Microsoft.SC-100J.v2023-10-16.q60

試験コード：	SC-100J
試験名称：	Microsoft Cybersecurity Architect (SC-100日本語版)
認証ベンダー：	Microsoft
無料問題の数：	60
バージョン：	v2023-10-16
ページの閲覧量：	391
問題集の閲覧量：	4260

https://www.jpnshiken.com/shiken/Microsoft.SC-100J.v2023-10-16.q60.html

質問**: 1**
Microsoft 365 サブスクリプションと Azure サブスクリプションをお持ちです。Microsoft 365 Defender と Microsoft Defender for Cloud が有効になっています。
Azure サブスクリプションには 50 台の仮想マシンが含まれています。各仮想マシンは Windows Server 2019 上で異なるアプリケーションを実行します。
承認されたアプリケーションのみが仮想マシン上で実行できるようにするソリューションを推奨する必要があります。許可されていないアプリケーションが実行またはインストールされようとすると、管理者がアプリケーションを許可するまで、そのアプリケーションは自動的にブロックされる必要があります。
どのセキュリティ制御を推奨する必要がありますか?
A. Azure Active Directory (Azure AD) 条件付きアクセス アプリ制御ポリシー
B. Microsoft Defender for Cloud Apps の OAuth アプリ ポリシー
C. Microsoft エンドポイント マネージャーのアプリ保護ポリシー
D. Microsoft Defender for Endpoint のアプリケーション制御ポリシー
正解**: (**正解を表示します**)**
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/select-types-of-rules-to-create#windows-defender-application-control-policy-rules

質問**: 2**
あなたは、Azure Front Door インスタンスを通じて Azure App Service Web アプリへのアクセスを提供するためのセキュリティ戦略を設計しています。
Web アプリが Front Door インスタンスを介したアクセスのみを許可するようにするソリューションを推奨する必要があります。
解決策: Front Door インスタンスのバックエンド IP アドレスからのトラフィックを許可するアクセス制限を推奨します。
これは目標を達成していますか?
A. いいえ
B. はい
正解**: (**正解を表示します**)**

質問: **3**
アプリケーションのセキュリティ要件を満たすために、アプリケーションはどの 2 つの認証方法をサポートする必要がありますか? 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. セキュリティ アサーション マークアップ言語 (SAML)
B. NTLMv2
C. 証明書ベースの認証
D. ケルベロス
正解: **A,D (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

質問: **4**
あなたの会社はクラウド導入の準備を進めています。
あなたは、Azure ランディング ゾーンのセキュリティを設計しています。
安全性スコアを向上させるために実装できる予防制御を 2 つ選択してください? 各注意: 正しい選択はそれぞれ 1 ポイントの価値があります。
A. Azure ファイアウォール
B. Azure Web アプリケーション ファイアウォール (WAF)
C. Microsoft Defender for Cloud アラート
D. Azure Active Directory (Azure AD Privileged Identity Management (PIM))
E. マイクロソフト センチネル
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

質問: **5**
Windows 11 デバイスと Microsoft 365 E5 ライセンスを持っています。
ギャンブル サイトなどのアダルト コンテンツを含む Web サイトにユーザーがアクセスできないようにするソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. Microsoft エンドポイント マネージャー
B. コンプライアンスマネージャー
C. クラウド アプリ向け Microsoft Defender
D. エンドポイント用 Microsoft Defender
正解: **(**正解を表示します**)**

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-worldwide#configure-web-content-filtering-policies

質問: **6**
あなたは、Azure にオンボードされたコンテナー化されたアプリケーションのセキュリティ標準を設計しています。Microsoft Defender for Containers の使用を評価しています。
Defender for Containers を使用して既知の脆弱性をスキャンできるのは、どの 2 つの環境ですか? 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. Azure Container Registry にデプロイされた Linux コンテナー
B. Azure Kubernetes Service (AKS) にデプロイされた Linux コンテナー
C. Azure Container Registry にデプロイされた Windows コンテナー
D. Azure Kubernetes Service (AKS) にデプロイされた Windows コンテナー
E. Azure Container Instances にデプロイされた Linux コンテナー
正解: **(正解を表示します)**
https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-security-requirements-for-containers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabilities-for-running-images

質問: **7**
Azure Pipelines と Azure Repos を使用して、アプリケーションを Azure にデプロイするための継続的インテグレーションおよび継続的デプロイメント (O/CD) ワークフローを実装します。Microsoft Cloud Adoption Framework for Azure の原則に基づいて、動的アプリケーション セキュリティ テスト (DAST) に何を含めるべきかを推奨する必要があります。何を勧めるべきですか?
A. 単体テスト
B. 侵入テスト
C. 依存関係のテスト
D. 脅威モデリング
正解: **(正解を表示します)**
Topic 2, Fabrikam, Inc
On-premises Environment
The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.
Azure Environment
Fabrikam has the following Azure resources:
* An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
* A single Azure subscription named Sub1

