信ネットワークトラフィック、またはそれらのリソースからの送信ネットワークトラフィックを許可または拒否するセキュリティルールが含まれている」と説明しており、ルールは仮想ネットワーク上のサブネットまたは個々のネットワークインターフェイス（NIC）に適用できます。したがって、NSGは特定のネットワークインターフェイスに適用されるトラフィックフィルタリングに最適な選択肢です。
これらのマッピングは、Azureの階層型ネットワークセキュリティモデルを反映しています。具体的には、NIC/サブネットでのルールベースのフィルタリングにはNSG、集中型のステートフルインスペクションとNATにはAzure Firewall、そして安全なブラウザベースのRDP/SSHアクセスにはAzure Bastionが用いられています。

最新問題: **34**
文を正しく完成させる選択肢を選びなさい。



Answer:

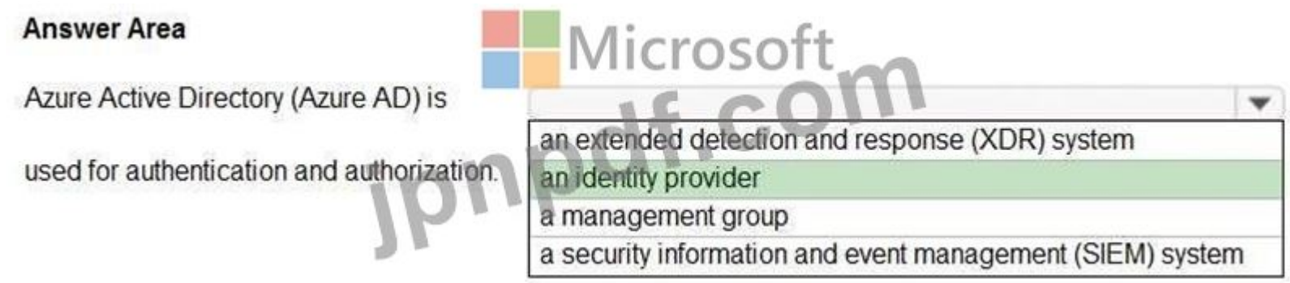


最新問題: **35**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

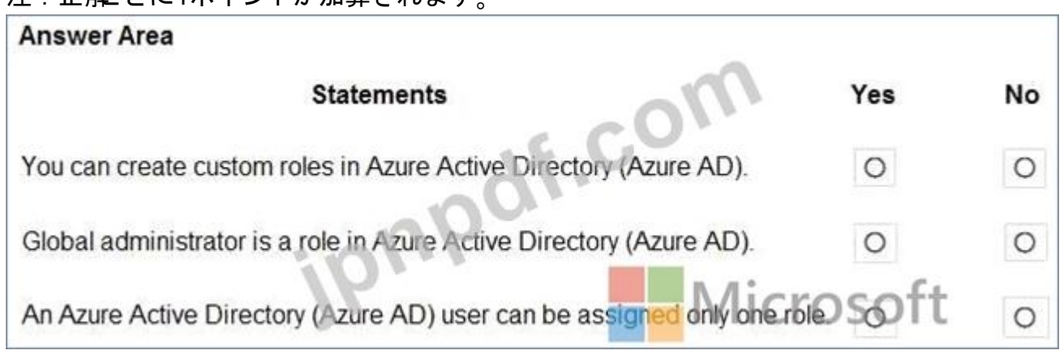


Azure Active Directory (Azure AD) は、クラウドベースのユーザーIDおよび認証サービスです。参照:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

最新問題: **36**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

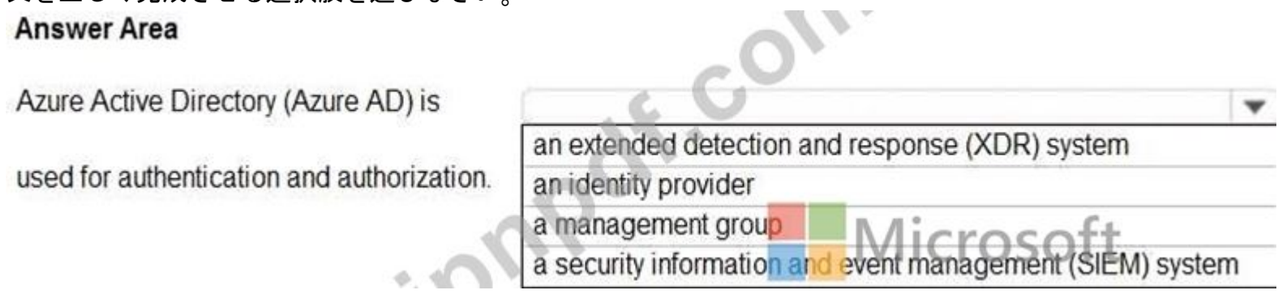
注：正解ごとに1ポイントが加算されます。



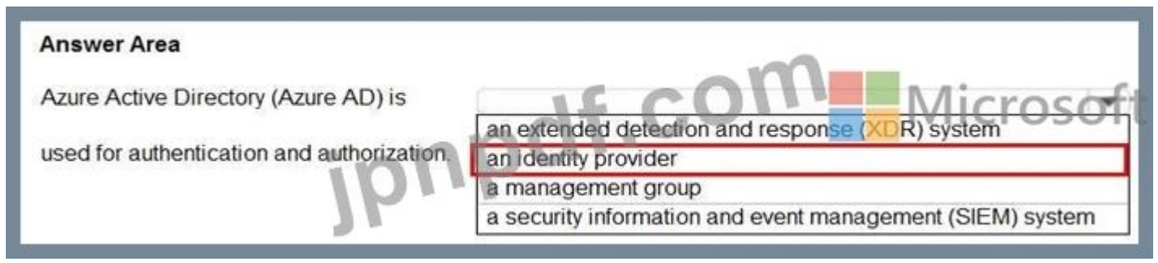
Answer:

参照：
https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

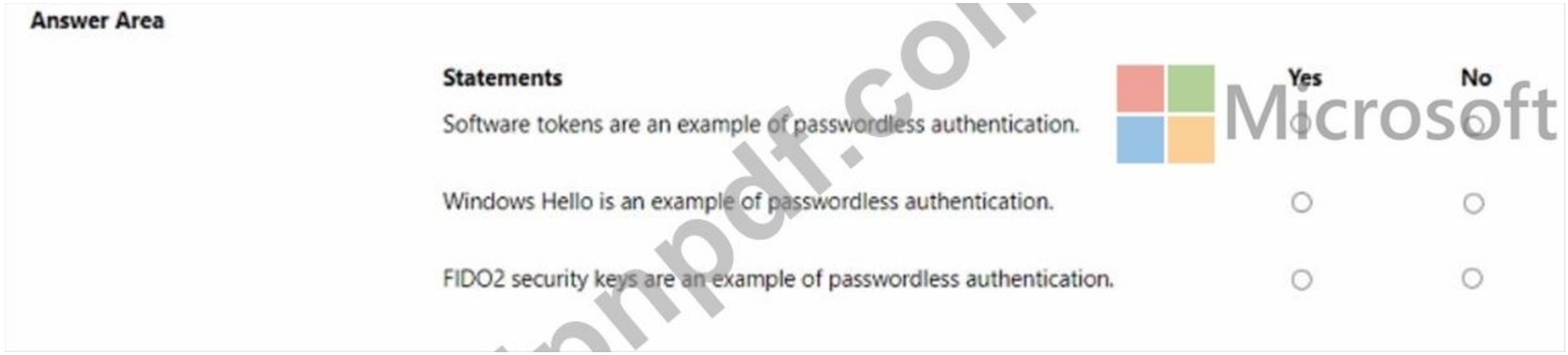
最新問題**: 37**
文を正しく完成させる選択肢を選びなさい。



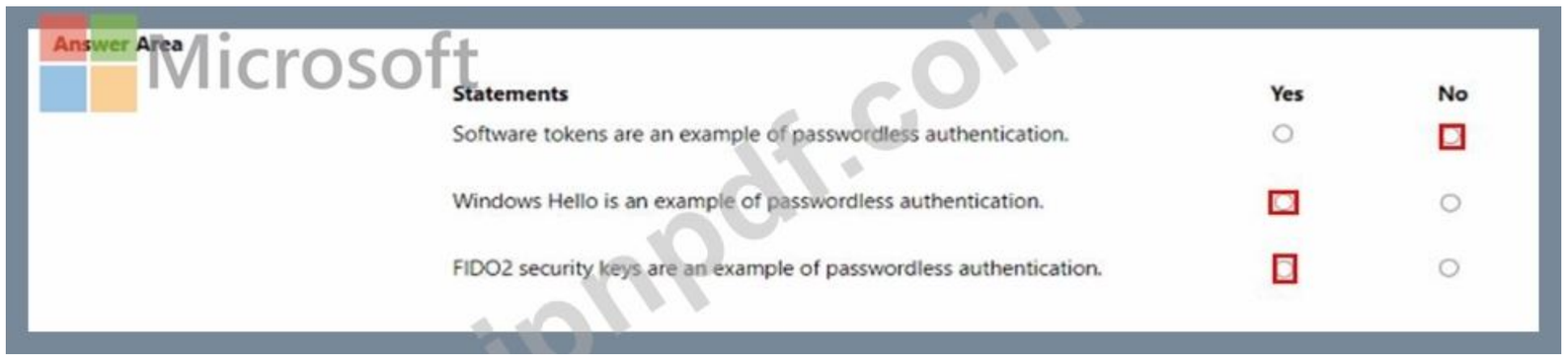
Answer:



最新問題**: 38**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

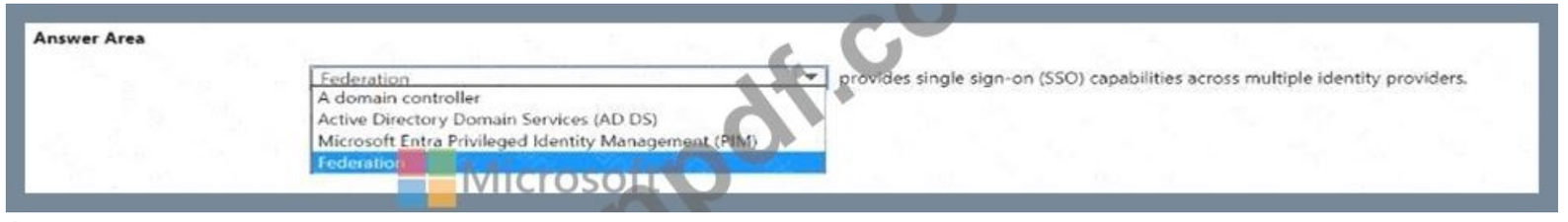


Answer:



最新問題: **39**

文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:

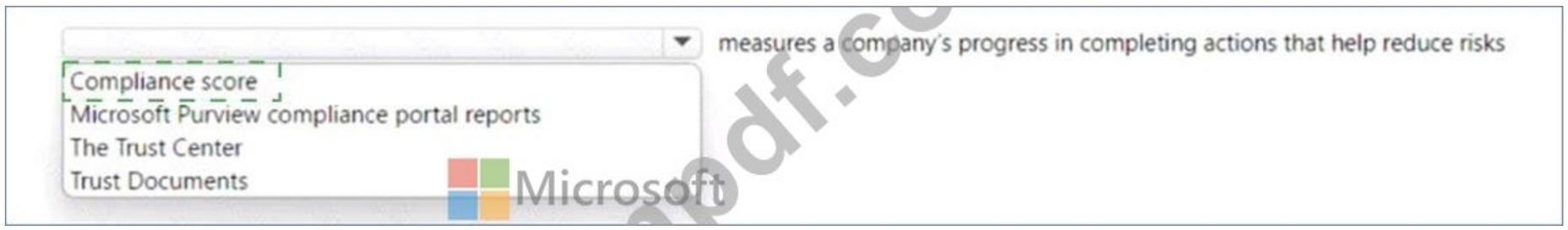
Microsoft の ID アーキテクチャでは、フェデレーションによって異なる ID プロバイダー間の信頼関係が確立され、組織やプラットフォームの境界を越えたシングル サインオン (SSO) が可能になります。Microsoft Learn では、フェデレーションは SAML、WS-Federation、OpenID Connect/OAuth 2.0 などの標準規格を使用し、ユーザーがホーム ID プロバイダーで認証を行い、リライングパーティ (アプリケーションまたはサービス) が受け入れるトークンを取得できるようにしていると説明しています。この信頼関係により、組織はパスワードをコピーしたり資格情報を同期したりすることなく、安全に ID を共有でき、複数のシステムやクラウド間でシームレスなサインイン エクスペリエンスを実現できます。

対照的に、Active Directoryドメインサービス（AD DS）とドメインコントローラーは、主に単一のWindowsドメイン/フォレスト内でKerberosを使用してオンプレミスのディレクトリおよび認証サービスを提供します。

/NTLMは、単独ではプロバイダー間SSOを実現しません。Microsoft Entra Privileged Identity Management（PIM）は、役割のジャストインタイム承認ベースの昇格を管理するものであり、SSO機能を提供するものではありません。したがって、複数のIDプロバイダー間でSSOを提供することを目的とした技術は、フェデレーションです。

最新問題: **40**
文を正しく完成させる選択肢を選びなさい。

Answer:

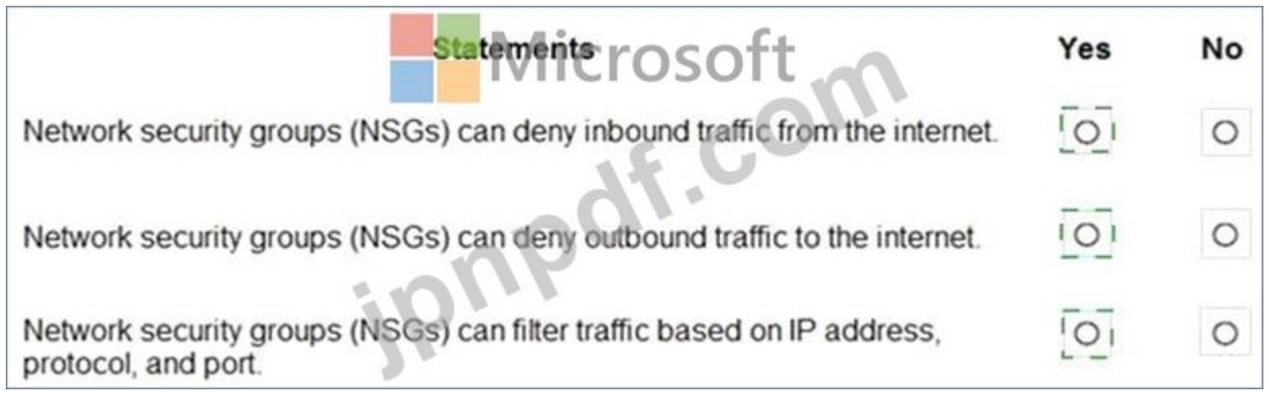


説明
コンプライアンススコア

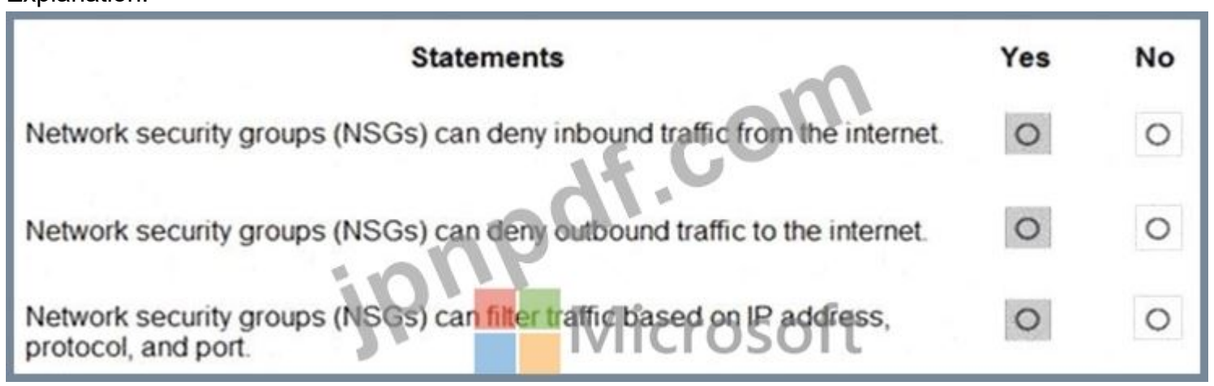
最新問題: **41**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:



Explanation:



Azure ネットワーク セキュリティ グループを使用すると、Azure 仮想ネットワーク内の Azure リソースとの間で送受信されるネットワーク トラフィックをフィルタリングできます。ネットワーク セキュリティ グループには、さまざまな種類の Azure リソースへの受信ネットワーク トラフィック、またはそこからの送信ネットワーク トラフィックを許可または拒否するセキュリティ ルールが含まれています。各ルールに対して、送信元と宛先、ポート、およびプロトコルを指定できます。

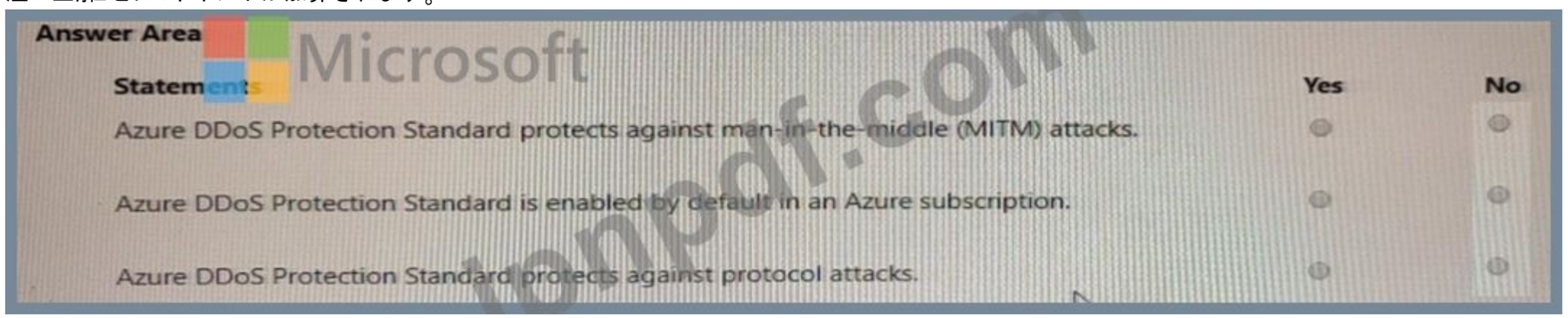
参照：

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

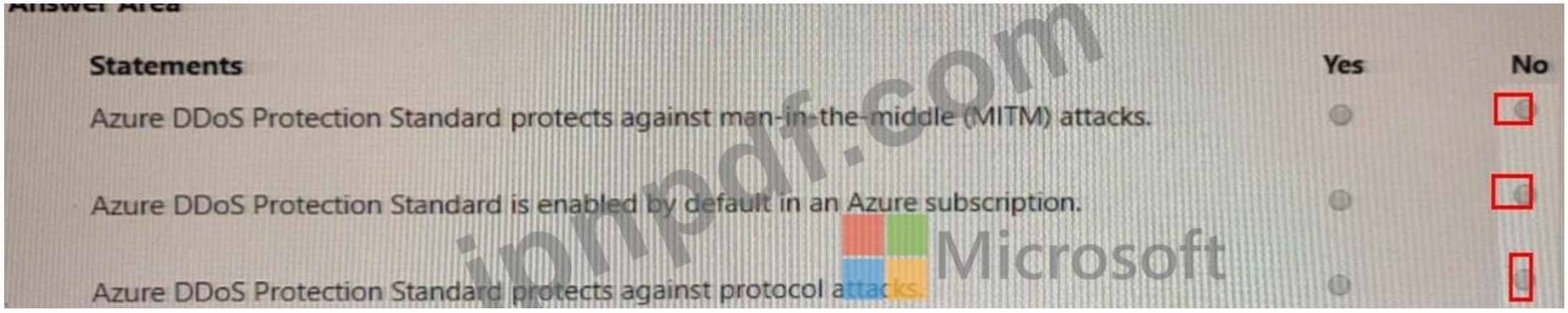
最新問題: 42

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



Answer:



最新問題: **43**

文を正しく完成させる選択肢を選びなさい。

Answer:

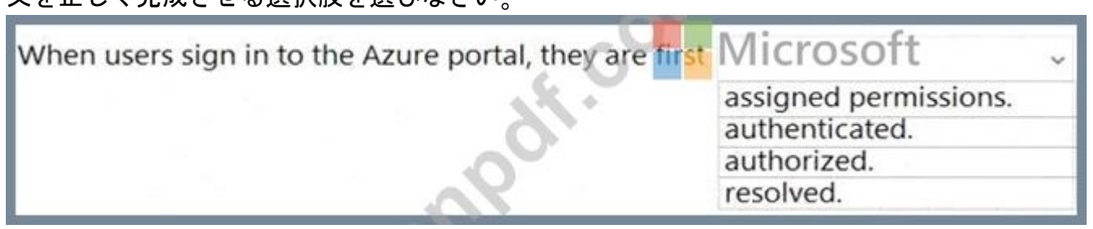
。

参照：

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

最新問題: **44**

文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:

Microsoft クラウド ID では、Azure リソースへのアクセスは、認証、認可という従来の順序に従います。Microsoft Learn では、この 2 つのステップを明確に定義しています。 認証とは、個人またはサービスの ID を確立するプロセスです」、一方 認可とは、個人またはサービスが実行できる操作を決定するプロセスです」。Azure サインインでは、Microsoft Entra ID (旧 Azure AD) がまずユーザーの資格情報 (パスワード、MFA、条件付きアクセス、デバイス準拠、リスク評価) を検証します。検証が成功すると、ユーザーの ID を証明するセキュリティ トークンが発行されます。この ID が確立されて初めて、Azure は認可に進みます。認可では、Azure Resource Manager がロールベースのアクセス制御 (RBAC) の割り当てを評価し、許可される操作を決定します。SCI ガイダンスでは、ゼロ トラストのこの順序を強調しています。 明示的に検証する」(強力なシグナルで認証する)、次に 最小権限アクセスを使用する」(RBAC または特権 ID 管理によって認可する)。したがって、ユーザーが Azure ポータルにサインインすると、最初のステップは認証、つまりユーザーが誰であるかを確認することです。次のステップは認証です。これは、役割、範囲、ポリシーに基づいて、ユーザーがアクセスできるリソースと操作を決定します。この順序付けは、Microsoft 365 および Azure 全体における安全な ID およびアクセス管理の基盤となります。

最新問題: **45**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

評価

Microsoft Purview Compliance Managerでは、評価は、特定の規制、基準、または要件に基づく管理策のグループへの準拠状況を追跡するために使用される主要な構成要素です。

マイクロソフトの公式セキュリティ、コンプライアンス、およびアイデンティティ（SCI）学習コンテンツ、特にSC-400およびSC-900認定資格トラックでは、評価の役割は明確に次のように定義されています。

「コンプライアンスマネージャーの評価機能は、規格や規制の要件への準拠状況を追跡、実装、改善するのに役立ちます。各評価は、ISO 27001、NIST、GDPR、HIPAAなどの特定の規制または管理フレームワークに対応しており、一連の管理策と推奨される改善策が含まれています。」SCIドキュメントから抽出された内容はさらに以下を裏付けています。

「評価は、特定の規制や基準に対するコンプライアンス状況を測定するために使用されます。これにはコントロールマッピングが含まれ、コンプライアンス目標を達成するために何が実施されているか、何に対処する必要があるかについての洞察を提供します。」ドロップダウンメニューのその他のオプション（テンプレート、改善策、ソリューション）は、それぞれ異なる機能を持ちます。

テンプレートは、評価を作成するための設計図を提供する。

改善策とは、評価の中で生成される具体的な行動ステップのことである。

Microsoftの管轄におけるソリューションとは、内部リスク管理、情報保護など、複数の機能を統合したものを指します。

したがって、特定の規制または要件に基づく管理策のグループへの準拠状況を追跡するには、マイクロソフトが検証した正しい用語は「評価」です。

最新問題: **46**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	●	○

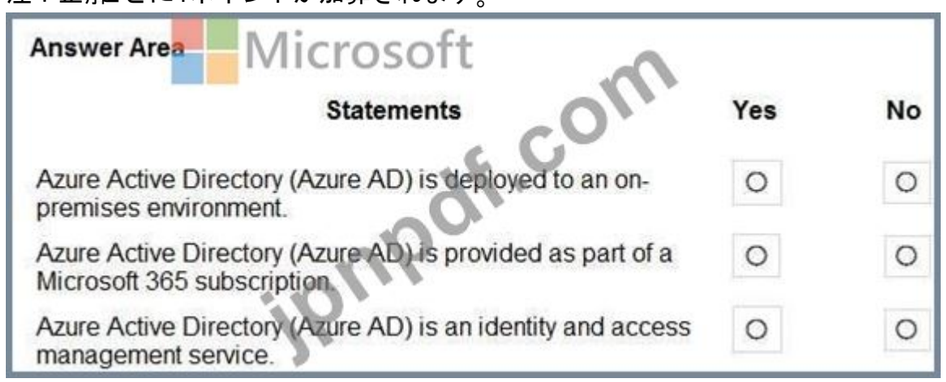
参照：

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

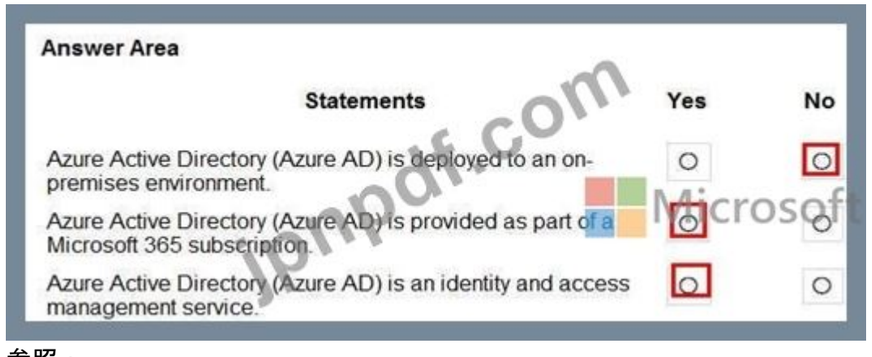
最新問題: **47**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



Answer:



参照：

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

最新問題: **48**

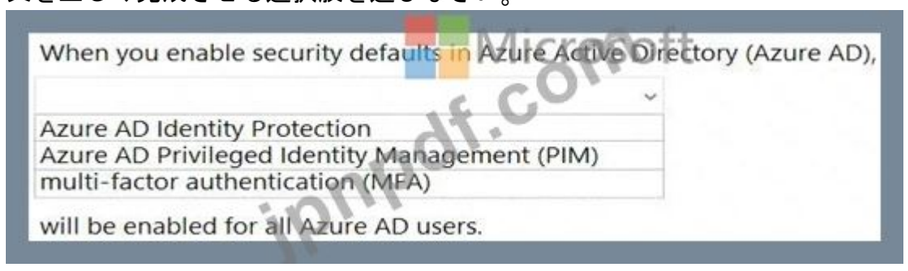
以下の各記述について、記述が正しい場合は「はい」を選択し、そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

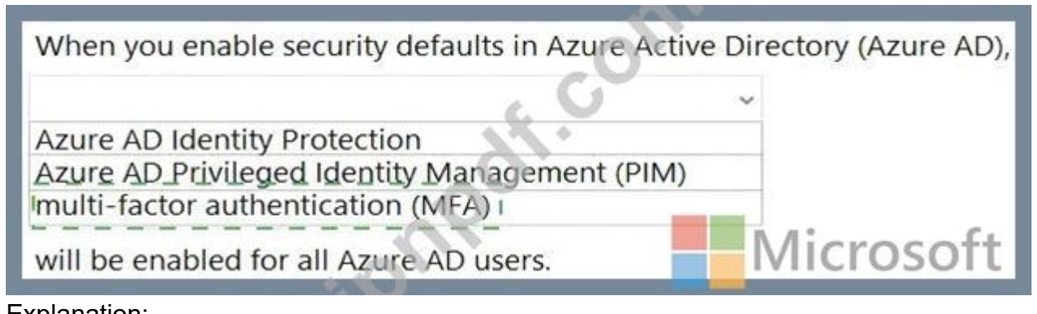
Answer:

最新問題: **49**

文を正しく完成させる選択肢を選びなさい。

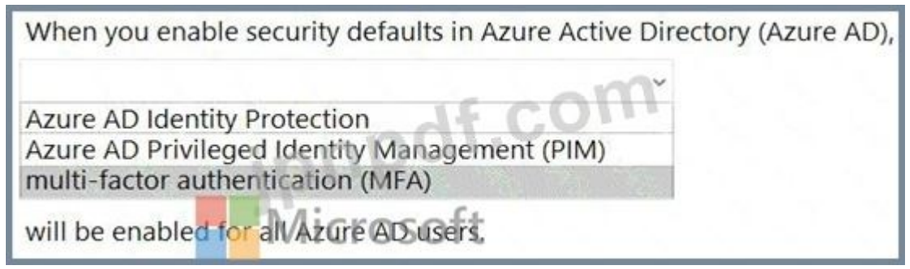


Answer:



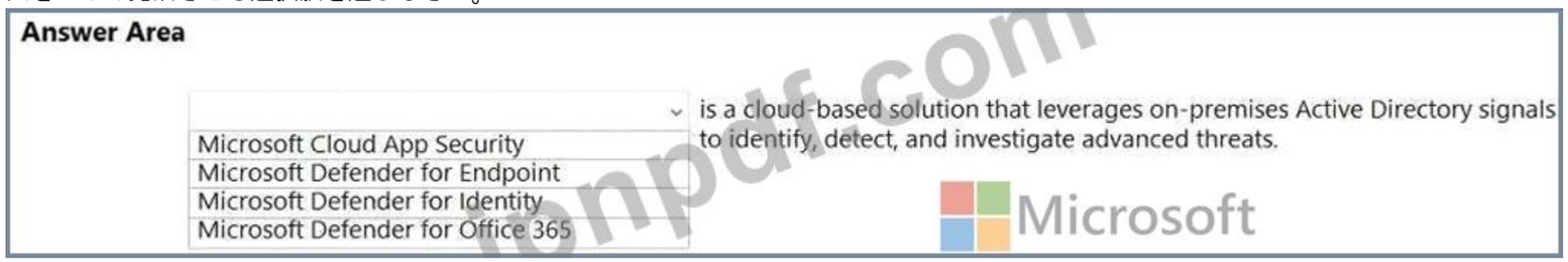
Explanation:

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます



最新問題: **50**

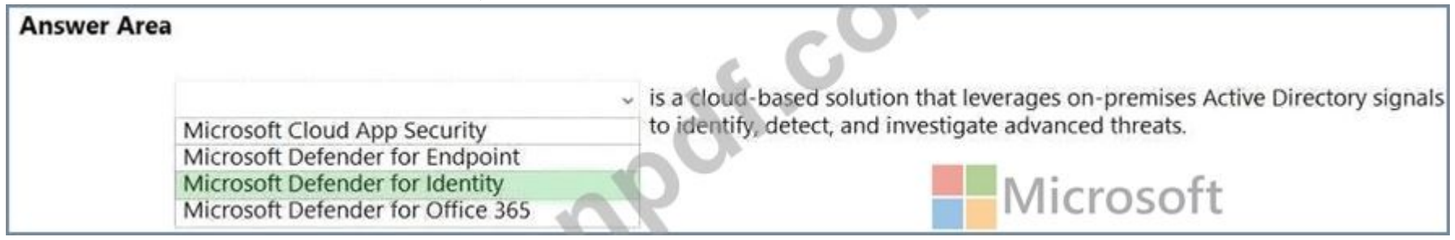
文を正しく完成させる選択肢を選びなさい。



Answer:

説明

グラフィカルユーザーインターフェース、テキスト説明は中程度の信頼度で自動生成されます



最新問題: **51**

文を正しく完成させる選択肢を選びなさい。

Answer:

Answer Area

Conditional Access policies are enforced after first-factor authentication.

