

Microsoft.SC-900J.v2026-09-04.q99

試験コード :

SC-900J

試験名称 :

Microsoft Security, Compliance, and Identity Fundamentals (SC-900日本語版)

認証ベンダー :

Microsoft

無料問題の数 :

99

バージョン :

v2026-09-04

ページの閲覧量 :

102

問題集の閲覧量 :

1015

<https://www.jpnsshiken.com/shiken/Microsoft.SC-900J.v2026-09-04.q99.html>

質問: 1

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
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.	☐	☐

正解:

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.	☐	☒

Explanation:

Yes

NO

NO

YES - As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

NO - The most restrictive lock in the inheritance takes precedence.

NO - If you delete a resource group with a locked resource, the portal UI will give you an error and no resources are deleted.

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?tabs=json>

質問: 2

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

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

正解: [\(正解を表示します\)](#)

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

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

質問: 3

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どれですか？

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

正解: **B** ([コメントを发表する](#))

Microsoft places Attack simulation training under the email and collaboration protection workloads of Microsoft Defender for Office 365 (MDO). The official product guidance describes it as a built-in capability that "lets you run realistic attack scenarios in your organization to identify vulnerable users and train users to recognize and report phishing and other social-engineering techniques." Microsoft further notes that Attack simulation training "provides editable phishing payloads, credential-harvesting and attachment scenarios, landing pages, user training, and detailed reporting," enabling security teams to measure compromise rates and improve user resilience over time. The service scope is explicit: "Attack simulation training is a feature of Microsoft Defender for Office 365 Plan 2," and it is included in suites that contain MDO P2 such as Microsoft

365 E5 and Office 365 E5. In the Microsoft 365 Defender portal, you access it under Email & collaboration # Attack simulation training, where admins can create simulations, target groups, assign training, and review metrics like repeat offenders, resilience score, and simulation results. By design, this feature is not part of Microsoft Defender for Cloud Apps (cloud app security and CASB functions), not part of Microsoft Defender for Identity (on-prem AD identity threat detection), and not part of Defender for SQL. Therefore, the Microsoft SCI documentation aligns that the correct service hosting Attack simulation training is Microsoft Defender for Office 365 (Plan 2).

質問: 4

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

注：正しい選択はそれぞれ1ポイントの価値があります。

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

正解:

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

Explanation:

Answer Area

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

Microsoft states that Microsoft Sentinel includes connectors for both Microsoft and non-Microsoft sources.

The product overview explains that Sentinel "comes with built-in connectors" for services such as Microsoft

365, Defender, and Azure sources, and also built-in connectors for non-Microsoft solutions like firewalls and other security products. Therefore, the claim that data connectors support only Microsoft services is false.

For visualization and monitoring, the documentation clarifies that "Microsoft Sentinel uses Azure Monitor workbooks to provide rich visualizations of your data."

Workbooks are the native dashboarding framework in Sentinel and can be customized to monitor logs, incidents, and telemetry that Sentinel ingests. Hence, using Azure Monitor Workbooks to monitor data collected by Sentinel is true.

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

質問: 5

お客様は、VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションをお持ちです。VNet1 には、複数のサブネットと仮想マシンが含まれています。

VNet1にFW1という名前のAzureファイアウォールをデプロイします。
FW1がVNet1との間のすべてのインターネットトラフィックを分析およびフィルタリングできることを確認する必要があります。ソリューションはコストを最小限に抑える必要があります。
あなたはすべきでしょうか？
A. サービスエンドポイントを作成します。
B. Azure Route Server を実装します。
C. ルートテーブルを作成して関連付けます。
D. ネットワークピアリングを設定します。
正解: (正解を表示します)

質問: 6
Microsoft Defender forOffice365の機能を正しい説明と一致させてください。
答えるには、適切な機能を左側の列から右側の説明にドラッグします。各機能は、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 :それぞれの正しい一致は1ポイントの価値があります。

Features

Threat Explorer

Threat Trackers

Anti-phishing protection

Answer Area

Feature Provides intelligence on prevailing cybersecurity issues

Feature Provides real-time reports to identify and analyze recent threats

Feature Detects impersonation attempts

Features

Threat Explorer

Threat Trackers

Anti-phishing protection

Answer Area

Anti-phishing protection Provides intelligence on prevailing cybersecurity issues

Threat Explorer Provides real-time reports to identify and analyze recent threats

Threat Trackers Detects impersonation attempts

Explanation:

Anti-phishing protection

Provides intelligence on prevailing cybersecurity issues

Threat Explorer

Provides real-time reports to identify and analyze recent threats

Threat Trackers

Detects impersonation attempts

In Microsoft Defender for Office 365, Threat Trackers (also known as threat analytics in the security portal) surface curated intelligence on prevailing and emerging cyberthreats, giving security teams insight into current campaigns, affected regions, and recommended actions. Threat Explorer (Explorer/Real-time detections) is the investigation workspace that provides near real-time visibility into detected phishing, malware, and other malicious email content, allowing analysts to identify, filter,

and analyze recent threats and take remediation actions (e.g., purge messages). Anti-phishing protection is configured via anti-phishing policies and uses machine learning and impersonation settings (user and domain impersonation) to detect and block impersonation attempts and other phishing techniques in Exchange Online. Together, these capabilities map directly to the statements: Trackers = intelligence on active threats, Explorer = real-time analysis and reporting, and Anti-phishing = detection of impersonation.

質問: 7

Microsoft 365の機密ラベルで何を指定できますか？

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

正解: [\(正解を表示します\)](#)

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

質問: 8

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

- A. Microsoft Defender for Identity
- B. Microsoft Defender for IoT
- C. Microsoft Defender for Office 365
- D. Microsoft Defender for Endpoint

正解: [\(正解を表示します\)](#)

質問: 9

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Microsoft

Statements

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

正解:

Answer Area

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

Microsoft states that Identity Protection is used to "detect potential vulnerabilities affecting your organization's identities, configure automated responses, and investigate suspicious actions related to your organization's identities." It evaluates user risk and sign-in risk using detections such as "leaked credentials, anonymous IP address, unfamiliar sign-in properties, [and] impossible travel." These built-in detections confirm that the service can detect whether valid user credentials have been found in public or criminal datasets-commonly referred to as leaked credentials-thereby reducing identity compromise risk.

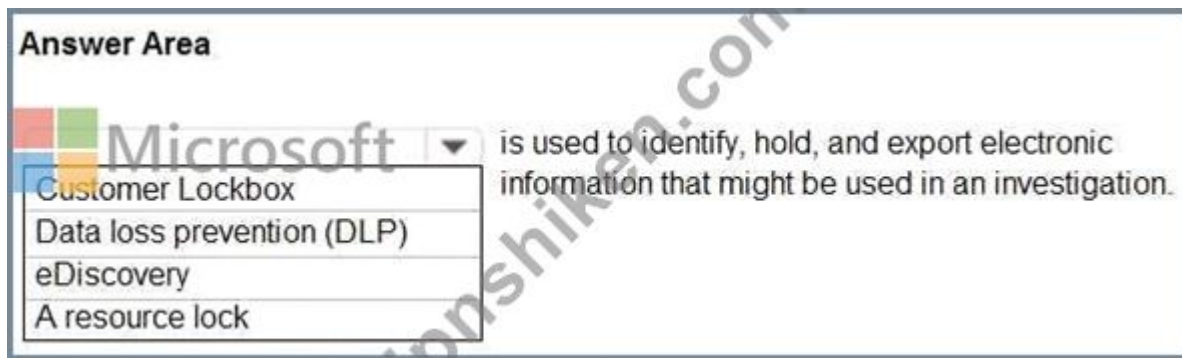
Identity Protection includes policy controls that "automate the response to detected risks," specifically the User risk policy and Sign-in risk policy. Microsoft describes that these policies can "require password change when user risk is detected" and "require multi-factor authentication when sign-in risk is detected." Therefore, Identity Protection can invoke MFA based on risk as part of Conditional Access-backed risk policies.

However, Identity Protection does not perform group lifecycle management. Microsoft positions group membership automation under Azure AD dynamic groups/Identity Governance, not Identity Protection.

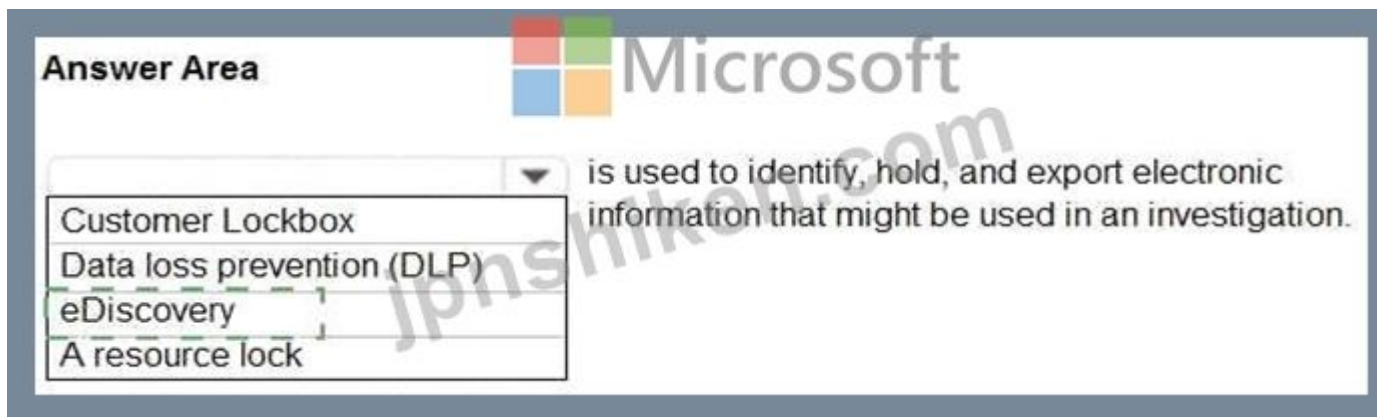
Consequently, adding users to groups based on risk level is not a function of Identity Protection, which focuses on detection, risk evaluation, and policy-driven remediation (e.g., MFA or password reset), not group assignment.

質問: 10

文を正しく完成させる答えを選択してください。



正解:



Explanation:

eDiscovery

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

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

質問: 11

アプリケーションをActiveDirectory (Azure AD)に登録すると、どのタイプのIDが作成されますか？

- A. ユーザーアカウント
- B. ユーザーが割り当てた管理対象ID
- C. システムによって割り当てられた管理対象ID
- D. サービスプリンシパル

正解: ([正解を表示します](#))

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant.

Reference:

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

質問: 12

Microsoft Defender for Cloud の無料モードで利用できるセキュリティ機能はどれですか？

- A. 仮想マシンの脆弱性スキャン
- B. セキュアスコア
- C. Azure 仮想マシンへのジャストインタイム (JIT) VM アクセス
- D. 脅威保護アラート

正解: [\(正解を表示します\)](#)

In Microsoft Defender for Cloud, the Free plan provides continuous security assessment and visibility into your posture via Secure Score and security recommendations. Microsoft explains that the free tier offers

"foundational CSPM capabilities," including recommendations and a security score (Secure score) to help you prioritize hardening tasks. Advanced features-such as vulnerability scanning for VMs (Qualys-based), Just- In-Time (JIT) VM access, and threat protection alerts-require the enhanced/paid Defender plans (for example, Defender for Servers). Consequently, among the listed options, only Secure score is available in the free mode. This score aggregates the effect of recommendations across subscriptions and resources so you can track and improve security posture without enabling any of the paid Defender plans.

