Microsoft.SC-100.v2024-08-24.q113

試験コード:	SC-100
試験名称:	Microsoft Cybersecurity Architect
認定資格:	Microsoft
無料問題数:	113
バージョン:	v2024-08-24
アクセス数:	540
ページビュー数:	1130
https://www.jpnpdf.com/Microsoft.SC-100.v2024-08-24.q113-mondaishu.html	

最新問題: **1**
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。注記; 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **2**
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。
Answer:

最新問題: **3**
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。
Answer:

最新問題: **4**
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。
ユーザーは、共有とコラボレーションに Microsoft Teams、Exchange Online、SharePoint Online、OneDrive を使用します。
同社は、保存された文書および通信内の保護された健康情報 (PHI) を特定します。
PHI が社外で共有されるのを防ぐには、何を使用することを推奨しますか?
A. インサイダー リスク管理ポリシー
B. データ損失防止 (DLP) ポリシー
C. 秘密度ラベル ポリシー
D. 保持ポリシー
Answer: C (メーッセージを残す**)**
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

最新問題: **5**
あなたの会社は、Azure 向け Microsoft Cloud Adoption Framework の DevSecOps ベスト プラクティスに従って、DevSecOps プロセスを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 (CI/CD) DevOps パイプラインに統合する予定です。DevOps の各段階にどのセキュリティ関連タスクを統合するかを推奨する必要があります。パイプライン。
何を勧めるべきでしょうか？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。
Answer:

最新問題: **6**
あなたの会社には Microsoft 365 E5 サブスクリプション、Azure サブスクリプション、オンプレミス アプリケーション、および Active Directory ドメイン サービス (AD DSV) があります。次の要件を満たす ID セキュリティ戦略を推奨する必要があります。
* 顧客が Facebook 資格情報を使用して Azure App Service Web サイトへの認証を行えることを保証します
* パートナー企業が、割り当てられているプロジェクトの Microsoft SharePoint Online サイトにアクセスできるようにします。ソリューションでは、追加のインフラストラクチャ コンポーネントを展開する必要性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? 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。
Answer:

最新問題: **7**
オンプレミス ネットワークには、Angular と Nodejs で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行す

る予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。
Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロトラスト モデルに従う必要があります。
解決策: 資格情報を保存するには、Azure Key Vault を実装することをお勧めします。
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
説明
Azure が提供する PaaS サービス (Azure Storage、Azure Cosmos DB、Azure Web App など) を使用する場合は、PrivateLink 接続オプションを使用して、すべてのデータ交換がプライベート IP 空間経由で行われ、トラフィックが Microsoft ネットワークから出ないようにする必要があります。

最新問題**: 8**
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。
次の図に示すように、Azure Security Benchmark V3 レポートを評価しています。
Windows を実行するすべての仮想マシンにサーバー用 Microsoft Defender がインストールされているかどうかを確認する必要があります。どのコンプライアンス管理を評価する必要がありますか?
A. エンドポイント セキュリティ
B. データ保護
C. インシデント対応
D. ポスチャと脆弱性の管理
E. 資産管理
Answer: A (メーッセージを残す**)**

最新問題**: 9**
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、回答内の適切なオプションを選択してください。
ａ． 注正しく選択するたびに 1 ポイントの価値があります。

Answer:

最新問題**: 10**
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. 共有アクセス署名 (SAS) を作成します。
B. アクセス キーの接続文字列を共有します。
C. プライベート リンク接続を構成します。
D. カスタマー マネージド キー (CMK) を使用して暗号化を構成します。
Answer: D (メーッセージを残す**)**
トピック 2、Fabrikam, Inc
オンプレミス環境
オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Azure環境
Fabrikam には次の Azure リソースがあります。
* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnetl という名前の仮想ネットワーク
* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。
パートナー
Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続し

ます。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。
ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。
コンプライアンスイベント
Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修復されています。
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。
アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。

* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題: **11**
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
Answer: A (メーッセージを残す**)**

最新問題: **12**
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。あなたは Microsoft Sentinel 展開を設計しています。
セキュリティ運用チームにソリューションを推奨する必要があります。ソリューションには、セキュリティ イベントを分析するためのカスタム ビューとダッシュボードが含まれている必要があります。Microsoft Sentinel で何を使用することをお勧めしますか?
A. ワークブック

B. 脅威インテリジェンス
C. ノートブック
D. プレイブック
Answer: (解答を表示する**)**

最新問題**: 13**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャ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? 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。
Answer:

最新問題**: 14**
セキュリティ アクセス戦略のセキュリティ レベルを計画しています。
どのジョブロールをどのセキュリティレベルで設定するかを特定する必要があります。ソリューションは、Microsoft Cybersecurity Reference Architectures (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。各職務に
どのセキュリティレベルを設定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。
注: 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題**: 15**
管理された環境全体にわたる法規制への準拠を評価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、法規制遵守要件とビジネス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。
Answer:

最新問題**: 16**
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. ユーザーの分離
B. メモリスキャン
C. アプリケーションの分離
D. 制御されたフォルダー アクセス
E. マシンの分離
Answer: E (メーッセージを残す**)**

最新問題: **17**
Contoso 開発者の要件を満たすには、Azure AD で何を作成する必要がありますか?
Answer:

最新問題: **18**
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。
Answer:

最新問題: **19**
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 ID を持つ HTTP ヘッダーに基づいてアクセス制限を行う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
Answer: A (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend-to-only-azure-正面玄関−

最新問題**: 20**
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. Microsoft センチネル
C. エンドポイント用 Microsoft Defender
D. Microsoft エンドポイント マネージャー
Answer: (解答を表示する**)**