最新問題: **52**
データ漏洩を特定するために使用できるMicrosoft Purviewソリューションはどれですか？
A. インサイダーリスク管理
B. コンプライアンスマネージャー
C. コミュニケーションコンプライアンス
D. eDiscovery
Answer: A (メーッセージを残す**)**
Microsoft Purview における Insider Risk Management は、知的財産の盗難やデータ漏洩といった活動を検出するために特別に設計されたソリューションです。Microsoft はこれを、多くのユーザーおよびシステム信号を関連付けて、機密データの漏洩やデータ流出など、悪意のある、あるいは意図しない内部リスクを特定するコンプライアンス ソリューションであると説明しています。
組織は、不審なファイルのダウンロード、リムーバブルメディアへのデータコピー、機密情報の外部共有といったリスクの高い行動を監視する内部リスク管理ポリシーを作成します。データ漏洩などのテンプレートで構成されたこれらのポリシーは、データ損失防止（DLP）ポリシーからの重大度の高いアラートをトリガーとして使用できるため、データ漏洩の疑いのあるイベントが発生すると、自動的にアラートと調査対象ケースが生成されます。このワークフローにより、調査担当者はデータ流出の可能性のあるインシデントを迅速にトリアージ、調査、および修復できます。
その他のオプションは、それぞれ異なる目的で使用されます。コンプライアンスマネージャーは、情報漏洩を監視するのではなく、規制や内部統制に対するコンプライアンス状況を評価および追跡します。コミュニケーションコンプライアンスは、不適切なメッセージやコンプライアンス違反のメッセージ（チャットやメールでの嫌がらせや不適切な共有など）に焦点を当てます。eDiscoveryは、情報漏洩が発生した際にそれを事前に検出するのではなく、訴訟や捜査のために既存のコンテンツを見つけて保存するために使用されます。
したがって、データ漏洩を特定するために使用されるMicrosoft Purviewソリューションは、Insider Risk Managementです。

最新問題: **53**
ホットスポット
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。
ホットエリア：
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.	○	○

Answer:

セクション :セキュリティ、コンプライアンス、およびアイデンティティの概念を説明する

Explanation:

ボックス1 :はい

システムアップデートはセキュリティ上の脆弱性を低減し、エンドユーザーにとってより安定した環境を提供します。アップデートを適用しないと、未修正の脆弱性が残り、攻撃を受けやすい環境となります。

ボックス2 :はい

ボックス3 :はい

ユーザー認証にパスワードのみを使用する場合、攻撃の脆弱性が残ります。多要素認証 (MFA) を有効にすることで、アカウントのセキュリティが向上します。

参照 :

https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls

最新問題: **54**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

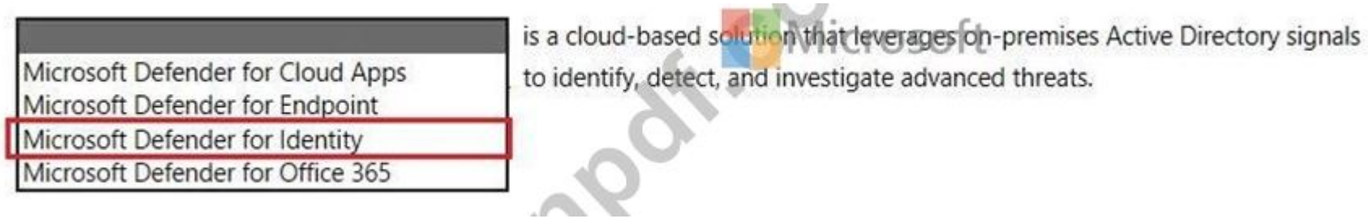
注 : 正解ごとに1ポイントが加算されます。

Answer:

最新問題: **55**
文を正しく完成させる選択肢を選びなさい。

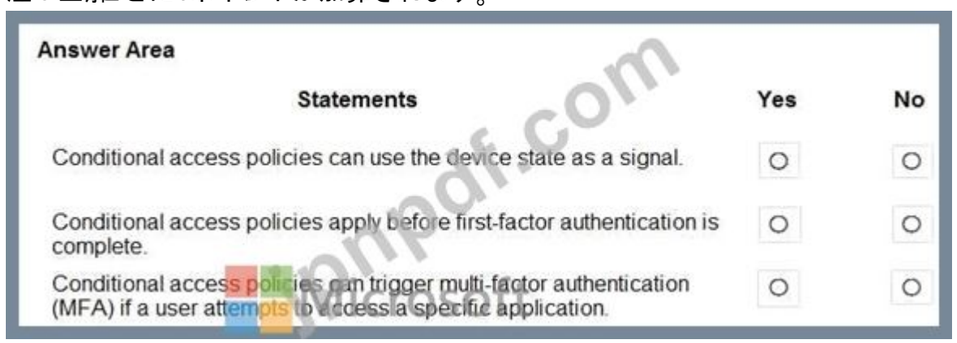
Answer:

Explanation:



Microsoft Defender for Identity（旧称Azure Advanced Threat Protection、Azure ATP）は、オンプレミスの Active Directory シグナルを活用して、組織を標的とした高度な脅威、侵害された ID、および悪意のある内部犯行を特定、検出、調査するクラウドベースのセキュリティ ソリューションです。

最新問題: **56**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:

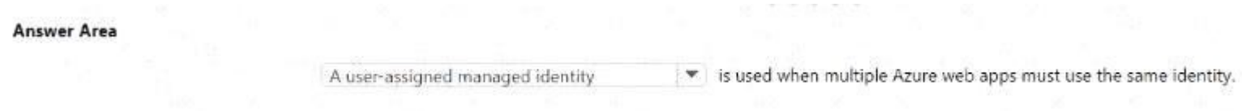
Explanation:

ボックス1 :はい
ボックス2 :いいえ
条件付きアクセス ポリシーは、第一要素認証が完了した後に適用されます。ボックス 3: はい

最新問題: **57**
文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

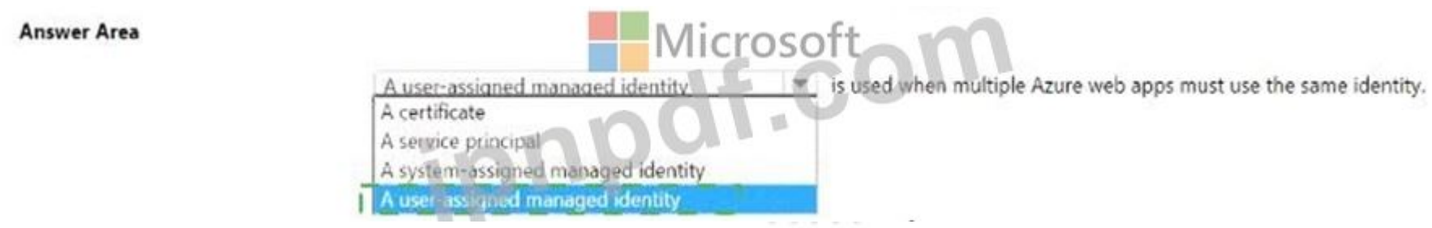


Microsoft の Azure リソースに関する ID ガイダンスでは、マネージド ID にはシステム割り当て ID とユーザー割り当て ID の 2 種類があるとされています。ドキュメントでは、システム割り当て ID は単一のリソースにスコープされ、そのライフサイクルに従うと説明されています。「システム割り当てマネージド ID は Microsoft Entra ID で作成され、その Azure サービス インスタンスのライフサイクルに紐付けられます。リソースが削除されると、Azure は ID を自動的に削除します。」一方、ユーザー割り当て ID は複数のリソースで再利用できます。「ユーザー割り当てマネージド ID はスタンドアロンの Azure リソースです。1 つ以上の Azure サービス インスタンスに割り当てることができ、それを使用するリソースとは独立して管理されます。」このシナリオでは、複数の Azure Web アプリで同じ ID を使用する必要があるため、この共有モデルをサポートするマネージド ID の種類はユーザー割り当てマネージド ID のみです。これにより、ID に RBAC アクセス許可を一度付与し、同じ ID を複数の App Service インスタンスにアタッチできるため、Azure リソース (Key Vault、ストレージ、SQL など) へのシークレットレス アクセスが簡素化され、ライフサイクルとローテーションの管理が一元化されます。証明書や汎用サービスプリンシパルを使用すると、認証情報の管理が再び必要になりますが、システム割り当てのIDは複数のアプリケーション間で共有できません。したがって、ユーザー割り当ての管理型IDが適切な選択肢となります。

最新問題: **58**
あなたはMicrosoft 365 E3のサブスクリプションをお持ちです。
統合監査ログと基本監査を使用して、ユーザーアクティビティを監査する予定です。
監査記録はどのくらいの期間保管されますか？
A. 180日
B. 90日間
C. 15日間
D. 30日間
Answer: B (メーッセージを残す)

最新問題: **59**
文を正しく完成させる選択肢を選びなさい。

Answer:



最新問題: **60**

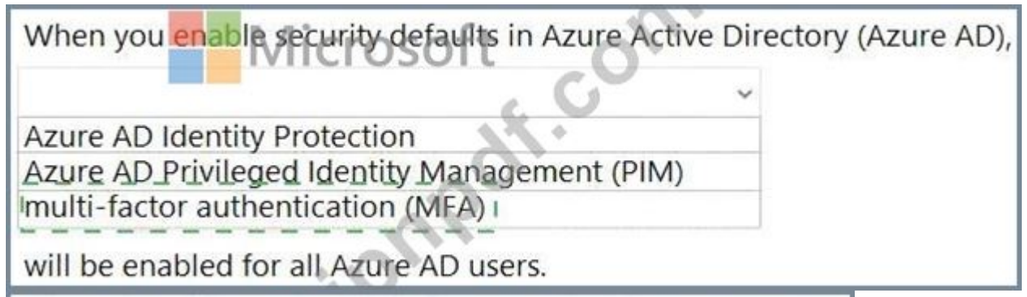
文を正しく完成させる選択肢を選びなさい。

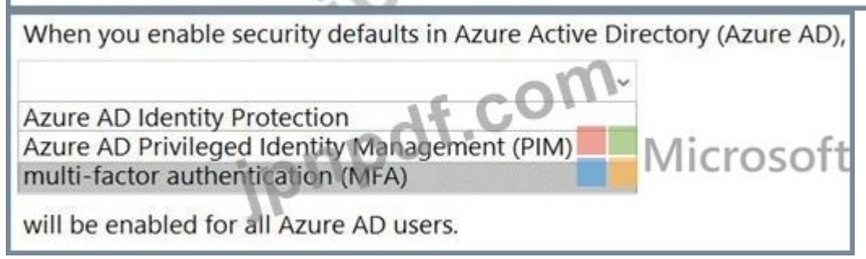
When you enable security defaults in Azure Active Directory (Azure AD),

Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Answer:





最新問題: **61**

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、完全なソリューションを示しています。

注：正解ごとに1ポイントが加算されます。

A. パートナー組織の外部アクセスを設定します。

B. 第三者ユーティリティへの輸出リスク検出。

C. IDベースのリスクの検出と修復を自動化します。

D. ユーザー認証に関連するリスクを調査する。

E. データに機密性ラベルを作成し、自動的に割り当てます。

Answer: (解答を表示する**)**

Microsoft Entra ID Identity Protectionは、リスクベースの条件付きアクセス機能であり、「IDベースのリスクの検出と修復を自動化」し、管理者がリスクの高いユーザーやサインインを調査できるようにします。

SCIのガイダンスによると、ID保護機能は、ユーザーリスクやサインインリスクなどのシグナルを評価し、リスク検出を促し、パスワードのリセットやリスクベースのポリシーによるアクセスブロックなどのアクションを適用することで、自動的に修復することができます。このポータルは、リスクの高いユーザー、リスクの高いサインイン、およびリスク検出に関する詳細な調査機能を提供し、セキュリティチームが証拠を確認し、リスクを確認または却下できるようにします。さらに、IDリスクデータはAzure Monitor/診断設定を通じてエクスポートでき、SIEM/SOARツールと統合することで、相関分析や対応のために「リスク検出とセキュリティアラートをサードパーティソリューションにエクスポート」することが可能になります。

パートナー組織の外部アクセス構成などのタスクは、B2Bコラボレーション機能によって処理され、機密ラベルの作成/割り当ては、Microsoftのパービュー情報保護に属し、ID保護には属しません。したがって、ID保護がサポートするタスクは、輸出リスクの検出（B）、IDベースのリスクの検出と修復の自動化（C）、およびユーザー認証に関連するリスクの調査（D）です。

最新問題: **62**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。
Answer Area

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

Answer:
Answer Area

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

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

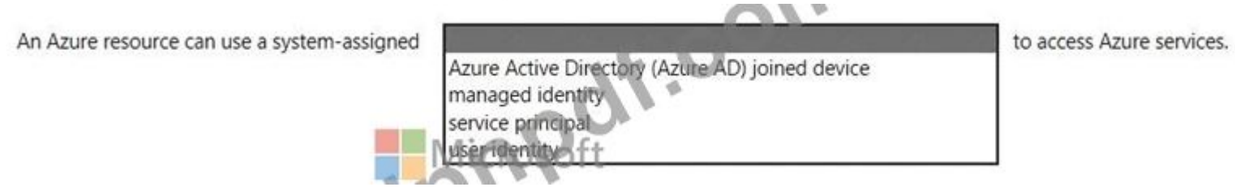
最新問題: **63**
Microsoft 365 コンプライアンス センターの情報保護ソリューションを使用することで、何を保護できますか？
A. ゼロデイ攻撃を受けたコンピュータ
B. フィッシング攻撃を受けたユーザー

C. マルウェアやウイルスからのファイル
D. 機密データが不正なユーザーに漏洩するのを防ぐ
Answer: D (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection?view=o365-worldwide

最新問題**: 64**
以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Answer:

最新問題**: 65**
文を正しく完成させる選択肢を選びなさい。



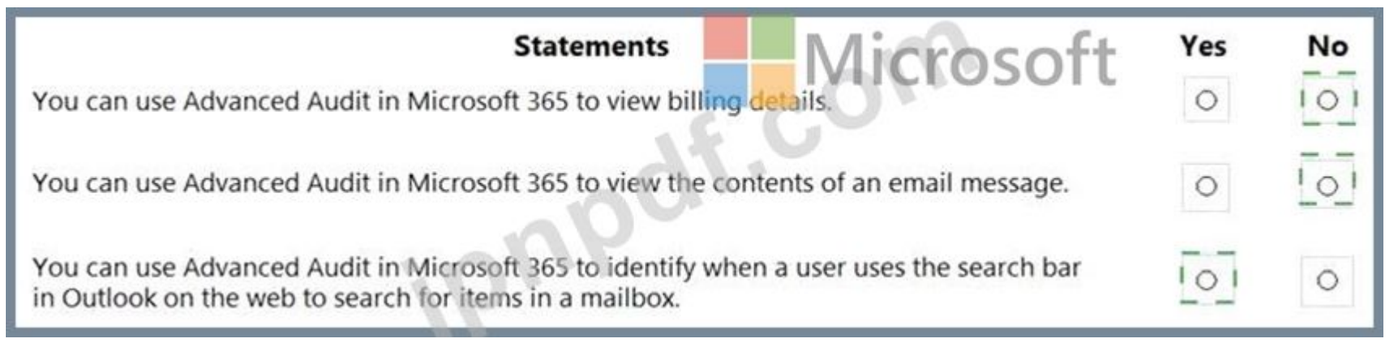
Answer:

最新問題: 66

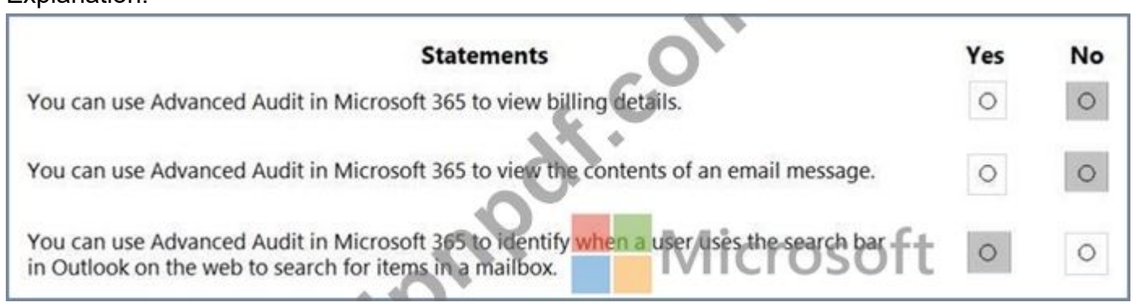
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer:



Explanation:



ボックス1 :いいえ

高度な監査機能は、監査ログの保持期間を延長することで、組織がフォレンジック調査やコンプライアンス調査を実施するのに役立ちます。
ボックス2 :いいえ
ボックス3 :はい

最新問題: **67**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Answer:
Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Explanation:

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Microsoft の ID プラットフォーム (Microsoft Entra ID、旧称 Azure AD) は、組み込みのディレクトリ ロールとカスタム ロールをサポートしています。公式ガイダンスでは、「Microsoft Entra リソースの管理権限を付与するために、独自のカスタム ロールを作成できる」と説明されており、これらのロールは、最小権限の管理をカスタマイズするために選択する特定のロール権限で構成されています。ドキュメントには、グローバル管理者 (旧称 会社管理者) が組み込みのロールとして記載されており、「すべての管理機能にアクセスできる」だけでなく、ロールの割り当ての委任、すべてのユーザーのパスワードのリセット、テナント全体の ID 設定の管理も可能です。割り当てに関して、Microsoft はロールの割り当てが多対多であることを明示しています。管理者は「1 つ以上のロールをユーザーに割り当てる」

ことができ、ユーザーの実効権限は割り当てられたすべてのロールの権限の和集合になります。したがって、(1) カスタム ロールの作成はサポートされています (はい)、(2) グローバル管理者は、Azure AD/Microsoft Entra で定義されたロールです (はい)、(3) 同じユーザーに複数のロールを割り当てることは許可されており、最小権限と職務の分離を実装するためによく使用されるため、ユーザーが 1 つのロールのみに制限されているというのは誤りです (いいえ)。
ボックス1 :はい
Azure AD はカスタムロールをサポートしています。
ボックス2 :はい
グローバル管理者は、Azure Active Directory のすべての管理機能にアクセスできます。ボックス 3: 参照なし:
https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

最新問題: **68**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

最新問題: **69**
文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題**: 70**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

Explanation:

生体認証テンプレートはデバイス上にローカルに保存されます。参照：

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

最新問題**: 71**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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

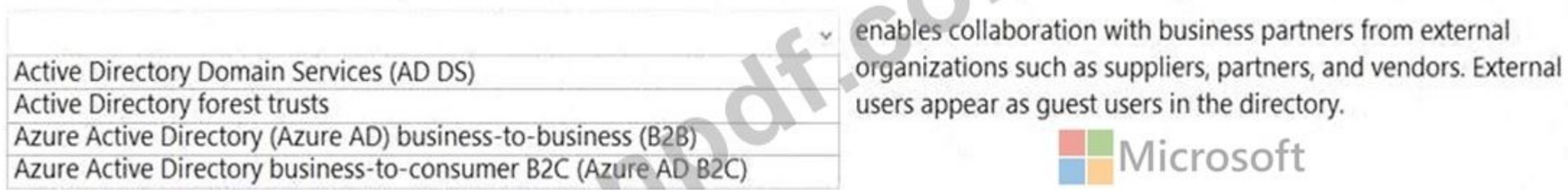
Statements	Yes	No
GitHub is a cloud-based identity provider.	●	○
Federation provides single sign-on (SSO) with multiple identity providers.	●	○
A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.	○	●

Microsoft の ID ガイダンスでは、ソーシャル ID サービス (GitHub、Google、Facebook など) を、Microsoft Entra ID で外部 ID に使用できるクラウドベースの ID プロバイダーとして分類しています。このモデルでは、GitHub は OAuth/OpenID Connect を使用してユーザーを認証し、アプリケーションまたは Entra ID が受け入れ可能なトークンを発行する ID プロバイダーとして機能します。Microsoft の用語でのフェデレーションは、組織の境界を越えて、Active Directory フェデレーション サービス (AD FS)、SAML、OpenID Connect プロバイダーなどの複数の ID プロバイダーとの間で SSO を可能にする信頼関係であり、ユーザーは一度認証するだけで、繰り返しサインインすることなく複数のアプリケーションにアクセスできます。

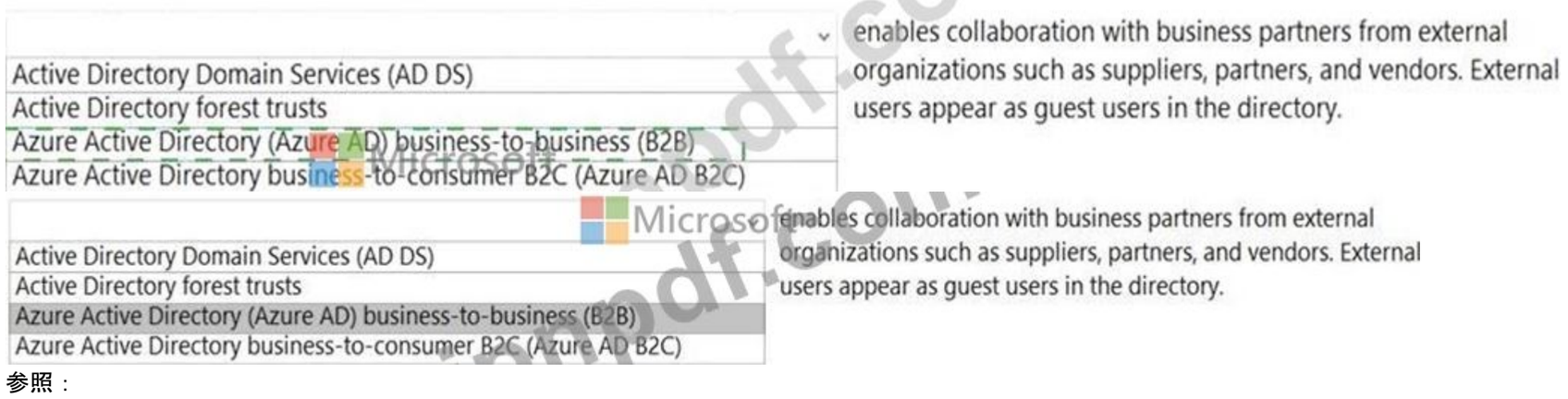
重要な点として、SCI資料では役割が明確に区別されています。IDプロバイダーは主に認証（ユーザーが誰であるかを証明し、クレーム／トークンを発行する）を担当します。認可（ユーザーが実行できる操作を決定する）は、アプリケーションまたはリソースによって実行されます（多くの場合、IDプロバイダーから提供される役割／クレームを使用します）。監査は複数のレベルに及びます。IDプロバイダーはサインインログと監査ログを提供し、アプリケーションやその他のサービスは独自の活動ログを保持します。

したがって、中央のIDプロバイダーが認可や監査を含む すべての最新の認証サービスを管理する」と言うのは誤りです。これらの責任は、IDプラットフォームとそれに依存するアプリケーション/リソース間で共有されています。

最新問題: **72**
文を正しく完成させる選択肢を選びなさい。

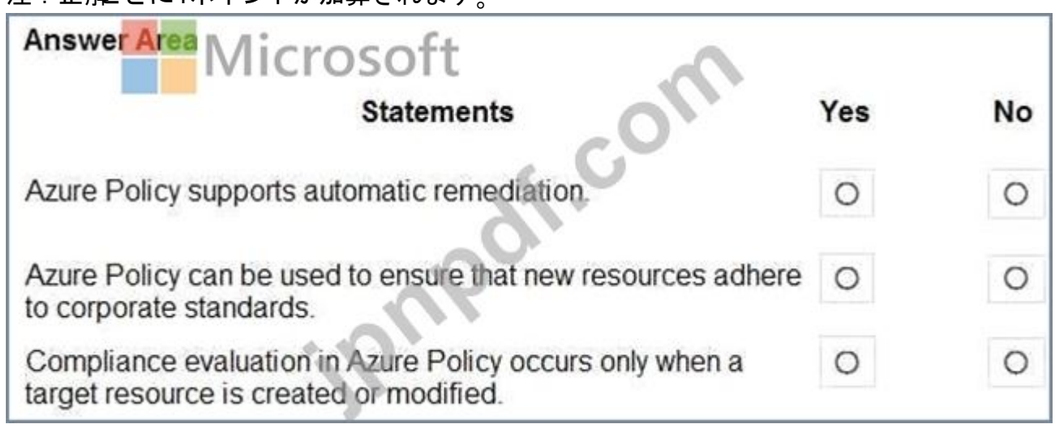


Answer:



参照：
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

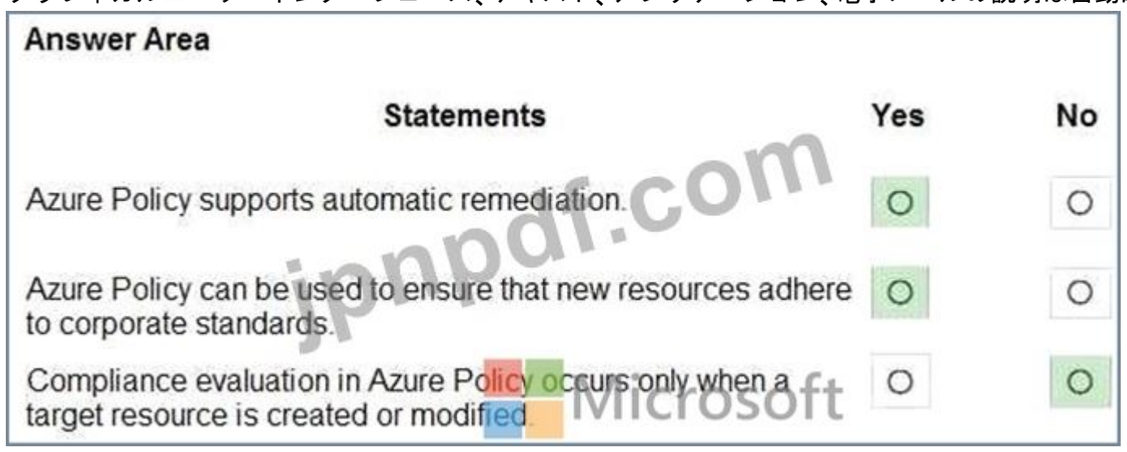
最新問題: **73**
以下の各記述について、正しい場合は はい」を選択してください。そうでない場合は いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:

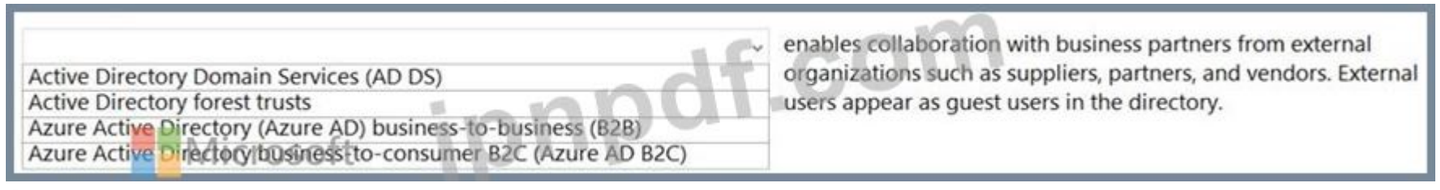
Explanation:

グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます

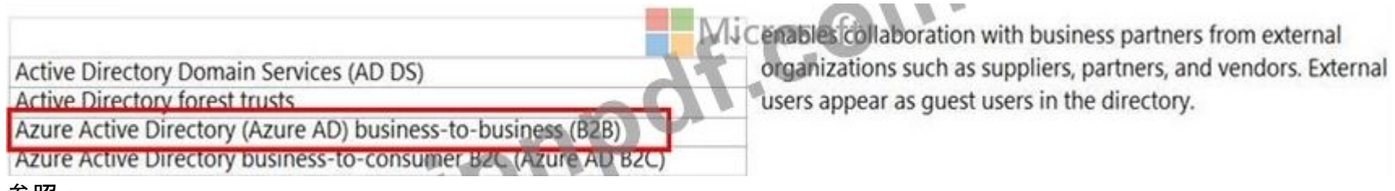


最新問題: 74

文を正しく完成させる選択肢を選びなさい。



Answer:



参照：

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

最新問題: 75

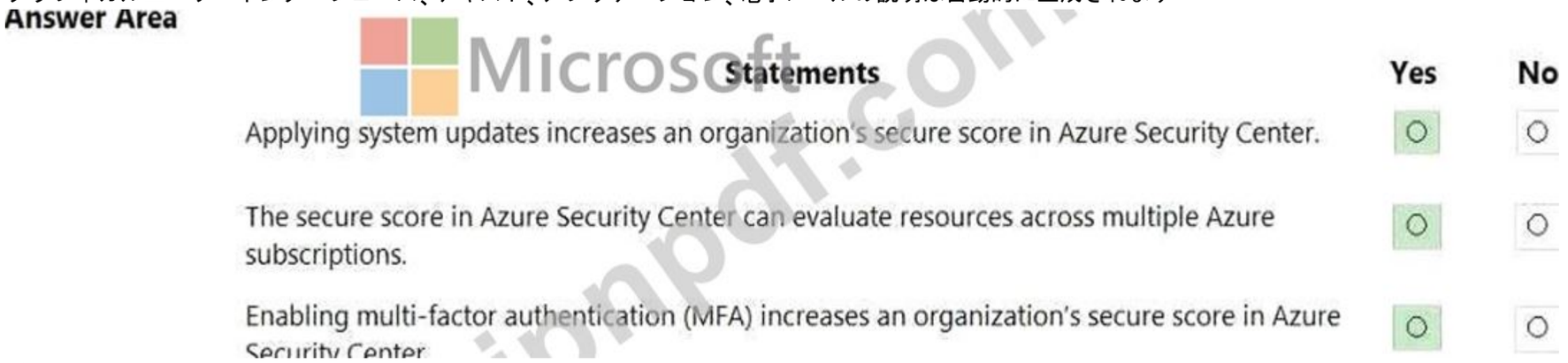
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer:

説明

グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます



ボックス1 :はい

システムアップデートはセキュリティ上の脆弱性を低減し、エンドユーザーにとってより安定した環境を提供します。アップデートを適用しないと、未修正の脆弱性が残り、攻撃を受けやすい環境となります。

ボックス2 :はい

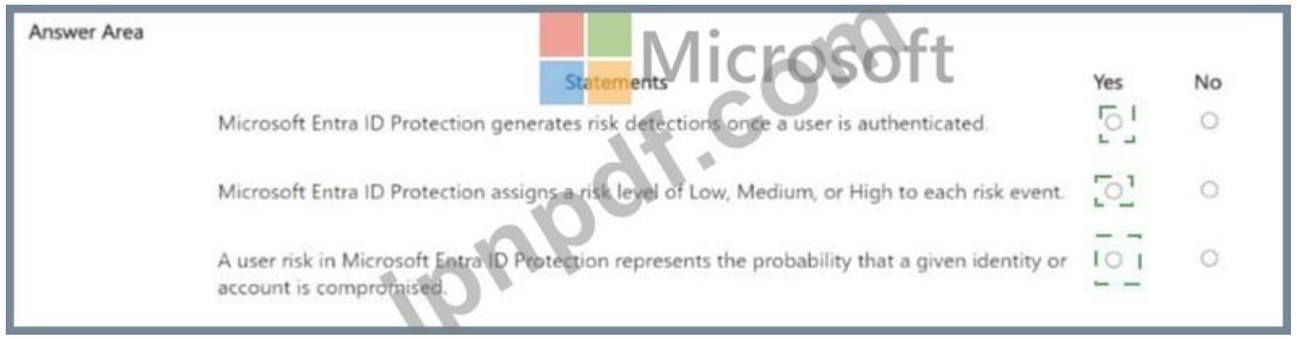
ボックス3 :はい

ユーザー認証にパスワードのみを使用する場合、攻撃の脆弱性が残ります。多要素認証（MFA）を有効にすることで、アカウントのセキュリティが向上します。

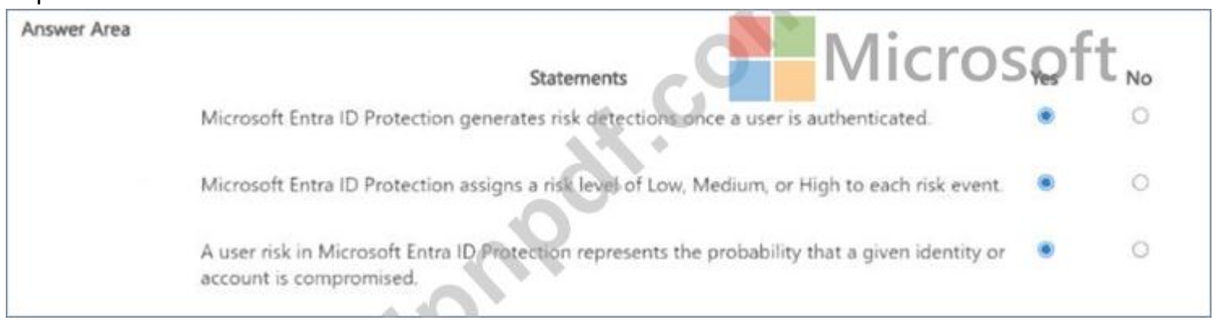
最新問題: **76**

以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Answer:



Explanation:



文書:

Microsoft Entra ID Protectionは、ユーザー認証後だけでなく、認証中にもリスクを評価します。このサービスは、サインインフローの一部として「リアルタイム」の評価を提供するとともに、「オフライン」での検出も処理し、セッションが許可される前に条件付きアクセスが機能できるようにします。マイクロソフトの用語では、「サインインリスク」とは、特定の認証要求がID所有者によって承認されていない確率を表し、「ユーザーリスク」とは、特定のIDまたはアカウントが侵害されている確率を表します。これらのリスクはリスク検出として表示され、多要素認証（MFA）のトリガー、アクセスのブロック、または安全なパスワードリセットの要求に使用できます。

Microsoft Entra ID Protection は、検出結果と計算されたリスクをそれぞれ「低、中、高」のレベルに分類し、管理者がポリシー対応を適切にトリアージおよび自動化できるようにします。検出結果はサインイン評価の一部としてリアルタイムで計算されるため (その後の分析でも計算されるため)、ユーザーが認証された後に生成されるというのは誤りです。正確には、Identity Protection はテレメトリを継続的に分析し、サインイン前、サインイン中、サインイン後に対応可能な検出結果とリスクレベルを生成します。ユーザーリスクは ID 自体が侵害される可能性を表し、サインインリスクは特定の認証試行が正当でない可能性を表します。

最新問題: **77**

文を正しく完成させる選択肢を選びなさい。

Answer Area

Microsoft

Azure Advisor	is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.
Azure Bastion	
Azure Monitor	
Azure Sentinel	

Answer:

Answer Area

Azure Advisor	is a cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution used to provide a single solution for alert detection, threat visibility, proactive hunting, and threat response.
Azure Bastion	
Azure Monitor	
Azure Sentinel	

参照：

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

最新問題**: 78**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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).	○	○

Answer:

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).	○	○

マイクロソフトは、ハイブリッドIDを、ディレクトリサービスを統合することでオンプレミスとクラウド間で共通のIDを実現するものと定義しています。Microsoft Learnでは、「ハイブリッドIDは、オンプレミスのActive DirectoryとAzure Active Directoryを統合することで実現されます」と述べています。この統合は、AD DSをAzure ADに接続する同期機能とオプションのフェデレーション機能によって実現され、ユーザーは単一のIDでオンプレミスとクラウドの両方のリソースにアクセスできるようになります。
この統合を実現するために、マイクロソフトのツールは明確に次のように述べています。「Azure AD Connectは、ハイブリッドIDの目標を満たすために設計されたマイクロソフトのツールです。」Azure AD Connect（現在はMicrosoft Entra Connect）は、ユーザー、グループ、そして必要に応じてパスワードやハッシュをAzure ADに同期し、シングルサインオンやシームレスサインインなどのハイブリッドシナリオの基盤を提供します。
テナントに関して、Microsoft の ID プラットフォームは「Microsoft 365 組織は単一の Azure AD テナントに関連付けられる」と明確にしています。したがって、ハイブリッド ID 展開では 2 つの Microsoft 365 テナントは必要なく、通常は単一の Azure AD (Microsoft Entra ID) テナントを 1 つ以上のオンプレミス AD DS フォレストにリンクします。要約すると、Azure AD Connect はハイブリッド ID を可能にし、ハイブリッド ID は同期です。
AD DSとAzure ADの統合であり、複数のMicrosoft 365テナントは必要ありません。

最新問題: **79**
文を正しく完成させる選択肢を選びなさい。
Answer Area

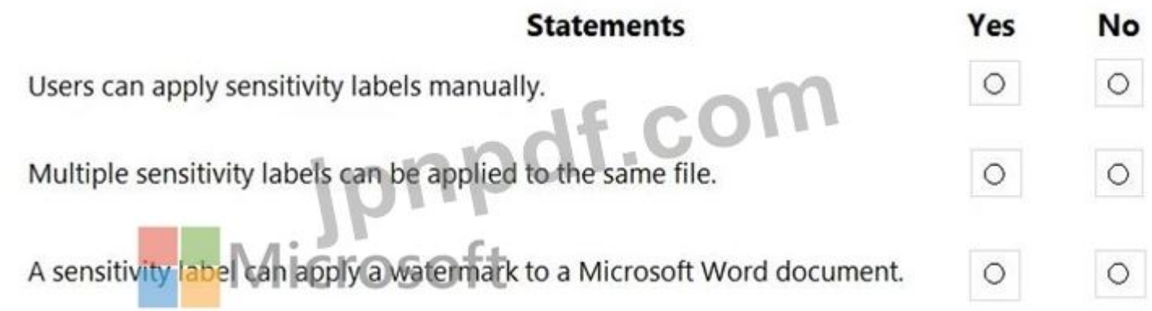
Federation is used to establish [ ] between organizations.
- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Answer:

フェデレーションとは、信頼関係が確立されたドメインの集合体です。参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

最新問題: **80**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



Answer:

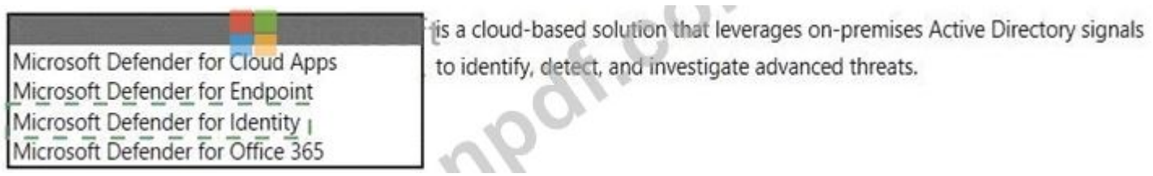
参照：
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-sensitivity-labels?view=o365-worldwide

最新問題: **81**
文を正しく完成させる選択肢を選びなさい。

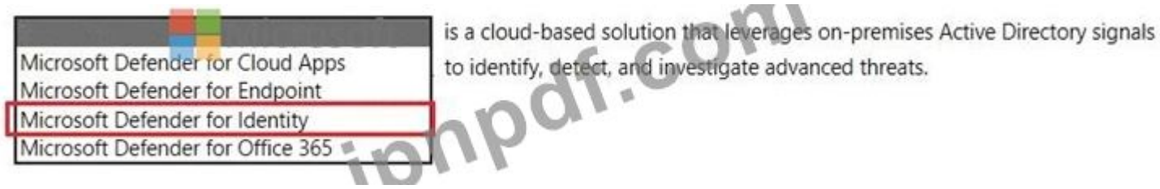
Answer:

最新問題: **82**
文を正しく完成させる選択肢を選びなさい。

Answer:



説明



Microsoft Defender for Identity（旧称Azure Advanced Threat Protection、Azure ATP）は、オンプレミスの Active Directory シグナルを活用して、組織を標的とした高度な脅威、侵害された ID、および悪意のある内部犯行を特定、検出、調査するクラウドベースのセキュリティ ソリューションです。

最新問題: **83**
Active Directory (Azure AD) にアプリケーションを登録すると、どのような種類のIDが作成されますか？
A. システムによって割り当てられた管理ID
B. ユーザーアカウント
C. ユーザーが割り当てた管理ID
D. サービス責任者
Answer: D (メーッセージを残す)
説明
Azure ポータルからアプリケーションを登録すると、ホーム ディレクトリまたはテナントにアプリケーション オブジェクトとサービス プリンシパルが自動的に作成されます。

最新問題: **84**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

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

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

最新問題: **85**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

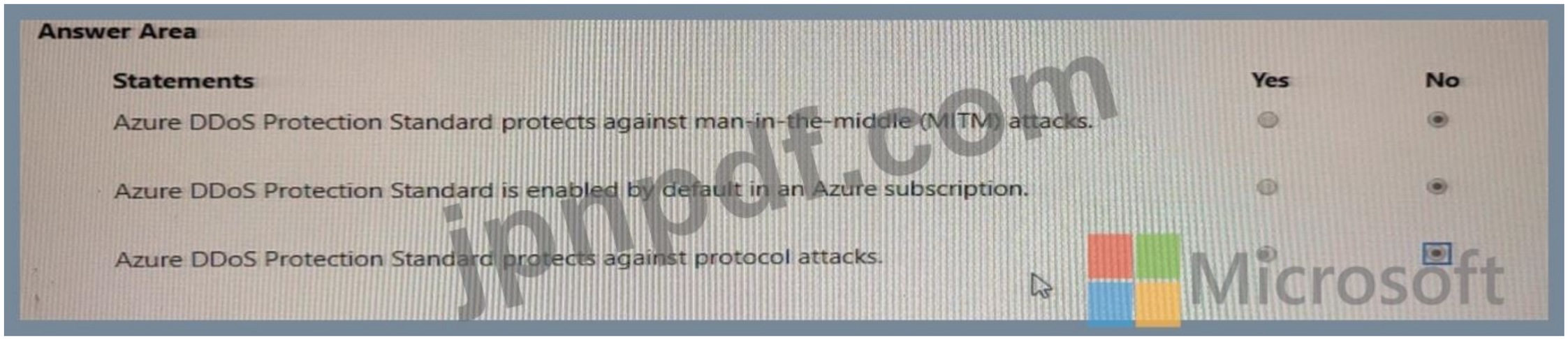
Answer Area

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.	○	○

Answer:

Answer Area

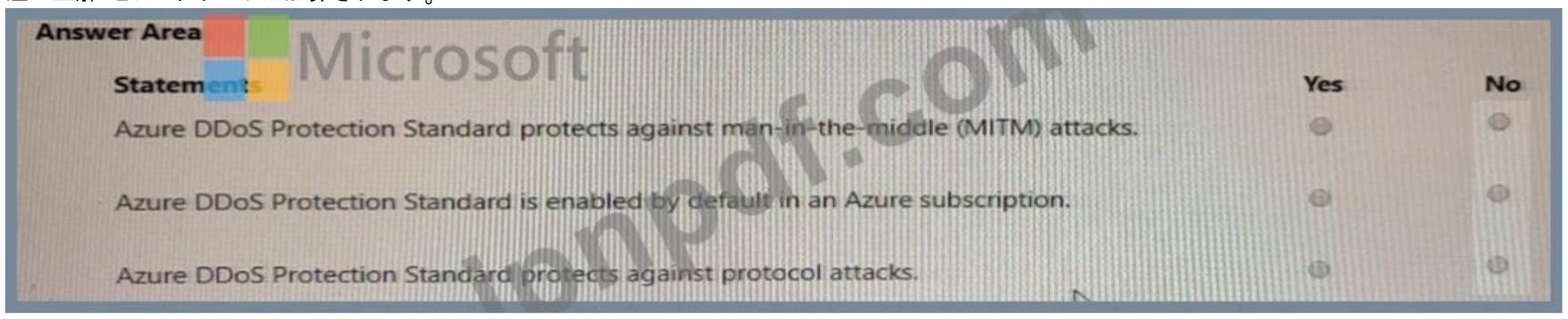
Statements	Yes	No
Azure DDoS Protection Standard protects against man-in-the-middle (MITM) attacks.	○	○
Azure DDoS Protection Standard is enabled by default in an Azure subscription.	○	○
Azure DDoS Protection Standard protects against protocol attacks.	○	○



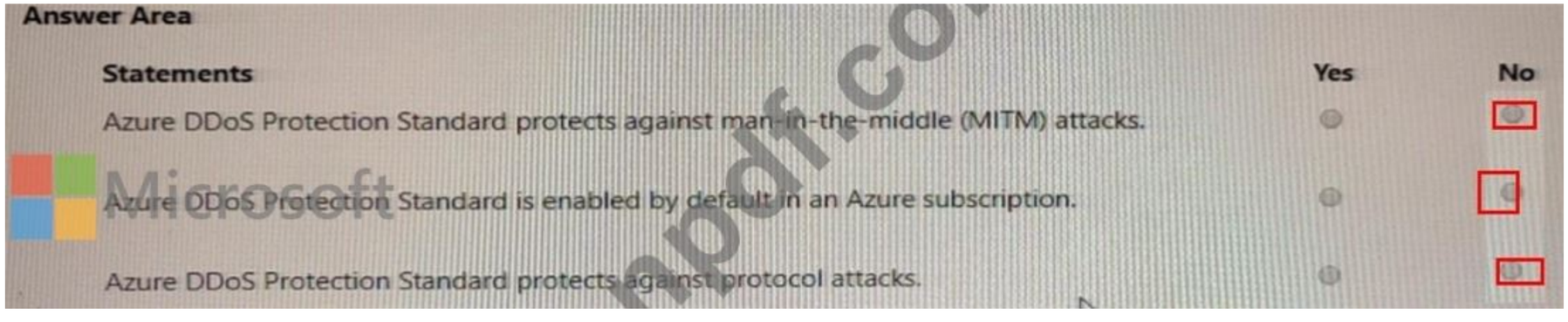
最新問題: **86**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

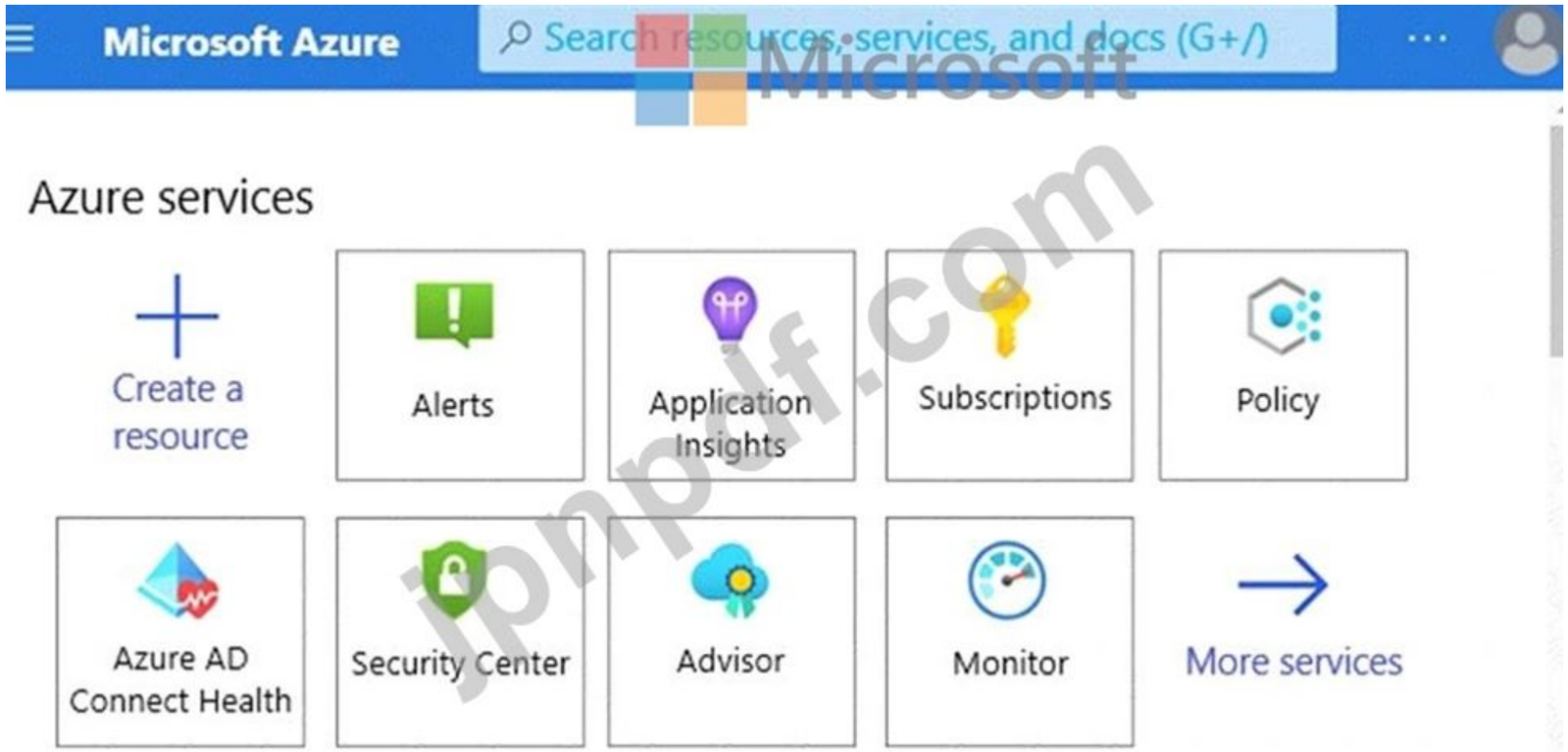


Answer:



最新問題: **87**

Azureのセキュリティスコアを確認するには、どのサービスを使用すればよいですか？回答するには、回答欄で適切なサービスを選択してください。


Microsoft Azure
Search resources, services, and docs (G+/)
Azure services
Create a resource
Alerts
Application Insights
Subscriptions
Policy
Azure AD Connect Health
Security Center
Advisor
Monitor
More services

Answer:

Explanation:
セキュリティセンター

最新問題: 88
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

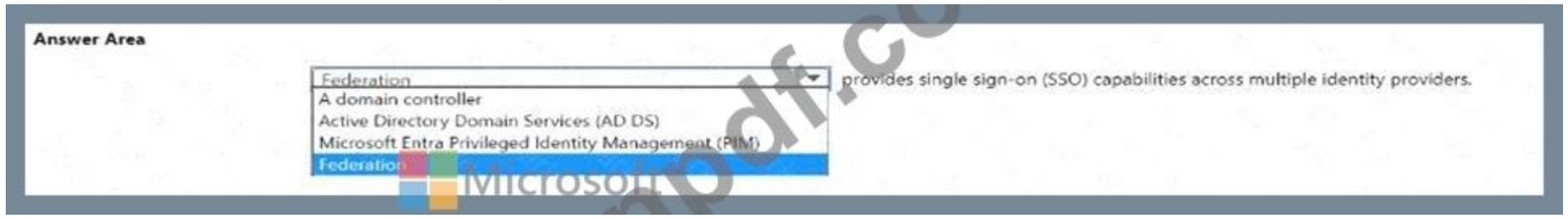
Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Answer:

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

参照：
https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal

最新問題: **89**
文を正しく完成させる選択肢を選びなさい。



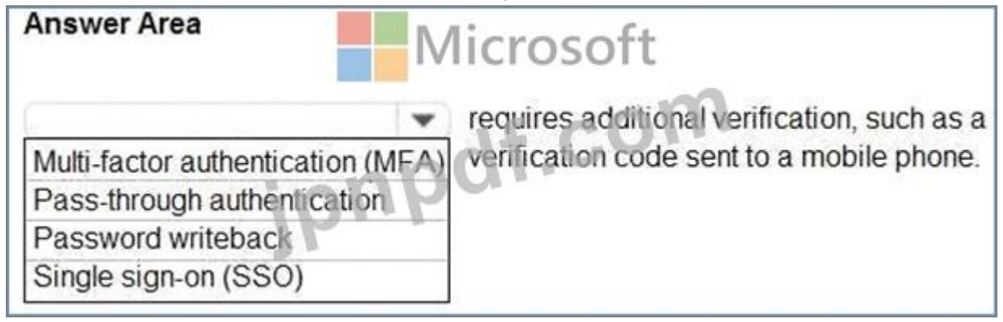
Answer:

Explanation:

Microsoft の ID アーキテクチャでは、フェデレーションによって異なる ID プロバイダー間の信頼関係が確立され、組織やプラットフォームの境界を越えたシングル サインオン (SSO) が可能になります。Microsoft Learn では、フェデレーションは SAML、WS-Federation、OpenID Connect/OAuth 2.0 などの標準規格を使用し、ユーザーがホーム ID プロバイダーで認証を行い、リライングパーティ (アプ