質問: 13

Azure SQL Managed Instance の脅威検出を提供するには何を使用できますか？

- A. Microsoft セキュア スコア
- B. アプリケーションセキュリティグループ
- C. クラウド用 Microsoft ディフェンダー
- D. アズールバスティオン

正解: C ([コメントを发表する](#))

For Azure data services such as Azure SQL Managed Instance, Microsoft provides threat detection and protection through Microsoft Defender for Cloud (via Microsoft Defender for SQL). Microsoft documentation states that Defender for Cloud "provides advanced threat protection for your SQL resources," including Azure SQL Database and Azure SQL Managed Instance, by "continuously monitoring for anomalous activities and potential SQL injection, brute force, and exploitation attempts." When enabled, the plan "generates security alerts when suspicious activities are detected," and these alerts can be surfaced in Defender for Cloud, forwarded to Microsoft Sentinel, or integrated with workflows for response. Microsoft Secure Score is a security posture metric, application security groups are for network segmentation in Azure, and Azure Bastion provides secure RDP/SSH over TLS-none of these deliver database-specific threat detection. Therefore, to provide threat detection for Azure SQL Managed Instance, you use Microsoft Defender for Cloud (Defender for SQL).

質問: 14

Microsoft Purviewの機密情報分類器は、どのような種類のファイルの分類に使用できますか？

- A. 文書
- B. 動画ファイル
- C. 画像
- D. 音声ファイル

正解: [\(正解を表示します\)](#)

質問: 15

文を正しく完成させる答えを選択してください。

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.

正解:

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.

Explanation:

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.

Microsoft states that Security defaults are baseline protections in Azure Active Directory (now Microsoft Entra ID) that "make it easier to help protect your organization from identity-related attacks." One of the core behaviors is that security defaults "require all users to register for Azure AD Multi-Factor Authentication," and enforce "multi-factor authentication for all users," with special emphasis that "administrators are required to do multi-factor authentication." Security defaults also "block legacy authentication" and add protections for privileged operations, but the universal control that applies to every user is MFA. Importantly, enabling security defaults does not turn on paid capabilities such as Azure AD Identity Protection or Privileged Identity Management (PIM); those are separate, premium features. The baseline is intentionally simple and tenant-wide: require MFA registration, challenge with MFA when risk or sensitive operations are detected, and reduce exposure by disabling legacy protocols. Therefore, when you enable security defaults, multi-factor authentication (MFA) will be enabled for all Azure AD users, aligning with Microsoft's guidance that security defaults "help protect all organizations by requiring MFA and disabling legacy authentication."

質問: 16

貴社では、セキュリティ情報・イベント管理(SIEM)ソリューションを含む様々なセキュリティ製品を評価中です。SIEMソリューションの機能に関する情報をご提供いただく必要があります。SIEMソリューションの機能とは何でしょうか？

A. 自動化されたインシデント修復

B. ネットワークアクティビティを確認し、どのアプリケーションとサービスが通信できるかに関するレポートを提供する機能

- C. 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
 - D. ユーザーが Azure の支出制限に達したときにアラートをトリガーするアラート システム
- 正解: (正解を表示します)

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

質問: 17
次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

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

正解:

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:

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

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

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

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

質問: 18

ステートメントが真実であれば、はい。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☐
Conditional access policies can be used to block access to an application based on the location of the user.	☐	☐
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	☐	☐

正解:

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☒
Conditional access policies can be used to block access to an application based on the location of the user.	☒	☐
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	☐	☒

Explanation:

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☒
Conditional access policies can be used to block access to an application based on the location of the user.	☒	☐
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	☐	☒

Microsoft Entra Conditional Access evaluates signals to make real-time access decisions. Microsoft describes it as bringing "signals together to make decisions and enforce organizational policies," where administrators choose controls such as Block access, Require multi-factor authentication, Require device to be marked as compliant, or Require hybrid Azure AD joined device. Because MFA is only one of several grant controls, it is incorrect that policies always enforce MFA; they can also simply block, allow, or require other conditions.

Location is a first-class condition. Microsoft states you can define named locations (by countries/regions or IP ranges) and then use them in policy conditions to block or grant access. A common scenario is "Block access from specific locations" or require additional controls when a sign-in originates from an untrusted network. Therefore, Conditional Access can block access to an application based on user location.

Finally, Conditional Access targets users, groups, workload identities, and cloud apps regardless of device join state. Device-related conditions and filters are optional; policies are not limited to "Azure AD-joined devices." Controls like Require device to be marked as compliant or Require Hybrid Azure AD joined device are only enforced if configured. Hence, Conditional Access does not only affect users on Azure AD-joined devices.

質問: 19

Microsoftクラウドサービスが国際標準化機構 (ISO)などの規制標準にどのように準拠しているかに関する情報を提供するMicrosoftポータルはどれですか？

- A. Microsoft EndpointManager管理センター
- B. Azureコスト管理+請求
- C. Microsoft Service Trust Portal
- D. Azure ActiveDirectory管理センター

正解: ([正解を表示します](#))

The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide>

質問: 20

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

Microsoft Sentinel をオンボードする必要があります。

最初に何をすべきですか？

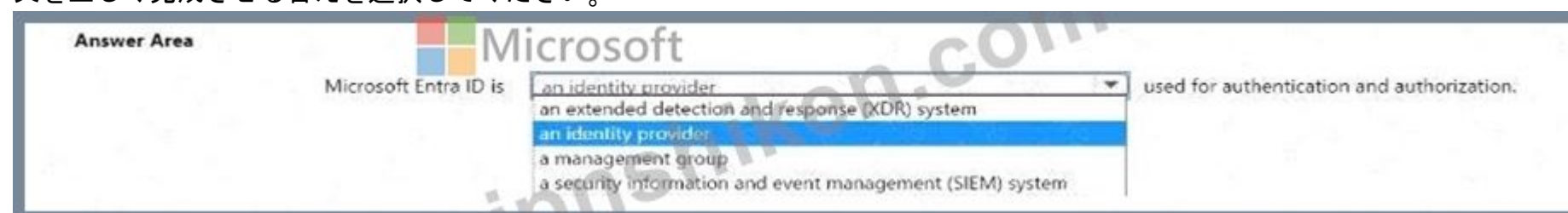
- A. ハンティング クエリを作成します。
- B. アラートをインシデントに関連付けます。
- C. セキュリティ ソースに接続します。
- D. カスタム検出ルールを作成します。

正解: ([正解を表示します](#))

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

質問: 21

文を正しく完成させる答えを選択してください。



正解:



Explanation:



Microsoft defines Microsoft Entra ID (formerly Azure Active Directory) as "a cloud-based identity and access management (IAM) service" that "helps your employees sign in and access resources." In SCI learning paths, Entra ID is positioned as the tenant's identity provider (IdP) that authenticates users and issues tokens for applications using standards such as OpenID Connect, OAuth 2.0, and SAML, which applications then use to authorize access based on roles/claims. Microsoft further explains that Entra ID provides single sign-on, Conditional Access, MFA, and token-based authorization-all core IdP capabilities that govern who can access what across Microsoft 365, Azure, and thousands of SaaS apps.

By contrast, an extended detection and response (XDR) system refers to Microsoft Defender XDR, which focuses on incident detection, correlation, and response-not identity provisioning or token issuance. A security information and event management (SIEM) system refers to Microsoft Sentinel, which aggregates and analyzes logs and alerts-not primary authentication. An Azure management group is a governance scope used to organize subscriptions and apply policy/RBAC at scale; it is not an authentication/authorization service. Therefore, within Microsoft's SCI scope, Microsoft Entra ID is an identity provider used to perform authentication (verifying identity and issuing tokens) and to enable authorization in applications and resources that consume those tokens.

質問: 22

コンプライアスマネージャーの評価とは何ですか？

- A. 特定の規制、標準、またはポリシーからのコントロールのグループ。
- B. 組織が企業標準に準拠するのに役立つ推奨ガイダンス。

- C. 会社の文書で許可されていない単語の辞書。
- D. 複数のポリシーを含むポリシーイニシアチブ。

正解: ([正解を表示します](#))

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

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

Compliance Manager helps simplify compliance and reduce risk by providing:

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

質問: 23

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

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

正解: ([正解を表示します](#))

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

"Each recommendation contributes to the secure score. Completing remediation steps increases the score and reduces risk." This single percentage view lets security teams quickly gauge how well current configurations and protections align with Microsoft's security best practices and regulatory mappings. Other elements surfaced in Defender for Cloud-like "resource health," "status of recommendations," or "completed controls" -are components and statuses that feed into or relate to the scoring model, but the overall subscription security health indicator presented and tracked over time is secure score.

質問: 24

ユーザーがサイトからファイルを削除した場合でも、MicrosoftSharePointサイト内のすべてのファイルのコピーを1年間保持する必要があります。サイトに何を適用する必要がありますか？

- A. データ損失防止 (DLP) ポリシー
- B. 保持ポリシー
- C. インサイダーリスクポリシー
- D. 機密ラベルポリシー

正解: ([正解を表示します](#))

In Microsoft Purview (Microsoft 365 compliance), a retention policy applied to a SharePoint site keeps content for the specified period (e.g., 1 year) even if users delete it. Items are retained and recoverable until the retention period expires, meeting your preservation requirement.

質問: 25

Microsoft Entra IDガバナンスには、どの機能が含まれていますか？

- A. 特権ID管理
- B. 個人情報保護
- C. 権限管理
- D. 検証可能な資格情報

正解: ([正解を表示します](#))

質問: 26

文を正しく完成させる答えを選択してください。



正解:



Explanation:

authorization

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

From Microsoft SCI training materials:

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

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

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

SCI documentation explains:

"Once authentication is successful, authorization policies are applied to determine whether the authenticated user is allowed to access the requested resource and at what level." This principle is implemented using role-based access control (RBAC) in Microsoft Azure and Microsoft 365 environments. For example, even if a user

successfully logs into the Microsoft 365 portal (authentication), their ability to manage Exchange Online settings or view compliance data depends on their assigned roles (authorization).

質問: 27

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

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

正解: ([正解を表示します](#))

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

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

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

質問: 28

ユーザー認証の方法として電子メールをサポートする機能は何ですか？

- A. Microsoft Entra ID 保護
- 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

正解: ([正解を表示します](#))

In Microsoft Entra ID (formerly Azure AD), self-service password reset (SSPR) is the feature that explicitly supports email as an authentication method when users need to verify their identity to reset or unlock their password.

According to Microsoft's identity and access documentation and the SCI learning content, SSPR lets administrators choose which verification methods are available to users, such as mobile phone, office phone, mobile app, security questions, and email. When email is enabled, a verification code can be sent to a registered alternate email address. The user proves their identity by entering this code, which is treated as an authentication step in the SSPR process.

By contrast:

Microsoft Entra Multi-Factor Authentication (MFA) does not support email as an MFA method; it focuses on methods like authenticator apps, phone calls, and text messages.

Microsoft Entra ID Protection detects and responds to risky sign-ins and users but does not provide email-based authentication.

Microsoft Entra Password Protection deals with banned and compromised passwords, not with email verification.

Therefore, the only option in the list that uses email as a supported authentication method is self-service password reset (SSPR).

質問: 29

文を正しく完成させる答えを選択してください。

Answer Area

▼

Archiving

Compressing

Deduplicating

Encrypting

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



正解:

Answer Area

▼

Archiving

Compressing

Deduplicating

Encrypting

Explanation:

Answer Area

▼

Archiving

Compressing

Deduplicating

Encrypting

In Microsoft's Security, Compliance, and Identity guidance, encryption is described as the control that "converts data into a form that cannot be understood by anyone who does not possess the appropriate decryption key." In the Microsoft Purview Information Protection (sensitivity labels with encryption) documentation, Microsoft explains that when encryption is applied to a file, "only authorized users and services that present the correct keys and usage rights can open and use the content," and that access is enforced even if the file is moved outside the organization. Azure Rights Management (part of Microsoft Purview) further states that encryption "protects data at rest and in transit by using keys so that only permitted identities can decrypt and use the information." This aligns precisely with the sentence: encrypting a file makes the data readable and usable to viewers that have the appropriate key (and unreadable to those who do not). By contrast, archiving organizes or preserves data for long-term storage; compressing reduces file size without controlling access; and deduplicating removes redundant copies to save space. None of these provide the key-based, identity-bound access control described in Microsoft SCl materials. Therefore, the correct completion is Encrypting.