最新問題**: 21**
Azure サブスクリプションとオンプレミス データセンターがあります。データセンターには、Windows Server を実行する 100 台のサーバーが含まれています。AJI サーバーは、Azure Backup と Microsoft Azure Recovery Services (MARS) エージェントを使用して Recovery Services コンテナーにバックアップされます。
オンプレミス サーバーを暗号化するランサムウェア攻撃に対する回復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 Microsoft セキュリティのベスト プラクティスに従い、次のリスクから保護する必要があります。
* 侵害された管理者アカウントは、サーバーを暗号化する前に Azure Backup からバックアップを削除するために使用されました
* サーバーを暗号化する前に MARS エージェントのバックアップを無効にするために侵害された管理者アカウントが使用されました 各リスクに対して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。
注: 正しく選択するたびに 1 ポイントの価値があります
Answer:

最新問題**: 22**
仮想マシン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。推奨事項には何を含めるべきですか?
A. Azure Bastion ホスト

B. ネットワーク セキュリティ グループ (NSG)
C. ジャストインタイム (JIT) VM アクセス
D. Azure 仮想デスクトップ
Answer: D (メーッセージを残す)
この質問で満たす必要があるセキュリティ要件は、"セキュア ホストはカスタム オペレーティング システム イメージからプロビジョニングされる必要がある」です。https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image

最新問題**: 23**
仮想マシンの問題を解決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? (2つ選択してください)
A. 仮想マシンを Microsoft Defender for Endpoint にオンボードします。
B. 仮想マシンを Azure Arc にオンボードします。
C. Microsoft エンドポイント マネージャーでデバイス コンプライアンス ポリシーを作成します。
D. Defender for Cloud で Qualys スキャナーを有効にします。
Answer: A,C (メーッセージを残す)
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide

最新問題**: 24**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
あなたは、Azure リソースの保存データの暗号化標準を設計しています。
保存データが AES-256 キーを使用して暗号化されるように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、暗号化キーの毎月のローテーションをサポートする必要があります。
解決策: Azure SQL データベースの場合は、Microsoft マネージド キーを使用する透過的データ暗号化 (TDE) 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
Answer: (解答を表示する)

最新問題**: 25**

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。
Answer:

最新問題**: 26**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
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 VMAccess 拡張機能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
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions アダプティブネットワークの強化: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify-network-security-configuration
トピック 2、Fabrikam, Inc
オンプレミス環境
オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Azure環境
Fabrikam には次の Azure リソースがあります。
* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnet1 という名前の仮想ネットワーク

* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。

パートナー

Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続します。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。

ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。

コンプライアンスイベント

Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修復されています。

※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。

問題の声明

Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。

すべての仮想マシンが Defender for Cloud に準拠している必要があります。

ClaimApp の導入

Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。

アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。
* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題**: 27**
ClaimsDB への接続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。

それぞれの要件に対して何を使用することを推奨しますか? 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。
Answer:

最新問題: **28**
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
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure-front-door-instance

最新問題: **29**
ClaimsDB への接続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。
それぞれの要件に対して何を使用することを推奨しますか? 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。
Answer:

最新問題: **30**
Microsoft セキュリティのベスト プラクティスに従ってランサムウェア対応計画を設計しています。ロックアウトされることなくランサムウェア攻撃の被害範囲を制限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. 特権アクセス ワークステーション (PAW)
B. Microsoft Azure のカスタマー ロックボックス
C. デバイスのコンプライアンス ポリシー
D. 緊急アクセス アカウント
Answer: D (メーッセージを残す**)**

最新問題: **31**
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。
Answer:

最新問題: **32**
ビジネス要件とハイブリッド要件を満たすマルチテナントおよびハイブリッド 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。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: 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **33**
Contoso 開発者の要件を満たすには、Azure AD で何を作成する必要がありますか?
Answer:

最新問題: **34**
あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。
* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。
* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。
ソリューションには何を含めるべきでしょうか? 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。

Answer:

最新問題**: 35**
Azure リソースの保存データの暗号化標準を設計している場合、保存データが AES-256 キーを使用して暗号化されるように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、暗号化キーの毎月のローテーションをサポートする必要があります。
解決策: Azure SQL データベースの場合は、カスタマー マネージド キー (CMK) を使用する透過的データ暗号化 (TDE) をお勧めします。
これは目標を達成していますか?
A. いいえ
B. はい
Answer: (解答を表示する**)**

最新問題**: 36**
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
Answer: A,B (メーッセージを残す**)**
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

最新問題**: 37**
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。
Answer:

最新問題: **38**
ClaimsDB への接続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。
それぞれの要件に対して何を使用することを推奨しますか? 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。
Answer:

最新問題: **39**
オンプレミス ネットワークには、Angular と Node.js で開発された e コマース Web アプリが含まれています。Web アプリは MongoDB データベースを使用します。Web アプリを Azure に移行する予定です。ソリューション アーキテクチャ チームは、Azure ランディング ゾーンとして次のアーキテクチャを提案します。
Web アプリとデータベース間の接続を保護するための推奨事項を提供する必要があります。ソリューションはゼロトラスト モデルに従う必要があります。
解決策: Azure Web アプリケーション ファイアウォール (WAF) を使用して Azure Front Door を実装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
Answer: (解答を表示する**)**
https://www.varonis.com/blog/securing-access-azure-webapps

最新問題: **40**
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。
Answer:

最新問題: **41**
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
Answer: B (メーッセージを残す**)**
https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeytoken-activity Sensitive タグは、価値の高い資産を識別するために使用されます。(ユーザー / デバイス / グループ)ハニートークン エンティティは悪意のある攻撃者の罠として使用されます。これらのハニートークン エンティティに関連付けられた認証により、アラートがトリガーされます。Defender for Identity は、Exchange サーバーを価値の高い資産と見なし、自動的に機密としてタグ付けします。

最新問題**: 42**
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。
Answer:

最新問題**: 43**
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。
Answer:

最新問題**: 44**
セキュリティ アクセス戦略のセキュリティ レベルを計画しています。
どのジョブロールをどのセキュリティレベルで設定するかを特定する必要があります。ソリューションは、Microsoft Cybersecurity Reference Architectures (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。
各職務にどのセキュリティ レベルを設定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。
注: 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題**: 45**

ハイブリッド要件、Microsoft Sentinel 要件、および法規制遵守要件を満たす SIEM および SOAR 戦略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。
Answer:

最新問題: **46**
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。注記; 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **47**
仮想マシンの問題を解決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? (2つ選択してください)
A. 仮想マシンを Microsoft Defender for Endpoint にオンボードします。
B. 仮想マシンを Azure Arc にオンボードします。
C. Microsoft エンドポイント マネージャーでデバイス コンプライアンス ポリシーを作成します。
D. Defender for Cloud で Qualys スキャナーを有効にします。
Answer: (解答を表示する**)**
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-w

最新問題: **48**
Azure 環境のコンプライアンスを評価しています。
リソースを変更せずにコンプライアンスを評価するために使用できる Azure Policy 実装を設計する必要があります。
Azure Policy ではどの効果を使用する必要がありますか?
A. 拒否
B. 無効
C. 変更
D. 追加

Answer: B (メーッセージを残す)
説明
新しいポリシー定義を使用して新規または更新されたリソースを管理する前に、テスト リソース グループなど、既存のリソースの限られたサブセットがどのように評価されるかを確認することをお勧めします。ポリシー割り当てで強制モードを無効 (DoNotEnforce) に設定すると、効果がトリガーされたり、アクティビティ ログ エントリが作成されたりするのを防ぐことができます。
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/evaluate-impact

最新問題: **49**
あなたは、クラウドのみの環境用のセキュリティ アーキテクチャを設計しています。
あなたは、Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) に基づいて、Microsoft 365 Defender と他の Microsoft クラウド サービスの間の統合ポイントを検討しています。
どの Microsoft クラウド サービスが Microsoft 365 Defender と直接統合され、次の要件を満たすかを推奨する必要があります。
* Microsoft 365 Defender ポータルから直接管理できるデータ損失防止 (DLP) ポリシーを適用します。
* 統合アラートによるユーザーおよびエンティティ行動分析 (UEBA) に基づいてセキュリティ脅威を検出し、対応します。
各要件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。
Answer:

最新問題: **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. クライアント アクセス トークンが更新されます。
D. 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。
Answer: C,D (メーッセージを残す)

最新問題: **51**

Azure リソースの保存データの暗号化標準を設計しています。
保存データが AES-256 キーを使用して暗号化されるように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、暗号化キーの毎月のローテーションをサポートする必要があります。
解決策: Azure SQL データベースの場合は、カスタマー マネージド キー (CMK) を使用する透過的データ暗号化 (TDE) をお勧めします。
これは目標を達成していますか?
A. いいえ
B. はい
Answer: B (メーッセージを残す**)**

最新問題**: 52**
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 Bastion を構成します。
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. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) ロールを仮想マシンの共同作成者として有効にします。
E. ジャストインタイム (JIT) VM アクセスを有効にします。
Answer: (解答を表示する**)**

最新問題**: 53**
あなたの会社には、Microsoft Defender for Cloud のセキュリティが強化された Azure サブスクリプションがあります。
同社は米国政府と契約を締結しました。NIST 800-53 に準拠するために現在のサブスクリプションを確認する必要があります。まず何をすべきでしょうか?
A. Defender for Cloud から、監査レポートの Azure セキュリティ ベースラインを確認します。
B. Defender for Cloud から、セキュリティ スコアの推奨事項を確認します。
C. Azure Policy から、サブスクリプションのスコープを持つ組み込みイニシアチブを割り当てます。
D. Defender for Cloud から、Defender for Cloud プランを有効にします。
Answer: C (メーッセージを残す**)**
説明

https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regulat

最新問題: **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. いいえ
B. はい
Answer: B (メーッセージを残す**)**

最新問題: **55**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。
App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャ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? 回答するには、回答内の適切なオプションを選択してください。
ａ. 注正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **56**
従来のオペレーショナル テクノロジー (OT) デバイスと LoT デバイスがあります。
Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) に基づいて、ゼロ トラスト原則を OT および LoT デバイスに適用するためのベスト プラクティスを推奨する必要があります。ソリューションは、業務運営を中断するリスクを最小限に抑える必要があります。
推奨事項に含めるべき 2 つのセキュリティ手法はどれですか? 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. ソフトウェアのパッチ適用
B. パッシブなトラフィック監視
C. 脅威の監視
D. アクティブなスキャン

Answer: (解答を表示する)

最新問題: **57**
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 ポリシー全体の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
Answer: B,E (メーッセージを残す)
説明
https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

最新問題: **58**
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、Microsoft Teams、SharePoint Online、および Exchange Online のデータを識別して分類したいと考えています。機密情報を含む文書を識別するための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. データ分類コンテンツ エクスプローラー
B. 電子情報開示
C. データ損失防止 (DLP)
D. 情報ガバナンス
Answer: A (メーッセージを残す)

最新問題: **59**
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 Monitor の Application Insights
B. GitHub の高度なセキュリティ
C. Azure DevTest Labs

D. Azure Key Vault
Answer: C (メーッセージを残す**)**

最新問題**: 60**
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。
Answer:

最新問題**: 61**
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。
次の図に示すように、Azure Security Benchmark V3 レポートを評価しています。
Windows を実行するすべての仮想マシンにサーバー用 Microsoft Defender がインストールされているかどうかを確認する必要があります。どのコンプライアンス管理を評価する必要がありますか?
A. データ保護
B. インシデント対応
C. ポスチャと脆弱性の管理
D. 資産管理
E. エンドポイント セキュリティ
Answer: (解答を表示する**)**
説明
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