リケーションまたはサービス) が受け入れるトークンを取得できるようにしていると説明しています。この信頼関係により、組織はパスワードをコピーしたり資格情報を同期したりすることなく、安全にID を共有でき、複数のシステムやクラウド間でシームレスなサインイン エクスペリエンスを実現できます。
対照的に、Active Directoryドメインサービス (AD DS) とドメインコントローラーは、主に単一のWindowsドメイン/フォレスト内でKerberosを使用してオンプレミスのディレクトリおよび認証サービスを提供します。
/NTLMは、単独ではプロバイダー間SSOを実現しません。Microsoft Entra Privileged Identity Management (PIM) は、役割のジャストインタイム承認ベースの昇格を管理するものであり、SSO機能を提供するものではありません。したがって、複数のIDプロバイダー間でSSOを提供することを目的とした技術は、フェデレーションです。

最新問題: **90**
文を正しく完成させる選択肢を選びなさい。



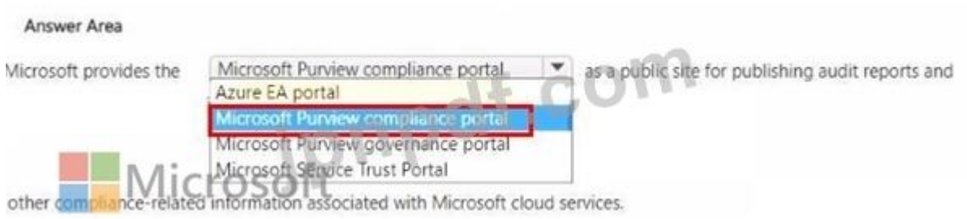
Answer:

説明
グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

多要素認証とは、ユーザーがサインインする際に、携帯電話に表示されるコードの入力や指紋認証など、追加の本人確認手段を要求するプロセスです。

最新問題: **91**
文を正しく完成させる選択肢を選びなさい。

Answer:



最新問題: **92**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Answer:

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Explanation:

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Microsoft Entra の条件付きアクセス (CA) は、ユーザー、デバイス、場所、リスクからのシグナルを評価してアクセス権限を決定します。プラットフォームでは、CA の決定はプライマリ サインイン後に行われることが明示的に示されています。 条件付きアクセス ポリシーは、第一要素認証が完了した後に適用されます。」つまり、CA エンジンがポリシー ロジックを評価する前に、ユーザーは最初の認証情報 (パスワード、Windows Hello、FIDO2 など) を正常に提示する必要があります。したがって、CA がユーザー認証前に評価されるという記述は正しくありません。
スコープに関して、条件付きアクセスでは、一般ユーザーと特権ユーザーの両方のIDを対象にできます。割り当てオプションを使用すると、管理者はポリシーをユーザー、グループ、およびディレクトリロールに適用できます。 「ユーザーとグループを含めるか除外するか...[および]特定のAzure ADディレクトリロールを条件付きアクセス ポリシーに含めるか除外するか」。グローバル管理者はディレクトリロールであるため、これらのアカウントにポリシーを適用できます（ただし、ロックアウトを防ぐために、少なくとも1つの緊急時用アカウントを除外しておくことをMicrosoftのベストプラクティスとして推奨しています）。
シグナル/条件に関して、CAはデバイスプラットフォームのフィルタリングをサポートしています。ドキュメントに記載されているデバイスプラットフォーム条件には、「この条件は、デバイスのオペレーティングシステムプラットフォーム（iOS、Android、Windows、macOSなど）に基づいています」と記載されています。管理者は、AndroidまたはiOSに基づいて異なる制御（MFAや準拠デバイスなど）を要求するために、この条件をよく使用します。
これらをまとめると：
* CAはグローバル管理者にも適用できます（はい）。
* CAは、第一要素認証の後に評価されます（「前」の場合は「いいえ」）。
* デバイスプラットフォーム（例Android/iOS）は有効なCAシグナルです（はい）。

最新問題: **93**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

Answer:

Statements	Yes	No
You can use Advanced Audit in Microsoft 365 to view billing details.	○	○
You can use Advanced Audit in Microsoft 365 to view the contents of an email message.	○	○
You can use Advanced Audit in Microsoft 365 to identify when a user uses the search bar in Outlook on the web to search for items in a mailbox.	○	○

参照：

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

最新問題: **94**

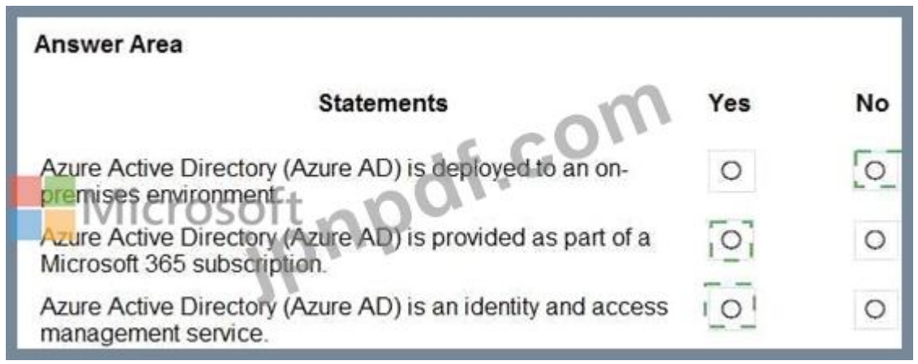
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

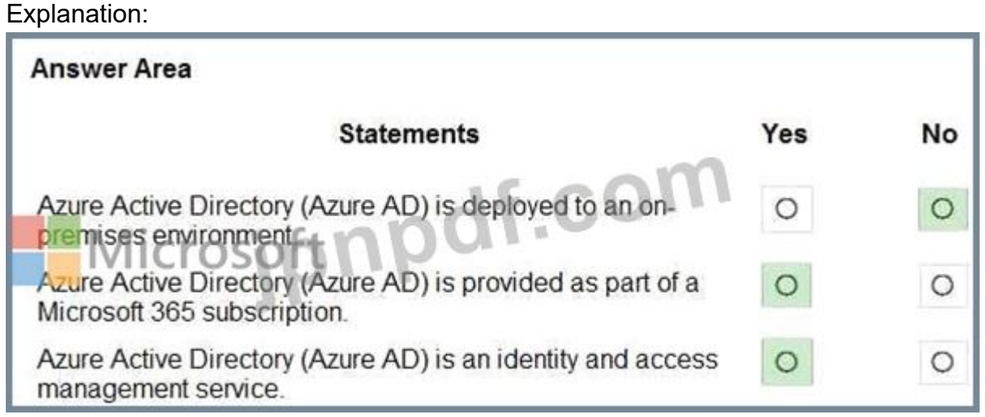
Answer Area

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.	○	○

Answer:



Explanation:



ボックス1 :いいえ
Azure Active Directory (Azure AD) は、クラウドベースのユーザーIDおよび認証サービスです。
ボックス2 :はい
Microsoft 365 は Azure Active Directory (Azure AD) を使用します。Azure Active Directory (Azure AD) は、Microsoft 365 サブスクリプションに含まれています。
ボックス3 :はい
Azure Active Directory (Azure AD) は、クラウドベースのユーザーIDおよび認証サービスです。

最新問題: **95**
Compliance Managerにおける評価とは何ですか？
A. 特定の規制、基準、または方針に基づく管理策のグループ。
B. 組織が企業基準に準拠するのに役立つ推奨ガイダンス。
C. 社内文書で使用が禁止されている単語の辞書。
D. 複数の政策を含む政策イニシアチブ。
Answer: A (メーッセージを残す**)**
説明
Microsoft Purview Compliance Managerは、Microsoft Purviewコンプライアンスポータルの機能の一つで、組織のコンプライアンス要件をより簡単かつ便利に管理するのに役立ちます。Compliance Managerは、データ保護リスクの把握から、複雑な制御策の実装、規制や認証への対応、監査人への報告まで、コンプライアンスのあらゆる段階でサポートを提供します。
以下のビデオをご覧いただくと、コンプライアンスマネージャーが組織のコンプライアンス管理をどのように簡素化できるかをご確認いただけます。
コンプライアンスマネージャーは、以下の機能を提供することで、コンプライアンスの簡素化とリスクの軽減を支援します。

一般的な業界および地域規格 規制に対応した既成の評価、またはお客様固有のコンプライアンスニーズを満たすためのカスタム評価（利用可能な評価はライセンス契約によって異なります。詳細はこちらをご覧ください）。
ワークフロー機能により、単一のツールでリスク評価を効率的に完了できます。
組織にとって最も関連性の高い規格や規制を遵守するために役立つ、推奨される改善策に関する詳細な手順ガイドを提供します。マイクロソフトが管理する対策については、実装の詳細と監査結果が表示されます。
リスクベースのコンプライアンススコアは、改善策の完了状況を測定することで、自社のコンプライアンス状況を把握するのに役立ちます。

最新問題: **96**
文を完成させる。

Answer:

Explanation:

マイクロソフトのセキュリティ、コンプライアンス、およびIDに関するガイダンスでは、Microsoft Service Trust Portal （STP）が、マイクロソフトのクラウドサービスに関する独立監査レポート、コンプライアンス認証、評価レポート、および信頼性関連ドキュメントを公開する公開場所として指定されています。このドキュメントでは、STPを通じて、SOC 1/SOC 2レポート、ISO/IEC認証、監査概要、コンプライアンスガイドなどの資料にアクセスできると説明されており、組織はマイクロソフトのコントロールを評価し、自社の規制要件に照らし合わせて検討することができます。STPは、透明性とデューデリジェンスを重視した設計となっており、顧客と監査担当者がマイクロソフトのコンプライアンス体制を確認し、マイクロソフトがクラウドプラットフォーム全体でセキュリティ、プライバシー、およびコンプライアンスをどのように管理しているかを理解できるようになっています。
対照的に、Microsoft Purview コンプライアンス ポータルは、組織内でコンプライアンス ソリューション (DLP、情報保護、eDiscovery、内部リスク、コンプライアンス マネージャーなど) を構成および管理するために使用されるテナント管理者ポータルであり、Microsoft の監査成果物の公開リポジトリではありません。Microsoft Purview ガバナンス ポータルは、データ ガバナンスとカタログ作成のシナリオに重点を置いています。Azure EA ポータルは、エンタープライズ契約の請求と使用状況の管理に使用されます。したがって、Microsoft クラウド サービスに関する監査レポートやその他のコンプライアンス関連情報を公開する公開サイトは、Microsoft Service Trust Portal です。

最新問題: **97**
以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	○	○
Compliance Manager provides predefined templates for creating assessments.	○	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	○	○

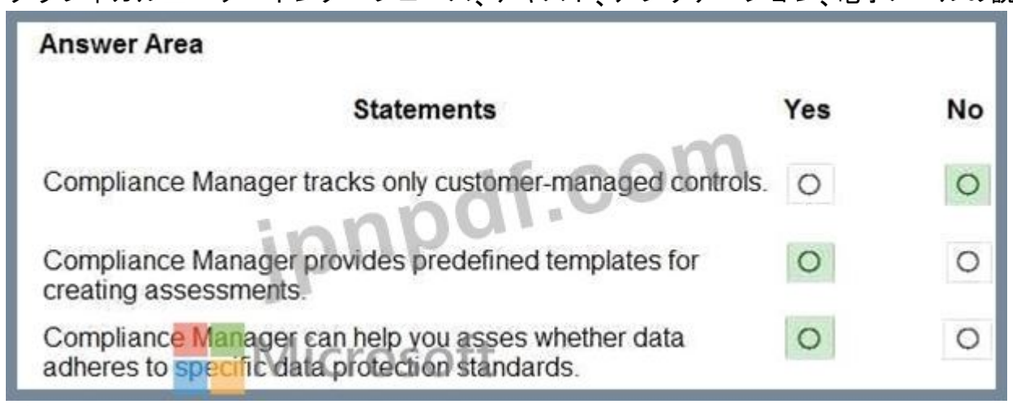
Answer:

Answer Area

Statements	Yes	No
Compliance Manager tracks only customer-managed controls.	○	○
Compliance Manager provides predefined templates for creating assessments.	○	○
Compliance Manager can help you asses whether data adheres to specific data protection standards.	○	○

説明

グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます



ボックス1 :いいえ

Compliance Managerは、Microsoftが管理するコントロール、顧客が管理するコントロール、および共有コントロールを追跡します。

ボックス2 :はい

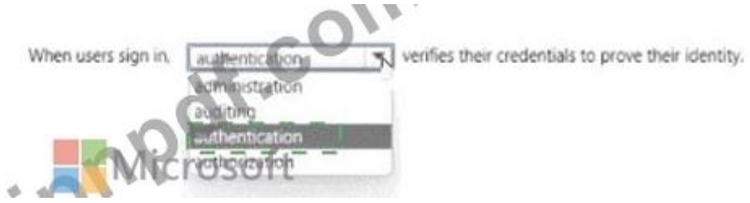
ボックス3 :はい

最新問題: 98

Azure Active Directory (Azure AD) のどの機能を使用して、Azure リソースを管理するためのジャストインタイム (JIT) アクセスを提供できますか？
A. 条件付きアクセスポリシー
B. Azure AD ID保護
C. Azure AD 特権ID管理 (PIM)
D. 認証方法ポリシー
Answer: C (メーッセージを残す**)**
Azure AD Privileged Identity Management (PIM) は、Azure AD および Azure リソースへのジャストインタイムの特権アクセスを提供します。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

最新問題**: 99**
文を正しく完成させる選択肢を選びなさい。

Answer:



Explanation:
Microsoft の ID 用語では、認証とは、ユーザーがサインインしようとしたときに、そのユーザーが誰であるかを証明する手順です。Microsoft Learn では、認証を次のように明確に定義しています。 認証とは、ユーザー、デバイス、またはサービスの ID を証明するプロセスです。」これに対し、 認可とは、ユーザー、デバイス、またはサービスが実行できる操作を決定するプロセスです。」Microsoft Entra ID (旧 Azure AD) へのサインイン中、 ID プロバイダーは資格情報を検証し、認証が成功すると、アプリケーションがアクセスを許可するために使用するトークンを発行します。」Microsoft は、利用可能な方法についてさらに次のように説明しています。 Microsoft Entra ID は、パスワード、多要素認証、FIDO2 セキュリティ キー、証明書ベースの認証、フェデレーション認証など、複数の認証方法をサポートしています。」監査と管理は、サインイン時に ID を検証するメカニズムではありません。監査は 調査とコンプライアンスのためにセキュリティ関連のイベントを記録する」ものであり、管理は ID、アクセス ポリシー、および設定の構成と管理」を指します。したがって、 ユーザーがサインインすると、_____ が認証情報を確認して本人確認を行います」という文では、認証が正しい補完語となります。なぜなら、認証は、認可の決定が行われる前に、ユーザーの認証情報を検証し、本人確認を行う制御だからです。

最新問題**: 100**

Azure 多要素認証 (MFA) で使用できる認証方法はどれですか？正解はそれぞれ完全なソリューションを示しています。注: 正解ごとに 1 ポイントが加算されます。
A. メール認証
B. 電話
C. Microsoft Authenticator アプリ
D. テキストメッセージ $MS）
E. セキュリティに関する質問
Answer: (解答を表示する**)**

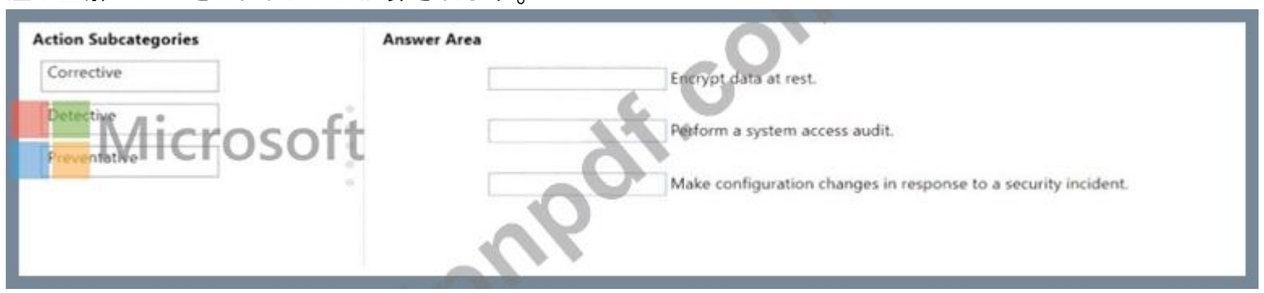
最新問題**: 101**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

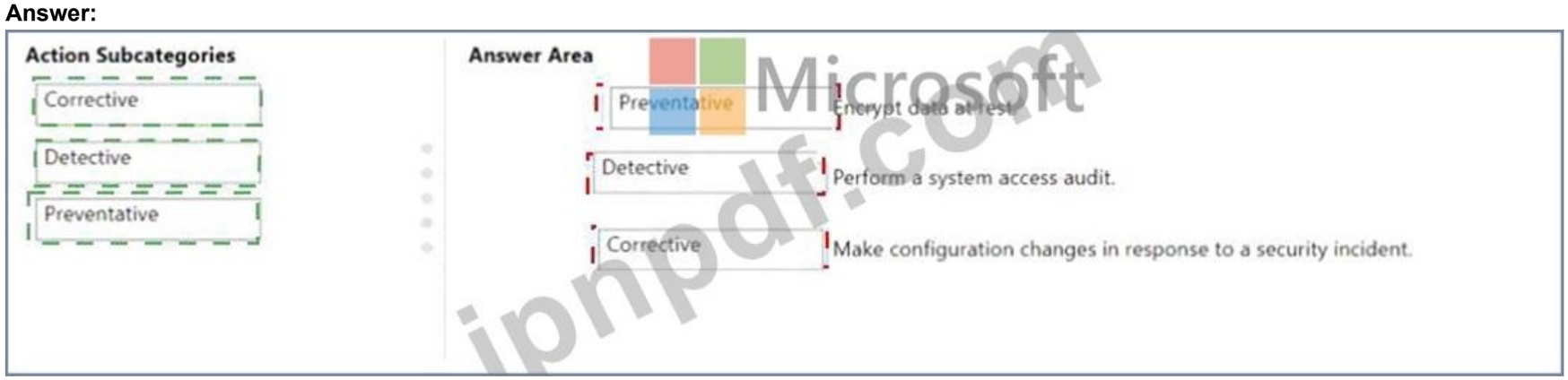
Answer Area

Statements	Yes	No
You can restrict communication between users in Exchange Online by using Information Barriers.	◉	○
You can restrict accessing a SharePoint Online site by using Information Barriers.	◉	○
You can prevent sharing a file with another user in Microsoft Teams by using Information Barriers.	◉	○

最新問題**: 102**
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のアクションサブカテゴリを、適切なアクションと照合してください。
回答するには、左側の列から適切なアクションサブカテゴリを右側のアクションにドラッグしてください。各アクションサブカテゴリは、1回、複数回、またはまったく使用しないことができます。
注：正解つにつき1ポイントが加算されます。



Answer:



最新問題: **103**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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).	○	○

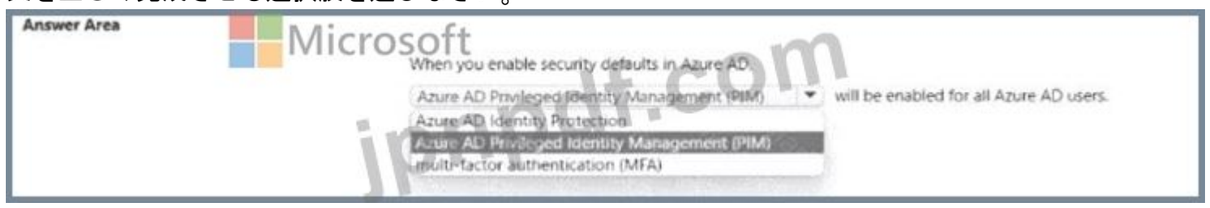
Answer:

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).	○	○

説明
グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

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).	○	○

最新問題: **104**
文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:
多要素認証（MFA）
Microsoft Entra ID (旧称 Azure AD) のセキュリティ既定値は、推奨される ID 保護の基本設定であり、有効にするとテナント全体に自動的に適用されます。Microsoft のガイダンスでは、セキュリティ既定値は 「事前構成されたセキュリティ設定で組織を保護する」のに役立ち、特に 「すべてのユーザーが Azure AD 多要素認証に登録する」必要があると説明しています。既定値を有効にすると、リスクの高い操作や機密性の高い操作中にユーザーと管理者に対して MFA チャレンジが強制され、最新の MFA 要件を満たせない従来の認証プロトコルがブロックされます。Microsoft はさらに、セキュリティ既定値は 「すべてのユーザーと管理者に対して多要素認証を要求するなど、基本的な ID セキュリティ メカニズムを提供する」と述べています。これらの制御は、カスタム ポリシーを設計することなく全体的なセキュリティ体制を強化するように設計されており、中小規模の組織や条件付きアクセスをまだ実装していないテナントに最適です。したがって、セキュリティ既定値を有効にすると、すべての Azure AD ユーザーに対して MFA が有効になり、強力な認証がデフォルトとして実行され、パスワードのみのサインインに起因するアカウント乗っ取りのリスクが軽減されます。

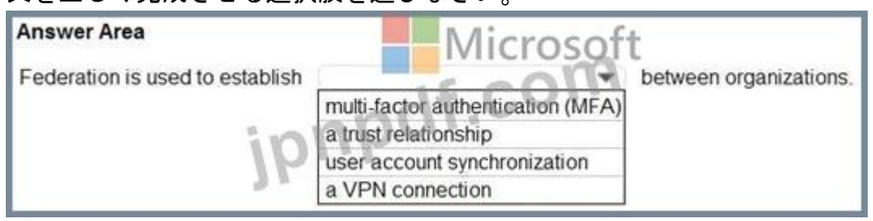
最新問題: **105**
文を正しく完成させる選択肢を選びなさい。

Answer:

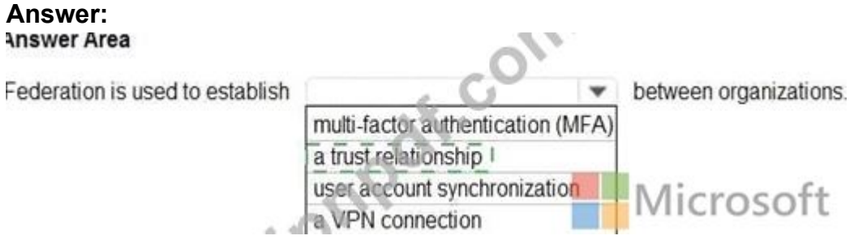
Explanation:

Microsoft は、コンプライアンス マネージャーを Microsoft 365 コンプライアンス センター (現在は Microsoft Purview コンプライアンス ポータル) 内で利用できる機能として位置付けています。Microsoft の SCI 学習コンテンツでは、コンプライアンス マネージャーはコンプライアンス ポータル内の集中ワークスペースとして説明されており、 組織のコンプライアンス要件の管理を支援し」、コンプライアンス スコア、事前構築済みおよびカスタムの評価、追跡および割り当て可能な改善アクションを提供します。ドキュメントでは、管理者は Microsoft を使用する」と説明されています。
365 コンプライアンス センターからコンプライアンス マネージャーにアクセスし、スコアを確認したり、コントロールを規制や標準にマッピングしたり、コントロールの証拠やテストを管理したりできます。また、コンプライアンス マネージャーはコンプライアンス ポータル ナビゲーションに直接表示されるため、承認された役割 (コンプライアンス管理者、グローバル管理者、コンプライアンス データ管理者など) のユーザーは、コンプライアンス マネージャー ブレードを開いて評価を作成または表示したり、アクションを割り当てたり、詳細なガイダンスを確認したりできることも明確にされています。これに対し、Microsoft 365 管理センターはテナント、請求、ユーザー管理に重点を置いており、Microsoft 365 Defender ポータルはセキュリティ運用と脅威対策に重点を置いており、Microsoft サポート ポータルはサービス リクエスト用です。したがって、コンプライアンス マネージャーへの直接的かつ意図されたエントリ ポイントは、Microsoft 365 コンプライアンス センターです。

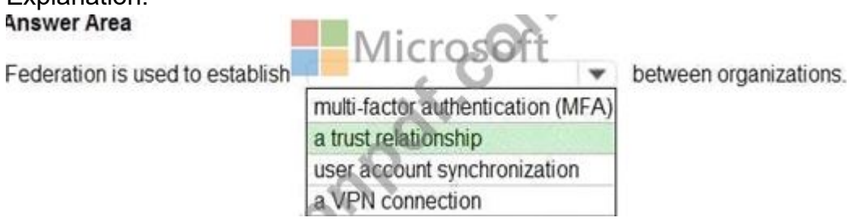
最新問題: **106**
文を正しく完成させる選択肢を選びなさい。



Answer:



Explanation:



フェデレーションとは、信頼関係が確立されたドメインの集合体です。参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

最新問題: 107
文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

Microsoft Defender for Cloud のセキュリティ、コンプライアンス、および ID 学習コンテンツでは、このサービスは継続的な姿勢管理と脅威保護を提供すると説明されています。公式の説明によると、Defender for Cloud は 『セキュリティ構成の誤りや脆弱性を特定するためにリソースを継続的に評価」し、サブスクリプション全体で 『リソースを継続的に検出および評価」します。推奨事項とセキュアスコアの更新は、プラットフォームが 『セキュリティ ポリシーと分析を使用して環境を継続的に分析」し、問題が検出された瞬間にそれを表面化して修復ガイダンスにマッピングすることで生成されます。この継続的な評価モデルは、Defender for Cloud のクラウド セキュリティ姿勢管理 (CSPM) 機能の基盤となり、新しく作成または変更されたリソースがスケジュールされたジョブを待つことなく評価されることを保証します。設計上、評価をトリガーするために必要な固定間隔 (1 時間ごと、15 分ごと、または毎日など) はなく、ポリシー駆動型の評価とデータ収集は、変更が発生しシグナルが受信されたときに実行されます。したがって、 『Microsoft Defender for Cloud は Azure リソースをセキュリティ上の問題に関して ____ 評価します」という文は、定期的なスキャンではなく、継続的なリアルタイムのセキュリティ態勢評価を重視する Microsoft の姿勢を反映して、continuous で正しく完成します。

最新問題: 108
以下の各記述について、正しい場合は 『はい」を選択してください。そうでない場合は 『いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

Explanation:

Microsoft Entra Accessレビューは、組織がアクセス権限を定期的に検証し、適切な規模に調整できるよう支援するために設計されています。
Microsoft のドキュメントによると、アクセス レビューはグループ メンバーシップ、エンタープライズ アプリの割り当て、Azure AD ロール、および Azure リソース ロール (特権 ID 管理経由) を対象とすることができ、レビュー担当者はユーザー、サービス プリンシパル、またはグループが Azure リソースへのアクセスを保持すべきかどうかを評価できます。これは最初の記述を裏付けています。アクセス レビューは自動化をサポートしています。レビューを 結果の自動適用」に構成できるため、レビューが終了すると、拒否されたユーザーまたはレビューされなかったユーザーはグループ、アプリケーションの割り当て、またはロールから自動的に削除されます。これは 2 番目の記述を検証しています。最後に、アクセス レビューは、PIM および高度な ID ガバナンスと並んで、Premium P2 の機能 (現在は Microsoft Entra ID P2) です。
これらはすべてのサービス プランに含まれているわけではありません。テナントは、レビュー担当者と対象ユーザーに対して適切な P2 ライセンスを必要とします。したがって、3 番目の記述は 「いいえ」です。

最新問題: **109**
文を正しく完成させる選択肢を選びなさい。

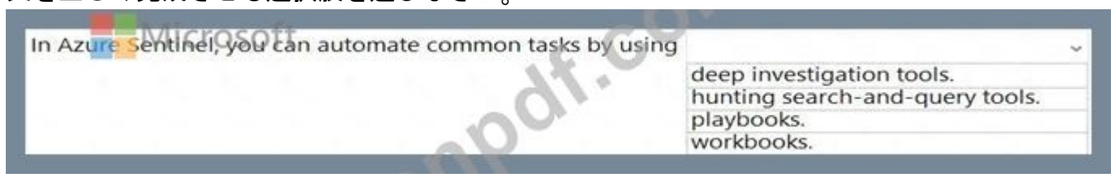
Answer:

参照：

https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

最新問題**: 110**

文を正しく完成させる選択肢を選びなさい。



Answer:

最新問題**: 111**

Azureのセキュリティスコアを確認するには、どのサービスを使用すればよいですか？回答するには、回答欄で適切なサービスを選択してください。

Answer:

Explanation:
セキュリティセンター

最新問題: 112
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

Answer Area

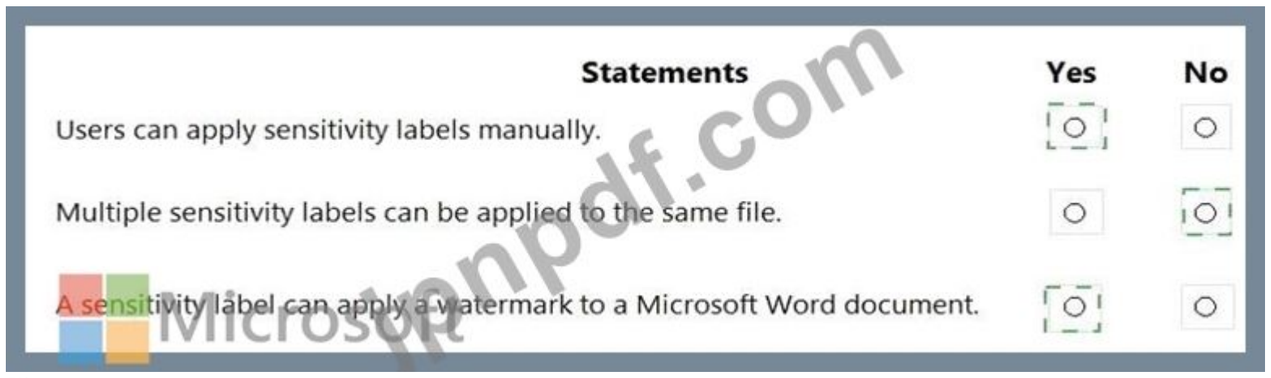
Statements	Yes	No
Control is a key privacy principle of Microsoft.	○	○
Transparency is a key privacy principle of Microsoft.	○	○
Shared responsibility is a key privacy principle of Microsoft.	○	○

最新問題: **113**
メール、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身を守るには、どのような対策が考えられますか？
A. Microsoft Defender for Identity
B. Microsoft Defender for Endpoint
C. Microsoft Defender for Cloud Apps
D. Microsoft Defender for Office 365
Answer: D (メーッセージを残す**)**
Microsoft Defender for Office 365 は、メールやコラボレーションワークロードを通じて配信される脅威からユーザーを保護するために設計された Microsoft 365 ソリューションです。SCI のトレーニング資料では、Defender for Office について説明しています。
365 は、メッセージや共有コンテンツを配信チャネルとして利用するマルウェア、フィッシング、その他の高度な攻撃を検知してブロックすることで、Exchange Online、Microsoft Teams、SharePoint Online、OneDrive for Business を保護します。
重要な機能の一つがセーフリンクです。これは特に悪意のあるURLからユーザーを保護します。ユーザーがハイパーリンクを含むメール、Teamsチャットメッセージ、またはチャネル投稿を受信すると、セーフリンクはそのURLをスキャンして書き換えます。ユーザーがクリックした瞬間にリンクが再度チェックされ、悪意のあるリンク、または既知のフィッシングサイトやマルウェアホスティングサイトにつながるリンクと判断された場合は、アクセスがブロックされ、警告ページが表示されます。このクリック時の保護機能は、メールや共同作業における悪意のあるリンクに対する主要な防御策として、マイクロソフトのセキュリティドキュメントで強調されています。

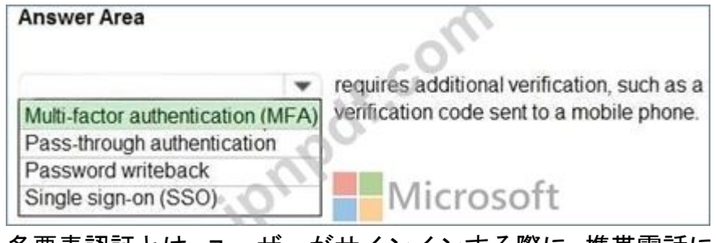
これに対し、Microsoft Defender for IdentityはオンプレミスのActive DirectoryにおけるID関連の脅威の検出に特化しており、Defender for Endpointはデバイスとエンドポイントを保護し、Defender for Cloud AppsはSaaSアプリケーションとシャドウITを保護します。これらのいずれも、メール、チャット、チャネル内の悪意のあるリンクをブロックするための主要なソリューションではありません。したがって、Microsoft Defender for Office 365が最適な選択肢となります。

最新問題: **114**
文を正しく完成させる選択肢を選びなさい。

Answer:

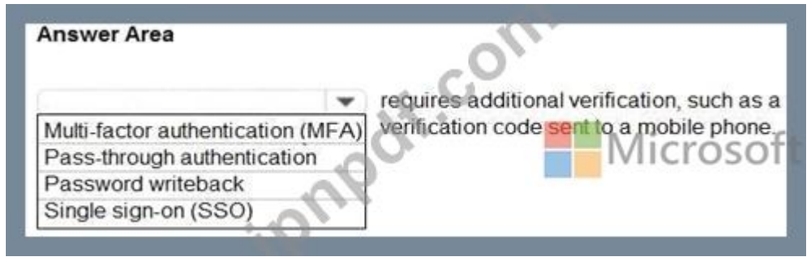


説明
グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます



多要素認証とは、ユーザーがサインインする際に、携帯電話に表示されるコードの入力や指紋認証など、追加の本人確認手段を要求するプロセスです。

最新問題: **115**
文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:

多要素認証とは、ユーザーがサインインする際に、携帯電話に表示されるコードの入力や指紋認証など、追加の本人確認手段を要求するプロセスです。

最新問題**: 116**

Microsoft 365 セキュリティセンターでセキュリティの傾向を確認したり、ID の保護状況を追跡したりするには、何を使用すればよいですか？

A. 攻撃シミュレーター

B. レポート

C. 狩猟

D. 事件

Answer: B (メーッセージを残す**)**

Microsoft 365 セキュリティ センター/Microsoft 365 Defender ポータルのレポート領域は、組織全体のセキュリティ体制とアクティビティを時系列で可視化できるように設計されています。Microsoft は、レポート機能について セキュリティの傾向を表示し、ID、エンドポイント、メールとコラボレーション、クラウド アプリ全体にわたる保護状況を追跡できる」と説明しています。レポート内の ID セクションでは、Microsoft Entra ID 保護と関連する ID 防御からのシグナルが集約されるため、セキュリティ チームは、リスクの高いサインイン、ユーザーのリスク、MFA の導入/登録、その他の ID 保護メトリックなどの傾向を監視できます。これらの厳選された読み取り専用のダッシュボードは、保護状況と時間の経過に伴う変化を測定することを目的としており、制御の効果を検証し、修復の優先順位付けに役立ちます。

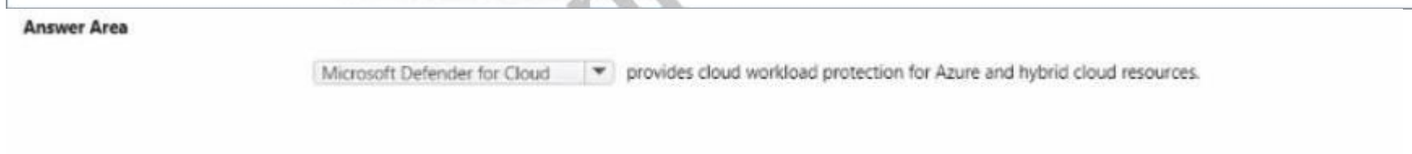
対照的に、攻撃シミュレーターはユーザー訓練シミュレーション フィッシングなど）を実行するために使用され、セキュリティ状態の傾向レポート作成を目的としたものではありません。ハンティング（高度なハンティング）では、アナリストが調査のために生のテレメトリを照会できますが、傾向ダッシュボードの概要を提供するものではありません。インシデントは、長期的な傾向や保護ステータス ビューを表示するのではなく、アラートをインシデントレコードに関連付けてトリアージと対応を行います。したがって、セキュリティの傾向を表示し、IDの保護ステータスを追跡するには、Microsoft 365 セキュリティセンターのレポートが適切な場所です。

/Microsoft 365 Defender ポータル。

最新問題**: 117**

文を正しく完成させる選択肢を選びなさい。

Answer:



最新問題**: 118**

文を正しく完成させる選択肢を選びなさい。

Answer:

参照：

https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

最新問題**: 119**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	○	○
You can access the insider risk management solution from the Microsoft 365 compliance center.	○	○
You can use the insider risk management solution to detect data leaks by unhappy employees.	○	○

Answer:

説明
ボックス1 :はい
フィッシング詐欺は外部からの脅威である。
ボックス2 :はい
内部リスク管理は、Microsoft 365 のコンプライアンスソリューションです。
ボックス3 :いいえ
内部リスク管理は、ユーザーによる内部リスクを最小限に抑えるのに役立ちます。これには以下が含まれます。
機密データの漏洩とデータ流出
機密保持義務違反
知的財産 (IP) の窃盗
詐欺
インサイダー取引
規制遵守違反

最新問題: **120**
文を正しく完成させる選択肢を選びなさい。

Answer:

Answer Area

A user-assigned managed identity is used when multiple Azure web apps must use the same identity.

最新問題**: 121**

Microsoft 365 エンドポイントのデータ損失防止 (Endpoint DLP) は、どのオペレーティングシステムで使用できますか？

A. Windows 10とiOSのみ

B. Windows 10とAndroidのみ

C. Windows 10、Android、iOS

D. Windows 10のみ

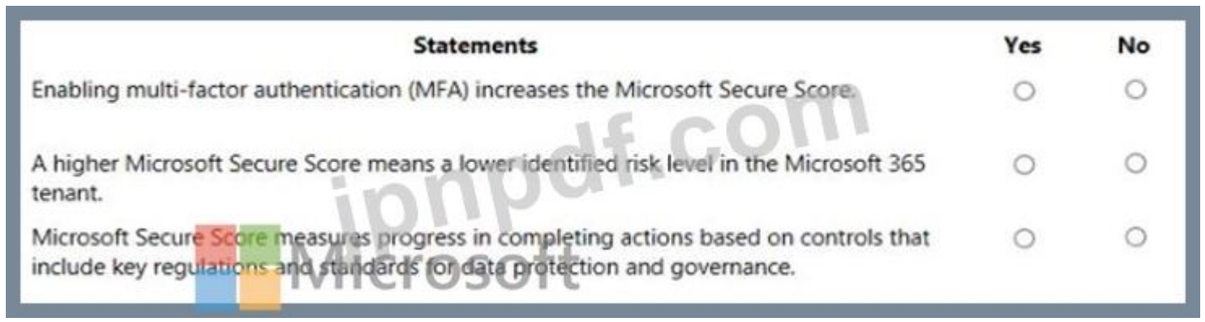
Answer: D (メーッセージを残す)

Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) は、DLP コントロールをエンドポイントに拡張します。Microsoft のドキュメントでは、Endpoint DLP は「Windows 10/11 デバイス」（現在のガイダンスでは macOS も含む）に保護を適用すると説明されています。この機能は、機密情報が含まれる場合に、USB へのコピー、印刷、Web へのアップロードなどの操作を監視し、制限します。重要な点として、Microsoft は iOS または Android に対する Endpoint DLP のサポートを文書化していません。これらのプラットフォームは、Endpoint DLP ではなく、Intune のアプリ保護ポリシーと Microsoft Defender for Endpoint モバイル機能によって管理されます。提示された選択肢を考慮すると、Microsoft の Endpoint DLP プラットフォームのサポートと一致し、サポートされていないモバイル OS を除外する唯一の正しいオプションは、Windows 10 のみとなります (Microsoft は現在 Windows 11 と macOS もサポートしていますが、これらは選択肢に含まれていません)。したがって、Endpoint DLP は iOS または Android では実行されないため、リストされたオプションの中では、Windows 10 のみが正しい選択です。

最新問題**: 122**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



Answer:

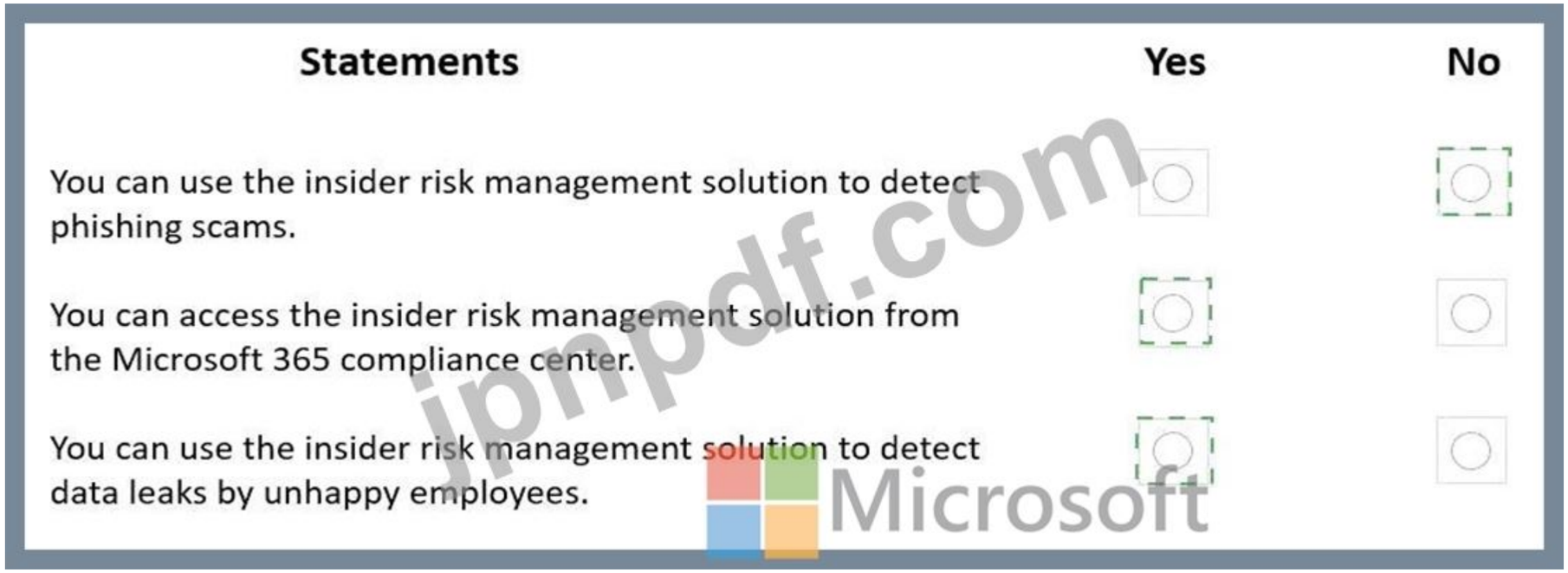
最新問題**: 123**
複数のサブスクリプションにわたってAzureリソースを一貫した方法でデプロイするには、どのようなツールを使用できますか？
A. Microsoft Defender for Cloud
B. Azure Policy
C. マイクロソフトセンチネル
D. アジュールブループリント
Answer: (解答を表示する**)**

最新問題**: 124**
Azure Bastionを使用してAzure仮想マシンに接続する必要があります。何を使用すればよいでしょうか？
A. Azureポータル
B. SSHクライアント
C. PowerShellリモート処理
D. リモートデスクトップ接続クライアント
Answer: D (メーッセージを残す**)**

最新問題**: 125**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
You can use the insider risk management solution to detect phishing scams.	○	○
You can access the insider risk management solution from the Microsoft 365 compliance center.	○	○
You can use the insider risk management solution to detect data leaks by unhappy employees.	○	○

Answer:



Explanation:

ボックス1 :いいえ

フィッシング詐欺は外部からの脅威である。

ボックス2 :はい

内部リスク管理は、Microsoft 365 のコンプライアンスソリューションです。

ボックス3 :はい

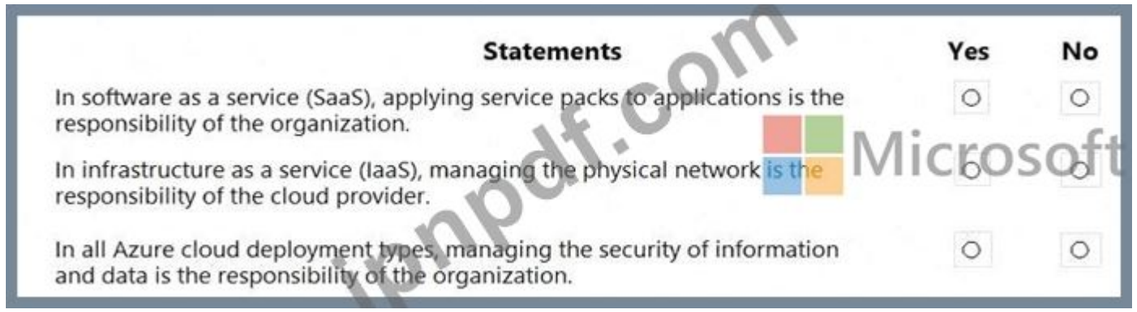
内部リスク管理は、ユーザーによる内部リスクを最小限に抑えるのに役立ちます。これには以下が含まれます。

機密データの漏洩およびデータ流出

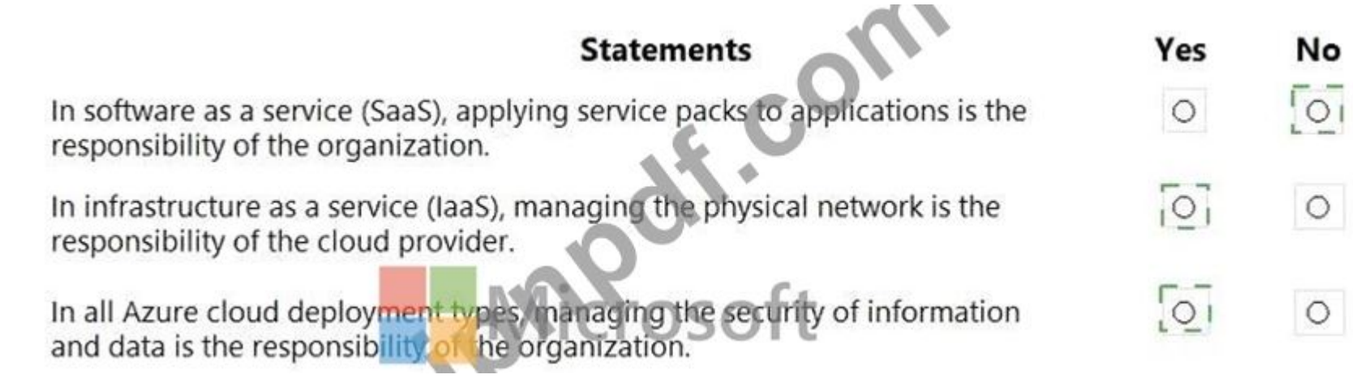
* 機密保持義務違反

知的財産（IP）の窃盗
* 詐欺
インサイダー取引
* 法令遵守違反

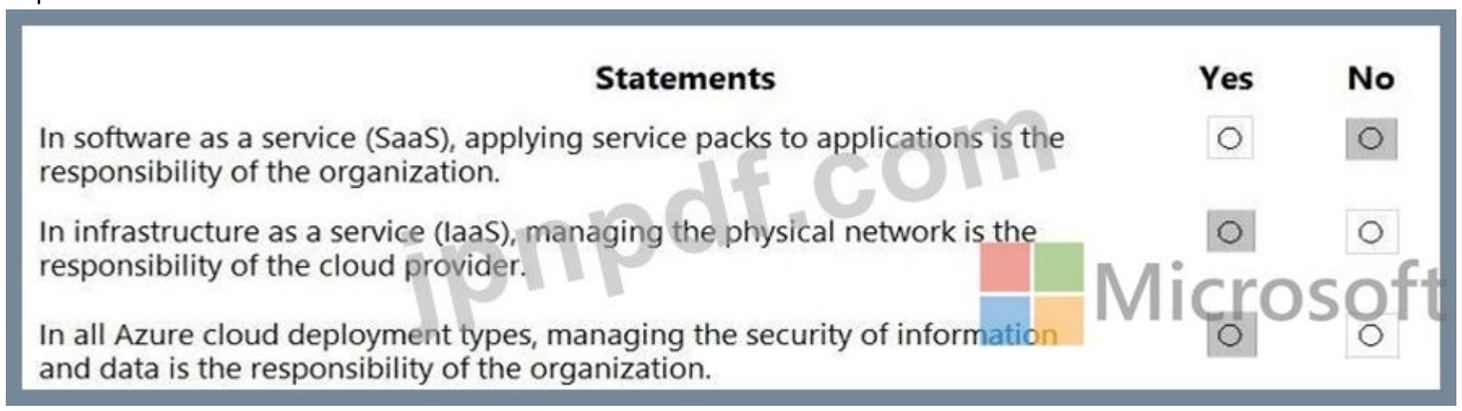
最新問題: 126
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:



Explanation:



Microsoftの責任共有モデルでは、クラウドプロバイダーがクラウドを保護し、顧客はクラウドに保存したデータを保護するとされています。Azureセキュリティのドキュメントには、「デプロイメントの種類に関係なく、データ、エンドポイント、アカウント、およびアクセス管理に対する責任は常に顧客にあります」と説明されています。これはIaaS、PaaS、SaaSのいずれにも適用されるため、組織は常に情報とデータのセキュリティに責任を負うことから、ステートメント3は「はい」となります。

SaaS に関して、マイクロソフトは、顧客は 「ネットワーク、サーバー、オペレーティングシステム、さらには個々のアプリケーション機能を含む基盤となるクラウドインフラストラクチャを管理または制御しない」と説明しており、プロバイダーがサービスの保守と更新を担当します。SaaS では、アプリケーションコードへのパッチ適用やサービスパックの適用などのタスクはサービスプロバイダーが担当し、顧客はデータ、ID、およびアクセスに集中します。したがって、ステートメント 1 は 「いいえ」です。
IaaS に関して、マイクロソフトはプロバイダーが物理的な環境を管理すると述べています。 「マイクロソフトは物理ホスト、ネットワーク、データセンター設備に責任を負います」一方、顧客はサブスクリプション内のゲスト OS、アプリケーション、ネットワーク制御を構成し、保護します。したがって、物理ネットワークの管理はクラウドプロバイダーの義務であり、ステートメント 2 は 「はい」となります。
これらのSCI原則は、Azureの共有責任に関するMicrosoft Learn/Docsガイダンスの基礎となるものです。
プロバイダーは 「クラウドのセキュリティ」を、顧客は 「クラウド内のセキュリティ」を担い、データ保護は常に顧客の責任となる。

最新問題: **127**
以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

Azure ネットワーク セキュリティ グループを使用すると、Azure 仮想ネットワーク内の Azure リソースとの間で送受信されるネットワーク トラフィックをフィルタリングできます。ネットワーク セキュリティ グループには、さまざまな種類の Azure リソースへの受信ネットワーク トラフィック、またはそこからの送信ネットワーク トラフィックを許可または拒否するセキュリティ ルールが含まれています。各ルールに対して、送信元と宛先、ポート、およびプロトコルを指定できます。
参照：
https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

最新問題: **128**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。
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.	○	○

Answer:

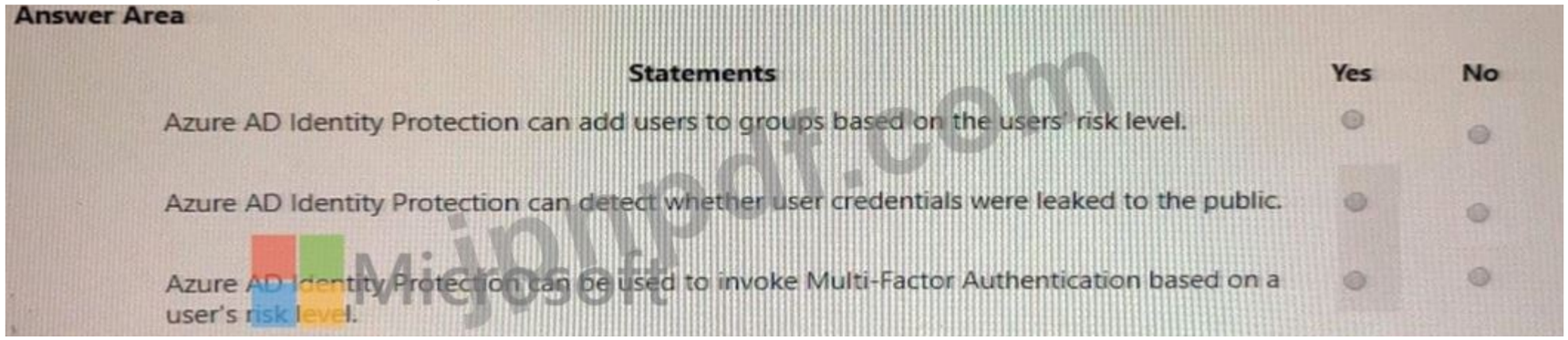
Answer Area

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.	○	○

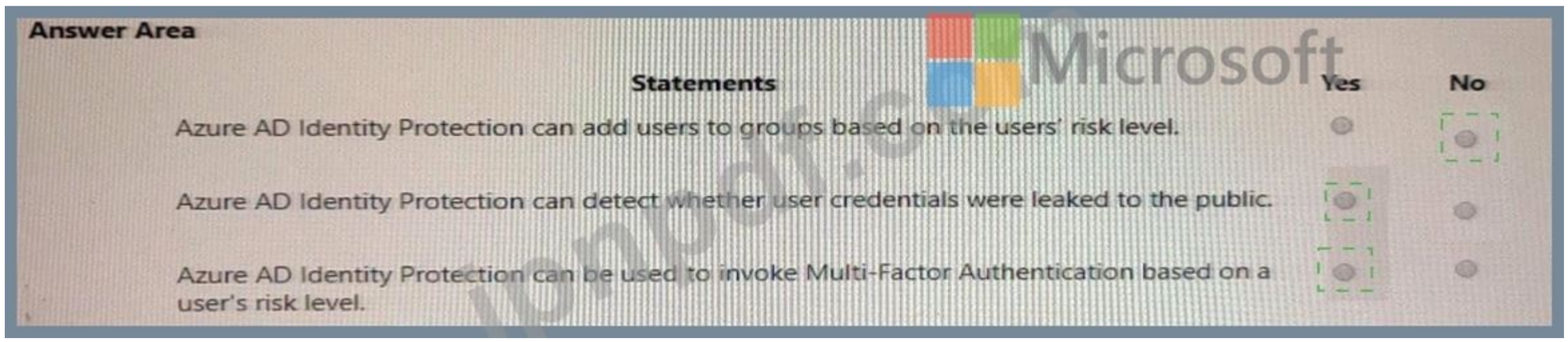
参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

最新問題: **129**

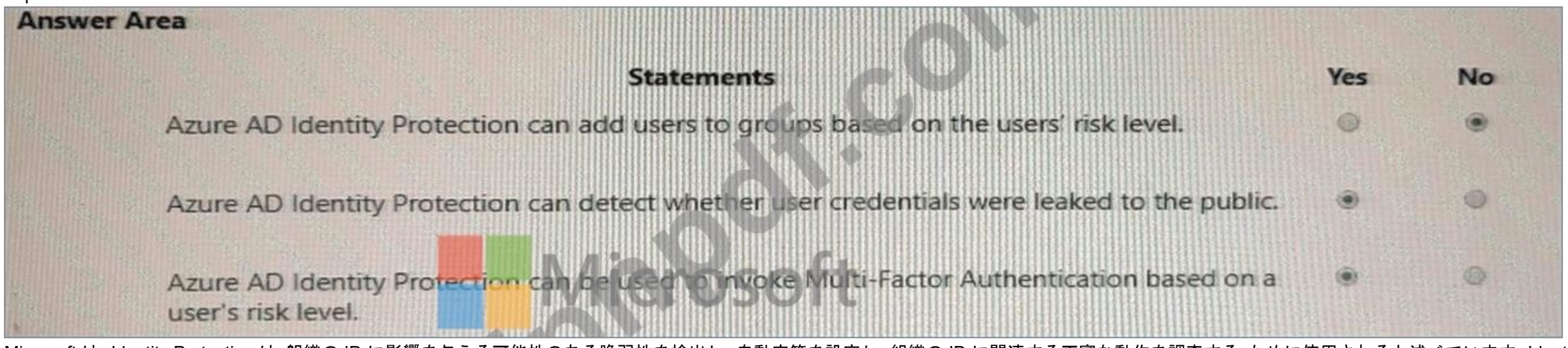
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:



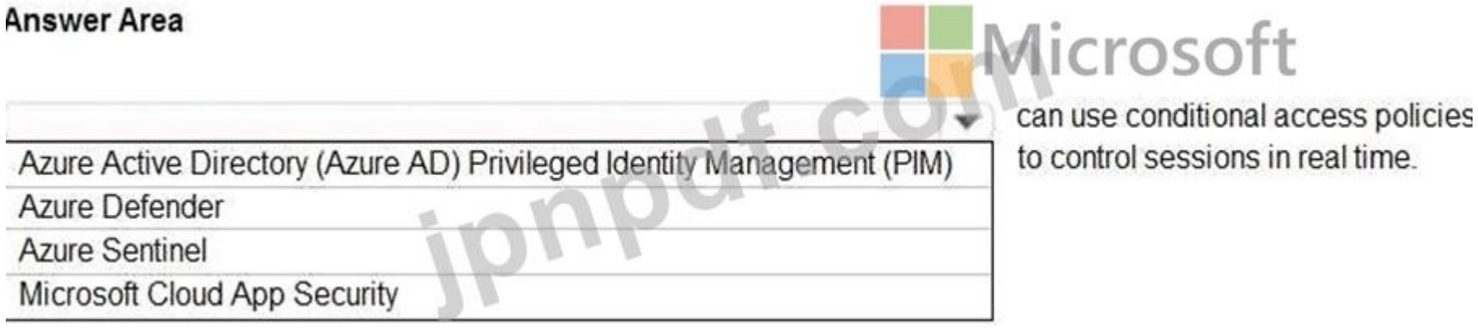
Explanation:



Microsoft は、Identity Protection は 組織の ID に影響を与える可能性のある脆弱性を検出し、自動応答を設定し、組織の ID に関連する不審な動作を調査する」ために使用されると述べています。Identity Protection は、 漏洩した認証情報、匿名 IP アドレス、見慣れないサインイン プロパティ、[および] 不可能な旅行」などの検出機能を使用して、ユーザーのリスクとサインインのリスクを評価します。これらの組み込みの検出機能により、このサービスは、公開データセットまたは犯罪データセット（一般的に漏洩した認証情報と呼ばれる）に有効なユーザー認証情報が見つかったかどうかを検出できるため、ID 侵害のリスクを軽減できます。

Identity Protectionには、「検出されたリスクへの対応を自動化する」ポリシー制御が含まれており、具体的にはユーザーリスクポリシーとサインインリスクポリシーが挙げられます。Microsoftは、これらのポリシーによって「ユーザーリスクが検出された場合、パスワードの変更を要求」したり、「サインインリスクが検出された場合、多要素認証を要求」したりできると説明しています。したがって、Identity Protectionは、条件付きアクセスに基づくリスクポリシーの一部として、リスクに基づいてMFAを呼び出すことができます。
ただし、ID保護機能はグループのライフサイクル管理は行いません。マイクロソフトは、グループメンバーシップの自動化をID保護機能ではなく、Azure ADの動的グループ/IDガバナンス機能の下に位置付けています。
したがって、リスクレベルに基づいてユーザーをグループに追加する機能は、ID保護の機能ではありません。ID保護は、検出、リスク評価、およびポリシーに基づく対策（MFAやパスワードのリセットなど）に重点を置いており、グループへの割り当ては行っていません。

最新問題: **130**
文を正しく完成させる選択肢を選びなさい。
Answer Area



Answer:

参照：
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

最新問題: **131**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	○
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	○	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

Answer:

Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	○
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	○	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	○	○

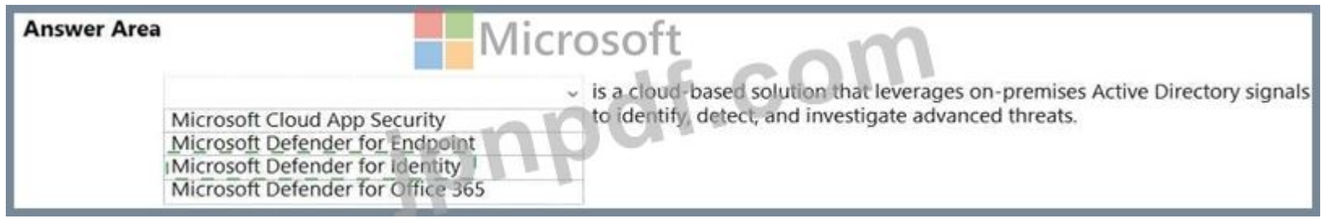
Answer Area

Statements	Yes	No
Microsoft Entra ID Protection can add users to groups based on the users' risk level.	○	●
Microsoft Entra ID Protection can detect whether user credentials were leaked to the public.	●	○
Microsoft Entra ID Protection can be used to invoke Multi-Factor Authentication based on a user's risk level.	●	○

最新問題: **132**

文を正しく完成させる選択肢を選びなさい。

Answer:

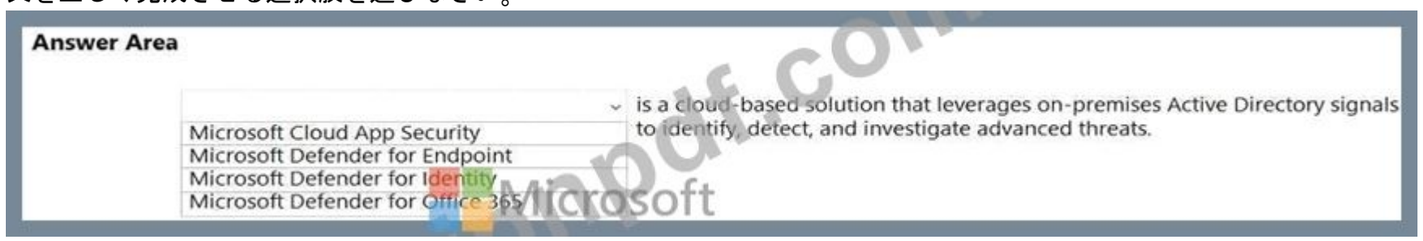


説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

最新問題: **133**

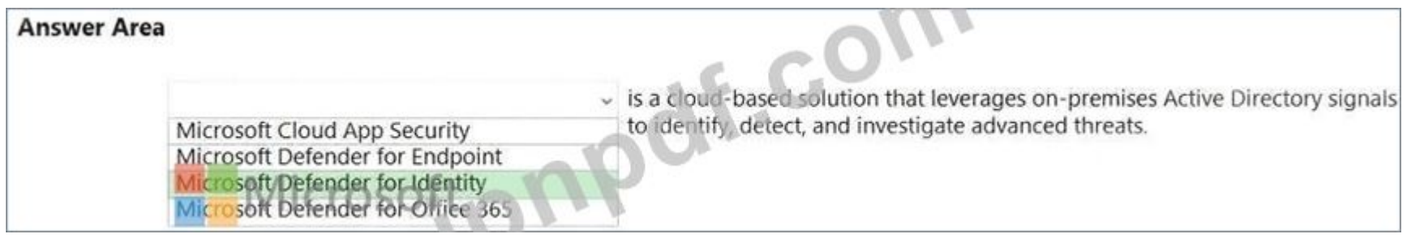
文を正しく完成させる選択肢を選びなさい。



Answer:

説明

グラフィカルユーザーインターフェース、テキスト説明は中程度の信頼度で自動生成されます

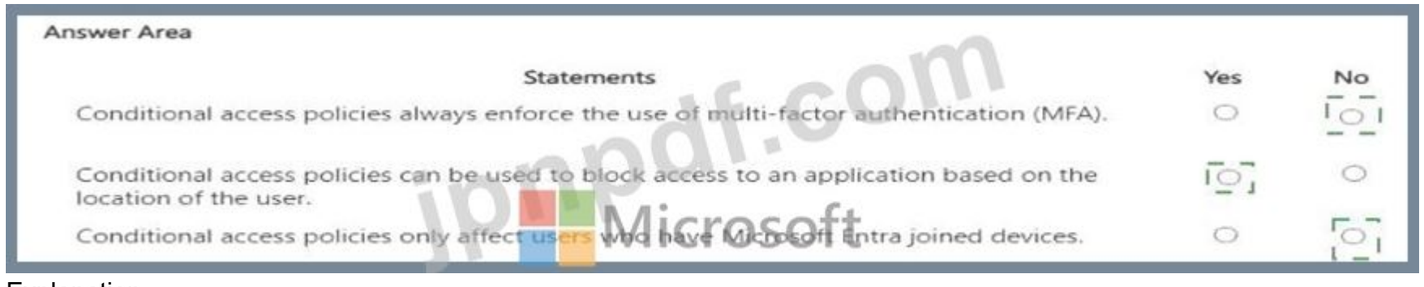


最新問題: **134**

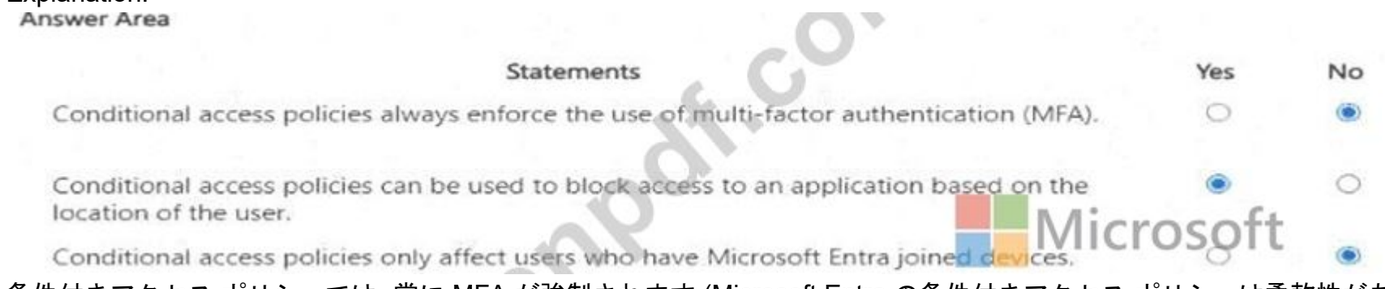
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer:



Explanation:



条件付きアクセス ポリシーでは、常に MFA が強制されます (Microsoft Entra の条件付きアクセス ポリシーは柔軟性があり、必ずしも MFA を必須とするわけではありません。MFA は可能な制御方法の 1 つですが、ポリシーでは、準拠したデバイスの要求、アクセスの完全なブロック、利用規約への同意の要求、セッション制御の強制など、他のアクセス制御を強制することもできます。

SCI 抜粋: 条件付きアクセスは、Azure AD がシグナルを統合し、意思決定を行い、組織のポリシーを適用するために使用するツールです。これらのポリシーでは MFA を要求することができますが、すべてのポリシーで必須ではありません。」場所に基づいてアクセスをブロック = はい条件付きアクセスは、名前付きロケーション (国や IP 範囲など) を使用したロケーションベースの条件をサポートします。ポリシーは、ユーザーがサインインしている場所に基づいてアクセスをブロックまたは許可できます。

SCI 抜粋: 管理者は条件付きアクセス ポリシーを使用して、ユーザーの場所に基づいてアクセスをブロックまたは許可できます。名前付き場所を使用して、信頼できるエリアまたは危険なエリアを定義します。」Entra に参加しているデバイスのみに影響します = 条件付きアクセスは、以下を含むすべてのユーザーとデバイスに適用されます。

エントラ結合、
ハイブリッド エントラ ジョイン、
登録済みデバイス（Microsoft IntuneまたはAzure AD経由）、
構成によっては、管理対象外のデバイス（BYOD）も対象となります。
SCI抜粋：条件付きアクセス ポリシーは、選択された条件に基づいて、Microsoft Entra に参加しているデバイスだけでなく、すべてのユーザーとデバイスに適用されます。」

最新問題: **135**
文を正しく完成させる選択肢を選びなさい。

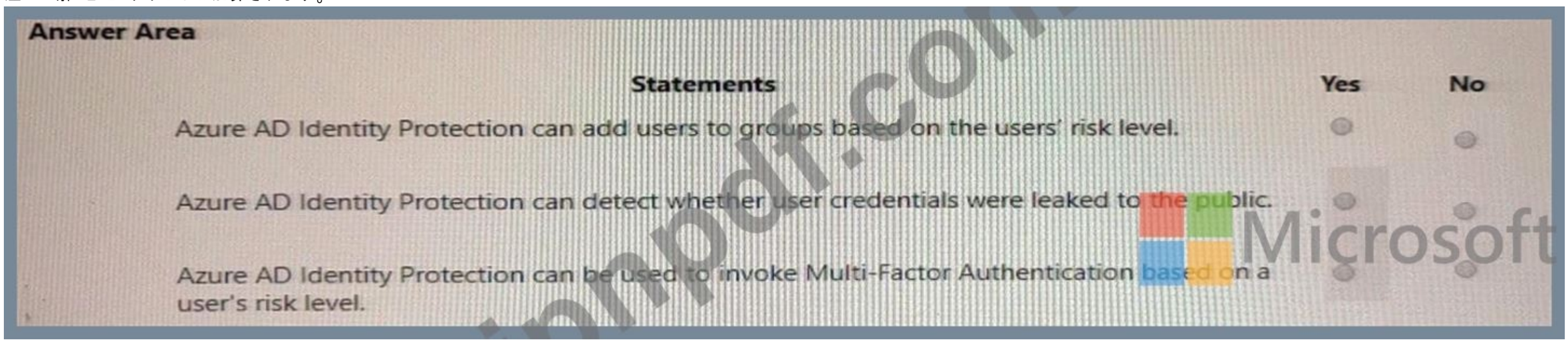
Answer:

最新問題: **136**
文を正しく完成させる選択肢を選びなさい。

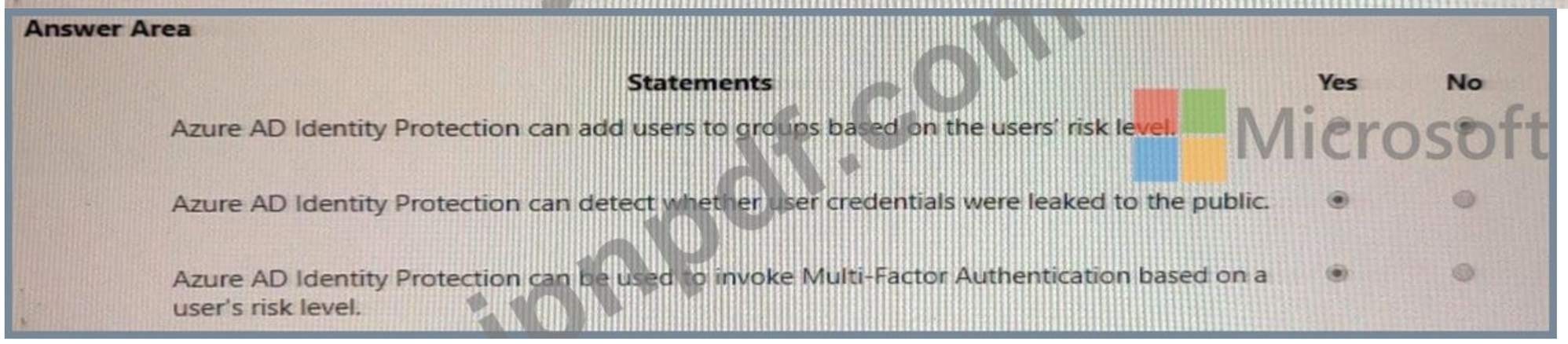
Answer:

Explanation:
テキスト、文字の説明は自動的に生成されます

最新問題: **137**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:



最新問題: **138**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

Answer Area

Conditional Access policies are enforced [after] first-factor authentication.

Microsoft Entra 条件付きアクセスでは、ポリシーの評価は、ユーザーが第一要素認証 (たとえば、ユーザー名 + パスワード、または Windows Hello for Business キー) を正常に完了した後に行われます。Microsoft Learn では、条件付きアクセスは Azure AD がシグナルを統合し、意思決定を行い、組織のポリシーを適用するために使用するツール」であり、 第一要素認証が完了した後」に適用される、と説明しています。プライマリ認証が成功すると、条件付きアクセスは、ユーザー、デバイスの状態、場所、リスク (ID 保護から)、アプリケーションなどのシグナルを評価し、MFA の要求、アクセスのブロック、セッション制御の適用などの制御を適用します。
この設計により、条件付きアクセスがプライマリ認証に取って代わることはなく、最初の資格情報検証の前または検証中に強制されることもありません。代わりに、より強力な証明 (MFAなど) を要求したり、アクセスパスを制限したり、セッションを制限したりできる2番目のポリシー決定ポイントが追加されます。したがって、 後」が正しいですが、
条件付きアクセスは、最初のサインインで必要なシグナルを収集し、その後、設定されたアクセス決定と保護を適用するため、 第一要素認証の前」、 最中」、 代わりに」といった表現は適切ではありません。

最新問題: **139**
文を正しく完成させる選択肢を選びなさい。

[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.

Answer:

[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.

Microsoft

最新問題: **140**
以下の各記述について、正しい場合は はい」を選択してください。そうでない場合は いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

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.	◉	○

最新問題: 141

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

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.	○	◉

最新問題: **142**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	○
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	○
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	○	○

Answer:

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	○
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	○
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	○	○

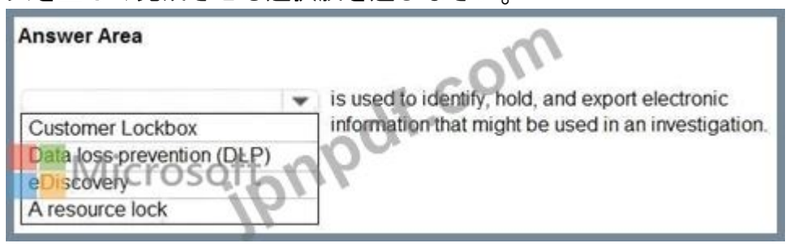
最新問題: **143**

文を正しく完成させる選択肢を選びなさい。

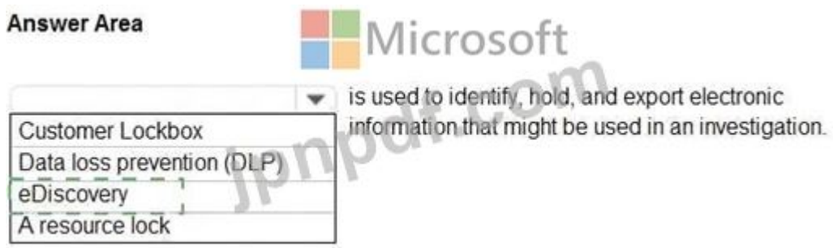
Answer:

最新問題: **144**

文を正しく完成させる選択肢を選びなさい。



Answer:



説明

電子情報開示

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

最新問題: **145**

Microsoft Defender for Endpointのどの機能が、攻撃対象領域を縮小することでサイバー脅威に対する第一線の防御を提供しますか？

A. 自動修復

B. 自動調査

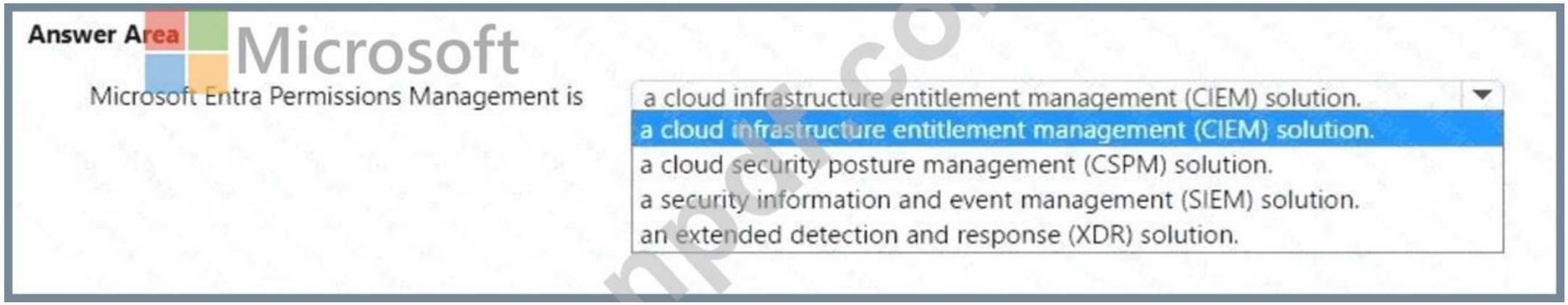
C. 高度な狩猟

D. ネットワーク保護

Answer: D (メーッセージを残す)

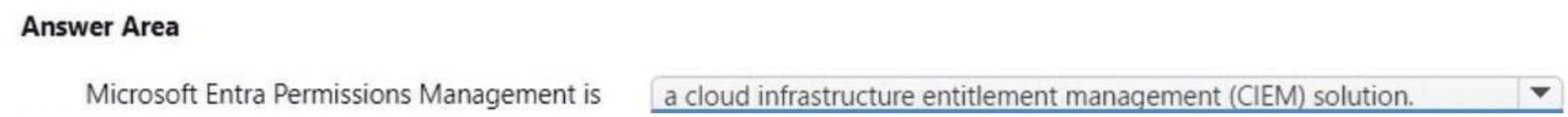
ネットワーク保護は、インターネット関連の脅威からデバイスを保護するのに役立ちます。ネットワーク保護は、攻撃対象領域を縮小する機能です。
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide

最新問題: **146**
文を正しく完成させる選択肢を選びなさい。



Answer:

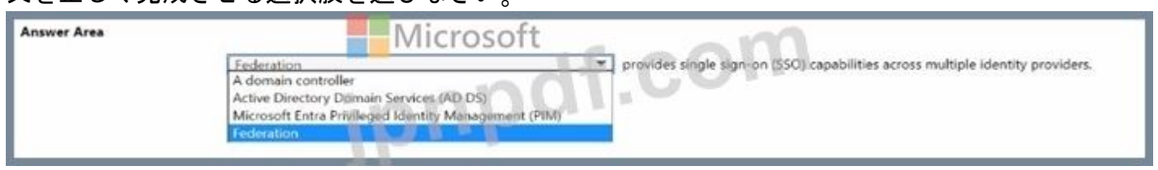
Explanation:



（CIEM）ソリューション。CIEMは、Microsoft Azure、AWS、Google Cloud Platform（GCP）などのマルチクラウド環境全体で、組織がIDとアクセス権限を管理するのに役立つセキュリティテクノロジーのカテゴリです。
マイクロソフトの公式セキュリティ、コンプライアンス、およびアイデンティティ（SCI）トレーニングとドキュメント（特にSC-300およびSC-900の学習パスに関連するもの）によると、次のとおりです。
「Microsoft Entra Permissions Managementは、マルチクラウド環境全体にわたるすべてのIDとリソースのアクセス許可を包括的に可視化し、制御するCIEMソリューションです。」CIEMとしてのMicrosoft Entra Permissions Managementの主な機能は以下のとおりです。
過剰な権限を持つアカウントや未使用の権限の発見。
最小権限の原則の適用。
詳細な権限分析とレポート機能。
Azure、AWS、およびGCP環境をサポートします。

このソリューションは、クラウドプラットフォームにおけるIDの乱立や権限の不正使用といった、増大するリスクに対処するために設計されています。これらのリスクは、従来のIDガバナンスツールやSIEMツールでは効果的に対処できません。
誤った選択肢：
CSPM（クラウドセキュリティ態勢管理）は、ID権限ではなく、クラウドの設定ミスに焦点を当てています。
SIEM（例Microsoft Sentinel）は、脅威検出のためにログやイベントを集約しますが、権限の可視化には役立ちません。
XDR（例Microsoft Defender XDR）は、エンドポイント、ID、データ全体にわたる検出と対応に重点を置いており、権限管理は対象としていません。
したがって、正しくマイクロソフトによって検証された分類は、クラウドインフラストラクチャ権限管理（CIEM）ソリューションです。

最新問題: **147**
文を正しく完成させる選択肢を選びなさい。



Answer:

最新問題: **148**
文を正しく完成させる選択肢を選びなさい。

Answer:

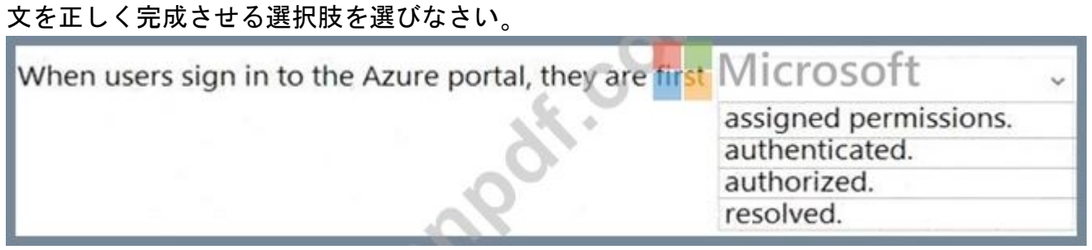
最新問題: **149**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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).	○	○

Answer:

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).	◉	○

最新問題: **150**
文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:

Microsoft クラウド ID では、Azure リソースへのアクセスは、認証、認可という従来の順序に従います。Microsoft Learn では、この 2 つのステップを明確に定義しています。 認証とは、個人またはサービスの ID を確立するプロセスです」、一方 認可とは、個人またはサービスが実行できる操作を決定するプロセスです」。Azure サインインでは、Microsoft Entra ID (旧 Azure AD) がまずユーザーの資格情報 (パスワード、MFA、条件付きアクセス、デバイス準拠、リスク評価) を検証します。検証が成功すると、ユーザーの ID を証明するセキュリティ トークンが発行されます。この ID が確立されて初めて、Azure は認可に進みます。認可では、Azure Resource Manager がロールベースのアクセス制御 (RBAC) の割り当てを評価し、許可される操作を決定します。SCI ガイダンスでは、ゼロ トラストのこの順序を強調しています。 明示的に検証する」(強力なシグナルで認証する)、次に 最小権限アクセスを使用する」(RBAC または特権 ID 管理によって認可する)。したがって、ユーザーが Azure ポータルにサインインすると、最初のステップは認証、つまりユーザーが誰であるかを確認することです。次のステップは認証です。これは、役割、範囲、ポリシーに基づいて、ユーザーがアクセスできるリソースと操作を決定します。この順序付けは、Microsoft 365 および Azure 全体における安全な ID およびアクセス管理の基盤となります。

最新問題: **151**

文を正しく完成させる選択肢を選びなさい。

Answer:

参照：

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

最新問題: **152**

以下の各設問について、該当する場合は 「はい」を選択してください。該当しない場合は 「いいえ」を選択してください。注：正解ごとに1点が加算されます。

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

Answer:

Explanation:

Microsoft は、情報バリア (IB) を、規制要件や利益相反要件を満たすために 「特定のユーザーまたはグループ間のコミュニケーションとコラボレーションを制限する」ポリシーと定義しています。Microsoft 365 では、IB の適用はコラボレーションワークロード全体にわたって行われ、特に Microsoft Teams や、IB v2 では SharePoint および OneDrive にも適用されます。これにより、相互作用すべきでないセグメントに割り当てられたユーザーは、チャット、会議、ファイルの共有ができなくなります。このサービスは 「誰が誰とコミュニケーションおよびコラボレーションできるかを制御する」ものであり、これらの制御を Teams のチャット/チャネル、SharePoint/OneDrive サイトおよびファイルに適用することで、ユーザーがコンテンツを共有またはアクセスしようとしたときにセグメントの境界が尊重されるようにします。

対照的に、Exchange Online のメールは情報バリア (IB) のサポート対象ではありません。IB はメールのブロックやルーティングを行いません。メールの制限は、IB ではなく、他の機能 (メールフロー規則など) で処理されます。したがって、Microsoft の SCI ガイダンスに沿って、IB は Microsoft Teams および Microsoft SharePoint/OneDrive と連携しますが、Exchange メールに対するポリシー適用機能は提供しません。

最新問題: **153**
以下の各設問について、該当する場合は 「はい」を選択してください。該当しない場合は 「いいえ」を選択してください。注：正解ごとに1点が加算されます。

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

Answer:

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

最新問題: **154**
以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

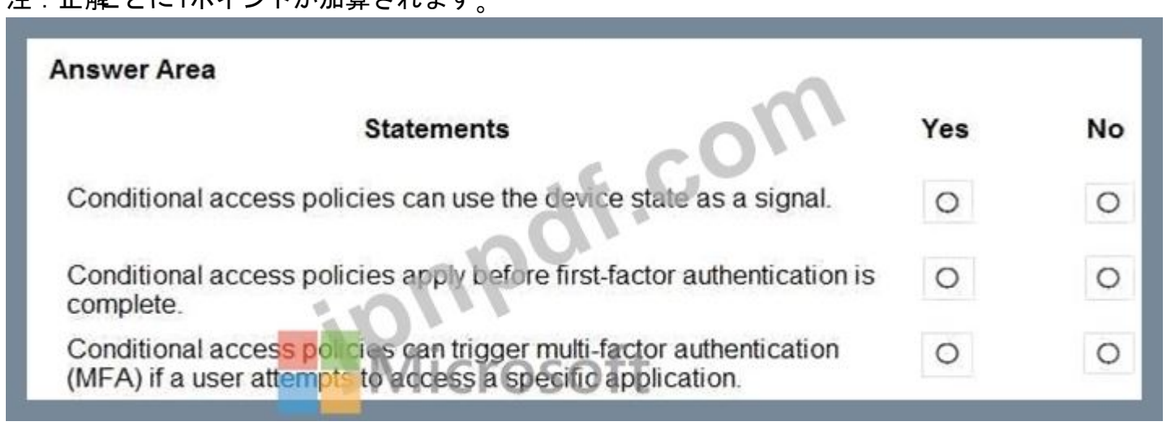
Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Answer:

Explanation:

ボックス1 :はい
条件付きアクセス ポリシーはすべてのユーザーに適用できます
ボックス2 :いいえ
条件付きアクセス ポリシーは、第一要素認証が完了した後に適用されます。
ボックス3 :はい
特定のプラットフォームのデバイスを使用しているユーザー、または特定の状態を示すマークが付いているユーザーは、条件付きアクセス ポリシーを適用する際に利用できます。

最新問題: **155**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。



Answer:

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:

グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます

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.	○	○

ボックス1 :はい

ボックス2 :いいえ

条件付きアクセス ポリシーは、第一要素認証が完了した後に適用されます。ボックス 3: はい

最新問題**: 156**

以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Answer:

参照：

https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

最新問題: **157**

文を正しく完成させる選択肢を選びなさい。

Answer Area

Answer:

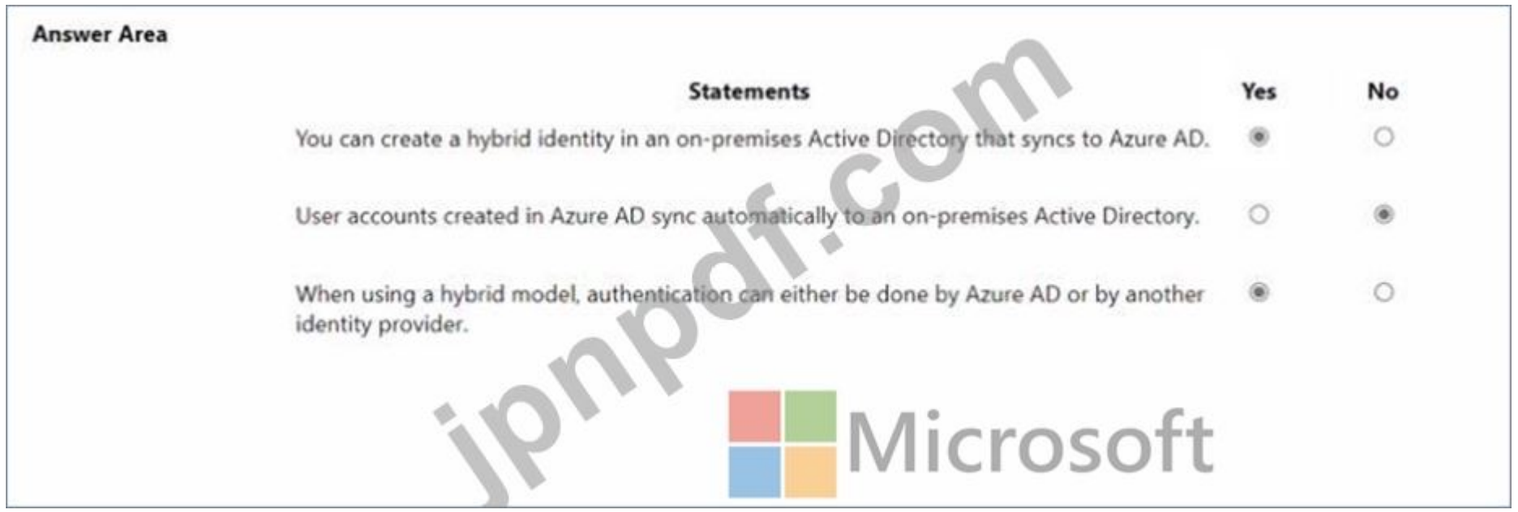
Explanation:

マイクロソフトのSCI学習コンテンツでは、情報保護という中核的な目的はCIAトライアドによって構成されている。

マイクロソフトは、「機密性、完全性、可用性は、セキュリティの基本原則である」と説明しています。このモデルにおいて、完全性とは、情報が信頼できる状態を維持し、意図された状態から変更されていないことを保証するものと定義されています。SCI資料では、完全性とは「不正な改ざんを防止し、データの正確性と完全性を確保すること」を意味するとされています。「取得したデータが保存したデータと同じであることを保証する」という要件は、この完全性原則に直接対応しており、保存中または送信中にデータが改ざん、破損、または不正操作されていないことを検証することを意味します。
マイクロソフトのガイダンスでは、整合性は「不正な変更を検出または防止する」制御によって支えられていることがさらに強調されています。これには、暗号化ハッシュ、チェックサム、デジタル署名など、「コンテンツが改ざんされていないことを証明できる」制御が含まれます。対照的に、機密性はアクセス制限（最小権限の原則や暗号化など）に重点を置き、可用性は「情報やシステムへの信頼性が高くタイムリーなアクセス」に重点を置きます。このシナリオでは、取得されたデータが保存されたデータと同一であることが強調されているため、アクセスや稼働時間ではなく、正確性の維持と改ざんの検出が重要となります。これはまさに、マイクロソフトのセキュリティ、コンプライアンス、およびIDに関するガイダンスにおける整合性の目標です。

最新問題: **158**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

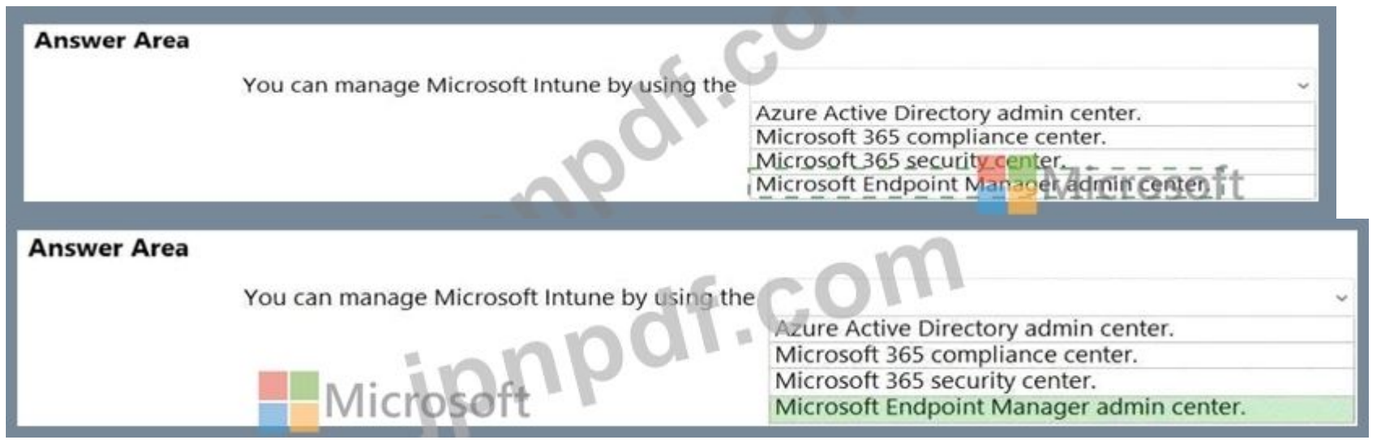
Answer:



最新問題: **159**

文を正しく完成させる選択肢を選びなさい。

Answer:



最新問題: **160**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

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

Answer:

Answer Area

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

最新問題: **161**

文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題: **162**

文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

マイクロソフトのセキュリティ、コンプライアンス、およびIDに関するガイダンスでは、多要素認証（MFA）は、独立したカテゴリの認証情報を組み合わせてユーザーを検証することに基づいています。マイクロソフトは、3つの要素タイプを次のように説明しています。

知っていること（知識）持っていること（所有）そして自分自身であること（本質）パスワードは、ユーザーが記憶してサインイン時に入力する秘密情報に基づいているため、「知っていること」に明確に分類されます。MFAは、これらの異なる要素のうち2つ以上を要求することでセキュリティを強化します。たとえば、パスワード（知っていること）に加えて、電話による承認やハードウェアトークン（持っていること）、またはWindows Helloのような生体認証（自分自身であること）などです。

異なるカテゴリの要素を使用することで、パスワードスプレー、クレデンシャルスタッフィング、フィッシングなどの一般的な攻撃を軽減できます。これは、1つの要素（たとえばパスワード）が侵害されても、2つ目の無関係な要素がなければアクセスできないためです。Microsoft は、MFA を広く有効にし、パスワードをより強力な所有または固有の認証方法と組み合わせることで、アカウント侵害のリスクを大幅に低減することを推奨しています。そのため、Microsoft Entra ID (Azure AD) で使用されている MFA モデルでは、パスワードは「知っているもの」とみなされます。

最新問題: **163**

マイクロソフトのどのポータルサイトで、マイクロソフトのクラウドサービスが国際標準化機構（ISO）などの規制基準にどのように準拠しているかについての情報が得られますか？

A. Microsoft Endpoint Manager 管理センター

B. Azure コスト管理 + 課金

C. マイクロソフト サービス トラスト ポータル

D. Azure Active Directory 管理センター

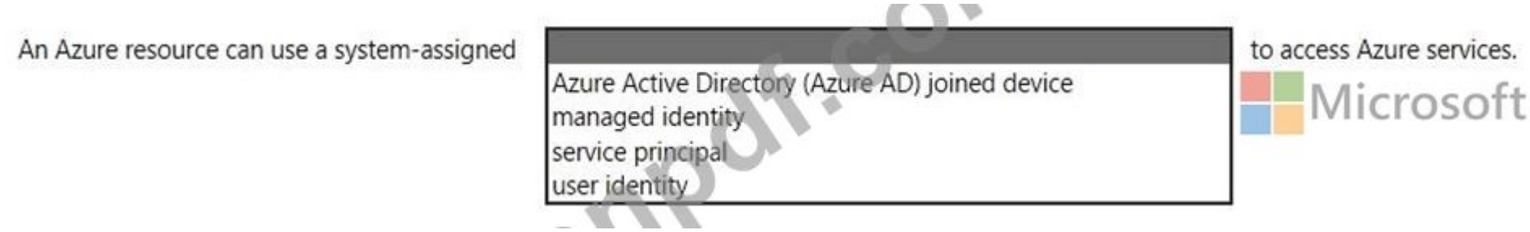
Answer: (解答を表示する**)**

説明

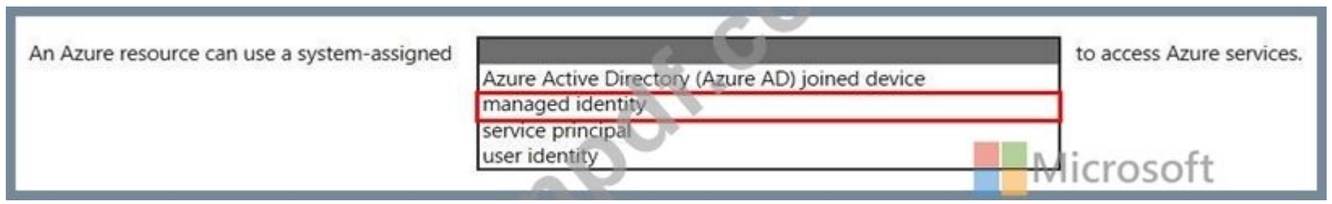
Microsoft Service Trust Portalには、Microsoftがクラウドサービスおよびそこに保存されている顧客データを保護するために実施している管理策とプロセスに関する詳細情報が掲載されています。

最新問題: **164**

文を正しく完成させる選択肢を選びなさい。



Answer:



最新問題: **165**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

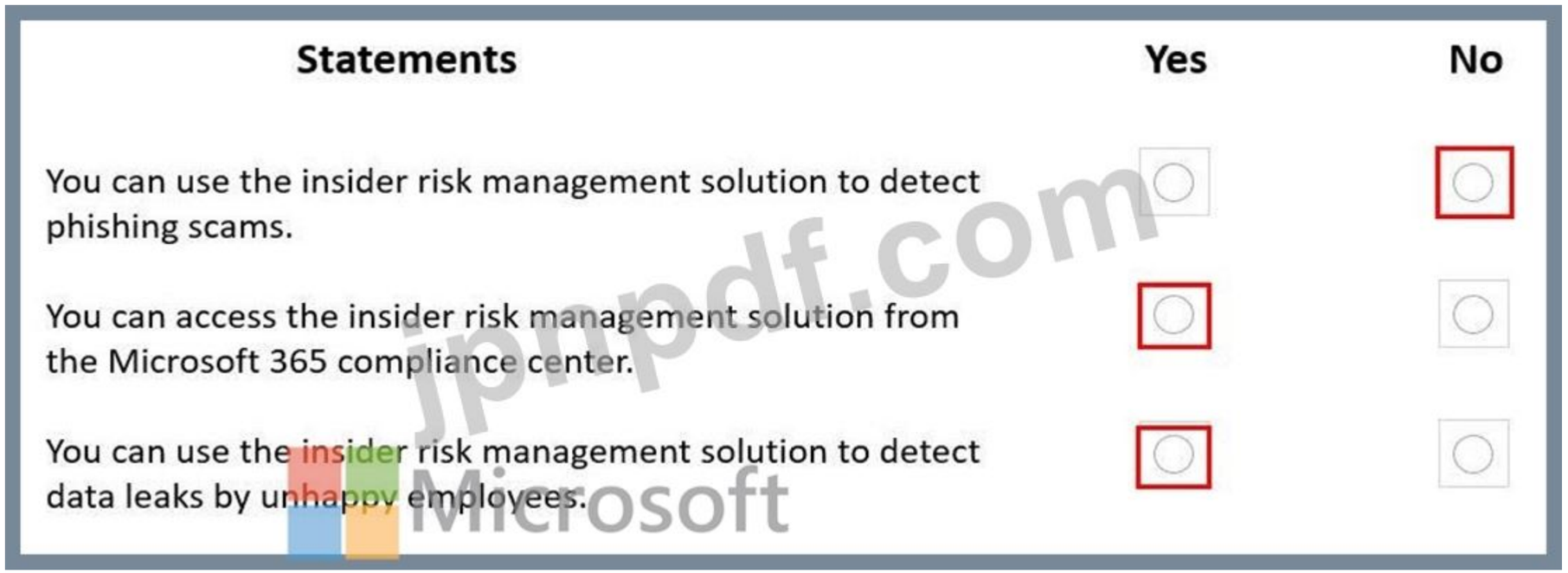
Answer:

最新問題: **166**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer:



参照：

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

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

最新問題: **167**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

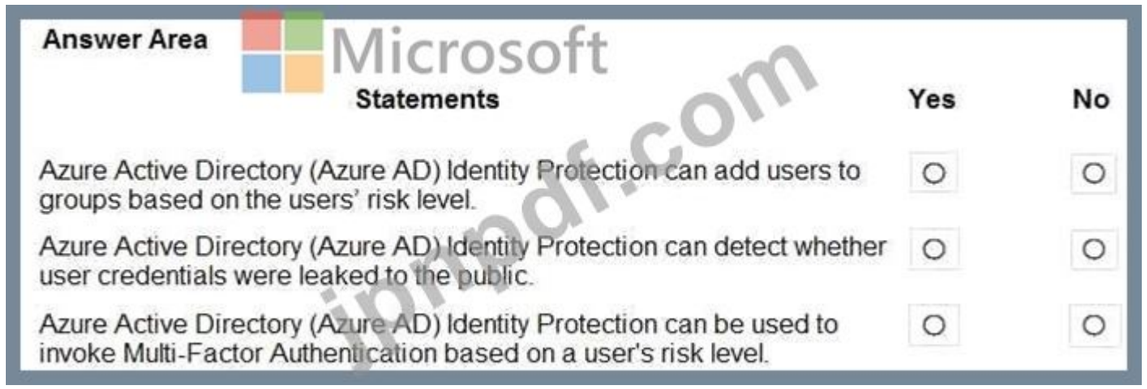
Statements	Yes	No
You can add a resource lock to an Azure subscription.	○	○
You can add only one resource lock to an Azure resource.	○	○
You can delete a resource group containing resources that have resource locks.	○	○

Answer:

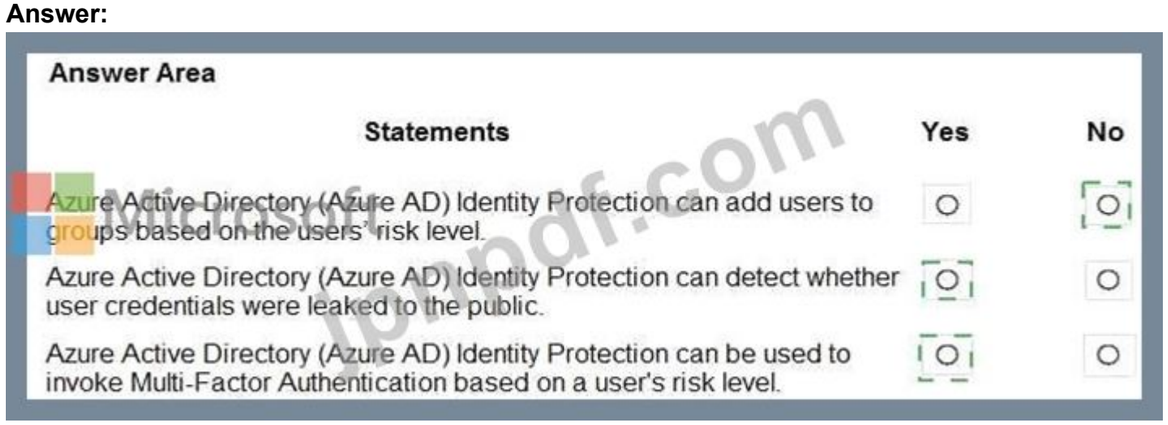
Statements	Yes	No
You can add a resource lock to an Azure subscription.	○	○
You can add only one resource lock to an Azure resource.	○	○
You can delete a resource group containing resources that have resource locks.	○	○

説明
はい
いいえ
いいえ
はい。管理者であれば、サブスクリプション、リソースグループ、またはリソースをロックして、組織内の他のユーザーが重要なリソースを誤って削除したり変更したりするのを防ぐことができます。ロックすると、ユーザーが持つ権限はすべて無効になります。
いいえ - 継承の中で最も制限の厳しいロックが優先されます。
いいえ - ロックされたリソースを含むリソース グループを削除しようとすると、ポータル UI にエラーが表示され、リソースは削除されません。
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json

最新問題: **168**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

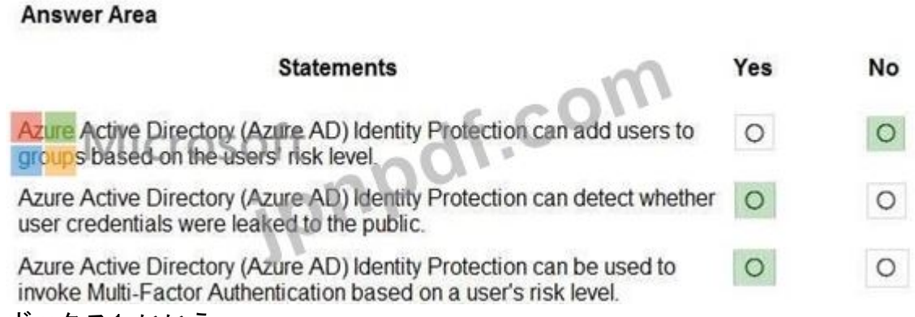


Answer:



説明

グラフィカルユーザーインターフェース、テキスト、アプリケーション、電子メールの説明は自動的に生成されます



ボックス1 :いいえ

ボックス2 :はい

認証情報漏洩とは、ユーザーの有効な認証情報が漏洩したことを示します。

ボックス3 :はい

多要素認証は、ユーザーのリスクなど、いくつかの条件に基づいて必要となる場合があります。

最新問題: **169**

文を正しく完成させる選択肢を選びなさい。

Answer:

参照：
https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

最新問題: **170**
セキュリティ戦略を策定し、ネットワークインフラ全体に複数の防御層を配置する計画を立てています。
これはどのセキュリティ手法に該当するのでしょうか？
A. セキュリティ境界としてのアイデンティティ
B. 共同責任モデル
C. 脅威モデリング
D. 多層防御
Answer: D (メーッセージを残す)

最新問題: **171**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer:

Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	○	○
Network security group (NSG) default rules can be deleted.	○	○
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	○	○

Answer Area

Statements	Yes	No
Each network security group (NSG) rule must have a unique name.	●	○
Network security group (NSG) default rules can be deleted.	○	●
Network security group (NSG) rules can be configured to check TCP, UDP, or ICMP network protocol types.	●	○

最新問題: **172**

ホットスポット

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

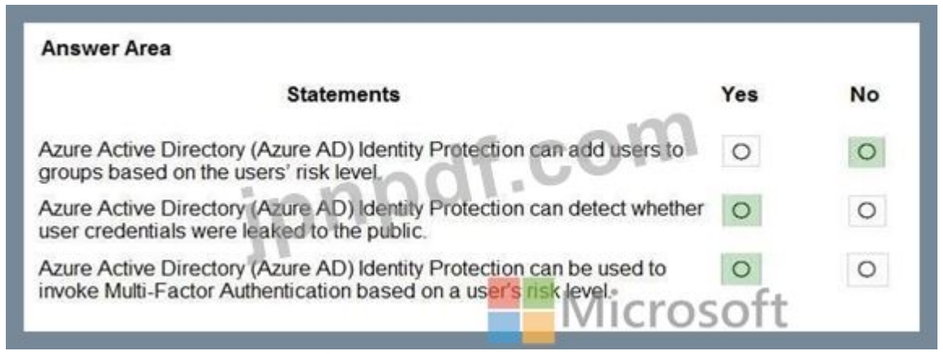
注：正解ごとに1ポイントが加算されます。

ホットエリア：

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.	○	○

Answer:



セクション :Microsoftコンプライアンスソリューションの機能について説明します

Explanation:

ボックス1 :いいえ

ボックス2 :はい

認証情報漏洩とは、ユーザーの有効な認証情報が漏洩したことを示します。

ボックス3 :はい

多要素認証は、ユーザーのリスクなど、いくつかの条件に基づいて必要となる場合があります。

参照 :

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa

最新問題: **173**

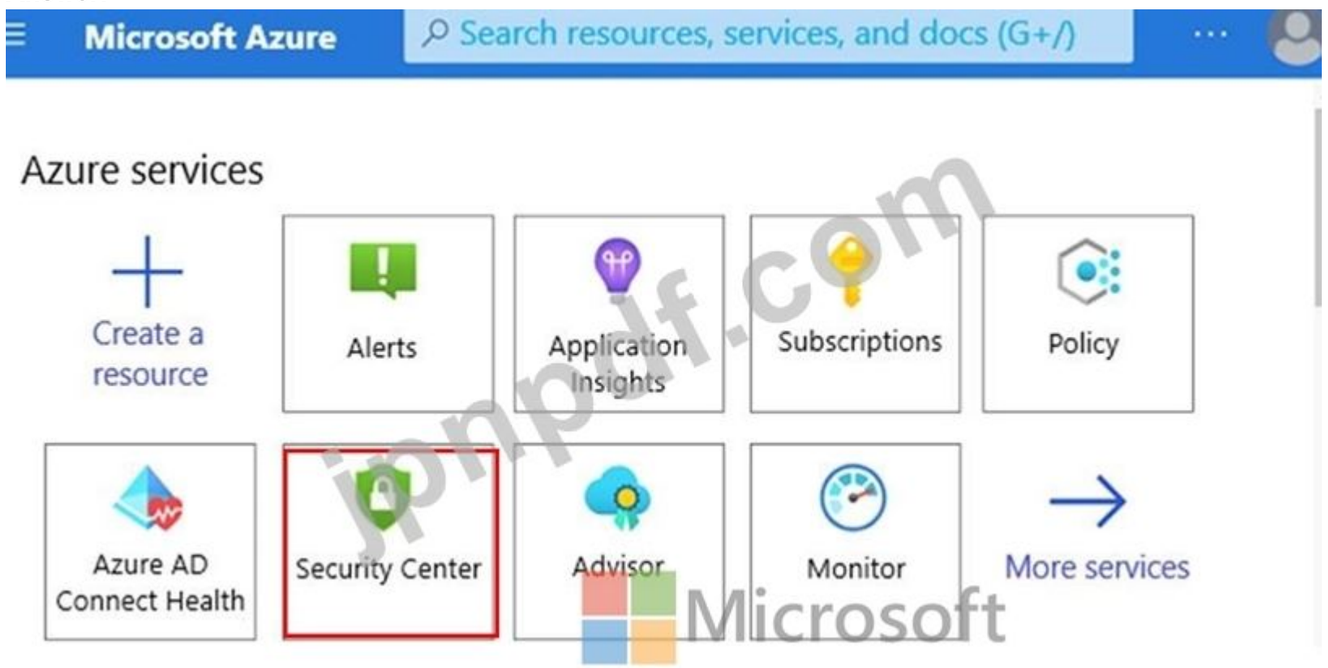
文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題: **174**

Azureのセキュリティスコアを確認するには、どのサービスを使用すればよいですか？回答するには、回答欄で適切なサービスを選択してください。

Answer:



参照：

https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

最新問題: **175**
文を正しく完成させる選択肢を選びなさい。

Answer:

最新問題: **176**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

最新問題: 177

Azureのセキュリティスコアを確認するには、どのサービスを使用すればよいですか？回答するには、回答欄で適切なサービスを選択してください。

Answer:

Explanation:
セキュリティセンター
参照：
https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

最新問題**: 178**
ユーザー認証方法としてメールをサポートする機能は何ですか？
A. Microsoft Entra ID Protection
B. Microsoft Entra多要素認証（MFA）
C. セルフサービスパスワードリセット（SSPR）
D. Microsoft Entra パスワード保護
Answer: C (メーッセージを残す**)**
Microsoft Entra ID（旧Azure AD）のセルフサービスパスワードリセット（SSPR）は、ユーザーがパスワードをリセットまたはロック解除するために本人確認を行う必要がある場合に、認証方法として電子メールを明示的にサポートする機能です。
MicrosoftのIDおよびアクセスに関するドキュメントとSCIの学習コンテンツによると、SSPRでは、管理者が携帯電話、オフィス電話、モバイルアプリ、セキュリティ質問、メールなど、ユーザーが利用できる認証方法を選択できます。メールが有効になっている場合、登録済みの代替メールアドレスに認証コードが送信されます。ユーザーはこのコードを入力することで本人確認を行い、これはSSPRプロセスにおける認証ステップとして扱われます。
対照的に：
* Microsoft Entra 多要素認証 (MFA) は、MFA の方法としてメールをサポートしていません。認証アプリ、電話、テキスト メッセージなどの方法に重点を置いています。
* Microsoft Entra ID Protectionは、危険なサインインやユーザーを検知して対応しますが、メールベースの認証は提供しません。

* Microsoft Entra Password Protectionは、禁止されたパスワードや漏洩したパスワードに対処するものであり、メールアドレスの認証には対応していません。
したがって、リストの中でメールを認証方法としてサポートしている唯一のオプションは、セルフサービスパスワードリセット（SSPR）です。

最新問題: **179**
文を正しく完成させる選択肢を選びなさい。
Answer Area

Answer:

最新問題: **180**
文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

Microsoft 365 Defender では、Microsoft 365 サービス全体からのセキュリティシグナルがアラートとして生成されます。Microsoft のドキュメントでは、インシデントを 「相関関係のあるアラートの集合」と定義しており、攻撃の全体像を表しています。インシデント オブジェクトは、関連するシグナル、エンティティ、および証拠を集約するため、アナリストは個々のアラートを個別に処理するのではなく、全体的にトリアージと修復を行うことができます。Microsoft はさらに、インシデントは 「関連するアラート、資産、ユーザー、および証拠をグループ化」することでノイズを減らし、調査のコンテキストを提供すると説明しています。また、自動相関により、Defender for Endpoint、Defender for Office 365、Defender for Identity、および Microsoft Defender for Cloud Apps からのアラートを 1 つのケースに統

合することで、SOC が最も重要なことに集中できるようになります」。インシデント内では、アナリストはタイムライン、影響を受ける資産とユーザー、アラートの詳細、推奨されるアクションを確認でき、対応策 (デバイスの隔離、URL のブロックなど) を実行できます。
/file を削除するか、ユーザーを無効にする）。これは、イベント (生のテレメトリ)、脆弱性 (Defender 脆弱性管理によって管理される露出の発見)、および Microsoft Secure Score の改善アクション (姿勢に関する推奨事項) とは対照的です。したがって、Microsoft 365 Defender ポータルでは、インシデントは、Microsoft 365 セキュリティ スタック全体で調査と調整された修復を効率化するように設計された、相関するアラートの集合です。

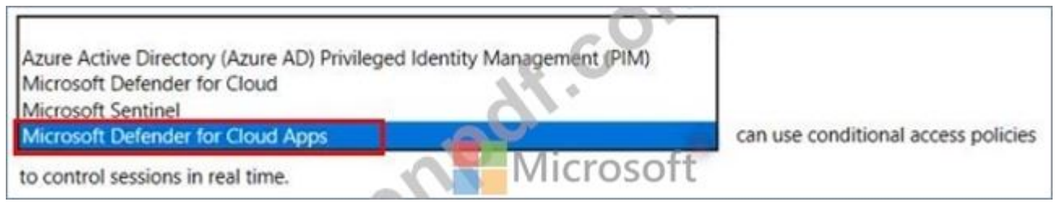
最新問題: **181**
文を正しく完成させる選択肢を選びなさい。

Answer:

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

最新問題: **182**
文を正しく完成させる選択肢を選びなさい。

Answer:



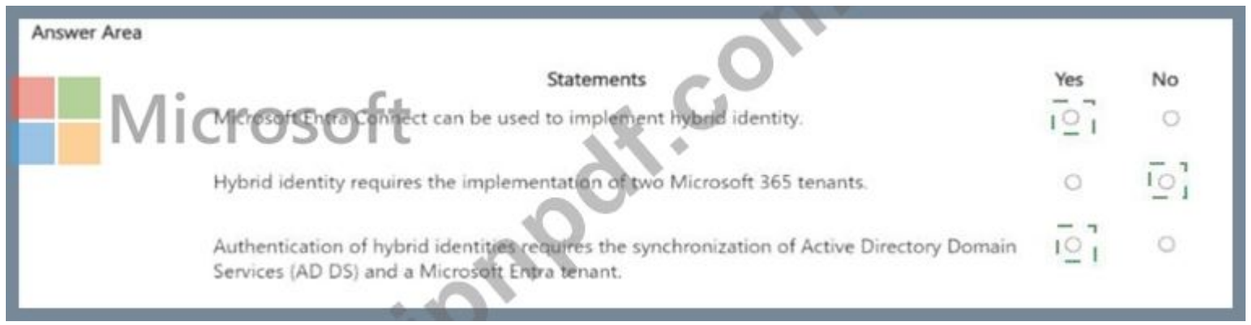
最新問題: **183**
文を正しく完成させる選択肢を選びなさい。

Answer:

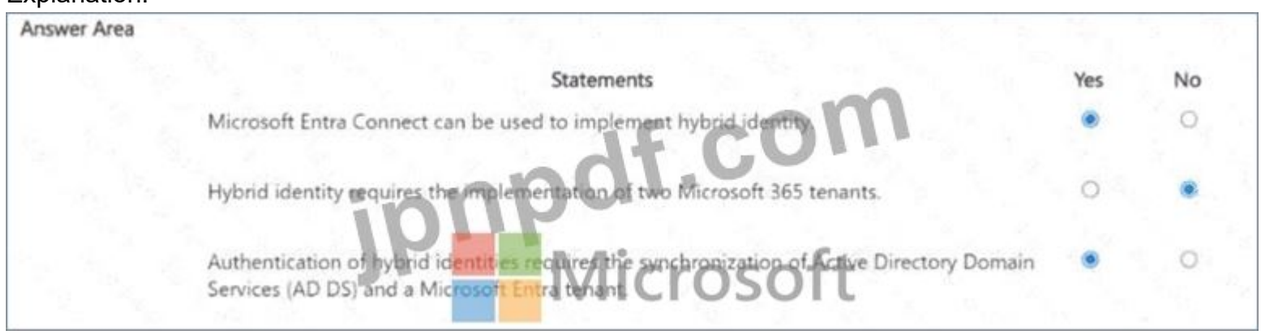
Explanation:
コンプライアンススコア
Microsoft Purview Compliance Manager では、コンプライアンス スコアは、コンプライアンスとデータ保護のリスクを軽減する改善策の完了状況を測定する指標です。Microsoft はこのスコアを、規制基準とデータ保護ベースライン全体にわたるコンプライアンス体制を定量化できる指標と説明しています。Compliance Manager で推奨される各改善策にはポイントが割り当てられ、これらの対策を完了、テスト、および証明することでスコアが上がります。ポイントはリスクに応じて重み付けされるため、リスク軽減効果の高いコントロールを実装すると、全体のスコアに大きく貢献します。Microsoft はまた、コンプライアンス スコアは運用上の進捗状況を示す指標であり、コンプライアンスの認証や法的判断ではないと明言していますが、GDPR、ISO/IEC 27001、NIST 800-53、Microsoft Data Protection Baselines などのフレームワーク全体にわたるコントロールの実装状況を追跡、優先順位付け、および実証することを可能にします。
対照的に、Microsoft Purview コンプライアンス ポータルのレポートは、レポートとインサイト (DLP、内部リスク、監査など) を提供しますが、リスク軽減の進捗状況を統一的に評価する指標は算出しません。トラスト センターは、セキュリティ、プライバシー、コンプライアンスへの取り組みに関する透明性を確保するための Microsoft の公開サイトであり、トラスト ドキュメント (監査レポート、認証、ホワイト ペーパー) は、証拠と参考資料を提供します。これらのいずれも、コンプライアンス スコアのように、製品内でポイントベースの進捗状況評価を提供するものではありません。

最新問題: **184**
以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Answer:



Explanation:



MicrosoftのハイブリッドIDに関するガイダンスでは、Microsoft Entra Connect（旧Azure AD Connect）は、オンプレミスのAD DSからMicrosoft Entraテナントに IDを同期し、ハイブリッドIDを実現するために使用されるツールであると説明されています。Microsoftによると、ハイブリッドIDは、オンプレミスのディレクトリとクラウドのディレクトリを接続することで実現され、ユーザーは単一のIDで両方の環境にアクセスできるようになります。これには2つのMicrosoft 365テナントは必要なく、オンプレミスのAD DSと統合された1つのMicrosoft Entraテナントが必要です。
認証モデル（パスワードハッシュ同期（PHS）、パススルー認証（PTA）、フェデレーション（AD FS））の場合、Microsoft は、ユーザー オブジェクトが Entra ID に存在し、一貫した ID を維持しながらクラウド サービスに対して認証できるように、ディレクトリ同期が必要であると規定しています。そのため、ハイブリッド ID の基盤となる同期を実装するために Entra Connect が使用され、2 つの M365 テナントは不要です。また、Microsoft クラウド サービス全体でハイブリッド ID を認証するには、AD DS と Entra ID 間の同期が必要です。

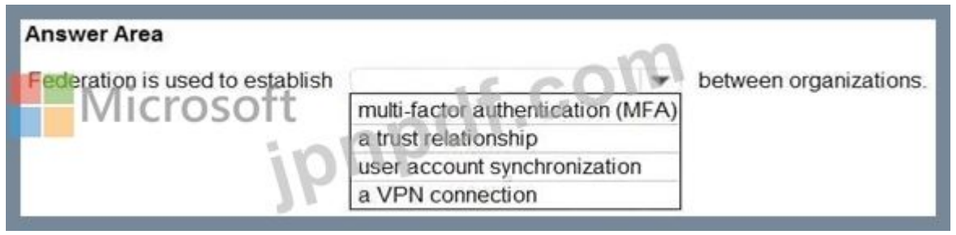
最新問題: **185**
文を正しく完成させる選択肢を選びなさい。

Answer:

参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide

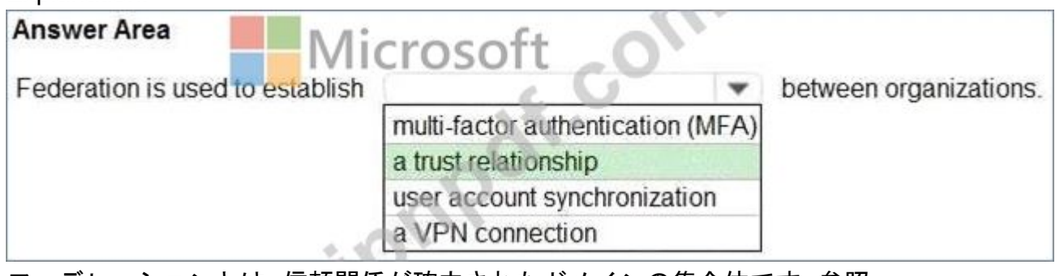
最新問題: **186**
複数のサブスクリプションにわたって一貫した方法でAzureリソースをプロビジョニングするには、どのようなツールを使用できますか？
A. Microsoft Defender for Cloud
B. アズールブループリント
C. マイクロソフトセンチネル
D. Azure Policy
Answer: (解答を表示する**)**
Azure Blueprintsを使用すると、ARM/Bicepテンプレート、ロール割り当て、Azure Policyなどの再現可能なアーティファクトセットを定義し、複数のサブスクリプションに割り当てることで、リソースとガードレールを一貫してデプロイできます。

最新問題: **187**
文を正しく完成させる選択肢を選びなさい。



Answer:

Explanation:



フェデレーションとは、信頼関係が確立されたドメインの集合体です。参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

最新問題: **188**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

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.	○	○

ボックス1 :いいえ
ボックス2 :はい
認証情報漏洩とは、ユーザーの有効な認証情報が漏洩したことを示します。
ボックス3 :はい
多要素認証は、ユーザーのリスクなど、いくつかの条件に基づいて必要となる場合があります。

最新問題**: 189**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

参照：

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

最新問題: **190**

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 security center, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 security center gives you points if you address the improvement action by using a third-party application or software.	○	○

Answer:

最新問題: **191**

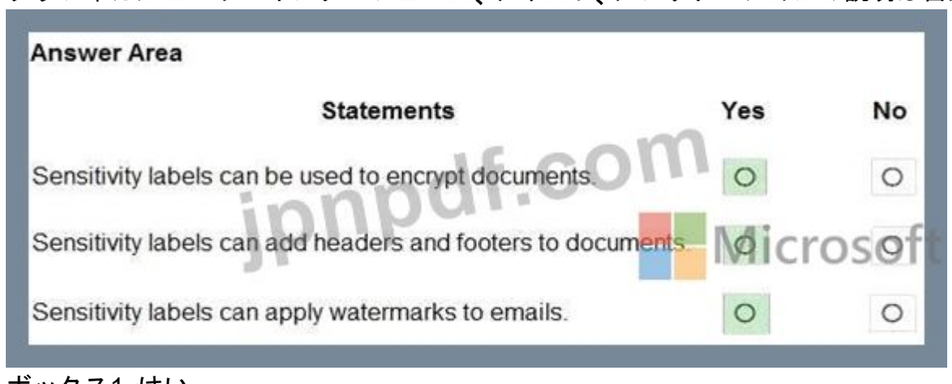
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer:

説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます



ボックス1 :はい

機密ラベルを使用すると、メールやドキュメントの暗号化などの保護設定を提供して、権限のない人がデータにアクセスするのを防ぐことができます。
ボックス2 :はい
Office アプリを使用する際に、機密ラベルを使用してコンテンツにマークを付けることができます。ラベルが適用されたドキュメントに、透かし、ヘッダー、またはフッターを追加することで、機密性を確認できます。
ボックス3 :はい
Office アプリを使用する際に、機密ラベルを使用してコンテンツにマークを付けることができます。ラベルが適用されたメールのヘッダーやフッターを追加することで、機密性を示すことができます。

最新問題**: 192**
マイクロソフトのどのポータルサイトで、マイクロソフトのクラウドサービスが国際標準化機構（ISO）などの規制基準にどのように準拠しているかについての情報が得られますか？
A. Microsoft Endpoint Manager 管理センター
B. Azure コスト管理 + 課金
C. マイクロソフト サービス トラスト ポータル
D. Azure Active Directory 管理センター
Answer: C (メーッセージを残す**)**
セクション :セキュリティ、コンプライアンス、およびアイデンティティの概念を説明する
Explanation:
Microsoft Service Trust Portalには、Microsoftがクラウドサービスおよびそこに保存されている顧客データを保護するために実施している管理策とプロセスに関する詳細情報が掲載されています。
参照：
https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

最新問題**: 193**
Azure Active Directory (Azure AD) のどの機能を使用して、Azure リソースを管理するためのジャストインタイム (JIT) アクセスを提供できますか？
A. 条件付きアクセスポリシー
B. Azure AD ID保護
C. Azure AD 特権ID管理 (PIM)
D. 認証方法ポリシー
Answer: (解答を表示する**)**
説明
Azure AD Privileged Identity Management (PIM) は、Azure AD および Azure リソースへのジャストインタイムの特権アクセスを提供します。

最新問題**: 194**
文を正しく完成させる選択肢を選びなさい。

Answer:

Answer Area

参照：
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/

最新問題: **195**
以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Answer:

最新問題: **196**
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

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.	○	○

Answer:

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.	○	○

参照：

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

最新問題: **197**

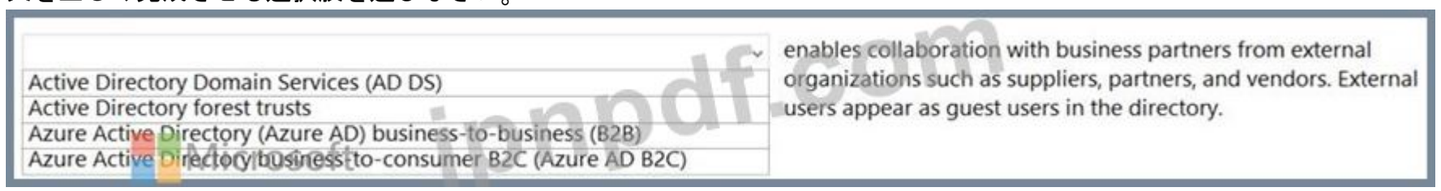
以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

Statements	Yes	No
Conditional Access is implemented by using policies in Microsoft Entra ID.	○	○
A Conditional Access policy can block or allow Microsoft Entra ID connections based upon the specific platform of a user's device.	○	○
A Conditional Access policy can be applied to a Microsoft 365 group.	○	○

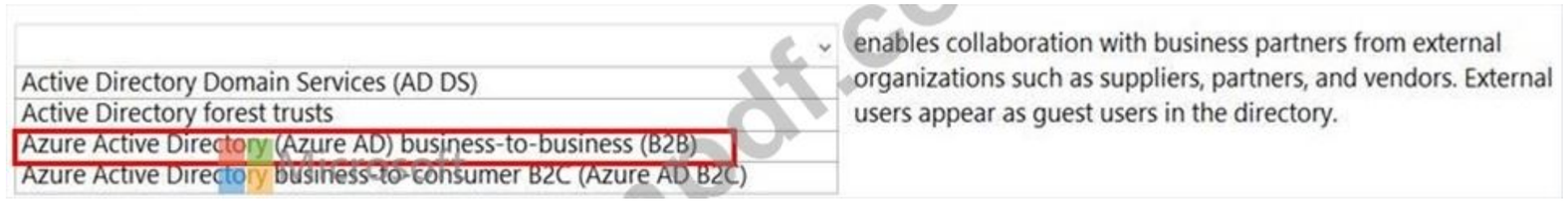
Answer:

最新問題**: 198**

文を正しく完成させる選択肢を選びなさい。



Answer:

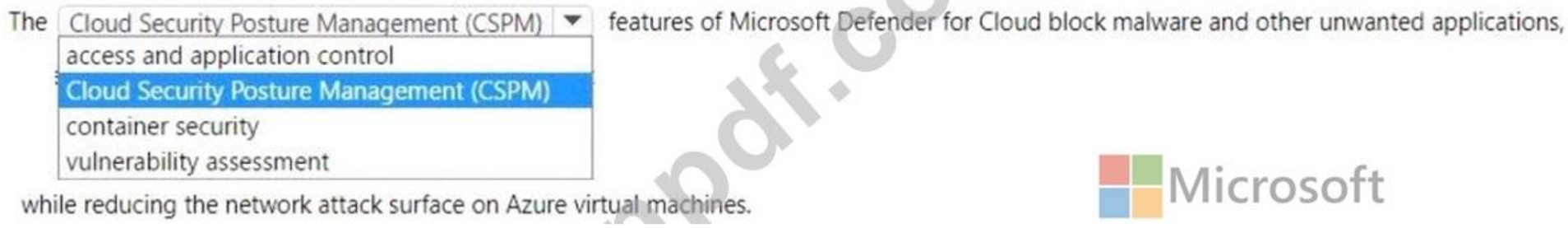


参照：

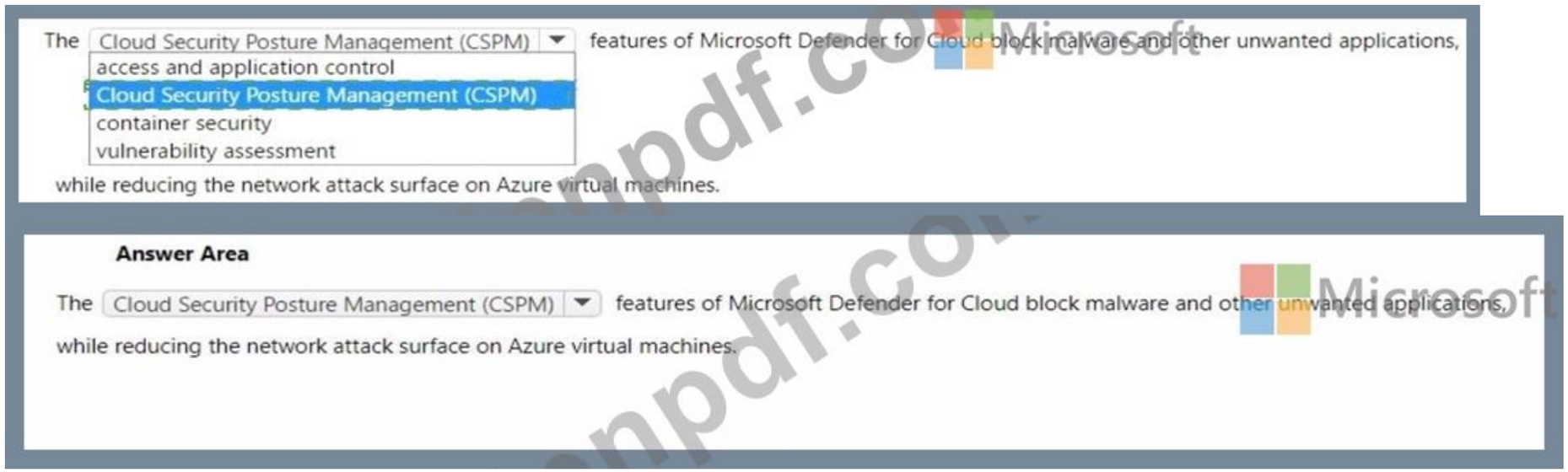
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

最新問題**: 199**

文を正しく完成させる選択肢を選びなさい。

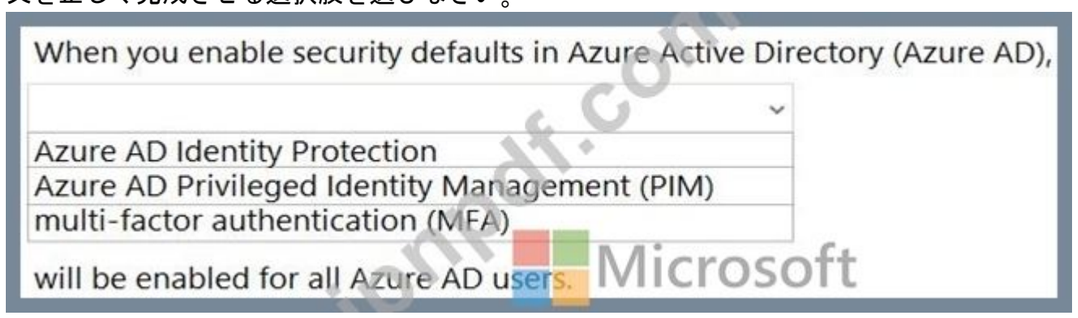


Answer:

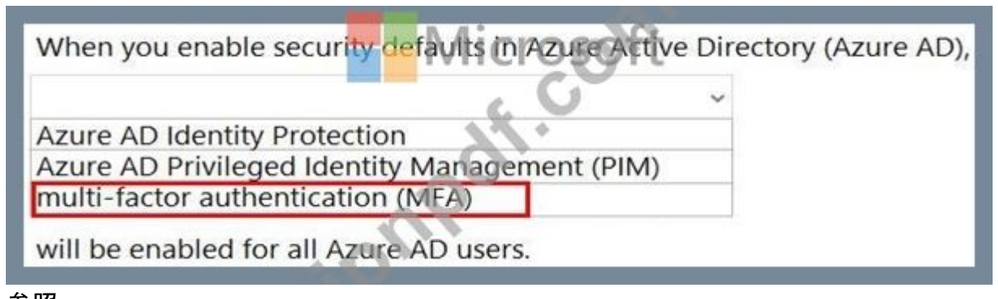


最新問題: **200**

文を正しく完成させる選択肢を選びなさい。



Answer:



参照：

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

最新問題: **201**

以下の各設問について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。注：正解ごとに1点が加算されます。

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.	○	○

Answer:

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.	○	○

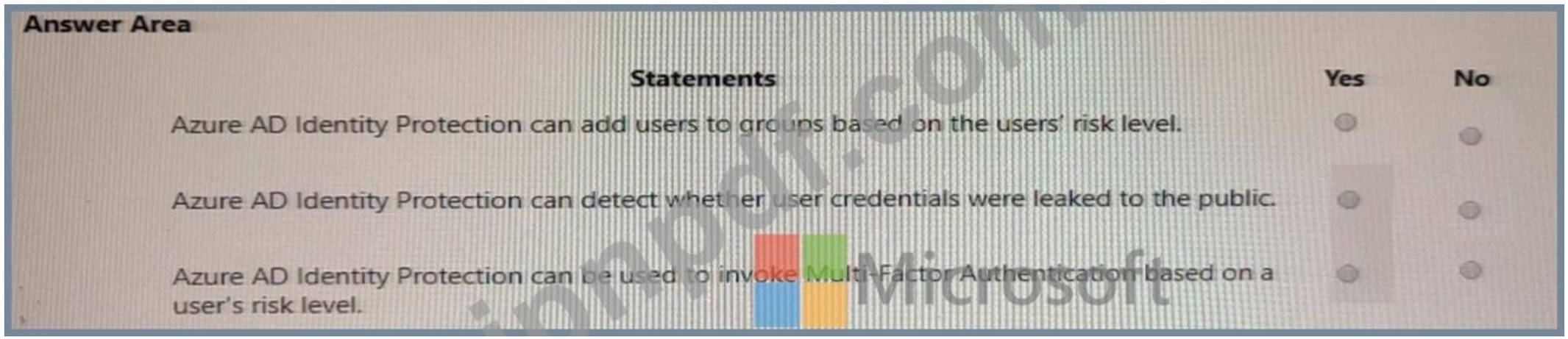
Answer Area

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.	●	○

最新問題: 202

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

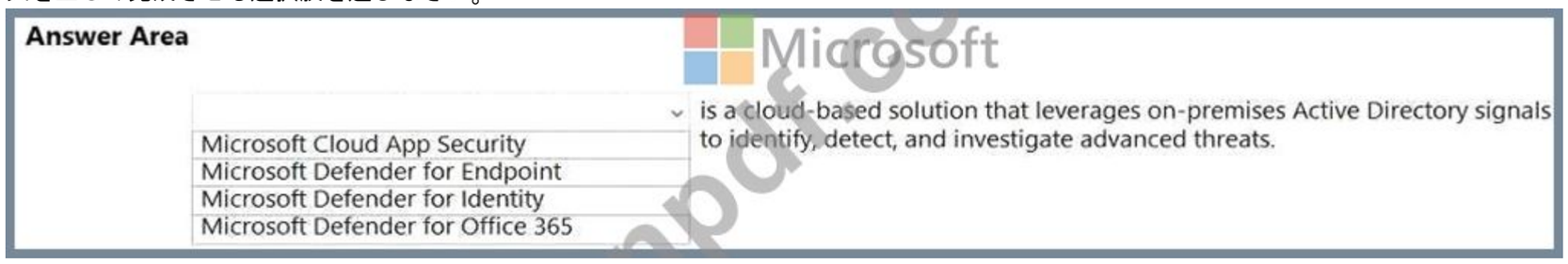
注：正解ごとに1ポイントが加算されます。



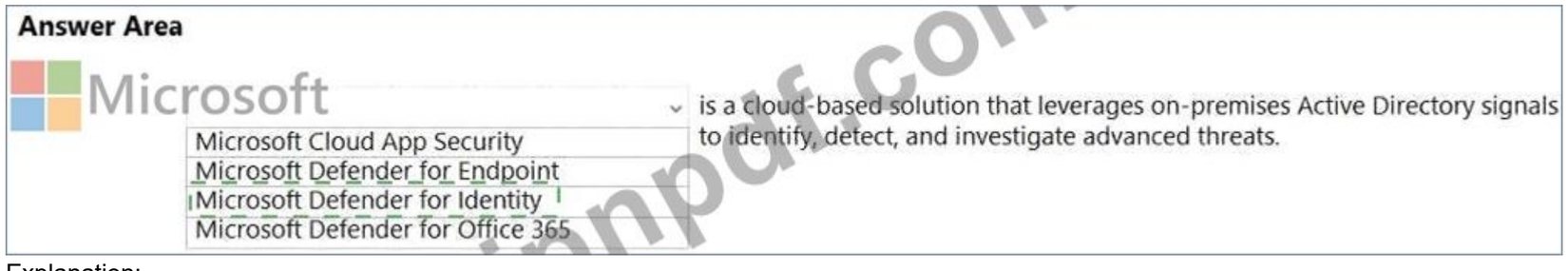
Answer:

最新問題**: 203**

文を正しく完成させる選択肢を選びなさい。



Answer:



Explanation:

グラフィカルユーザーインターフェース、テキスト説明は中程度の信頼度で自動生成されます

最新問題: **204**
文を正しく完成させる選択肢を選びなさい。

Answer:

Explanation:

Microsoft 365 セキュリティ センター (現在は Microsoft 365 Defender) では、インシデントを使用してテナント全体の脅威をトリアージおよび調査します。Microsoft のセキュリティ ドキュメントでは、「インシデントとは、関連するアラートの集合」であり、アナリストが攻撃の全体像をエンドツーエンドで把握できるように自動的に関連付けられると説明しています。各インシデント内では、ポータルにデバイス、ユーザー、メールボックス、アプリケーションなどの影響を受ける資産が表示され、対応担当者は特定のアラートによって影響を受けるエンドポイントを迅速に特定し、対応アクション (デバイスの隔離、調査パッケージの収集、ウイルス対策スキャンの実行など) を実行できます。この設計により、セキュリティ チームは個々のアラートにとどまらず、インシデントの [証拠と対応/資産] セクションに影響を受けるデバイスを一覧表示し、アラートのタイムラインとデバイスの詳細を含む統合調査に取り組むことができます。
これに対し、セキュアスコアは組織のセキュリティ体制と推奨事項を測定するものであり、ポリシーは構成/適用対象（Defenderポリシーやコンプライアンスポリシーなど）であり、アラートの調査ビューではありません。分類はアラートの調査ではなく、情報保護のラベル付けに関するものです。したがって、アラートの影響を受けるデバイスを特定するには、Microsoft 365 Defenderのインシデント機能を使用します。この機能では、関連するアラートとともに、脅威に関連するエンティティや証拠とともに、関係するデバイスが表示されます。
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

最新問題: **205**
文を正しく完成させる選択肢を選びなさい。

Answer:

参照：

https://docs.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide MIP 機能は Microsoft 365 コンプライアンスに含まれており、データの把握、データの保護、データ損失の防止のためのツールを提供します。

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