質問: 30

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Microsoft

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☐
Conditional access policies can be used to block access to an application based on the location of the user.	☐	☐
Conditional access policies only affect users who have Microsoft Entra joined devices.	☐	☐

正解:

Answer Area

Microsoft

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☒
Conditional access policies can be used to block access to an application based on the location of the user.	☒	☐
Conditional access policies only affect users who have Microsoft Entra joined devices.	☐	☒

Explanation:

Answer Area

Microsoft

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	☐	☒
Conditional access policies can be used to block access to an application based on the location of the user.	☒	☐
Conditional access policies only affect users who have Microsoft Entra joined devices.	☐	☒

Conditional access policies always enforce MFA = No
Microsoft Entra Conditional Access policies are flexible and do not always require MFA. MFA is one possible control, but policies can enforce other access controls such as requiring a compliant device, blocking access entirely, requiring Terms of Use acceptance, or enforcing session controls.

SCI Extract: "Conditional Access is the tool used by Azure AD to bring signals together, to make decisions, and enforce organizational policies. These policies can require MFA, but it is not mandatory for all policies." Block access based on location = Yes
Conditional Access supports location-based conditions using named locations (such as country or IP ranges). Policies can block or allow access based on where the user is signing in from.

SCI Extract: "Administrators can use Conditional Access policies to block or grant access based on user location, using named locations to define trusted or risky areas." Only affects Entra joined devices = No
Conditional Access applies to all users and devices, including:

Entra-joined,

Hybrid Entra-joined,

Registered devices (via Microsoft Intune or Azure AD),

And even unmanaged (BYOD) devices depending on configuration.

SCI Extract: "Conditional Access policies apply to all users and devices based on selected conditions, not only Microsoft Entra joined devices."

質問: 31

リソースをクラウドに移動する予定です。

サービスとしてのインフラストラクチャ (IaaS) の使用を評価している、

サービスとしてのプラットフォーム (PaaS) およびサービスとしてのソフトウェア (SaaS) クラウド モデル。

クラウドベースのアプリのデータ、ユーザー アカウント、およびユーザー デバイスのみを管理する予定です。

どのクラウド モデルを使用しますか？

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

正解: [\(正解を表示します\)](#)

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

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

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

質問: 32

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area	Statements	Yes	No
	All Azure Active Directory (Azure AD) license editions include the same features.	☐	☐
	You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	☐	☐
	You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	☐	☐

正解:

Answer Area		Statements	Yes	No
		All Azure Active Directory (Azure AD) license editions include the same features.	☐	☒
		You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	☒	☐
		You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	☐	☒

Explanation:

Answer Area

		Statements	Yes	No
		All Azure Active Directory (Azure AD) license editions include the same features.	☐	☒
		You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	☒	☐
		You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	☐	☒

Microsoft Learn explains that Azure Active Directory (now Microsoft Entra ID) is a Microsoft-managed identity and access management service delivered from the cloud. It does not require you to provision or host infrastructure such as virtual machines; the directory is operated as a service by Microsoft, and tenants are created and administered within Microsoft's cloud environment. The official learning paths further clarify that administration is performed through the Azure portal (the Entra/Microsoft Entra admin center and Azure portal blades), PowerShell, and Graph-so managing a tenant in the Azure portal is fully supported. Regarding licensing, Microsoft's SCI study materials detail that Azure AD/Entra ID is offered in multiple editions (Free, Microsoft 365 apps edition, Premium P1, and Premium P2). Each edition unlocks different capabilities: for example, features like Conditional Access are in Premium tiers; Identity Protection and Privileged Identity Management (PIM) are P2 capabilities. Because capabilities vary by tier, the statement that all license editions include the same features is incorrect. Putting this together: feature parity across editions is not the case (No); tenant management in the Azure portal is supported (Yes); and you do not need to deploy Azure VMs to host an Azure AD/Entra ID tenant (No).

質問: 33

文を正しく完成させる答えを選択してください。

Answer Area



can use conditional access policies to control sessions in real time.

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
Azure Defender
Azure Sentinel
Microsoft Cloud App Security

正解:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Azure Defender

Azure Sentinel

Microsoft Cloud App Security

Microsoft

can use conditional access policies to control sessions in real time.

Explanation:

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Azure Defender

Azure Sentinel

Microsoft Cloud App Security

Microsoft

can use conditional access policies to control sessions in real time.

In Microsoft's Security, Compliance, and Identity guidance, Microsoft Cloud App Security (now Microsoft Defender for Cloud Apps) integrates with Azure AD Conditional Access to provide Conditional Access App Control. This capability enables organizations to "monitor and control user sessions in real time" by routing traffic through a reverse proxy once a Conditional Access policy is triggered. With session controls, admins can enforce actions such as block, allow with inspection, apply download restrictions, require label application, or limit access to web apps based on context (user, device state, location, risk). SCI learning paths describe that Defender for Cloud Apps works with Conditional Access policies to provide session-based conditional access that "protects data in real time," giving granular control after authentication while a session is active.

By comparison, Azure AD Privileged Identity Management (PIM) focuses on just-in-time elevation and governance of privileged roles, not real-time in-app session control. Azure Defender (Defender for Cloud) provides cloud workload protection and posture management, not Conditional Access session enforcement. Azure Sentinel (Microsoft Sentinel) is a SIEM/SOAR platform for analytics, hunting, and automation and does not apply Conditional Access session policies. Therefore, the Microsoft product that uses Conditional Access policies to control sessions in real time is Microsoft Cloud App Security (Defender for Cloud Apps).

質問: 34

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

Answer Area

Statements

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

Yes

No

☐

☐

☐

☐

☐

☐

正解:

Answer Area

Statements

GitHub is a cloud-based identity provider.

Yes

No

☒☐

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

GitHub is a cloud-based identity provider.

Yes

No

☒☐

Federation provides single sign-on (SSO) with multiple identity providers.

☒☐

A central identity provider manages all modern authentication services, such as authentication, authorization, and auditing.

☐☒

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

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

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

質問: 35

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area			
Statements		Yes	No
Microsoft Entra 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.		☐	☐

正解:

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.		☒	☐

Explanation:

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.		☒	☐

Microsoft Entra ID Protection is designed to detect and respond to identity compromise by calculating user risk and sign-in risk and surfacing risk detections such as "leaked credentials," "anonymous IP address," "impossible travel," and related signals. Microsoft explains that Identity Protection "uses adaptive machine learning and threat intelligence to detect risky users and risky sign-ins and assigns each a risk level of Low, Medium, or High." These detections include "Leaked credentials (found on public or dark-web lists)", confirming that Identity Protection can detect when user credentials have been exposed.

ID Protection is integrated with Conditional Access to take policy-driven actions: "Risk-based Conditional Access policies let you require multi-factor authentication (MFA), block access, or require password change when a user or sign-in risk level is met." The built-in policies include User risk policy and Sign-in risk policy, which can automatically enforce MFA or password reset when the configured risk threshold is reached.

However, Identity Protection does not manage Azure AD group membership. There is no capability to add users to groups based on risk level; group membership changes are outside the scope of Identity Protection's controls. Instead, remediation is applied through Conditional Access or password reset policies driven by the calculated risk.

Therefore: adding users to groups based on risk (No); detecting leaked credentials (Yes); invoking MFA based on risk via Conditional Access (Yes).

質問: 36

Microsoft Defender for Cloud Appsの機能は何ですか？

- A. SaaSセキュリティ態勢管理(SSPM)
- B. クラウドワークロード保護プラットフォーム(CWPP)
- C. クラウドセキュリティ態勢管理(CSPM)
- D. 自動調査および対応(AIR)

正解: A ([コメントを发表する](#))

質問: 37

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	☐	☐
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	☐	☐
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	☐	☐

正解:

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	☒	☐
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	☒	☐
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	☐	☒

Explanation:

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	☒	☐
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	☒	☐
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	☐	☒

 Microsoft

Microsoft documents for Defender for Endpoint (MDE) describe it as an enterprise endpoint security platform that supports Windows 10/11, Windows Server, Linux, macOS, and mobile platforms (Android and iOS

/iPadOS). The platform provides threat and vulnerability management, attack surface reduction, next- generation protection, endpoint detection and response, and automated investigation and remediation across those supported operating systems. Because MDE supports Windows client operating systems and servers, it can also be used on Azure virtual machines that run supported Windows versions; onboarding methods include local scripts, Microsoft Endpoint Manager, or cloud integrations, allowing VM endpoints to receive the same protection and EDR capabilities as physical devices.

By contrast, malware scanning in SharePoint Online, OneDrive, and Microsoft Teams is provided by Microsoft Defender for Office 365 (Safe Attachments for SharePoint, OneDrive, and Teams)-a different service within the Microsoft 365 Defender family. This service analyzes files as they are uploaded or shared to detect and block malicious content in collaboration workloads, which is outside the scope of MDE's endpoint-focused protections. Therefore: Android protection (Yes), Azure VMs running Windows 10 (Yes), and SharePoint Online anti-virus protection by MDE (No, handled by Defender for Office 365).

質問: 38

Azure展開の責任分担モデルでは、Microsoftが単独で管理する責任は何ですか？

- A. モバイルデバイスの管理
- B. Azureに保存されているユーザーデータのアクセス許可
- C. ユーザーアカウントの作成と管理
- D. 物理ハードウェアの管理

正解: ([正解を表示します](#))

In Microsoft's shared responsibility model for Azure, responsibilities are divided between Microsoft and the customer. Microsoft Learn explains that Microsoft is responsible for security of the cloud, while customers are responsible for security in the cloud. The platform owner's scope includes the underlying facilities and infrastructure. As the documentation states: "Microsoft is responsible for the security OF the cloud, which includes protecting the infrastructure that runs all of the services offered in Microsoft Azure," and this encompasses "physical datacenters, physical hosts, and the physical network." The customer, by contrast, is responsible for items within their tenant and workloads, including "data, endpoints, accounts, and access management," as well as configuration of services, identities, and devices.

Applied to the options given: managing mobile devices (A), setting permissions for user data (B), and creating /managing user accounts (C) fall under the customer's responsibility because they relate to identity, access, data, and endpoint management within the tenant. The one item that Microsoft solely manages is the physical layer-the "physical hardware and facilities" that host Azure services. Therefore, the correct answer is D. the management of the physical hardware.

質問: 39

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

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

正解: [\(正解を表示します\)](#)

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

質問: 40

文を正しく完成させる答えを選択してください。

Answer Area

Microsoft

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

▼

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

正解:

Answer Area

Microsoft

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

▼

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

Explanation:

Answer Area

Microsoft

Azure Advisor

Azure Bastion

Azure Monitor

Azure Sentinel

▼

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

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

Reference:

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

質問: 41

文を正しく完成させる答えを選択してください。

Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

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

正解:

Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

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

Explanation:

Answer Area

Azure Active Directory (Azure AD) is

used for authentication and authorization.

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

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

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

質問: 42

組織内の 2 つの部門のメンバー間のコミュニケーションと情報の共有を制限するために使用できる Microsoft 365 の機能はどれですか?

- A. 機密ラベルポリシー
- B. 顧客ロックボックス
- C. 情報障壁
- D. 特権アクセス管理 (PAM)

正解: ([正解を表示します](#))

Microsoft's SCI documentation explains that Information Barriers (part of Microsoft Purview and enforced across Microsoft Teams, SharePoint, OneDrive, and Exchange) are used to "restrict communication and collaboration between specific groups of users to avoid conflicts of interest or to comply with regulatory obligations." Policies define which segments can communicate and which must be blocked, and they control chat, channel conversations, meetings, file sharing, and e-discovery visibility between the defined segments.