* A virtual network named Vnet1 in the East US Azure region
* A virtual network named Vnet2 in the West Europe Azure region
* An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
* A Microsoft Sentinel workspace
* An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
* 20 virtual machines that are configured as application servers and are NOT onboarded to Segment Microsoft Defender for Cloud
* A resource group named TestRG that is used for testing purposes only
* An Azure Virtual Desktop host pool that contains personal assigned session hosts All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-.
* An Azure AD tenant named contoso.onmicrosoft.com
* An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:
* Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
* Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
* Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification
* ClaimsApp will be deployed to Azure App Service instances that connect to Vnetl and Vnet2.
* Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
* ClaimsApp will access data in ClaimsDB.
* ClaimsDB must be accessible only from Azure virtual networks.
* The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:
* Azure DevTest labs will be used by developers for testing.
* All the application code must be stored in GitHub Enterprise.
* Azure Pipelines will be used to manage application deployments.
* All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.
Security Requirement
Fabrikam identifies the following security requirements:
* Internet-accessible applications must prevent connections that originate in North Korea.
* Only members of a group named InfraSec must be allowed to configure network security groups (NSGs} and instances of Azure Firewall, VJM. And Front Door in Sub1.
* Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.
AWS Requirements
Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.
* Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
* Ensure that the security administrators can query AWS service logs directly from the Azure environment.
Contoso Developer Requirements
Fabrikam identifies the following requirements for the Contoso developers;
* Every month, the membership of the ContosoDevelopers group must be verified.
* The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
* The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.
Compliance Requirement
Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

質問**: 8**
あなたの会社では、いくつかの Azure App Service Web アプリを展開する予定です。Web アプリは西ヨーロッパの Azure リージョンにデプロイされます。Web アプリには、ヨーロッパと米国の顧客のみがアクセスできます。
悪意のあるボットが Web アプリの脆弱性をスキャンするのを防ぐソリューションを推奨する必要があります。ソリューションでは、取り付け面を最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Azure Firewall Premium
B. Azure Application Gateway Web Application Firewall (WAF)

C. network security groups (NSGs)
D. Azure Traffic Manager and application security groups
正解**: D (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection

質問**: 9**
あなたの会社には、Microsoft 365 サブスクリプション、Azure サブスクリプション、アマゾン ウェブ サービス (AWS) 実装を含むマルチクラウド環境があります。次のコンポーネントに対してセキュリティ体制管理ソリューションを推奨する必要があります。
* Azure LOT Edge デバイス
* AWS EC2 インスタンス
どのサービスを推奨事項に含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。
正解**:**

質問**: 10**
あなたの会社は Microsoft 365 E5 ライセンスと Azure サブスクリプションを持っています。
同社は、次の場所に保存されている機密データに自動的にラベルを付けることを計画しています。
* Microsoft SharePoint Online
* Microsoft Exchange Online
*マイクロソフトチーム
機密データを特定して保護するための戦略を推奨する必要があります。
機密ラベル ポリシーにはどの範囲を推奨する必要がありますか? 答えるには、適切なスコープを正しい場所にドラッグします。各スコープは 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。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解**:**

質問**: 11**
あなたの会社には、オンプレミスの Active Directory ドメイン サービス (AD DS) フォレスト、Microsoft B65 サブスクリプション、および Azure サブスクリプションを含むハイブリッド クラウド インフラストラクチャがあります。
会社のオンプレミス ネットワークには、Kerberos 認証を使用する内部 Web アプリが含まれています。現在、Web アプリにはネットワークからのみアクセスできます。
Windows 11 を実行する個人用デバイスを持っているリモート ユーザーがいます。
リモート ユーザーが Web アプリにアクセスできるようにするソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* リモート ユーザーがネットワーク上の他のリソースにアクセスできないようにします。

* Azure Active Directory (Azure AD) 条件付きアクセスをサポートします。
* エンドユーザー エクスペリエンスを簡素化します。
推奨事項には何を含めるべきですか?
A. Azure AD アプリケーション プロキシ
B. Azure 仮想 WAN
C. Microsoft トンネル
D. Microsoft Defender for Endpoint の Web コンテンツ フィルター
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore

質問: **12**
Microsoft クラウド環境の場合、Microsoft Cybersecurity Reference Architectures (MCRA) に基づいてセキュリティ アーキテクチャを設計しています。次の攻撃チェーンの外部脅威から保護する必要があります。
* 攻撃者は外部 Web サイトにデータを流出させようとします。
* 攻撃者は、ドメインに参加しているコンピューター間で横方向の移動を試みます。
各脅威の推奨事項には何を含める必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
正解:

質問: **13**
Microsoft 365 E5 サブスクリプションをお持ちです。
機密データを含む電子メールの添付ファイルにウォーターマークを追加するソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. クラウド アプリ向け Microsoft Defender
B. インサイダーリスク管理
C. Microsoft 情報保護
D. アズール パービュー
正解: **C (**コメントを発表する**)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services,

such as SalesForce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

質問: **14**
あなたの会社はシアトルにオフィスを持っています。
同社には、異なる仮想ネットワークでホストされている 2 つの Azure 仮想マシン スケール セットがあります。
同社はインドで開発者と契約する予定だ。
Azure portal から SSL 経由で仮想マシンに接続できる機能を開発者に提供するソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* 仮想マシンのパブリック IP アドレスの公開を防止します。
* VPN を使用せずに接続する機能を提供します。
*コストを最小限に抑えます。
どの 2 つのアクションを実行する必要がありますか? それぞれの正解は、解決策の一部を示しています。
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. Azure Bastion を 1 つの仮想ネットワークにデプロイします。
B. Azure Bastion を各仮想ネットワークにデプロイします。
C. 仮想マシン上でジャストインタイム VM アクセスを有効にします。
D. 仮想ネットワーク ピアリングを使用してハブ アンド スポーク ネットワークを作成します。
E. Azure Firewall で NAT ルールとネットワーク ルールを作成します。
正解: **(正解を表示します)**
https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion

質問: **15**
Microsoft 365 サブスクリプションと Azure サブスクリプションをお持ちです。Microsoft 365 Defender と Microsoft Defender for Cloud が有効になっています。
Azure サブスクリプションには Microsoft Sentinel ワークスペースが含まれています。Microsoft Sentinel データ コネクタは、Microsoft 365、Microsoft 365 Defender、Defender for Cloud、および Azure 用に構成されています。
Windows Server を実行する Azure 仮想マシンをデプロイする予定です。
Microsoft Sentinel の拡張検出と応答 (EDR) およびセキュリティ オーケストレーション、自動化、および応答 (SOAR) 機能を有効にする必要があります。
各機能を有効にすることをどのように推奨しますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **16**
顧客は、4 つの Azure サブスクリプションにわたる 10 の Azure Kubernetes Service (AKS) リソースに Docker イメージをデプロイしています。あなたは顧客のセキュリティ体制を評価しています。
AKS リソースがセキュリティ スコアの推奨事項から除外されていることがわかります。正確な推奨事項を作成し、安全なスコアを更新する必要があります。
Microsoft Defender for Cloud で推奨すべき 2 つのアクションはどれですか? それぞれの正解は、解決策の一部を示しています。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. 自動プロビジョニングを構成します。
B. 法規制順守ポリシーを割り当てます。
C. 在庫を確認します。
D. ワークフローの自動化を追加します。
E. Defender プランを有効にします。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

質問: **17**
あなたの会社にはハイブリッド クラウド インフラストラクチャがあります。
データとアプリケーションはクラウド環境間で定期的に移動されます。
同社のオンプレミス ネットワークは、次の図に示すように管理されています。
あなたは、ハイブリッド クラウド インフラストラクチャをサポートするセキュリティ運用を設計しています。ソリューションは次の要件を満たす必要があります。
複数の環境にわたる仮想マシンとサーバーを管理します。
Azure ポリシー全体で、すべての環境のすべてのリソースに標準を適用します。
オンプレミス ネットワークに推奨する 2 つのコンポーネントはどれですか? それぞれの正解は、解決策の一部を示しています。
注意 正しい選択はそれぞれ 1 ポイントの価値があります。
A. Azure VPN ゲートウェイ
B. Azure Policy のゲスト構成
C. オンプレミス データ ゲートウェイ
D. アズールバスティオン

E. アズールアーク
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

質問: **18**
あなたの会社は、Azure Storage アカウントを使用して BLOB ストレージをプロビジョニングする予定です。BLOB ストレージには、インターネット上の 20 のアプリケーション 下水道からアクセスできます。アプリケーション サーバーのみがストレージ アカウントにアクセスできるようにするソリューションを推奨する必要があります。BLOB ストレージを保護するために何を使用することを推奨しますか?
A. ネットワーク セキュリティ グループ (NSG) のサービス タグ
B. ストレージ アカウントのファイアウォール ルール
C. Azure Web アプリケーション ファイアウォール (WAF) ポリシーの管理されたルール セット
D. ネットワーク セキュリティ グループ (NSG) の受信ルール
E. Azure Firewall の受信ルール
正解: **E (**コメントを発表する**)**