最新問題**: 62**

ビジネス要件とハイブリッド要件を満たすマルチテナントおよびハイブリッド 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。何を勧めるべきですか? 回答するには、回答内の適切なオプションを選択してください。
ａ．注正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題**: 63**
管理された環境全体にわたる法規制への準拠を評価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、法規制遵守要件とビジネス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。
Answer:

最新問題**: 64**
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。
Answer:

最新問題**: 65**
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。
最高コンプライアンス責任者は、職場環境におけるプライバシー管理を強化する予定です。プライバシー管理を強化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。
* 未使用の個人データを特定し、ユーザーがデータの取り扱いに関する賢明な決定を下せるようにします。
* ユーザーが Microsoft Teams で個人データを送信するときに、ユーザーに通知とガイダンスを提供します。
* プライバシー リスクを軽減するための推奨事項をユーザーに提供します。
推奨事項には何を含めるべきですか?
A. 高度な電子情報開示
B. インサイダーリスク管理におけるコミュニケーションコンプライアンス
C. Microsoft Viva Insights
D. Microsoft Priva でのプライバシー リスク管理

Answer: (解答を表示する)

最新問題**: 66**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャ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? 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。
Answer:
説明
ボックス 1 は Azure AD アプリケーションです
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app ボックス 2 は、Identity Governance の Access パッケージです。
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cre

最新問題**: 67**
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。
Answer:

最新問題**: 68**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャ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? 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。

Answer:

最新問題**: 69**
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。
Answer:

最新問題**: 70**
App1 という名前の Azure App Service Web アプリのセキュリティ推奨事項を作成しています。
App1 の仕様は次のとおりです。
* ユーザーは、My Apps ポータルを通じて App1 へのアクセスをリクエストします。人事マネージャーがリクエストを承認します。
* ユーザーは、Azure Active Directory (Azure AD) ユーザー アカウントを使用して認証します。
App1 のアクセス セキュリティ アーキテクチャ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? 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。
Answer:

最新問題**: 71**
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。
Answer:

最新問題**: 72**
あなたの会社では Microsoft Defender for Cloud と Microsoft Sentinel を使用しています。同社は、次の展示に示すアーキテクチャを持つアプリケーションを設計しています。
あなたは、提案されたアーキテクチャ用のログ記録および監査ソリューションを設計しています。ソリューションは次の要件を満たしている必要があります。
* Azure Web アプリケーション ファイアウォール (WAF) ログを Microsoft Sentinel と統合します。
* Defender for Cloud を使用して、仮想マシンからのアラートを確認します。

ソリューションには何を含めるべきでしょうか? 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。
Answer:

最新問題: **73**
仮想マシンの問題を解決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. 仮想マシンを Microsoft Defender for Endpoint にオンボードします。
B. 仮想マシンを Azure Arc にオンボードします。
C. Microsoft エンドポイント マネージャーでデバイス コンプライアンス ポリシーを作成します。
D. Defender for Cloud で Qualys スキャナーを有効にします。
Answer: A (メーッセージを残す)
トピック 1、Fabrikam, Inc
オンプレミス環境
オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Azure環境
Fabrikam には次の Azure リソースがあります。
* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnetl という名前の仮想ネットワーク
* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。
パートナー
Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Contoso の Fabrikam 開発者のアプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装は、アプリケーションをテストまたは更新するために Fabrikam のリソースに接続し

ます。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。
ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。
コンプライアンスイベント
Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修復されています。
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。
アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。

* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題: **74**
Contoso 開発者の要件を満たすには、Azure AD で何を作成する必要がありますか?
Answer:

最新問題: **75**
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
Answer: B (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure

最新問題: **76**
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. Microsoft センチネル
D. Microsoft Intune
Answer: D (メーッセージを残す**)**
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboar

最新問題: **77**
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、Microsoft Teams、SharePoint Online、および Exchange Online のデータを識別して分類したいと考えています。
機密情報を含む文書を識別するための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. データ分類コンテンツ エクスプローラー
C. 情報ガバナンス
D. データ損失防止 (DLP)
Answer: D (メーッセージを残す**)**

最新問題: **78**
Azure サブスクリプションとアマゾン ウェブ サービス (AWS) アカウントを含むマルチクラウド環境があります。
両方のサブスクリプションのリソースを管理するには、Azure にセキュリティ サービスを実装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。

* AWS CloudTrail イベントで見つかった脅威を自動的に識別します。
* Azure ポリシーを使用して、AWS 仮想マシンにセキュリティ設定を適用します。
各要件のソリューションには何を含め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。
Answer:

最新問題: **79**
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。ISOを適用する必要がある
サブスクリプションの 2700V2013 規格。ソリューションでは、準拠していないリソースが自動的に修復されるようにする必要があります。何を使用する必要がありますか?
A. Azure ブループリント
B. Defender for Cloud の規制遵守ダッシュボード
C. Azure ロールベースのアクセス制御 (Azure RBAC)
D. Azure ポリシー
Answer: C (メーッセージを残す**)**

最新問題: **80**
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。
Answer: C,D (メーッセージを残す**)**
説明
https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-
https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

最新問題: **81**
セキュリティ アクセス戦略のセキュリティ レベルを計画しています。

どのジョブロールをどのセキュリティレベルで設定するかを特定する必要があります。ソリューションは、Microsoft Cybersecurity Reference Architectures (MCRA) のセキュリティのベスト プラクティスを満たしている必要があります。
各職務にどのセキュリティ レベルを設定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。
注: 正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **82**
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. ケルベロス
B. 証明書ベースの認証
C. NTLMv2
D. セキュリティ アサーション マークアップ言語 (SAML)
Answer: (解答を表示する**)**

最新問題: **83**
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。
Answer:

最新問題: **84**
あなたの会社は、Azure App Service Web アプリとして実行される最新のアプリケーションを開発しています。Microsoft 脅威モデリング ツールを使用して脅威モデリングを実行し、潜在的なセキュリティ問題を特定することを計画しています。
どのタイプの図を作成する必要がありますか?
A. システムフロー
B. データフロー
C. 処理フロー
D. ネットワーク フロー
Answer: C (メーッセージを残す**)**

最新問題: **85**

ClaimsDB への接続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。
それぞれの要件に対して何を使用することを推奨しますか? 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。
Answer:

最新問題: **86**
あなたの会社は、すべてのオンプレミス仮想マシンを Azure に移行することを計画しています。
ネットワーク エンジニアは、次の表に示す Azure 仮想ネットワーク設計を提案します。
すべての仮想マシンへの安全なリモート アクセスを提供するには、Azure Bastion デプロイを推奨する必要があります。仮想ネットワーク設計に基づいて、Azure Bastion サブネットはいくつ必要ですか?
A. 3
B. 4
C. 2
D. 5
E. 1
Answer: A (メーッセージを残す**)**

最新問題: **87**
あなたの会社は、ランサムウェア インシデントの調査を最適化したいと考えています。
Microsoft Detection and Response Team (DART) のアプローチに基づいてランサムウェア インシデントを調査する計画を推奨する必要があります。
計画内で順番に実行することを推奨する 3 つのアクションはどれですか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。
Answer:
1 - 現在の状況を評価し、範囲を特定します。
2 - ランサムウェア インシデントにより利用できない基幹業務 (LOB) アプリを特定します。
3 - 侵害からの回復プロセスを特定します。

最新問題: **88**
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。
Answer:

最新問題: **89**

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. Azure Cosmos DB ログを Log Analytics ワークスペースに送信します。
B. Azure Cosmos DB のローカル認証を無効にします。
C. ID 用に Microsoft Defender を有効にします。
D. Azure Active Directory (Azure AD) サインイン ログを Log Analytics ワークスペースに送信します。
E. Cosmos DB に対して Microsoft Defender を有効にします。
Answer: C,E (メーッセージを残す)

最新問題**: 90**
ClaimsDB への接続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。
それぞれの要件に対して何を使用することを推奨しますか? 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。
Answer:

最新問題**: 91**
仮想マシン、ストレージ アカウント、および Azure SQL データベースを含む Azure サブスクリプションを持っています。すべてのリソースは、Azure Backup を使用して 1 日に複数回バックアップされます。あなたはランサムウェア攻撃から保護する戦略を開発しています。
ランサムウェア攻撃が成功した場合に Azure Backup を使用してリソースを復元できるようにするには、どの制御を有効にする必要があるかを推奨する必要があります。
推奨事項に含めるべき 2 つのコントロールはどれですか? 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. バックアップ構成が変更されたときに Azure Monitor 通知を使用します。
B. 重要な操作には PIN が必要です。
C. Azure Data Box へのオフライン バックアップを実行します。
D. カスタマー マネージド キー (CMK) を使用してバックアップを暗号化します。
E. バックアップの論理的な削除を有効にします。
Answer: A,B (メーッセージを残す)
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware
「ランサムウェア攻撃が成功した場合に Azure Backup を使用してリソースを復元できるようにするには、どのコントロールを有効にする必要があるかを推奨する必要があります。」監査の目的や悪意のある攻撃の検出には役立ちますが、構成変更の監視と変更後のアラートは、Azure Backup を使用してリソースを復元できることを保証する制御を表すものではありません。

最新問題: **92**
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。
承認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承認するまで、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。
どのセキュリティ管理を推奨する必要がありますか?
A. Microsoft Defender for Cloud Apps の OAuth アプリ ポリシー
B. Azure Active Directory (Azure AD) 条件付きアクセス アプリ制御ポリシー
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
Answer: B (メーッセージを残す**)**

最新問題: **93**
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. Microsoft Defender for Endpoint の Web コンテンツ フィルター

B. Azure AD アプリケーション プロキシ
C. Azure 仮想 WAN
D. Microsoft トンネル
Answer: C (メーッセージを残す)

最新問題**: 94**
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。
Answer:
Explanation:
中程度の信頼度で自動生成されるテキスト説明

最新問題**: 95**
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。
Answer:

最新問題**: 96**
Windows Server を実行する次のオンプレミス サーバーがあります。
* Active Directory ドメイン サービス (AD DS) ドメイン内の 2 つのドメイン コントローラー
* ASP.NET Web アプリを実行する Server1 および Server2 という名前の 2 つのアプリケーション サーバー
* RADIUS と AD DS を使用して認証する Server3 という名前の VPN サーバー エンド ユーザーは、VPN を使用してインターネット経由で Web アプリにアクセスします。
Web アプリへの接続のセキュリティを強化するには、ユーザー アクセス ソリューションを再設計する必要があります。ソリューションは攻撃対象領域を最小限に抑え、Microsoft サイバーセキュリティ リファレンス アーキテクチャ (MCRA) のゼロトラスト原則に従う必要があります。
推奨事項には何を含めるべきですか?
A. Microsoft Defender for Endpoint で Web 保護を構成します。
B. Azure AD 認証を使用するように VPN を構成します。
C. Microsoft Defender for Cloud Apps でコネクタとルールを構成します。
D. Azure AD アプリケーション プロキシを使用して Web アプリを公開します。
Answer: (解答を表示する)

最新問題: **97**
管理された環境全体にわたる法規制への準拠を評価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、法規制遵守要件とビジネス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。
Answer:
説明