Typical scenarios include preventing communication between investment banking and research, or between merger deal teams and the rest of the organization. This is fundamentally different from other features:

Sensitivity label policies classify and protect content but do not block who can talk to whom; Customer Lockbox manages Microsoft engineer access to customer data during support; and Privileged Access Management (PAM) limits admin task approvals and elevated operations, not end-user communication. When the requirement is to "restrict communication and the sharing of information between members of two departments," Microsoft prescribes Information Barriers as the purpose-built capability to enforce those restrictions across collaboration workloads.

質問: 43

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

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	☐	☐
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	☐	☐
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	☐	☐

正解:

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	☐	☒
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	☒	☐
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	☒	☐

Explanation:

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	☐	☒
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	☒	☐
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	☒	☐

Microsoft's shared-responsibility model states that the cloud provider secures the cloud, while the customer secures what they put in the cloud. The Azure Security documentation explains: "Regardless of the type of deployment, you always retain responsibility for your data, endpoints, accounts, and access management." This applies to IaaS, PaaS, and SaaS, so statement 3 is Yes because the organization is always accountable for the security of information and data.

For SaaS, Microsoft describes that customers "don't manage or control the underlying cloud infrastructure- including network, servers, operating systems, or even individual application capabilities" and that the provider handles service maintenance and updates. In SaaS, tasks like patching or applying service packs to the application code are owned by the service provider, while the customer focuses on data, identity, and access. Therefore, statement 1 is No.

For IaaS, Microsoft notes the provider manages the physical estate: "Microsoft is responsible for the physical hosts, network, and datacenter facilities," while the customer configures and secures the guest OS, applications, and network controls within their subscription. Thus, managing the physical network is the cloud provider's duty, making statement 2 Yes.

These SCI principles are foundational to Microsoft Learn/Docs guidance on Azure's shared responsibility: provider-"security OF the cloud"; customer-"security IN the cloud," with data protection always remaining the customer's responsibility.

質問: 44

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

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

正解:

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

Explanation:

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

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

Reference:

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

質問: 45

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	☐	☐
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	☐	☐
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	☐	☐

正解:

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	☐	☐
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	☐	☐
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	☐	☐

Explanation:

Statements	Yes	No
You can create a hybrid identity in an on-premises Active Directory that syncs to Azure AD.	☒	☐
User accounts created in Azure AD sync automatically to an on-premises Active Directory.	☐	☒
When using a hybrid model, authentication can either be done by Azure AD or by another identity provider.	☒	☐

Microsoft describes hybrid identity as integrating on-premises Active Directory with Microsoft Entra ID (Azure AD) so that "your on-premises identities are synchronized to Azure AD" for a single identity across cloud and on-prem apps. In this model, directory objects (users, groups, and selected attributes) flow from on-premises AD to Azure AD using Azure AD Connect or Cloud Sync; this is the canonical direction for provisioning in hybrid environments. Microsoft further explains that while certain writeback features (such as password writeback, device or group writeback scenarios) are supported, cloud-created users do not automatically sync down to on-premises AD; account provisioning remains authoritative on-prem unless you deploy specific, limited writeback features-there is no default "user account creation from Azure AD to AD DS." For authentication, Microsoft states that hybrid identity supports cloud authentication (Password Hash Synchronization or Pass-through Authentication) where Azure AD performs the sign-in, or federation with another identity provider (e.g., AD FS or a third-party IdP) where that provider validates credentials and issues tokens to Azure AD. These statements align with Microsoft's SCI guidance on hybrid identity: on-prem to cloud sync is standard; automatic reverse user sync is not; and authentication can be handled by Azure AD or a federated IdP depending on the chosen sign-in method.

質問: 46

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

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

正解: D (コメントを发表する)

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

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

質問: 47

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area	Statements	Yes	No
	Microsoft Entra ID is deployed to an on-premises environment.	☐	☐
	Microsoft Entra ID is provided as part of a Microsoft 365 subscription.	☐	☐
	Microsoft Entra ID is an identity and access management service.	☐	☐

正解:

Statements	Yes	No
Microsoft Entra ID is deployed to an on-premises environment.	☒	☐
Microsoft Entra ID is provided as part of a Microsoft 365 subscription.	☒	☐
Microsoft Entra ID is an identity and access management service.	☒	☐

Explanation:

Statements	Yes	No
Microsoft Entra ID is deployed to an on-premises environment.	☐	☒
Microsoft Entra ID is provided as part of a Microsoft 365 subscription.	☒	☐
Microsoft Entra ID is an identity and access management service.	☒	☐

Microsoft Entra ID (formerly Azure Active Directory) is a cloud-based directory and identity platform. In Microsoft's SCI materials, Entra ID is described as "Microsoft's cloud-based identity and access management service that helps your employees sign in and access resources," underscoring that it's not deployed on-premises; instead, organizations can synchronize or federate with on-premises Active Directory using tools like Entra Connect. The same documentation explains that Entra ID is included with Microsoft 365 subscriptions, providing tenant identity services for apps such as Exchange Online, SharePoint Online, and Teams. Core capabilities listed include authentication, single sign-on (SSO), Conditional Access, device registration, and application access management, all of which classify Entra ID as an identity and access management (IAM) service. Thus: (1) on-premises deployment - No (it's cloud-native), (2) provided with Microsoft 365 - Yes (a directory is created for each tenant), and (3) IAM service - Yes (it delivers identity, access, and governance controls used across Microsoft cloud services).

質問: 48

Microsoft のプライバシー原則を表す声明はどれですか？

- A. Microsoft は顧客データを収集しません。
- B. Microsoft は、ターゲットを絞った広告のためにホストされた顧客の電子メールとチャット データを使用します。
- C. Microsoft は顧客のプライバシー設定を管理します。
- D. Microsoft は、顧客に適用される現地のプライバシー法を尊重します。

正解: [\(正解を表示します\)](#)

Microsoft's privacy commitments are framed as principles that include Control, Transparency, Security, Strong legal protections, No content-based targeting, and Benefits to you. Under these commitments, Microsoft emphasizes compliance with regional and sectoral laws: it provides "strong legal protections" for data and commits to handling data "in accordance with applicable laws," including respecting local privacy and data-protection requirements and supporting cross-border transfers only as permitted by law. The principles also state Microsoft does not use customer content for advertising, and it enables customers to manage their own privacy settings and choices. Therefore:

* A is false (Microsoft does collect data but minimizes and protects it).

- * B is false (Microsoft states no content-based targeting for customer email/chat).
- * C is false (Microsoft provides settings; customers control them).
- * D aligns with Microsoft's principle to respect and comply with applicable local privacy laws.

質問: 49

Azureネットワークサービスを適切な説明に一致させます。

回答するには、適切なサービスを左側の列から右側の説明にドラッグします。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 :それぞれの正しい一致は1ポイントの価値があります。

Services

Azure Bastion

Azure Firewall

Network security group (NSG)

Answer Area

Service

Provides Network Address Translation (NAT) services

Provides secure and seamless Remote Desktop connectivity to Azure virtual machines

Provides traffic filtering that can be applied to specific network interfaces on a virtual network

正解:

Services

Azure Bastion

Azure Firewall

Network security group (NSG)

Answer Area

Azure Firewall

Azure Bastion

Network security group (NSG)

Provides Network Address Translation (NAT) services

Provides secure and seamless Remote Desktop connectivity to Azure virtual machines

Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Explanation:

Services

Azure Bastion

Azure Firewall

Network security group (NSG)

Answer Area

Azure Firewall

Azure Bastion

Network security group (NSG)

Provides Network Address Translation (NAT) services

Provides secure and seamless Remote Desktop connectivity to Azure virtual machines

Provides traffic filtering that can be applied to specific network interfaces on a virtual network

Microsoft's Azure networking services have distinct roles that map directly to the statements in the prompt.

Azure Firewall is a stateful, cloud-native network security service that explicitly supports Source NAT (SNAT) and Destination NAT (DNAT) to control and translate traffic flows. In Microsoft's description, Azure Firewall "provides network address translation (SNAT/DNAT) and filtering for inbound and outbound traffic," making it the correct match for NAT services.

Azure Bastion is designed to deliver "secure and seamless RDP and SSH connectivity to your virtual machines directly from the Azure portal over TLS" without exposing a public IP on the VM. This aligns precisely with secure Remote Desktop connectivity to Azure virtual machines.

Network security groups (NSGs) are Azure's built-in mechanism for traffic filtering. Microsoft explains that an NSG "contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources" and that rules can be applied to subnets or to individual network interfaces (NICs) on a virtual network. Therefore, NSGs are the right choice for traffic filtering applied to specific network interfaces.

Together, these mappings reflect Azure's layered network security model: NSGs for rule-based filtering at NIC/subnet, Azure Firewall for centralized stateful inspection and NAT, and Azure Bastion for secure, browser-based RDP/SSH access.

質問: 50

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

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

正解:

Answer Area

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

Explanation:

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.	☐	☒

Microsoft

Microsoft describes Windows Hello for Business (WHfB) as replacing passwords with a device-bound credential: "Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or a PIN." WHfB authenticators are biometric gesture or PIN unlocking an asymmetric key stored on the device (typically in the TPM). Microsoft clarifies that the PIN is not a password and is "local to the device" and used to unlock the user's private key. Consequently, Yes-a PIN is a supported WHfB sign-in gesture. Conversely, the Microsoft Authenticator app is a separate Azure AD (Microsoft Entra ID) authentication method (push notifications, TOTP, passwordless phone sign-in). It is not the WHfB credential; WHfB relies on keys/certificates on the device, not on the Authenticator app. Finally, WHfB credentials are per-device: Microsoft states the credential is "tied to a device" and the private key never leaves the device, which means it does not roam/sync across a user's different devices. Each device enrolls and provisions its own WHfB key and gesture. These statements from Microsoft SCI documentation lead to the outcomes: No / Yes / No.

質問: 51

文を正しく完成させる答えを選択してください。

Answer Area

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

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

正解:

Answer Area

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

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

Explanation:

Answer Area

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

federation.

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

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

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

SCI documentation further states:

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

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

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

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

質問: 52

文を正しく完成させる答えを選択してください。

Answer Area

You can use

classifications

incidents

policies

Secure score

in the Microsoft 365 security center to identify devices that are affected by an alert.

正解:

Answer Area

You can use

classifications

incidents

policies

Secure score

in the Microsoft 365 security center to identify devices that are affected by an alert.

Explanation:

Answer Area

You can use

classifications

incidents

policies

Secure score

in the Microsoft 365 security center to identify devices that are affected by an alert.

In the Microsoft 365 security center (now Microsoft 365 Defender), incidents are used to triage and investigate threats across the tenant. Microsoft's security documentation explains that "an incident is a collection of related alerts" that are automatically correlated to give analysts a single, end-to-end view of an attack. Within each incident, the portal surfaces impacted assets such as devices, users, mailboxes, and applications, enabling responders to quickly identify which endpoints are affected by a given alert and to take response actions (isolate device, collect investigation package, run AV scan, etc.). This design allows security

teams to move beyond individual alerts and instead work a consolidated investigation that lists affected devices in the incident's Evidence & Response/Assets sections, complete with alert timelines and device details.

By comparison, Secure Score measures the organization's security posture and recommendations; policies are configuration/enforcement objects (e.g., Defender or compliance policies) and are not the investigative view for alerts; classifications relate to information protection labeling rather than alert investigation. Therefore, to identify devices that are affected by an alert, you use the Incidents experience in Microsoft 365 Defender, where correlated alerts show the devices involved alongside the entities and evidence connected to the threat.

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

- 質問: 53
- Core eDiscoveryワークフローでは、コンテンツを検索する前に何をする必要がありますか？
- A. eDiscoveryホールドを作成します。
 - B. ExpressAnalysisを実行します。
 - C. 弁護士/依頼人特権の検出を構成します。
 - D. 結果をエクスポートおよびダウンロードします。

正解: [\(正解を表示します\)](#)

In the Core eDiscovery (Microsoft Purview) workflow, you first create a case, add case members, and then (typically) apply eDiscovery holds to relevant locations to preserve potentially responsive content before you run searches. While a hold isn't strictly required to execute a search, Microsoft's documented workflow shows holds occur prior to creating and running content searches so that items aren't altered or deleted during the investigation. After holds, you create searches, review, and export.