質問: **19**
次の図に示すように、Microsoft Defender for Cloud を開きます。
ドロップダウン メニューを使用して、図に示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **20**
あなたの会社は、Microsoft セキュリティのベスト プラクティスに基づいて、Microsoft Defender for Endpoint の使用を最適化し、ランサムウェアからリソースを保護したいと考えています。Microsoft セキュリティのベスト プラクティスの Microsoft Detection and Response Team (DART) のアプローチに基づいて、侵害されたコンピューターに対する侵害後の対応計画を準備する必要があります。
対応計画には何を含めるべきですか?
A. メモリスキャン
B. マシンの隔離
C. フォルダーアクセスの制御
D. ユーザーの分離
E. アプリケーションの分離
正解: **(**正解を表示します**)**

質問: **21**

アプリケーションの Azure ランディング ゾーンとして使用される Azure サブスクリプションがあります。ランディング ゾーン内のすべてのワークロードのセキュリティ体制を評価する必要があります。まず何をすべきでしょうか?
A. 継続的インテグレーション/継続的デプロイメント (CI/CD) の脆弱性スキャンを構成します。
B. Microsoft Defender for Cloud のすべてのリソースの種類に対して Defender プランを有効にします。
C. Microsoft Sentinel データ コネクタを追加します。
D. Azure Active Directory Premium Plan 2 ライセンスを取得します。
正解: **(**正解を表示します**)**

質問: **22**
あなたの会社は、リソースをランサムウェアから保護するために Azure の使用を最適化したいと考えています。
Azure Backup と Azure Storage のどの機能がランサムウェア攻撃に対して最も強力な保護を提供するかを推奨する必要があります。ソリューションは Microsoft セキュリティのベスト プラクティスに従う必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **23**
顧客は、Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを含むハイブリッド クラウド インフラストラクチャを所有しています。
境界ネットワーク内のすべてのオンプレミス サーバーは、インターネットに直接接続できません。
この顧客は最近、ランサムウェア攻撃から回復しました。
顧客は Microsoft Sentinel の導入を計画しています。
次の要件を満たす構成を推奨する必要があります。
* セキュリティ運用チームがセキュリティ ログと操作ログにアクセスできることを確認してください。
* IT 運用チームが、境界ネットワーク内のサーバーのイベント ログを含む運用ログのみにアクセスできるようにします。
推奨事項に含めることができる 2 つの構成はどれですか? 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. Microsoft Sentinel にリソースベースのロールベースのアクセス制御 (RBAC) を実装します。
B. Log Analytics エージェントを使用するカスタム コレクターを作成します。
C. Azure Active Directory (Azure AD) 条件付きアクセス ポリシーを構成します。
D. マルチホーミング構成で Azure Monitor エージェントを使用します。
正解: **A,D (**コメントを発表する**)**

質問: **24**
いくつかのレガシー アプリケーションを含むオンプレミス ネットワークがあります。アプリケーションは、既存のディレクトリ サービスに対して LDAP クエリを実行します。オンプレミスのインフラストラクチャをクラウドのみのインフラストラクチャに移行しています。
レガシー アプリケーションをサポートするインフラストラクチャ用の ID ソリューションを推奨する必要があります。ソリューションでは、インフラストラクチャを維持するための管理労力を最小限に抑える必要があります。
どの ID サービスを推奨事項に含めるべきですか?
A. Azure Active Directory Domain Services (Azure AD DS)
B. Azure Active Directory (Azure AD) B2C
C. Azure Active Directory (Azure AD)
D. Active Directory Domain Services (AD DS)
正解: **A (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview

質問: **25**
App Service Web アプリ接続の戦略を推奨する必要があります。ソリューションはランディング ゾーンの要件を満たしている必要があります。何を勧めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。注意 正しい選択はそれぞれ 1 ポイントの価値があります。
正解:

質問: **26**
ClaimsDetail テーブルの MedicalHistory データを保護するソリューションを推奨する必要があります。ソリューションは Contoso 開発者の要件を満たしている必要があります。
推奨事項には何を含めるべきですか?
A. 透過的データ暗号化 (TDE)
B. 常に暗号化
C. 行レベルのセキュリティ (RLS)
D. 動的データマスキング
E. データ分類
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-enclaves

質問: **27**
アプリケーション コードをスキャンするためのソリューションを推奨する必要があります。ソリューションはアプリケーション開発要件を満たしている必要があります。推奨事項には何を含めるべきですか?
A. Azure Key Vault