最新問題: **98**
あなたの会社は、Azure Active Directory (Azure AD) B2C を使用する請求書発行アプリケーションを開発しています。
アプリケーションは App Service Web アプリとしてデプロイされます。ID 関連の攻撃からアプリケーションを保護するためのソリューションをアプリケーション開発チームに推奨する必要があります。どの 2 つの構成をお勧めしますか? 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 AD B2C のスマート アカウント ロックアウト
B. Azure AD 条件付きアクセスとユーザー フローおよびカスタム ポリシーの統合
C. Identity Governance のパッケージにアクセスします
D. リスク検出を監視するための Azure AD ワークブック
E. Azure AD B2C のカスタム リソース所有者パスワード資格情報 (ROPC) フロー
Answer: (解答を表示する**)**

最新問題: **99**
AWS の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。
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。
Answer:
トピック 1、Fabrikam, Inc
オンプレミス環境
オンプレミス ネットワークには、corp.fabrikam.com という名前の単一の Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Azure環境
Fabrikam には次の Azure リソースがあります。
* corp.fabnkam.com と同期する fabrikam.onmicrosoft.com という名前の Azure Active Directory (Azure AD) テナント
* Sub1 という名前の単一の Azure サブスクリプション
* 米国東部 Azure リージョンの Vnetl という名前の仮想ネットワーク

* 西ヨーロッパ Azure リージョンの Vnet2 という名前の仮想ネットワーク
* Azure Web アプリケーション ファイアウォール (WAR が有効) を備えた FD1 という名前の Azure Front Door のインスタンス
* Microsoft Sentinel ワークスペース
* ClaimDetails という名前のテーブルを含む ClaimsDB という名前の Azure SQL データベース
* アプリケーション サーバーとして構成され、Microsoft Defender for Cloud にオンボードされていない 20 台の仮想マシン
* テスト目的のみに使用される TestRG という名前のリソース グループ
* 個人に割り当てられたセッション ホストを含む Azure Virtual Desktop ホスト プール
Sub1 のすべてのリソースは、米国東部または西ヨーロッパ リージョンのいずれかにあります。
パートナー
Fabrikam は、Contoso, Ltd. という会社とアプリケーションの開発契約を結んでいます。Contoso には次のインフラストラクチャがあります。
* contoso.onmicrosoft.com という名前の Azure AD テナント
* Fabrikam アプリケーションのテスト ワークロードをホストするために使用される AWS EC2 インスタンスを含む ContosoAWS1 という名前のアマゾン ウェブ サービス (AWS) 実装
Contoso の開発者は、Fabrikam のリソースに接続して、アプリケーションをテストまたは更新します。開発者は、fabrikam.onmicrosoft.com の Contoso Developers という名前のセキュリティ グループに追加され、Sub1 のロールに割り当てられます。
ContosoDevelopers グループには、ClaimsDB データベースの db.owner ロールが割り当てられます。
コンプライアンスイベント
Fabrikam は次のコンプライアンス環境を展開します。
* Defender for Cloud は、Sub1 内のすべてのリソースが HIPAA HITRUST 標準に準拠しているかどうかを評価するように構成されています。
* 現在、HIPAA HITRUST 標準に準拠していないリソースは手動で修復されています。
※サーバーの標準脆弱性診断ツールとしてQualysを採用しています。
問題の声明
Defender for Cloud のセキュリティ スコアは、すべての仮想マシンが次の推奨事項を生成していることを示しています。マシンには脆弱性評価ソリューションが必要です。
すべての仮想マシンが Defender for Cloud に準拠している必要があります。
ClaimApp の導入
Fabrikam は、次の仕様を持つ、ClaimsApp という名前のインターネットにアクセス可能なアプリケーションを実装する予定です。
* ClaimsApp は、Vnetl および Vnet2 に接続する Azure App Service インスタンスにデプロイされます。
* ユーザーは、https://claims.fabrikam.com の URL を使用して ClaimsApp に接続します。
* ClaimsApp は ClaimsDB のデータにアクセスします。
* ClaimsDB は Azure 仮想ネットワークからのみアクセスできる必要があります。
* ClaimsApp のアプリ サービス権限を ClaimsDB に割り当てる必要があります。

アプリケーション開発要件
Fabrikam は、アプリケーション開発の次の要件を特定します。
* Azure DevTest ラボは、開発者がテストのために使用します。
* すべてのアプリケーション コードは GitHub Enterprise に保存する必要があります。
* Azure Pipelines はアプリケーションのデプロイメントの管理に使用されます。
* すべてのアプリケーション コードの変更は、クリア テキストのシークレットを含むアプリケーション コードや構成ファイルを含め、セキュリティの脆弱性をスキャンする必要があります。スキャンは、コードがリポジトリにプッシュされるときに実行する必要があります。
セキュリティ要件
Fabrikam は次のセキュリティ要件を特定します。
* インターネットにアクセスできるアプリケーションは、北朝鮮からの接続を防止する必要があります。
* InfraSec という名前のグループのメンバーのみが、ネットワーク セキュリティ グループ (NSG) と、Sub1 の Azure Firewall、VJM、Front Door のインスタンスを構成できる必要があります。
* 仮想マシンのリモート管理を実行するには、管理者は安全なホストに接続する必要があります。セキュア ホストは、カスタム オペレーティング システム イメージからプロビジョニングする必要があります。
AWSの要件
Fabrikam は、ContosoAWSV でホストされるデータに対する次のセキュリティ要件を特定します。
* AWS EC2 インスタンスがセキュア スコアの推奨事項に準拠していない場合は、Fabrikam のセキュリティ管理者に通知します。
* セキュリティ管理者が Azure 環境から AWS サービス ログを直接クエリできることを確認します。
Contoso 開発者の要件
Fabrikam は、Contoso 開発者に対する次の要件を特定します。
* 毎月、ContosoDevelopers グループのメンバーシップを確認する必要があります。
* Contoso 開発者は、Sub1 のリソースにアクセスするには、既存の contoso.onmicrosoft.com 資格情報を使用する必要があります。
* コモロの開発者は、ClaimDetails テーブルの MedicalHistory という名前の列のデータを表示できないようにする必要があります。
コンプライアンス要件
Fabrikam は、Sub1 の仮想マシンを HIPPA HITRUST 標準に準拠するように自動的に修復したいと考えています。TestRG 内の仮想マシンは、コンプライアンス評価から除外する必要があります。