- 質問: 54
- 次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
- 注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
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.	☐	☐

正解:

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.	☒	☐

Explanation:

Microsoft Purview Insider Risk Management is designed to identify, investigate, and act on risky activities by internal users-for example data exfiltration, data theft, policy violations, and user sentiments/signals that may indicate insider risk. SCI documentation explains that Insider Risk policies analyze signals such as file downloads, copying to USB, sharing to personal cloud, printing, or anomalous activity following events like performance warnings or resignation notices. Because it focuses on insider behaviors, it is not used to detect external threat vectors like phishing scams; those are addressed by Microsoft Defender for Office 365 and related anti-phishing protections-hence statement 1 is No. The solution is accessed in the Microsoft Purview (formerly Microsoft 365) compliance center under Insider risk management, where admins configure policies, alerts, and workflows-so statement 2 is Yes. Finally, its core purpose includes detecting and investigating potential data leaks by disgruntled or departing employees, using built-in policy templates (e.g., Data theft by departing employee, Data leaks), making statement 3 Yes.

質問: 55

添付ファイルにマルウェアが含まれていない場合にのみ、電子メールの添付ファイルをスキャンして受信者に転送するには、何を使用できますか？

- A. Office365用のMicrosoftDefender
- B. Microsoft Defender Antivirus
- C. Microsoft Defender for Identity
- D. エンドポイント用のMicrosoft Defender

正解: A ([コメントを发表する](#))

Microsoft Defender for Office 365 includes Safe Attachments, a protection that "checks attachments in a secure, virtual environment to detect malicious behavior." In Microsoft's guidance, Safe Attachments is described as part of the anti-malware pipeline that "routes messages with attachments to a detonation chamber; if no suspicious activity is detected, the message is released to the recipient, and if malicious behavior is found, the attachment is blocked or removed." Administrators can choose Block, Replace, Dynamic Delivery, or Monitor actions. The Dynamic Delivery option specifically supports the use case in the question: the email body is delivered while the attachment is scanned, and "the attachment is automatically reattached and forwarded to the recipient only when it is determined to be safe." This capability is unique to Defender for Office 365's Safe Attachments, not to be confused with endpoint antivirus or identity tools.

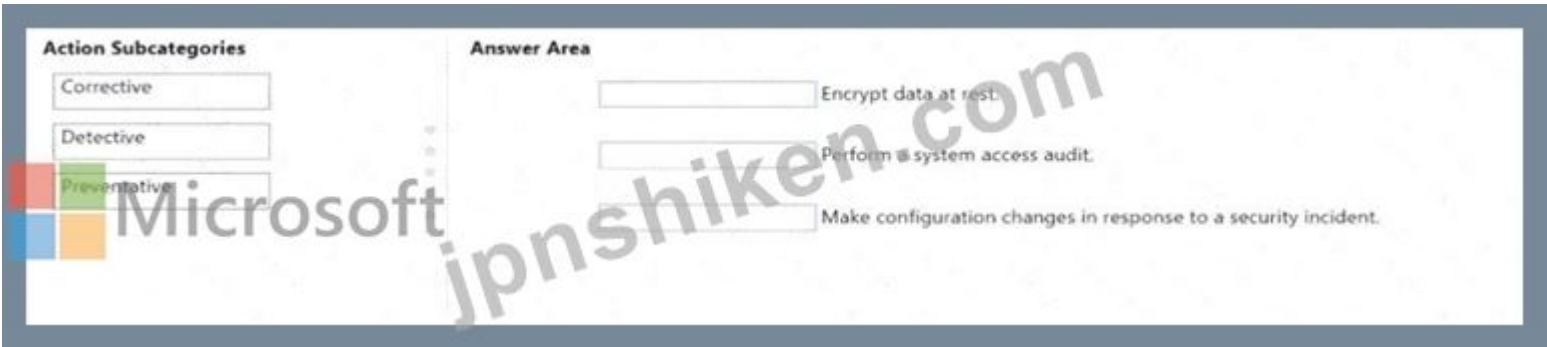
Defender Antivirus protects Windows devices, Defender for Identity secures on-premises identities, and Defender for Endpoint focuses on endpoint detection and response. Therefore, the Microsoft service you use to scan email attachments and forward them only when clean is Microsoft Defender for Office 365 (Safe Attachments).

質問: 56

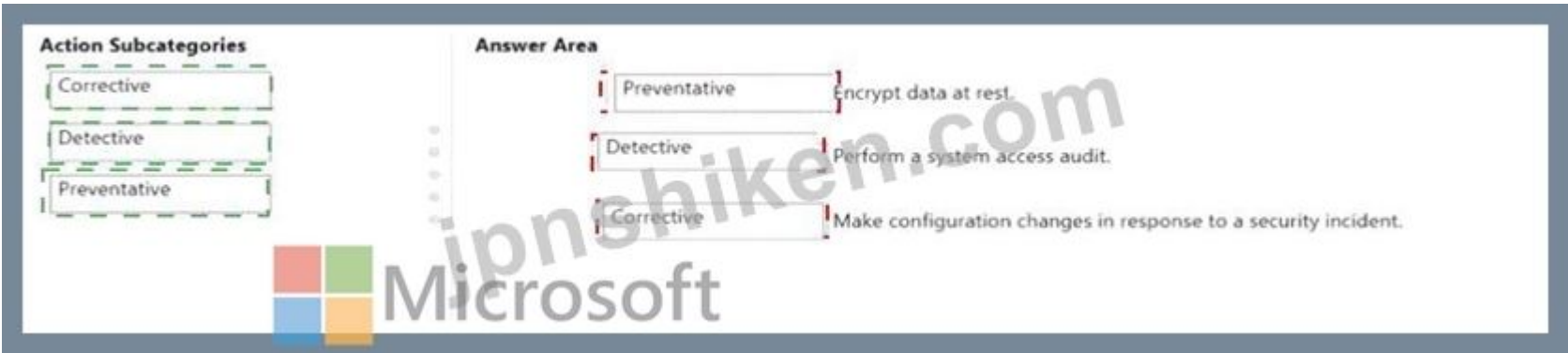
Microsoft Purview Compliance Manager でコンプライアンス スコアを評価しています。
コンプライアンス スコア アクションのサブカテゴリを適切なアクションと一致させます。

答えるには、適切なアクション サブカテゴリを左側の列から右側のアクションにドラッグします。各アクション サブカテゴリは、1 回だけ使用することも、複数回使用することも、まったく使用しないこともできます。

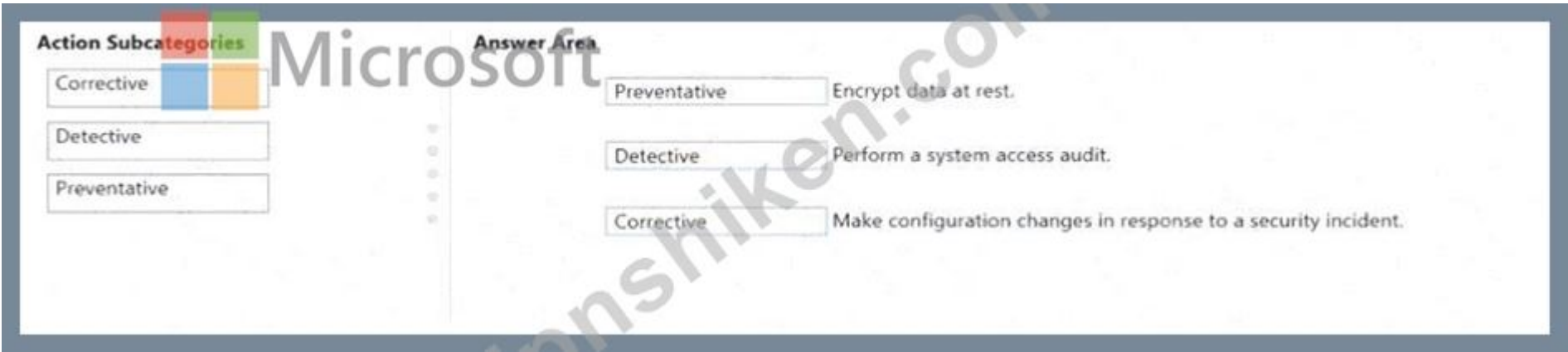
注: 正しく一致するたびに 1 ポイントの価値があります。



正解:



Explanation:



Microsoft Purview Compliance Manager organizes improvement actions into control action subcategories that mirror core security control types used throughout Microsoft Learn's SCI content: preventative, detective, and corrective. In the SC-900 security fundamentals guidance, Microsoft describes these control types as follows:

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

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

質問: 57

文を正しく完成させる答えを選択してください。

Customer Lockbox

Information barriers

Privileged Access Management (PAM)

Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

正解:

Customer Lockbox

Information barriers

Privileged Access Management (PAM)

Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

Explanation:

Customer Lockbox

Information barriers

Privileged Access Management (PAM)

Sensitivity labels

can be used to provide Microsoft Support Engineers with access to an organization's data stored in Microsoft Exchange Online, SharePoint Online, and OneDrive for Business.

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

質問: 58

文を正しく完成させる答えを選択してください。

Templates

Assessments

Improvement actions

Solutions

Templates

track compliance with groupings of controls from a specific regulation or requirement.

正解:

ANSWER AREA



Explanation:

Assessments

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

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

"Assessments in Compliance Manager help you track, implement, and improve compliance with requirements from standards and regulations. Each assessment maps to a specific regulation or control framework, such as ISO 27001, NIST, GDPR, or HIPAA, and includes a set of controls and recommended improvement actions." Further extracted content from SCI documentation confirms:

"An assessment is used to measure your compliance posture against a particular regulation or standard. It includes control mappings and provides insight into what's in place and what still needs to be addressed to meet the compliance goals." The other options in the dropdown - Templates, Improvement actions, and Solutions - serve different functions:

Templates provide a blueprint for creating assessments.

Improvement actions are actionable steps generated within assessments.

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

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

質問: 59

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

注：正しい選択はそれぞれ1ポイントの価値があります。

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

正解:

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

Explanation:

Security defaults require an Azure Active Directory (Azure AD) Premium license. No Security defaults can be enabled for a single Azure Active Directory (Azure AD) user. No When Security defaults are enabled, all administrators must use multi-factor authentication (MFA). Yes Microsoft explains that Security defaults are baseline identity protections that are "available to all tenants at no additional cost" and are intended to "help protect your organization from common identity-related attacks." They are a tenant-wide setting: Microsoft states that security defaults are "either on or off for the entire tenant" and "can't be customized or targeted to specific users or groups." If you require per-user or granular targeting, Microsoft directs customers to use Conditional Access policies instead. A core behavior of security defaults is enforcing MFA: "All users are required to register for Azure AD Multi- Factor Authentication," and "administrators are required to perform MFA." In addition, security defaults "block legacy authentication" and apply other baseline requirements, but they do not enable premium features such as Azure AD Identity Protection or PIM. Summarizing the implications for the statements: no premium license is required; you cannot enable security defaults for just one user because the control is global; and when enabled, administrators must use MFA, with Microsoft recommending exclusion only for a break-glass account if necessary.

質問: 60

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

注意: 正解ごとに 1 ポイントが付与されます。

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

正解: ([正解を表示します](#))

Microsoft Purview Data Loss Prevention (DLP) defines supported service locations for policy enforcement.