B. GitHub の高度なセキュリティ
C. Application Insights in Azure Monitor
D. Azure DevTest Labs
正解**: B (**コメントを発表する**)**
https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanced-security

質問**: 28**
Microsoft 365 サブスクリプションをお持ちです
次のアクティビティを監視するには、セキュリティ ソリューションを推奨する必要があります。
* 侵害された可能性のあるユーザー アカウント
* Microsoft SharePoint Online からファイルの一括ダウンロードを実行するユーザー 各アクティビティの推奨事項には何を含める必要がありますか? 答えるには、適切なコンポーネントを正しいアクティビティにドラッグします。各コンポーネントは 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。コンテンツを表示するには、ペイン間で分割バーをドラッグするか、スクロールする必要がある場合があります。
注: 各正解の選択は 1 ポイントの価値があります。
正解**:**

質問**: 29**
Azure Pipelines と Azure Repos を使用して、継続的インテグレーションと継続的デプロイ (CI/CO) ワークフローを実装します。
Microsoft Cloud Adoption Framework for Azure に基づいて、CI/CD ワークフローの段階を保護するためのベスト プラクティスを推奨する必要があります。
各段階の推奨事項には何を含めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解**:**

質問**: 30**
あなたの会社には、オンプレミス ネットワーク、Azure サブスクリプション、および Microsoft 365 E5 サブスクリプションがあります。同社は次のデバイスを使用しています。
* Windows 10 または Windows 11 を実行するコンピューター
* Android または iOS を実行するタブレットおよび携帯電話
データの保存場所に関係なく、Microsoft Office 365 の機密データを分類して暗号化するソリューションを推奨する必要があります。推奨事項には何を含めるべきですか?
A. 電子情報開示
B. 保存ポリシー
C. コンプライアンスマネージャー
D. Microsoft 情報保護

正解: (正解を表示します)
https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection
https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

質問: **31**
あなたの会社にはオンプレミスの Microsoft SQL Server データベースがあります。
同社はデータベースを Azure に移行する予定です。
パッチ適用のための運用要件を最小限に抑え、動的データ マスキングを使用して機密データを保護する、データベースの安全なアーキテクチャを推奨する必要があります。ソリューションではコストを最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Azure SQL マネージド インスタンス
B. Azure 仮想マシン上の SQL Server
C. Azure SQL データベース
D. Azure Synapse Analytics 専用 SQL プール
正解: (正解を表示します)

質問: **32**
Azure Storage を使用する Azure サブスクリプション。
同社は特定の BLOB をベンダーと共有する予定です。BLOB を公に公開せずに、特定の BLOB への安全なアクセスをベンダーに提供するソリューションを推奨する必要があります。アクセスは t\me-Vim\ted である必要があります。推奨事項には何を含めるべきですか?
A. カスタマー マネージド キー (CMK) を使用して暗号化を構成する
B. プライベートリンク接続を設定します。
C. アクセスキーの接続文字列を共有します。
D. 共有アクセス署名 (SAS) を作成します。
正解: (正解を表示します)

質問: **33**
次の図に示すように、顧客は Azure を使用して、外部ユーザーが使用するモバイル アプリを開発しています。

アプリの ID 戦略を設計する必要があります。ソリューションは次の要件を満たす必要があります。
* Google、Facebook、Microsoft アカウントなどの外部 ID の使用を有効にします。
※顧客のアイデンティティストアとは別に管理されます。
* 各アプリの完全にカスタマイズ可能なブランディングをサポートします。
デザインを完成させるためにどのサービスをお勧めしますか?
A. Azure Active Directory (Azure AD) B2C
B. Azure Active Directory (Azure AD) B2B
C. Azure AD コネクト
D. Azure Active Directory ドメイン サービス (Azure AD DS)
正解**: (**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow
https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

質問**: 34**
Microsoft 365 E5 サブスクリプションと Azure サブスクリプトを持っている。次のコンポーネントの全体的なセキュリティ体制を強化するには、既存の環境を評価する必要があります。
* Microsoft Intune によって管理される Windows 11 デバイス
* Azure ストレージ アカウント
* Azure仮想マシン
コンポーネントを評価するには何を使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
正解**:**

質問**: 35**
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。アマゾン ウェブ サービス (AWS) が実装されています。
Azure のセキュリティ戦略を AWS の実装に拡張することを計画しています。このソリューションでは Azure Arc は使用されません。AWS リソースのセキュリティを提供するために使用できる 3 つのサービスはどれですか? 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. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
B. Azure Active Directory (Azure AD) 条件付きアクセス
C. サーバー用 Microsoft Defender
D. Azure ポリシー
E. コンテナー用 Microsoft Defender
正解**: (**正解を表示します**)**

https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=aws-eks

質問: **36**
ClaimsApp のセキュリティを評価しています。
次の各ステートメントについて、そのステートメントが 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。
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。
正解:

質問: **37**
SharePoint Online と Exchange Online のデータを保護するための戦略を設計する必要があります。ソリューションはアプリケーションのセキュリティ要件を満たしている必要があります。
戦略で活用すべき 2 つのサービスはどれですか? それぞれの正解は、解決策の一部を示しています。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. Azure AD 条件付きアクセス
B. クラウド アプリ向け Microsoft Defender
C. クラウド用 Microsoft Defender
D. エンドポイント用 Microsoft Defender
E. Azure AD でのアクセスレビュー
正解: **(正解を表示します)**
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#conditional-access-application-control
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cloud-application-security

質問: **38**
litware.com フォレストを保護するための戦略を推奨する必要があります。ソリューションは ID 要件を満たしている必要があります。推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。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。
正解:

質問: **39**
Microsoft クラウド環境の場合、Microsoft クラウド セキュリティ ベンチマークに基づいてセキュリティ アーキテクチャを設計しています。
Azure セキュリティ ベンチマークに基づく ID 管理の 3 つのベスト プラクティスは何ですか? 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. アプリケーション ID を安全かつ自動的に管理します。

B. ID と資格のライフサイクルを管理する
C. 集中型の ID および認証システムを使用します。
D. ID とアクセス管理のための脅威検出を有効にします。
E. ID および認証システムを保護します。
正解: **A,C,E (**コメントを発表する**)**

質問: **40**
顧客は Microsoft 365 E5 サブスクリプションと Azure サブスクリプションを持っています。
お客様は、セキュリティ インシデントを一元管理し、ログを分析し、アクティビティを監査し、展開されているすべてのサービスにわたる潜在的な脅威を検索したいと考えています。
顧客にソリューションを推奨する必要があります。ソリューションではコストを最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. Microsoft 365 Defender
B. Microsoft Defender for Cloud Apps
C. Microsoft Sentinel
D. Microsoft Defender for Cloud
正解: **(**正解を表示します**)**

質問: **41**
ハイブリッド クラウド インフラストラクチャがあります。
次の表に示す Azure アプリケーションをデプロイする予定です。
各アプリの要件を満たすには何を使用する必要がありますか? 回答するには、回答内の適切な選択肢を選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **42**
あなたの会社には、Windows 10、Windows 11、または Windows Server のいずれかを実行するデバイスがあります。
あなたはデバイスのセキュリティ体制を改善しているところです。
Microsoft Security Compliance Toolkit のセキュリティ ベースラインを使用する予定です。
ベースラインと現在のデバイス構成を比較するには何を使用することをお勧めしますか?
A. Microsoft Intune
B. ポリシーアナライザー
C. ローカル グループ ポリシー オブジェクト (LGPO)
D. Windows オートパイロット
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10

質問: **43**
あなたの会社は Microsoft 365 サブスクリプションを持っており、ID に Microsoft Defender を使用しています。ID の侵害に関連するインシデントについて通知されます。
攻撃者が悪用できるように複数のアカウントを公開するソリューションを推奨する必要があります。攻撃者がアカウントを悪用しようとした場合、アラートをトリガーする必要があります。どの Defender for Identity 機能を推奨事項に含めるべきですか?
A. スタンドアロンセンサー
B. ハニートークン エンティティ タグ
C. 機密ラベル
D. カスタム ユーザー タグ
正解: **(正解を表示します)**
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

質問: **44**
コンプライアンス要件を満たすソリューションを推奨する必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **45**
Microsoft 365 サブスクリプションと Azure サブスクリプションを持つ顧客がいます。
顧客は、Windows、iOS、Android、または macOS のいずれかを実行するデバイスを持っています。Windows デバイスはオンプレミスと Azure にデプロイされます。
すべてのデバイスが顧客のコンプライアンス ルールを満たしているかどうかを評価するセキュリティ ソリューションを設計する必要があります。
ソリューションには何を含めるべきでしょうか?
A. Microsoft 情報保護
B. エンドポイント用 Microsoft Defender
C. マイクロソフト センチネル
D. Microsoft エンドポイント マネージャー
正解: **(正解を表示します)**
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