最新問題**: 100**
Microsoft 365 E5 サブスクリプションをお持ちです。

あなたは、100 万を超えるドキュメントを含む Microsoft SharePoint Online サイトの機密データを保護するソリューションを設計しています。
個人識別情報 (PII) の共有を防ぐ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: 正しく選択するたびに 1 ポイントの価値があります。
A. データ損失防止 (DLP) ポリシー
B. 機密ラベルのポリシー
C. 保持ラベルのポリシー
D. 電子情報開示ケース
Answer: A,B (メーッセージを残す**)**
Office 365 のデータ損失防止。データ損失防止 (DLP) は、機密情報を保護し、不用意な開示を防ぐのに役立ちます。組織外への漏洩を防止したい機密情報の例には、財務データや、クレジット カード番号、社会保障番号、健康記録などの個人識別情報 (PII) が含まれます。データ損失防止 (DLP) ポリシーを使用すると、Office 365 全体で機密情報を識別、監視し、自動的に保護できます。
Microsoft Purview Information Protection の機密ラベルを使用すると、ユーザーの生産性や共同作業能力を妨げることなく、組織のデータを分類して保護できます。より広範な情報保護スキームへの統合を計画します。OME との共存に加えて、秘密度ラベルは Microsoft Purview データ損失防止 (DLP) や Microsoft Defender for Cloud Apps などの機能と併用できます。
https://motionwave.com.au/keeper-your-confidential-data-secure-with-microsoft-office-365/
https://docs.microsoft.com/en-us/microsoft-365/solutions/information- protection-deploy-protect-information?view=o365-worldwide#sensitivity-labels

最新問題**: 101**
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。ISOを適用する必要がある
サブスクリプションの 2700V2013 規格。ソリューションでは、準拠していないリソースが自動的に修復されるようにする必要があります。何を使用する必要がありますか?
A. Defender for Cloud の規制遵守ダッシュボード
B. Azure ポリシー
C. Azure ブループリント
D. Azure ロールベースのアクセス制御 (Azure RBAC)
Answer: B (メーッセージを残す**)**
説明
https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-w

最新問題**: 102**
管理された環境全体にわたる法規制への準拠を評価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、法規制遵守要件とビジネス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。
Answer:

最新問題: **103**
Contoso 開発者の要件を満たすには、Azure AD で何を作成する必要がありますか?
Answer:

最新問題: **104**
あなたの会社には、Splunk と Microsoft Sentinel を使用するサードパーティのセキュリティ情報およびイベント管理 (SIEM) ソリューションがあります。Microsoft Sentinel と Splunk を統合する予定です。
Microsoft Sentinel から Splunk にセキュリティ イベントを送信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 Event Hubs
B. Azure データ要素
C. Microsoft Sentinel ワークブック
D. Microsoft Sentinel データ コネクタ
Answer: (解答を表示する**)**
説明
https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eve

最新問題: **105**
Azure サブスクリプションをお持ちです。サブスクリプションには、Windows Server を実行する 100 台の仮想マシンが含まれています。仮想マシンは、Azure Policy と Microsoft Defender for Servers を使用して管理されます。
仮想マシンのセキュリティを強化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。
* 許可リストにあるアプリのみを実行できるようにしてください。
* 管理者は許可リストに追加された各アプリを確認する必要があります。
* 不正なアプリを起動しようとすると、自動的にブロックリストに追加されます。
* アプリをブロックリストから許可リストに移動するには、管理者がアプリを承認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. Defender for Servers の適応型アプリケーション コントロール
B. Azure AD のエンタープライズ アプリケーションの管理者の同意設定
C. Microsoft Defender for Cloud Apps のアプリ ガバナンス
D. Azure Policy のコンピューティング ポリシー

Answer: A (メーッセージを残す)

最新問題: **106**
あなたの会社は、すべてのオンプレミス ワークロードを Azure および Microsoft 365 に移行しようとしています。次の要件を満たす Microsoft Sentinel でセキュリティ オーケストレーション、自動化、および応答 (SOAR) 戦略を設計する必要があります。
* セキュリティ運用アナリストによる手動介入を最小限に抑えます
* Microsoft Teams チャネル内での Waging アラートをサポート
戦略には何を含めるべきでしょうか?
A. データ コネクタ
B. プレイブック
C. ワークブック
D. KQL
Answer: B (メーッセージを残す)
説明
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

最新問題: **107**
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。
Answer: C,E (メーッセージを残す)