The Microsoft Learn/SCI materials state that DLP policies "help protect sensitive information across Microsoft 365 services" and can be scoped to common workloads. In the DLP overview, Microsoft explicitly lists the core cloud locations: "You can create DLP policies that protect content in Exchange Online, SharePoint Online, and OneDrive for Business." The Teams workload is also included: "DLP can monitor and take protective actions on Microsoft Teams chat and channel messages." These statements confirm that applying a DLP policy to Exchange Online email (A), OneDrive accounts (B), and Teams chat and channel messages (D) is supported.

By contrast, Exchange Online public folders (C) are not listed among supported DLP locations in the SCI documentation, and Viva Engage (formerly Yammer) (E) is not a standard Microsoft Purview DLP location in the core list above (Viva Engage has separate governance and communication compliance controls).

Therefore, from the supported locations enumerated in Microsoft's DLP guidance, the correct answers are Exchange Online email, OneDrive accounts, and Teams chat and channel messages.

質問: 61

文を正しく完成させる答えを選択してください。

Answer Area

Compliance Manager assesses compliance data for an organization.

continually
monthly
on-demand
quarterly

正解:

Answer Area

Compliance Manager assesses compliance data for an organization.

continually
monthly
on-demand
quarterly

Explanation:

Answer Area

Compliance Manager assesses compliance data for an organization.

continually
monthly
on-demand
quarterly

In Microsoft Purview Compliance Manager, the built-in Compliance score and assessments are designed for ongoing, risk-based monitoring of your organization's compliance posture. Microsoft's SCI materials describe Compliance Manager as a solution that "helps you track, improve, and demonstrate your compliance posture" by mapping regulations and standards to improvement actions and assessments. The experience is not a one-time or periodic snapshot; it is intended to be continuous. As you implement controls, provide evidence, or when automated tests record results, "your score is updated as you complete actions," reflecting current progress toward data protection and regulatory requirements.

Assessments in Compliance Manager persist over time and are maintained through continuous evaluation:

actions can be automatically tested when supported (for example, configuration-based controls in Microsoft

365) or manually assessed on an ongoing basis by compliance teams. This design enables organizations to prioritize and remediate issues as they arise, rather than waiting for monthly or quarterly reviews. Because of this continuous scoring and reassessment model, Compliance Manager assesses compliance data continually for an organization, providing near real-time insight into control effectiveness and residual risk across standards such as GDPR, ISO 27001, and NIST frameworks.

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

質問: 62

Microsoft Entra ID ガバナンスにはどの機能が含まれていますか？

- A. 検証可能な認証情報
- B. 権限管理
- C. ID 保護
- D. 特権 ID 管理

正解: ([正解を表示します](#))

Microsoft defines Microsoft Entra ID Governance as the capability to manage "the identity lifecycle, access lifecycle, and privileged access" so organizations can ensure "the right people have the right access to the right resources at the right time." The product family explicitly lists the following core features: "Lifecycle workflows, Entitlement management, Access reviews, and Privileged Identity Management (PIM)." Microsoft further explains that PIM helps you "manage, control, and monitor access within your organization," enabling just-in-time elevation, approval workflows, MFA/justification on activation, and detailed auditing for privileged roles. By contrast, the other options are separate Microsoft Entra offerings outside ID Governance:

Verifiable credentials (Microsoft Entra Verified ID) issues and validates digital credentials; Permissions Management (Microsoft Entra Permissions Management) provides CIEM for multi-cloud permissions; and Identity Protection offers risk-based detection and policies for sign-ins and users. Therefore, among the choices, the feature that is included in Microsoft Entra ID Governance is Privileged Identity Management (PIM), which is specifically called out by Microsoft as a pillar of ID Governance and is used to govern privileged access with policy-based controls, time-bound assignments, approvals, and comprehensive auditability.

質問: **63**

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

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

正解: ([正解を表示します](#))

In Microsoft's identity platform, Active Directory Domain Services (AD DS) is the on-premises directory that maintains directory objects such as users, groups, and computers. Microsoft documentation describes AD DS as a service that "stores information about objects on the network and makes this information easy for administrators and users to find and use." It further explains that AD DS contains objects like "users, groups, computers, and other resources," and that administrators use tools such as Active Directory Users and Computers to create and manage these objects. A key object type is the computer account; Microsoft states that "a computer that's joined to a domain has a corresponding computer account object in Active Directory" and that these accounts are created and managed within AD DS to enable secure authentication and authorization for domain-joined devices.

By contrast, mobile devices are typically enrolled and managed through Microsoft Intune/Endpoint Manager and Azure AD device objects, not created in AD DS. Likewise, SaaS applications that require modern authentication integrate with Microsoft Entra ID (Azure AD) using OpenID Connect/OAuth 2.0-not with AD DS. Line-of-business apps that rely on modern authentication are also registered in Entra ID, while AD DS supports traditional Kerberos/NTLM for domain resources. Therefore, among the options provided, the object you can create in AD DS is computer accounts.

質問: **64**

Azure Active Directory (Azure AD) テナントに対してセキュリティの既定値が有効になっている場合、どの2つの要件が適用されますか？それぞれの正解は完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. すべてのユーザーは登録済みのデバイスから認証する必要があります。
- B. 管理者は常にAzure Multi-Factor Authentication (MFA)を使用する必要があります。

- C. すべてのユーザーにAzure Multi-Factor Authentication (MFA) 登録が必要です。
- D. すべてのユーザーは、パスワードなしのサインインを使用して認証する必要があります。
- E. すべてのユーザーはWindowsHelloを使用して認証する必要があります。

正解: ([正解を表示します](#))

Security defaults make it easy to protect your organization with the following preconfigured security settings:

Requiring all users to register for Azure AD Multi-Factor Authentication.

Requiring administrators to do multi-factor authentication.

Blocking legacy authentication protocols.

Requiring users to do multi-factor authentication when necessary.

Protecting privileged activities like access to the Azure portal.

Reference:

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

質問: 65

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

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

正解: ([正解を表示します](#))

In Microsoft 365, Data Loss Prevention (DLP) policies are designed to "help you identify, monitor, and automatically protect sensitive information" across services such as Exchange Online, SharePoint Online, OneDrive, and Microsoft Teams. Microsoft's guidance explains that DLP uses sensitive information types- including built-in classifiers like Credit Card Number-to detect when content matches a defined pattern and then enforce protective actions. With DLP, you can create rules that trigger when email messages contain customer lists with credit card numbers, and choose actions to block the message, restrict access, or notify and educate users via policy tips and incident reports. Microsoft further notes that DLP "prevents the accidental sharing of sensitive information," can require user justification to override, and supports granular conditions (e.g., number of matches, recipients internal vs. external) to ensure that only risky transmissions are stopped.

By applying a DLP policy to Exchange with the Credit Card Number sensitive info type, an organization can block or quarantine outbound mail that includes those numbers, thereby reducing regulatory and data- exposure risk. Other options listed-retention policies, conditional access, and information barriers-serve different purposes (data lifecycle, access/authentication conditions, and restricting communication between groups) and do not inspect message contents for sensitive data. Hence, DLP policies are the correct control to restrict sending emails that contain customer lists and associated credit card numbers.

質問: 66

文を正しく完成させる答えを選択してください。

 Microsoft

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services.

正解:

▼

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services.

▼

Azure Application Insights

Azure Network Watcher

Log Analytics workspaces

Security baselines for Azure

provides benchmark recommendations and guidance for protecting Azure services

Reference:

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

質問: 67

文を正しく完成させる答えを選択してください。

▼

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Microsoft Defender for Cloud

Microsoft Sentinel

Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

正解:

▼

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Microsoft Defender for Cloud

Microsoft Sentinel

Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

Explanation:

▼

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Microsoft Defender for Cloud

Microsoft Sentinel

Microsoft Defender for Cloud Apps

can use conditional access policies

to control sessions in real time.

In Microsoft's Security, Compliance, and Identity portfolio, Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) integrates directly with Microsoft Entra Conditional Access to provide Conditional Access App Control-Microsoft's real-time session control. Microsoft's documentation describes this capability as enabling organizations to "monitor and control user sessions in real time" and to "protect downloads, restrict uploads, block copy/paste and print, and apply access or

session policies" for sanctioned and unsanctioned applications. The enforcement is achieved through a reverse-proxy session that is invoked by Conditional Access policy decisions, allowing continuous inspection and dynamic controls after authentication.

By contrast, other options in the list do not offer real-time session enforcement via Conditional Access. Azure AD Privileged Identity Management (PIM) focuses on just-in-time role activation, approval workflows, and access reviews for privileged accounts-not session control of app usage. Microsoft Defender for Cloud provides cloud security posture management and workload protection across Azure, multicloud, and hybrid resources-again, not Conditional Access-based user session governance. Microsoft Sentinel is a SIEM

/SOAR solution used for ingestion, detection, investigation, and response; it does not apply Conditional Access policies to control user sessions. Therefore, the service that can use Conditional Access policies to control sessions in real time is Microsoft Defender for Cloud Apps through Conditional Access App Control.

質問: 68

Microsoft 365 エンドポイント データ 損失防止 (エンドポイント 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 以降のみ
- B. Windows 10 以降および Android のみ
- C. Windows 10 以降および macOS のみ
- D. Windows 10 以降、Android、および macOS

正解: [\(正解を表示します\)](#)

Microsoft 365 Endpoint Data Loss Prevention (Endpoint DLP) extends DLP controls directly to supported desktops. Microsoft states: "Endpoint DLP extends the activity monitoring and protection capabilities of DLP to Windows 10 (and later) devices." The platform coverage is explicitly broadened to Apple desktops: "Endpoint DLP for macOS enables the same set of DLP capabilities on macOS devices (supported versions) so you can monitor and protect sensitive items across Windows and Mac endpoints." At the same time, Microsoft clarifies the mobile scope: "Endpoint DLP is supported on Windows and macOS devices." This means Android is not a supported operating system for Endpoint DLP (mobile data protection on Android uses different controls such as app protection policies via Microsoft Intune and conditional access). Therefore, the correct pairing of operating systems for Endpoint DLP support is Windows 10 and newer, and macOS- not Android. This aligns with Microsoft's Endpoint DLP platform support guidance and the intended desktop- focused endpoint protections for activities such as file copy, print, upload, and removable media interactions.

質問: 69

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

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

正解:

Answer Area

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

Explanation:

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

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

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

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

質問: 70

Microsoft 365E3サブスクリプションがあります。

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ことを計画しています。

監査記録はどのくらいの期間保持されますか？

- A. 15日
- B. 30日
- C. 90日
- D. 180日

正解: ([正解を表示します](#))

In Microsoft 365, the unified audit log retention depends on the audit tier included with the subscription.

Current SCI/Compliance documentation states that Audit (Standard)-which is available with Microsoft 365 E3-retains audit records for 180 days. The docs describe that organizations with E3 receive "up to 180 days of audit log retention" for user and admin activities captured in the unified audit pipeline. Longer retention (for

example 365 days and beyond with customizable policies) is part of Audit (Premium) features generally associated with E5/E5 Compliance. Because the scenario specifies a Microsoft 365 E3 subscription using the unified audit log and Basic/Standard Audit, the retention period for audit records is 180 days.

質問: 71

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

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

正解: D (コメントを发表する)

Microsoft Defender for Office 365 is the Microsoft 365 solution designed to protect users from threats delivered through email and collaboration workloads. SCI training material explains that Defender for Office 365 protects Exchange Online, Microsoft Teams, SharePoint Online, and OneDrive for Business by detecting and blocking malware, phishing, and other advanced attacks that use messages and shared content as the delivery channel. A key capability is Safe Links, which specifically protects against malicious URLs. When a user receives an email, Teams chat message, or channel post that contains a hyperlink, Safe Links scans and rewrites that URL. At the moment the user clicks, the link is checked again; if it is identified as malicious or leads to a known phishing or malware-hosting site, access is blocked and a warning page is shown. This time-of-click protection is emphasized in Microsoft's security documentation as a primary defense against weaponized links in email and collaborative communications. By comparison, Microsoft Defender for Identity focuses on detecting identity-related threats in on-premises Active Directory, Defender for Endpoint protects devices and endpoints, and Defender for Cloud Apps secures SaaS applications and shadow IT. None of these are the primary solution for blocking malicious links in email, chats, and channels. Therefore, the correct choice is Microsoft Defender for Office 365.

質問: 72

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

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

Microsoft

正解:

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.	☐	☐

Explanation:

Answer Area

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

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

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

質問: 73

文を正しく完成させる答えを選択してください。

Answer Area

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

Microsoft Defender for Cloud

Azure Monitor

Microsoft cloud security benchmark

Microsoft Secure Score

正解:

Answer Area

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

Microsoft Defender for Cloud

Azure Monitor

Microsoft cloud security benchmark

Microsoft Secure Score

Explanation:

Answer Area

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

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

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

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

質問: 74

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
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	☐	☐

正解:

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	☒	☐

Explanation:

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	☒	☐

Microsoft explains that Conditional Access (CA) evaluates signals and then enforces access decisions using grant and session controls: "Conditional Access policies are enforced after first-factor authentication is completed" and are used to "make access control decisions." CA policies target users and groups-including administrators-unless explicitly excluded. Microsoft guidance recommends excluding only break-glass accounts: "Customers with Azure AD roles such as Global administrator should have at least one emergency access account excluded from policies." This means admins are not exempt by default; they are in scope unless you configure exclusions.

CA does not manage directory role assignments; that is handled by role assignment and Privileged Identity Management (PIM). CA's grant controls focus on access conditions: "Grant access... Require multi-factor authentication" and Microsoft lists a common baseline: "Require multi-factor authentication for all users." Therefore, CA can require MFA to access cloud apps, but it cannot add users to Azure AD roles.

These statements from Microsoft's SCI materials confirm the outcomes: Admins are not inherently exempt (No), CA cannot assign roles (No), and CA can force MFA for app access (Yes).

質問: 75

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Statements	Yes	No
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.	☐	☐

正解:

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.	☐	☒

Explanation:

Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score. Yes A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant. Yes Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance. No Microsoft Secure Score is a measurement of an organization's security posture in Microsoft 365. The SCI materials explain that Secure Score is calculated from improvement actions such as requiring multi-factor authentication for users, especially administrators. When you configure and enforce MFA, you complete one of these recommended actions, and Secure Score awards points, so enabling MFA directly increases Microsoft Secure Score. The documentation further states that Secure Score reflects how many recommended security controls you have implemented. A higher score indicates that more recommended controls are in place, which reduces exposure to common threats and therefore represents a lower residual risk level in the tenant. While it is not an absolute guarantee of security, it is an indicator that risk has been reduced compared to a lower score.

The third statement, however, describes the purpose of Microsoft Purview Compliance Manager and its compliance score, which tracks progress against controls mapped to regulations and standards for data protection and governance. Secure Score does not measure alignment with regulatory frameworks; it is focused on technical security configurations and behaviors in Microsoft 365. Therefore, that statement is No.

質問: 76

文を正しく完成させる答えを選択してください。

Answer Area

Microsoft

In Microsoft Sentinel, you can automate common tasks by using

playbooks.

deep investigation tools.

hunting search-and-query tools.

playbooks.

workbooks.

Answer Area

Microsoft

In Microsoft Sentinel, you can automate common tasks by using

playbooks.

deep investigation tools.

hunting search-and-query tools.

playbooks.

workbooks.

Answer Area

Microsoft

In Microsoft Sentinel, you can automate common tasks by using

playbooks.

In Microsoft Sentinel, automation of routine or repetitive SOC tasks is delivered through playbooks.

Microsoft's Sentinel guidance defines playbooks as "collections of procedures that can be run from Microsoft Sentinel in response to an alert or incident." They are "built on Azure Logic Apps" and enable teams to "automate and orchestrate responses to threats" such as enriching incidents, opening tickets, notifying responders, quarantining entities, or blocking indicators. The documentation further clarifies that automation rules can "trigger playbooks automatically based on analytics alerts or incident conditions," allowing consistent, scalable actions without manual intervention. By contrast, workbooks provide "data visualization and reporting" for analysis; hunting search-and-query tools (built on KQL) are used to "proactively hunt for threats"; and deep investigation tools assist analysts during incident investigation. Therefore, when the goal is to automate common tasks-for example, sending incident notifications, enriching with threat intelligence, or creating tickets in ITSM-the correct capability in Microsoft Sentinel is playbooks, because they encapsulate repeatable response procedures and can be executed automatically via automation rules or manually from incidents, alerts, or entities.

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

質問: 77

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

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

正解: C ([コメントを発表する](#))

Sensitive Information Types (SITs) support regular expressions (regex), which allow for custom pattern matching to detect sensitive content like credit card numbers, social security numbers, or custom identifiers.

Regex is fundamental to the detection logic within SITs.

SCI Extract: "Sensitive information types use pattern matching techniques, including regular expressions, keyword matches, and checksums to identify sensitive data."

質問: 78

特定のキーワードを含むMicrosoftSharePoint Onlineサイト上のすべてのドキュメントを識別するために使用できるMicrosoft365コンプライアンスセンターの機能はどれですか。

- A. 監査
- B. コンプライアンスマネージャー
- C. コンテンツ検索
- D. アラート

正解: C ([コメントを発表する](#))

The Content Search tool in the Security & Compliance Center can be used to quickly find email in Exchange mailboxes, documents in SharePoint sites and OneDrive locations, and instant messaging conversations in Skype for Business.

The first step is to starting using the Content Search tool to choose content locations to search and configure a keyword query to search for specific items.

Reference:

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

質問: 79

Microsoft Defender for Endpointの2つの機能は何ですか？それぞれの正しい選択は、完全な解決策を提示します。

注：正しい選択はそれぞれ1ポイントの価値があります。

- A. 自動化された調査と修復
- B. トランスポート暗号化
- C. シャドーIT検出
- D. 攻撃対象領域の削減

正解: [\(正解を表示します\)](#)

Microsoft Defender for Endpoint includes Automated investigation and remediation (AIR) and Attack surface reduction (ASR) as core capabilities. Microsoft's guidance states that AIR "uses inspection algorithms and playbooks to examine alerts, determine if they are malicious, and then take remediation actions such as stopping processes, quarantining files, and rolling back changes." It is designed to "reduce the volume of alerts that require analyst attention and to remediate threats at machine speed across your estate," helping security teams contain and fix issues without manual intervention.

Defender for Endpoint also provides attack surface reduction features to proactively limit exposure. The Microsoft learn materials describe that ASR "helps organizations minimize areas that attackers can exploit," and includes "attack surface reduction rules, network protection, web protection, application control (Windows Defender Application Control), and controlled folder access." These controls "block or constrain risky behaviors and common attacker techniques," thereby preventing many initial compromise and lateral- movement attempts before they generate incidents.

By contrast, transport encryption is a general platform/security baseline capability rather than a specific Defender for Endpoint feature, and shadow IT detection is addressed through Microsoft Defender for Cloud Apps (App discovery), which can use Defender for Endpoint network signals but is not itself a native MDE capability. Therefore, the two correct capabilities of Microsoft Defender for Endpoint are Automated investigation and remediation and Attack surface reduction.

質問: 80

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. Azure Resource Manager (ARM) テンプレートを保存します。
- B. Azure DDoS Protection を実装します。
- C. ネットワーク セキュリティ グループ (NSG) を実装します。
- D. キーを保存します。
- E. 秘密を保存します。

正解: **D,E** ([コメントを发表する](#))

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

By contrast, the SCI content makes clear that infrastructure features like Azure DDoS Protection and Network Security Groups (NSGs) are networking/security controls delivered by Azure networking services, not Key Vault. Likewise, ARM templates are deployment artifacts stored in repositories such as Azure Repos or

GitHub; Key Vault does not store or manage template files. Therefore, the two correct actions you can perform with Azure Key Vault-aligned with Microsoft's documentation-are to store (and manage) keys and store (and manage) secrets.

質問: 81

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

Yes

No

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

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

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

Yes

No

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

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

Explanation:

Answer Area

Statements

eDiscovery (Standard) search results can be exported.

Yes

No

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

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

In Microsoft Purview, eDiscovery (Standard) (formerly Core eDiscovery) provides case management, holds, searches, and export. Microsoft describes that eDiscovery (Standard) lets investigators "search across Microsoft 365 data sources and export the results," including options to export native files, email to PST, and CSV reports for further review. It uses the same Content search engine and supports selecting locations such as "Exchange Online mailboxes, Microsoft 365 Groups, Teams, SharePoint sites, OneDrive accounts, and Exchange public folders," enabling organization-wide discovery that includes public folders. Integration for end-to-end legal review from Microsoft Purview Insider Risk Management is specifically aligned to eDiscovery (Premium) (formerly Advanced eDiscovery). Insider Risk cases provide actions like "Send to eDiscovery (Premium)" to create a review set and apply advanced processing, analytics, and review workflows. Those advanced integrations (review sets, analytics, legal hold communications) are not features of eDiscovery (Standard). Therefore: exporting results (Yes), Insider Risk integration (No, as it targets

eDiscovery Premium), and searching Exchange Online public folders (Yes) are the correct evaluations based on the Microsoft Security, Compliance, and Identity study materials for Purview eDiscovery capabilities.

質問: 82

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

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

正解: (正解を表示します)

質問: 83

文を正しく完成させる答えを選択してください。

Answer Area

A security information and event management (SIEM)

A security information and event management (SIEM)

A security orchestration automated response (SOAR)

A Trusted Automated eXchange of Indicator Information (TAXII)

An attack surface reduction (ASR)

system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.



正解:

Answer Area

A security information and event management (SIEM)

A security information and event management (SIEM)

A security orchestration automated response (SOAR)

A Trusted Automated eXchange of Indicator Information (TAXII)

An attack surface reduction (ASR)

system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.



Explanation:

Answer Area

A security information and event management (SIEM)

system is a tool that collects data from multiple systems, identifies correlations or anomalies, and generates alerts and incidents.



A Security Information and Event Management (SIEM) system is designed to collect and aggregate security data from multiple sources-such as servers, devices, applications, and security appliances-across an organization. It then analyzes the data for anomalies, correlations, and patterns that could indicate potential threats or breaches.

From the SCl certification learning paths, especially SC-200 (Microsoft Security Operations Analyst), Microsoft defines SIEM as follows:

"SIEM tools collect and analyze activity from multiple resources across your IT infrastructure. Microsoft Sentinel is Microsoft's cloud-native SIEM that provides intelligent security analytics and threat intelligence to help detect and respond to security threats." A SIEM system:

Ingests large volumes of data (logs, events).
Uses built-in rules, AI, and analytics to identify threats.
Correlates alerts from various sources to form incidents.
Generates alerts and dashboards for security analysts.
Microsoft Sentinel, as Microsoft's SIEM solution, embodies all of these capabilities.
Other options in the dropdown (incorrect for this context):
SOAR is focused on automating responses after SIEM alerts.
TAXII is a threat intel transport protocol, not a detection system.
ASR (Attack Surface Reduction) refers to endpoint hardening, not centralized event analysis.
Therefore, the correct and Microsoft-verified term is: A security information and event management (SIEM).

質問: 84

文を正しく完成させる答えを選択してください。

Answer Area

requires additional verification, such as a verification code sent to a mobile phone.

Multi-factor authentication (MFA)

Pass-through authentication

Password writeback

Single sign-on (SSO)

正解:

Answer Area

requires additional verification, such as a verification code sent to a mobile phone.

Multi-factor authentication (MFA)

Pass-through authentication

Password writeback

Single sign-on (SSO)

Explanation:

Answer Area

requires additional verification, such as a verification code sent to a mobile phone.

Multi-factor authentication (MFA)

Pass-through authentication

Password writeback

Single sign-on (SSO)

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks>

質問: 85

コンプライアンス スコア アクションのタイプを適切なタスクに一致させます。

答える。適切なアクション タイプを左側の列から右側のタスクにドラッグします。各タイプは1回ずつ使用できます。複数回、またはまったく。

注: それぞれの正しい一致は 1 ポイントの価値があります。



正解:



Explanation:



In Microsoft Purview Compliance Manager, improvement actions are categorized by control type to reflect how they reduce risk and contribute to your compliance score. Microsoft's SCI guidance explains that preventative controls are safeguards that "prevent a security or compliance incident from occurring by enforcing protections in advance (for example, enforcing encryption of data at rest and in transit, access restrictions, and configuration baselines)." This directly aligns with the task "Use encryption to protect data at rest", which is a classic prevention mechanism intended to stop unauthorized disclosure before it can happen.

The guidance also states that detective controls are measures that "identify, log, and surface anomalous or non-compliant activities so they can be investigated and addressed (for example, continuous monitoring, alerting, audit logging, and analytics)." This maps to "Actively monitor systems to identify irregularities that might represent risks", because the goal is to detect suspicious behavior or drift as it occurs.

By comparison, corrective controls are used to "remediate issues and restore a desired state after a problem is discovered (for example, patching, incident response, or configuration correction)." No corrective action is described in the two listed tasks, so Corrective is not selected. This mapping reflects how Compliance Manager classifies actions that contribute points to the compliance score based on their risk-reducing impact.

質問: 86

1つの仮想ネットワークだけを使用するのではなく、複数の仮想ネットワークをデプロイする2つの理由は何ですか? それぞれの正解は完全な解決策を示します。ノート; 正しく選択するたびに 1 ポイントの価値があります。

A. 予算編成のためにリソースを分離するため

B. ガバナンス ポリシーを満たすため

- C. リソースを隔離する
- D. 複数種類のリソースを接続する場合

正解: **B,C** ([コメントを発表する](#))

In Microsoft guidance, network segmentation and isolation are core security principles. Azure virtual networks (VNets) are "a fundamental building block... that enable isolation and segmentation of resources," and multiple VNets are commonly used to separate environments, business units, or security boundaries. This aligns with Zero Trust and SCI guidance that recommends isolating workloads to reduce blast radius and to apply least privilege and policy-based controls per boundary. Microsoft also emphasizes governance alignment, stating that enterprises should structure Azure resources so that policies, RBAC, and compliance requirements can be applied at appropriate scopes (management group, subscription, resource group, or network boundary). Deploying multiple VNets supports these goals by enabling per-environment policy assignment (for example, dev/test vs. production), differentiated security controls (such as NSGs, ASGs, and firewalls), and independent address spaces to prevent overlap across organizations or regions. Options A and D are not primary drivers: budgeting is handled at subscription/resource group scopes rather than VNet count, and a single VNet can already host and connect many resource types; creating multiple VNets is therefore primarily about governance and isolation that reduce risk and enforce organizational policies.

質問: **87**

セキュリティの傾向を表示し、ID の保護状態を追跡するには、Microsoft Defender ポータルで何を使用すればよいですか？

- A. セキュアスコア
- B. レポート
- C. ハンティング
- D. インシデント

正解: ([正解を表示します](#))

In the Microsoft 365 Defender (Microsoft Defender XDR) portal, the Reports area is the feature designed to surface security trends and provide protection status views across workloads, including identities. Microsoft guidance explains that the Reports workspace offers curated dashboards and exportable reports for specific domains (for example, Identities, Email & collaboration, Endpoints), so security teams can review trend lines, coverage/health, and status without running queries. For identities specifically (backed by Microsoft Defender for Identity), the reports include overview dashboards and scheduled/on-demand reports that show items such as identity security posture, open health issues, alert volumes over time, and sensor/coverage status. This aligns with SCI learning paths that distinguish portal areas by purpose: Secure score is a measurement of overall posture and recommended actions, Incidents is for triage and response to individual cases, and Hunting is for ad-hoc, query-driven investigations. When the task is to "view security trends and track the protection status of identities," Microsoft directs administrators to the Reports > Identities experience in the Defender portal, which provides the built-in, continuously updated visualizations and summaries required for ongoing monitoring.

質問: **88**

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

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

正解: ([正解を表示します](#))

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

質問: 89

文を正しく完成させる答えを選択してください。

Answer Area

You can use  in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reports

Hunting

Attack simulator

Incidents



正解:

Answer Area

You can use  in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reports

Hunting

Attack simulator

Incidents



Explanation:

Answer Area

You can use  in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

Reports

Hunting

Attack simulator

Incidents



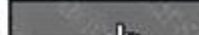
In Microsoft 365 Defender (Microsoft 365 security center), Incidents are designed to consolidate and correlate security signals so analysts can see the full scope of an attack. Microsoft's documentation explains that an incident is "a collection of related alerts that, when viewed together, provide a richer context for the attack and its impact." The service "automatically groups alerts that are likely to be associated with the same threat activity," which allows security teams to investigate a single incident rather than many fragmented alerts.

Microsoft further notes that incidents "aggregate alerts, affected assets (users, devices, mailboxes), evidences, and entities into one view," helping analysts triage, investigate, and remediate more efficiently.

This is distinct from other areas in the portal: Reports provide trend and posture reporting; Hunting offers proactive, query-based threat hunting across raw data; and Attack simulator (in Defender for Office 365) is used to run training and awareness simulations (e.g., phishing), not to aggregate real alerts. Therefore, when you need to "view an aggregation of alerts that relate to the same attack" in the Microsoft 365 security center, the correct place is Incidents, which presents the correlated attack story and enables end-to-end response and remediation from a single, consolidated record.

質問: 90

文を正しく完成させる答えを選択してください。

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

are

have

know

share

正解:



Explanation:



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

something you know (knowledge), something you have (possession), and something you are (inherence). A password is explicitly categorized as "something you know," because it relies on a secret the user memorizes and types during sign-in. MFA improves security by requiring two or more of these distinct factors-e.g., a password (know) plus a phone approval or hardware token (have), or a biometric like Windows Hello (are).

Using factors from different categories mitigates common attacks such as password spray, credential stuffing, and phishing, because compromising one factor (for example, the password) does not grant access without the second, unrelated factor. Microsoft recommends enabling MFA broadly and pairing passwords with stronger possession or inherence methods to achieve a measurable reduction in account compromise risk. Therefore, in the MFA model used by Microsoft Entra ID (Azure AD), a password is considered something you know.

質問: 91

条件付きアクセス信号のタイプを適切な定義と一致させます。

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

注: 正しく一致するたびに 1 ポイントの価値があります。

Conditional access signals

Device

Location

Sign-in risk

User risk

Answer Area

The probability that an identity or account is compromised.

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

Microsoft

正解:



Explanation:



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

User risk:

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

Sign-in risk:

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

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

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

質問: 92

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

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

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

正解:

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

Explanation:

Answer Area

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

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

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

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

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

質問: 93
文を正しく完成させる答えを選択してください。

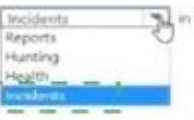
Answer Area

You can use  in the Microsoft Defender portal to view an aggregation of alerts that relate to the same attack.

Microsoft

正解:

Answer Area

You can use  in the Microsoft Defender portal to view an aggregation of alerts that relate to the same attack.

Microsoft

質問: 94
文を正しく完成させる答えを選択してください。

Answer Area

Microsoft Defender for Identity can identify advanced threats from  signals.

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

正解:

Answer Area

Microsoft Defender for Identity can identify advanced threats from  signals.

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

Explanation:

Answer Area

Microsoft Defender for Identity can identify advanced threats from  signals.

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

Microsoft Defender for Identity (formerly Azure ATP) is designed to protect on-premises identity infrastructures by analyzing signals from Active Directory Domain Services (AD DS). In Microsoft's SCI guidance, Defender for Identity is described as a "cloud service that uses sensors installed on your domain controllers to monitor

and analyze user activities and information across your on-premises Active Directory." The sensors "collect authentication, replication, and other security-relevant events and network traffic," enabling analytics to detect techniques such as Pass-the-Hash, Pass-the-Ticket, Golden Ticket, reconnaissance, lateral movement, and domain dominance. The product's purpose is to surface advanced threats, compromised identities, and malicious insider actions by continuously profiling and learning from AD DS behavior and security events.

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

質問: 95

文を正しく完成させる答えを選択してください。



正解:



Explanation:

access and application control

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

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

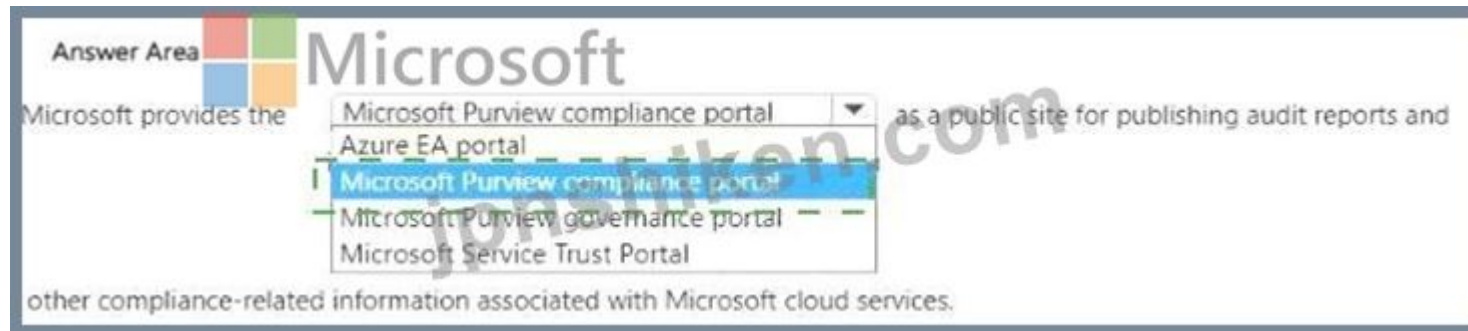
Container security targets container images and runtimes, and vulnerability assessment identifies software vulnerabilities but doesn't enforce allow-listing or time-bound access. Therefore, the correct completion is access and application control, which encompasses Adaptive application controls and JIT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

質問: 96

文を完成させます。



正解:



Explanation:



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

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

質問: 97

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

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

正解: B ([コメントを发表する](#))

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

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

質問: 98

エンドポイント データ損失防止 (エンドポイント DLP) を使用して管理できる 2 種類のデバイスはどれですか? それぞれの正解は完全なソリューションを示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

- A. Windows 11
- B. Linux
- C. iOS
- D. macOS
- E. Android

正解: ([正解を表示します](#))

Endpoint data loss prevention (Endpoint DLP), a feature in Microsoft Purview, supports Windows 10 and 11 and now also supports macOS for core DLP capabilities. It allows organizations to monitor and restrict actions like copying sensitive files to USBs, printing, or uploading to unapproved cloud services.

SCI Extract: " Endpoint DLP extends Microsoft Purview Data Loss Prevention to Windows 10, Windows 11, and macOS devices, allowing for monitoring and control of sensitive data usage at the endpoint. " Other platforms like Linux, iOS, and Android are not currently supported for Endpoint DLP

質問: 99

お客様は、Vnet1 という名前の仮想ネットワークを含む Azure サブスクリプションを所有しています。VNet1 には、Windows Server を実行し、パブリックにアクセス可能な VM1 という名前の仮想マシンが含まれています。

VM1が悪意のあるネットワーク攻撃の標的になった疑いがある。

VM1へのネットワークトラフィックを監視し、SYNパケット数などの攻撃メトリクスを収集し、新たな攻撃が開始された場合に自動的にアラートを生成する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。

何を使うべきでしょうか?

- A. Azure Application Gateway の診断
- B. Azure DDoS保護プラン
- C. Azure Monitor のメトリックとアラート
- D. Azure Network Watcher パケットキャプチャ

正解: ([正解を表示します](#))

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