質問: **46**

Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。不審な認証アクティビティのアラートがワークロード保護ダッシュボードに表示されます。
ワークフローの自動化を使用してアラートを評価および修正するソリューションを推奨する必要があります。ソリューションでは、開発労力を最小限に抑える必要があります。推奨事項には何を含めるべきですか?
A. Azure Monitor webhooks
B. Azure Logics Apps
C. Azure Event Hubs
D. Azure Functions apps
正解: **(**正解を表示します**)**
The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems. With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

質問: **47**
InfraSec グループのセキュリティ要件を満たすソリューションを推奨する必要があります。アクセスを委任するには何を使用する必要がありますか?
A. リソースグループ
B. カスタムのロールベースのアクセス制御 (RBAC) ロール
C. 管理グループ
D. サブスクリプション
正解: **(**正解を表示します**)**

質問: **48**
Litware の Azure AD テナントに ID セキュリティ ソリューションを推奨する必要があります。ソリューションは、ID 要件と法規制遵守要件を満たしている必要があります。
何を勧めるべきですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **49**
あなたの会社はビッグ データ ソリューションを Azure に移行しようとしています。
同社は次のストレージ ワークロードを使用する予定です。
* Azure Storage BLOB コンテナー
* Azure データ レイク ストレージ Gen2
* Azure Storage ファイル共有
* Azure ディスク ストレージ
Azure Active Directory (Azure AD) を使用した認証をサポートする 2 つのストレージ ワークロードはどれですか?
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. Azure ディスク ストレージ
B. Azure Storage BLOB コンテナー
C. Azure Storage ファイル共有
D. Azure Data Lake Storage Gen2
正解: **B,D (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory
https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

質問: **50**
顧客はゼロ トラスト モデルに従い、企業アプリケーションへのアクセスを試みるたびに明示的に検証します。
顧客は、いくつかのエンドポイントがマルウェアに感染していることを発見しました。
顧客は、感染したエンドポイントからのアクセス試行を一時停止します。
マルウェアはエンドポイントから削除されます。
エンドポイント ユーザーが企業アプリケーションに再びアクセスするには、どの 2 つの条件を満たす必要がありますか? それぞれの正解は、解決策の一部を示しています。
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. Microsoft Defender for Endpoint はエンドポイントを準拠していると報告します。
B. Microsoft Intune はエンドポイントを準拠していると報告します。
C. 新しい Azure Active Directory (Azure AD) 条件付きアクセス ポリシーが適用されます。
D. クライアント アクセス トークンが更新されます。
正解: **C,D (**コメントを発表する**)**
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/
https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

質問: **51**

複数のストレージ アカウントを含む Azure サブスクリプションがあります。ストレージ アカウントには、アクセス キーを使用して認証される従来のアプリケーションによってアクセスされます。
新しいアプリケーションがストレージ アカウントのアクセス キーを取得できないようにするソリューションを推奨する必要があります。ソリューションでは、レガシー アプリケーションへの影響を最小限に抑える必要があります。
推奨事項には何を含めるべきですか?
A. ストレージ アカウントに読み取り専用ロックを適用します。
B. AllowSharcdKeyAccess プロパティを false に設定します。
C. AllowBlobPublicAcccss プロパティを false に設定します。
D. 自動キーローテーションを設定します。
正解**: A (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

質問**: 52**
Azure Cosmos DB Core (SQL) API アカウントのセキュリティ要件を計画しています。Azure Cosmos DB アカウントのデータにアクセスするすべてのユーザーを監査するソリューションを推奨する必要があります。推奨事項に含めるべき 2 つの構成はどれですか? それぞれの正解は、解決策の一部を示しています。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. Cosmos DB に対して Microsoft Defender を有効にします。
B. Azure Active Directory (Azure AD) のサインイン ログを Log Analytics ワークスペースに送信します。
C. Azure Cosmos DB のローカル認証を無効にします。
D. ID 用に Microsoft Defender を有効にします。
E. Azure Cosmos DB ログを Log Analytics ワークスペースに送信します。
正解**: B,C (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs

質問**: 53**
Microsoft Defender for Cloud が Azure 管理グループに割り当てられています。
Microsoft Sentinel を展開しています。
アラートのトリアージ中に、修復の提案など、セキュリティ イベントに関する追加情報が必要になります。目標を達成するために使用できる 2 つのコンポーネントはどれですか? 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. Defender for Cloud のワークロード保護
B. Defender for Cloud の脅威インテリジェンス レポート
C. Microsoft Sentinel ノートブック
D. Microsoft Sentinel 脅威インテリジェンス ワークブック
正解**: (**正解を表示します**)**

https://docs.microsoft.com/en-us/azure/sentinel/understand-threat-intelligence
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

質問: **54**
Microsoft Defender for Cloud が有効になっている Azure サブスクリプションがあります。
Azure セキュリティ ベンチマーク V3 レポートを評価しています。
安全な管理ポート制御では、潜在的な 8 ポイントのうち 0 ポイントを持っていることがわかります。
安全な管理ポート制御のスコアを向上させる構成を推奨する必要があります。
解決策: すべての仮想マシンでジャストインタイム (JIT) VM アクセスを有効にすることをお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **A (**コメントを発表する**)**
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions

質問: **55**
管理者に仮想マシンへの安全なリモート アクセスを提供するソリューションを設計する必要があります。ソリューションは次の要件を満たす必要があります。
* インターネットからのポート 3389 および 22 を有効にする必要がなくなります。
* 必要な場合にのみ、仮想マシンへの接続許可を提供します。
* 管理者は必ず Azure portal を使用して仮想マシンに接続してください。
ソリューションに含めるべき 2 つのアクションはどれですか? それぞれの正解は、解決策の一部を示しています。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. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) ロールを仮想マシン共同作成者として有効にします。
B. Azure VPN ゲートウェイを構成します。
C. Just Enough Administration (JEA) を有効にします。
D. ジャストインタイム (JIT) VM アクセスを有効にします。
E. Azure Bastion を構成します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2 https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

質問: **56**

ランディング ゾーンからインターネットに向かうトラフィックをルーティングするための戦略を推奨する必要があります。ソリューションはランディング ゾーンの要件を満たしている必要があります。
ランディング ゾーン展開の一部として何を推奨する必要がありますか?
A. サービスチェーン
B. ローカルネットワークゲートウェイ
C. 強制トンネリング
D. VNet 間接続
正解: **A (**コメントを発表する**)**
https://docs.microsoft.com/en-us/learn/modules/configure-vnet-peering/5-determine-service-chaining-uses

質問: **57**
あなたの会社は、Azure Pipelines と Azure Repos を使用して、アプリケーションを Azure にデプロイするための継続的インテグレーションと継続的デプロイメント (CI/CD) ワークフローを実装しています。
Azure 向け Microsoft Cloud Adoption Framework の DevSecOps 制御ガイダンスに合わせて展開プロセスを更新しています。
すべてのコード変更が CI/CD ワークフローによってデプロイされる前に、プル リクエストを使用して確実に送信されるようにするソリューションを推奨する必要があります。
推奨事項には何を含めるべきですか?
A. Azure ポリシー
B. カスタム Azure ロール
C. Azure Pipelines のカスタム ロール
D. Azure Repos のブランチ ポリシー
正解: **(**正解を表示します**)**

質問: **58**
次のコンポーネントを含む Azure ランディング ゾーンの監査ソリューションを設計しています。
* Azure SQL データベースの SQL 監査ログ
* Azure 仮想マシンからの Windows セキュリティ ログ
* App Service Web アプリからの Azure App Service 監査ログ
ランディング ゾーンに対して集中ログ ソリューションを推奨する必要があります。ソリューションは次の要件を満たす必要があります。
* すべての特権アクセスをログに記録します。
* ログは少なくとも 365 日間保持します。
*コストを最小限に抑えます。
推奨事項には何を含めるべきですか? 回答するには、回答内の適切な選択肢を選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
正解:

質問: **59**
あなたは、Azure Front Door インスタンスを通じて Azure App Service Web アプリへのアクセスを提供するためのセキュリティ戦略を設計しています。
Web アプリが Front Door インスタンスを介したアクセスのみを許可するようにするソリューションを推奨する必要があります。
解決策: ゲートウェイが必要な仮想ネットワーク統合を構成することをお勧めします。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance

質問: **60**
あなたの会社は Microsoft 365 E5 サブスクリプションを持っています。
同社は、Windows 10 を実行するモバイル セルフサービス キオスクを 45 台導入する予定です。キオスクを保護するための推奨事項を提供する必要があります。ソリューションは次の要件を満たす必要があります。
* 許可されたアプリケーションのみがキオスク上で実行できるようにしてください。
* 新しい脅威に対してキオスクを定期的に強化します。
推奨事項に含めるべき 2 つのアクションはどれですか? それぞれの正解は、解決策の一部を示しています。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. キオスクを Azure Monitor にオンボードします。
B. キオスクに特権アクセス ワークステーション (PAW) を実装します。
C. Microsoft Defender for Endpoint に自動調査と修復 (AIR) を実装します。
D. Microsoft Defender for Endpoint で脅威と脆弱性の管理を実装します。
E. キオスクを Microsoft Intune および Microsoft Defender for Endpoint にオンボードします。
正解: **(**正解を表示します**)**
(https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerability-management?view=o365-worldwide)