トピック 1、Litware, Inc.
既存の環境
Litware には、Utvvare.com という名前の Active Directory Domain Services (AD D%) フォレストと同期する Azure Active Directory (Azure AD) テナントがあり、20 の Azure サブスクリプションにリンクされています。Azure AD Connect は、パススルー認証の実装に使用されます。パスワード ハッシュ同期は無効になり、パスワード ライトバックは有効になります。すべての Litware ユーザーは Microsoft 365 E5 ライセンスを持っています。
この環境には、いくつかの AD DS フォレスト、Azure AD テナント、および Litware の子会社に属する数百の Azure サブスクリプションも含まれています。
計画された変更
Litware は次の変更を実装する予定です。
* Azure AD テナントごとに管理グループ階層を作成します。
* Litware の既存の Azure 環境をリファクタリングし、将来のすべての Azure ワークロードをデプロイするためのランディング ゾーン戦略を設計します。
* Azure AD アプリケーション プロキシを実装して、現在 VPN を使用してアクセスされている内部アプリケーションへの安全なアクセスを提供します。
ビジネス要件
Litware は次のビジネス要件を特定します。
* 追加のオンプレミス インフラストラクチャを最小限に抑えます。
* 管理オーバーヘッドに関連する運用コストを最小限に抑えます。
ハイブリッドの要件
Litware では、次のハイブリッド クラウド要件を特定しています。
* Azure からの次のようなオンプレミス リソースの管理を有効にします。
* 施行とコンプライアンスの評価には Azure Policy を使用します。
* 変更追跡と資産インベントリを提供します。
* パッチ管理を実装します。
* ゲスト アカウントの維持にかかるオーバーヘッドを発生させずに、一元的なクロステナントのサブスクリプション管理を提供します。
Microsoft Sentinelの要件
Litware は、Microsoft Sentinel のセキュリティ情報およびイベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAK) 機能を活用する予定です。同社は、Microsoft Sentinel を使用して Security Operations Center (SOQ) を一元化したいと考えています。
アイデンティティ要件
Litware は次の ID 要件を特定します。
* AD DS ユーザー アカウントを直接ターゲットとするブルート フォース攻撃を検出します。
* Litware の Azure AD テナントに漏洩した資格情報の検出を実装します。
* Azure AD ユーザー アカウントをターゲットとしたブルート フォース攻撃によって AD DS ユーザー アカウントがロックアウトされるのを防ぎます。

* Litware の Azure AD テナントにユーザーとグループの委任管理を実装します (サポートを含む)。
* グループのプロパティ、メンバーシップ、およびライセンスの管理
* ユーザーのプロパティ、パスワード、ライセンスの管理
* ビジネスユニットに基づいたユーザー管理の委任。

規制遵守要件

Litware では、次の規制遵守要件を特定しています。
* 米国およびフランスに拠点を置く各子会社が所有するログ、テレメトリ、およびデータを収集する際に、データ常駐に関するコンプライアンスを保証します。
* 組み込みの Azure Policy 定義を活用して、管理された環境全体にわたる法規制への準拠を評価します。
* 最小特権の原則を使用します。

Azure ランディング ゾーンの要件

Litware は、次のランディング ゾーン要件を特定します。
* インターネットに向かうすべてのトラフィックを、専用の Azure サブスクリプションの Azure Firewall 経由でランディング ゾーンからルーティングします。
* ランディング ゾーンを対象とした安全なスコアを提供します。
* 各ランディング ゾーンの Azure 仮想マシンが、パブリック エンドポイントではなく、Microsoft バックボーン ネットワークを介して同じゾーン内の Azure App Service Web アプリと通信していることを確認します。
* データ漏洩の可能性を最小限に抑えます。
* ネットワーク帯域幅を最大化します。

ランディング ゾーン アーキテクチャには、インターネットおよびハイブリッド接続のハブとして機能する専用のサブスクリプションが含まれます。各ランディング ゾーンには次の特徴があります。
* 専用のサブスクリプションで作成されます。
* litware.com の DNS 名前空間を使用します。

アプリケーションのセキュリティ要件

Litware は、次のアプリケーションのセキュリティ要件を特定します。
* Azure AD アプリケーション プロキシを使用してシングル サインオン (SSO) をサポートする内部アプリケーションを特定します。
* Microsoft SharePoint Online および Exchange Online データへのアクセスをリアルタイムで監視および制御します。

最新問題**: 108**

あなたの会社はデータを Azure に移行しています。データには個人を特定できる情報 (PII) が含まれています。同社は、Azure の PII データ ストアに Microsoft Information Protection を使用する予定です。Azure リソース内でリスクにさらされている PLL データを検出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? 回答するには、回答内の適切なオプションを選択してください。
ａ．注正しく選択するたびに 1 ポイントの価値があります。
Answer:

最新問題: **109**
Microsoft 365 テナントがあります。
あなたの会社では、Azure AD テナントと統合されている App1 という名前のサードパーティのサービスとしてのソフトウェア (SaaS) アプリを使用しています。次の要件を満たすセキュリティ戦略を設計する必要があります。
* ユーザーは、セルフサービス リクエストを使用して App1 へのアクセスをリクエストできる必要があります。
* ユーザーが App1 へのアクセスをリクエストする場合、リクエストに関する追加情報の提供を求めるプロンプトが表示される必要があります。
* 3 か月ごとに、管理者はユーザーが依然として Appl へのアクセスを必要としているかどうかを確認する必要があります。
デザインには何を含めるべきでしょうか?
A. Microsoft Defender for Cloud Apps のアクセス ポリシー
B. Microsoft Entra Identity Governance
C. Microsoft Defender for Cloud Apps の接続されたアプリ
D. Azure AD アプリケーション プロキシ
Answer: (解答を表示する**)**

最新問題: **110**
Microsoft 365 E5 サブスクリプションをお持ちです。
あなたは、100 万を超えるドキュメントを含む Microsoft SharePoint Online サイトの機密データを保護するソリューションを設計しています。
個人識別情報 (PII) の共有を防ぐ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: 正しく選択するたびに 1 ポイントの価値があります。
A. 電子情報開示ケース
B. データ損失防止 (DLP) ポリシー
C. 保持ラベルのポリシー
D. 秘密度ラベル ポリシー
Answer: A,D (メーッセージを残す**)**

最新問題: **111**
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。
Answer:

最新問題: **112**
ハイブリッド要件、Microsoft Sentinel 要件、および法規制遵守要件を満たす SIEM および SOAR 戦略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。
Answer:

最新問題: **113**
あなたの会社はデータを Azure に移行しています。データには個人を特定できる情報 (PII) が含まれています。同社は、Azure の PII データ ストアに Microsoft Information Protection を使用する予定です。Azure リソース内でリスクにさらされている PLL データを検出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? 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。
Answer: