Microsoft.SC-200.v2021-12-13.q104

試験コード：	SC-200
試験名称：	Microsoft Security Operations Analyst
認証ベンダー：	Microsoft
無料問題の数：	104
バージョン：	v2021-12-13
ページの閲覧量：	1114
問題集の閲覧量：	29844

https://www.jpnshiken.com/shiken/Microsoft.SC-200.v2021-12-13.q104.html

質問: **1**
Microsoft 365E5サブスクリプションがあります。
Microsoft 365Defenderを使用してクロスドメイン調査を実行することを計画しています。
悪意のある電子メールの添付ファイルの影響を受けるデバイスを特定するには、高度なハンティングクエリを作成する必要があります。
どのようにクエリを完了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。
正解:
説明
カンファレンス：
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36

質問: **2**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryとのID統合のためにMicrosoftDefenderを構成しています。
Microsoft Defender for Identityポータルから、攻撃者が悪用できるようにいくつかのアカウントを構成する必要があります。
解決策 :エンティティタグから、アカウントをハニートークンアカウントとして追加します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: (正解を表示します)

説明/参照：
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts
AzureDefender質問セット1を使用して脅威を軽減する

質問: **3**
Azure Sentinelの要件を満たすように、AzureSentinel統合を構成する必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:
説明
グラフィカルユーザーインターフェイス、テキスト、アプリケーションの説明が自動的に生成されます
リファレンス：
https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

質問: **4**
新しいAzureサブスクリプションを作成し、AzureMonitorのログの収集を開始します。
疑わしいIPアドレスからAzure仮想マシンへのサインインに関連する可能性のある脅威を検出するようにAzureSecurityCenterを構成する必要があります。ソリューションは構成を検証する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
1-サブスクリプションに対してAzureDefenderを有効にします。
2-仮想マシンに実行可能ファイルをコピーし、ファイルの名前をASC_AlertTest_662jfi039N.exeに変更します。
3-実行可能ファイルを実行し、適切な引数を指定します。
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **5**
ホットスポット
Microsoft 365E5サブスクリプションがあります。
Microsoft 365Defenderを使用してクロスドメイン調査を実行することを計画しています。
悪意のある電子メールの添付ファイルの影響を受けるデバイスを特定するには、高度なハンティングクエリを作成する必要があります。
どのようにクエリを完了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。
ホットエリア：

正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices？
view = o365-全世界

質問: **6**
サポートされているすべてのリソースタイプに対してAzureDefenderが有効になっているAzureサブスクリプションがあります。
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）ソリューションからアラートを取得できるようにするには、重大度の高いアラートの継続的なエクスポートを構成する必要があります。
アラートをどのサービスにエクスポートする必要がありますか？
A. Azureイベントハブ
B. Azureイベントグリッド
C. Azure Data Lake
D. Azure Cosmos DB
正解: **(**正解を表示します**)**

質問: **7**
AzureSentinelで脅威を検出するためのカスタム分析ルールがあります。
分析ルールの実行が停止したことがわかります。ルールが無効にされており、ルール名のプレフィックスはAUTODISABLEDです。
問題の考えられる原因は何ですか？
A. データソースとLogAnalyticsの間に接続の問題があります。
B. アラートの数が2分以内に10,000を超えました。
C. ルールクエリの実行に時間がかかりすぎてタイムアウトします。
D. ルールクエリのデータソースの1つへのアクセス許可が変更されました。
正解: **D (**コメントを発表する**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **8**
ドラッグドロップ
新しいAzureサブスクリプションを作成し、AzureMonitorのログの収集を開始します。
疑わしいIPアドレスからAzure仮想マシンへのサインインに関連する可能性のある脅威を検出するようにAzureSecurityCenterを構成する必要があります。ソリューションは構成を検証する必要があります。

順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **9**
Azure Defender for KeyVaultからアラートを受け取ります。
アラートが複数の疑わしいIPアドレスから生成されていることがわかりました。
問題を調査している間、KeyVaultシークレットが漏洩する可能性を減らす必要があります。ソリューションはできるだけ早く実装する必要があり、正当なユーザーへの影響を最小限に抑える必要があります。
あなたは最初に何をすべきですか？
A. キーボールトのアクセス制御設定を変更します。
B. KeyVaultファイアウォールを有効にします。
C. アプリケーションセキュリティグループを作成します。
D. キーボールトのアクセスポリシーを変更します。
正解: **B** (コメントを発表する)
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

質問: **10**
あなたの会社はAzureSentinelを使用して、10,000を超えるIoTデバイスからのアラートを管理しています。
同社のセキュリティマネージャーは、インシデントの数が多いため、セキュリティの脅威を追跡することがますます困難になっていると報告しています。
脅威の調査を簡素化し、機械学習を使用して脅威を推測するためのカスタム視覚化を提供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必要がありますか？
A. 組み込みのクエリ
B. ライブストリーム
C. ノートブック
D. ブックマーク
正解: (正解を表示します)
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

質問: **11**
Azure Sentinelの要件を満たすには、分析ルールを作成する必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:

質問: **12**
Microsoft Defender for Endpointを使用して解決できるチームの問題は？
A. エグゼクティブ
B. 販売
C. マーケティング
正解: **B** (コメントを発表する)
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios
テストレット1
ケーススタディ
これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。
あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。
ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。
概要
Contoso Ltd.という名前の会社には、北米全体に本社と5つの支店があります。

本社はシアトルにあります。支店はトロント、マイアミ、ヒューストン、ロサンゼルス、バンクーバーにあります。
Contosoには、ニューヨークとサンフランシスコにオフィスを構えるFabrikam、Ltd。という名前の子会社があります。
既存の環境
エンドユーザー環境
ContosoのすべてのユーザーはWindows10デバイスを使用しています。各ユーザーはMicrosoft365のライセンスを取得しています。さらに、iOSデバイスはContosoの営業チームのメンバーに配布されます。
クラウドとハイブリッドインフラストラクチャ
すべてのContosoアプリケーションはAzureにデプロイされます。
Microsoft Cloud AppSecurityを有効にします。
ContosoとFabrikamには、異なるAzure Active Directory（Azure AD）テナントがあります。Fabrikamは最近Azureサブスクリプションを購入し、サポートされているすべてのリソースタイプに対してAzureDefenderを有効にしました。
現在の問題
Contosoのセキュリティチームは、多数のサイバーセキュリティアラートを受信します。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威であり、どれがそうでないかを特定するのに多くの時間を費やしています。
Contosoの営業チームはiOSデバイスのみを使用しています。営業チームのメンバーは、さまざまなサードパーティツールを使用して顧客とファイルを交換します。過去に、営業チームはデバイスに対してさまざまな攻撃を経験しました。
Contosoのマーケティングチームには、外部ベンダーと協力するためのMicrosoft SharePointOnlineサイトがいくつかあります。マーケティングチームには、ベンダーがマルウェアを含むファイルをアップロードするという事件がいくつかありました。
Contosoのエグゼクティブチームは、セキュリティ違反を疑っています。エグゼクティブチームは、Microsoft Cloud App Securityで保護されたアプリケーションのデータアクセス、ダウンロード、削除など、過去48時間に5つを超えるアクティビティがあったファイルを特定するように要求します。
要件
計画された変更
Contosoは、両社のセキュリティ運用を統合し、すべてのセキュリティ運用を一元管理することを計画しています。
技術要件
Contosoは、次の技術要件を識別します。
* Azure仮想マシンがブルートフォース攻撃を受けている場合にアラートを受信します。
* Azure Sentinelを使用して、環境に対するアクティブな攻撃を迅速に修正することにより、組織のリスクを軽減します。

* ContosoとFabrikamのAzureADテナント間でデータを相互に関連付けるAzureSentinelクエリを実装します。
*外部の攻撃者や独自のAzureADアプリケーションの潜在的な侵害が発生した場合に、FabrikamのKeyVaultアラート用のAzureDefenderを修正する手順を開発します。
*特定の国から初めてAzureリソースにサインインできなかったユーザーのすべてのケースを特定します。ジュニアセキュリティ管理者は、次の不完全なクエリを提供します。
BehaviorAnalytics
| ここで、ActivityType == "FailedLogOn"
| ここで、_____ == True

質問: **13**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure SecurityCenterを使用します。
セキュリティセンターでセキュリティアラートを受け取ります。
セキュリティセンターでアラートを解決するには、推奨事項を表示する必要があります。
解決策：規制順守から、レポートをダウンロードします。
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**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

質問: **14**
あなたは、新しいランサムウェア株を展開する潜在的な攻撃を調査しています。
機密情報を含む非常に価値のあるマシンのグループで自動化されたアクションを実行することを計画しています。
3つのカスタムデバイスグループがあります。
デバイスでアクションを実行するには、マシンを一時的にグループ化できる必要があります。
実行する必要がある3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：正しい選択はそれぞれ1ポイントの価値があります。
A. デバイスグループにタグを割り当てます。

B. デバイスユーザーを管理者ロールに追加します。
C. マシンにタグを追加します。
D. ランク1の新しいデバイスグループを作成します。
E. 新しい管理者ロールを作成します。
F. ランク4の新しいデバイスグループを作成します。
正解**: A,C,D (**コメントを発表する**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

質問**: 15**
ドラッグドロップ
環境に影響を与える新しいCommonVulnerability and Exposures（CVE）の脆弱性が通知されます。
文書化されたアクティブなエクスプロイトが利用可能な場合は、Microsoft Defender Security Centerを使用して、影響を受けるシステムを担当するチームに修復を要求する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解**:**
セクション :[なし]
説明/参照：
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

質問**: 16**
あなたの会社はAzureSentinelを使用しています。
新しいセキュリティアナリストは、AzureSentinelでインシデントを割り当てて解決できないと報告しています。
アナリストがインシデントを割り当てて解決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、最小特権の原則を使用する必要があります。
アナリストにどの役割を割り当てる必要がありますか？
A. Azure Sentinel Responder
B. ロジックアプリの貢献者
C. AzureSentinelコントリビューター
D. Azure Sentinel Reader
正解**: (**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/roles

質問: **17**
AzureSentinelでハンティングクエリを作成します。
ハンティングクエリがクエリで一致を検出するとすぐに、Azureポータルで通知を受信する必要があります。ソリューションは労力を最小限に抑える必要があります。
何を使うべきですか？
A. プレイブック
B. ノートブック
C. ライブストリーム
D. ブックマーク
正解: **(**正解を表示します**)**
ライブストリームを使用して特定のクエリを常に実行し、結果が届いたときに結果を表示します。
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/hunting

質問: **18**
Azure Defenderの要件とビジネス要件を満たすには、AzureDefenderを実装する必要があります。ソリューションに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。
正解:

質問: **19**
会社は、すべてのプロジェクトのデータを異なるAzureサブスクリプションに保存します。すべてのサブスクリプションは、同じAzure Active Directory（Azure AD）テナントを使用します。
すべてのプロジェクトは、WindowsServerを実行する複数のAzure仮想マシンで構成されています。仮想マシンのWindowsイベントは、各マシンのそれぞれのサブスクリプションのLogAnalyticsワークスペースに保存されます。
AzureSentinelを新しいAzureサブスクリプションにデプロイします。
すべてのサブスクリプションのすべてのLogAnalyticsワークスペースを検索するには、AzureSentinelでハンティングクエリを実行する必要があります。

実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. セキュリティイベントコネクタをAzureSentinelワークスペースに追加します。
B. workspaceexpressionとunionoperatorを使用するクエリを作成します。
C. aliasstatementを使用します。
D. resourceexpressionとaliasoperatorを使用するクエリを作成します。
E. AzureSentinelソリューションを各ワークスペースに追加します。
正解**: B,E (**コメントを発表する**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問**: 20**
ホットスポット
Azure Sentinelを使用して、不規則なAzureアクティビティを監視します。
次の展示に示すように、脅威を検出するためのカスタム分析ルールを作成します。
ルール定義の一部としてインシデント設定を定義しないでください。
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了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
ホットエリア：
正解**:**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問**: 21**
AzureSentinelを構成しています。
疑わしいIPアドレスからのサインインが検出されるたびに、MicrosoftTeamsメッセージをチャネルに送信する必要があります。
Azure Sentinelで実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. プレイブックを追加します。
B. プレイブックをインシデントに関連付けます。
C. エンティティの動作分析を有効にします。
D. ワークブックを作成します。
E. フュージョンルールを有効にします。

正解: (正解を表示します)
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **22**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryとのID統合のためにMicrosoftDefenderを構成しています。
Microsoft Defender for Identityポータルから、攻撃者が悪用できるようにいくつかのアカウントを構成する必要があります。
解決策 :エンティティタグから、アカウントをハニートークンアカウントとして追加します。
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)
リファレンス：
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

質問: **23**
あなたの会社はAzureSentinelをデプロイしています。
AzureSentinelの管理をさまざまなグループに委任することを計画しています。
次のタスクを委任する必要があります。
*プレイブックを作成して実行する
*ワークブックと分析ルールを作成します。
ソリューションは、最小特権の原則を使用する必要があります。
各タスクにどの役割を割り当てる必要がありますか？答えるには、適切な役割を正しいタスクにドラッグします。各役割は、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：正しい選択はそれぞれ1ポイントの価値があります。
正解:
説明
自動生成されたグラフィカルユーザーインターフェイスの説明を含む画像
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/roles

質問: **24**
Azure仮想マシンの技術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必要がありますか？
A. ジャストインタイム（JIT）アクセス
B. Azure Defender
C. Azureファイアウォール
D. Azure Application Gateway
正解: **(正解を表示します)**
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/azure-defender
トピック1、Contoso Ltd
既存の環境
エンドユーザー環境
ContosoのすべてのユーザーはWindows10デバイスを使用しています。各ユーザーはMicrosoft365のライセンスを取得しています。さらに、iOSデバイスはContosoの営業チームのメンバーに配布されます。
クラウドとハイブリッドインフラストラクチャ
すべてのContosoアプリケーションはAzureにデプロイされます。
Microsoft Cloud AppSecurityを有効にします。
ContosoとFabrikamには、異なるAzure Active Directory（Azure AD）テナントがあります。Fabrikamは最近Azureサブスクリプションを購入し、サポートされているすべてのリソースタイプに対してAzureDefenderを有効にしました。
現在の問題
Contosoのセキュリティチームは、多数のサイバーセキュリティアラートを受信します。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威であり、どれがそうでないかを特定するのに多くの時間を費やしています。
Contosoの営業チームはiOSデバイスのみを使用しています。営業チームのメンバーは、さまざまなサードパーティツールを使用して顧客とファイルを交換します。過去に、営業チームはデバイスに対してさまざまな攻撃を経験しました。
Contosoのマーケティングチームには、外部ベンダーと協力するためのMicrosoft SharePointOnlineサイトがいくつかあります。マーケティングチームには、ベンダーがマルウェアを含むファイルをアップロードするという事件がいくつかありました。
Contosoのエグゼクティブチームは、セキュリティ違反を疑っています。エグゼクティブチームは、Microsoft Cloud App Securityで保護されたアプリケーションのデータアクセス、ダウンロード、削除など、過去48時間に5つを超えるアクティビティがあったファイルを特定するように要求します。
要件
計画された変更
Contosoは、両社のセキュリティ運用を統合し、すべてのセキュリティ運用を一元管理することを計画しています。

技術要件
Contosoは、次の技術要件を識別します。
Azure仮想マシンがブルートフォース攻撃を受けている場合にアラートを受信します。
Azure Sentinelを使用して、環境に対するアクティブな攻撃を迅速に修正することにより、組織のリスクを軽減します。
ContosoとFabrikamのAzureADテナント間でデータを相互に関連付けるAzureSentinelクエリを実装します。
外部の攻撃者や独自のAzureADアプリケーションの潜在的な侵害が発生した場合に備えて、FabrikamのKeyVaultアラート用のAzureDefenderを修正する手順を開発します。
特定の国から初めてAzureリソースにサインインできなかったユーザーのすべてのケースを特定します。ジュニアセキュリティ管理者は、次の不完全なクエリを提供します。
BehaviorAnalytics
| ここで、ActivityType == "FailedLogOn"
| ここで、_____ == True

質問: **25**
次の展示に示すように、Azure Sentinelから、重大度の高いインシデントの調査ウィンドウを開きます。
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了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:
説明
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-di

質問: **26**
ドラッグドロップ
次の展示に示すように、Cloud AppSecurityポータルを開きます。
ご使用の環境で、Microsoft Defender forEndpointが有効になっていません。
Launchpadアプリのリスクを修正する必要があります。
順番に実行する必要がある4つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

質問: **27**
vm1とvm2という名前の2つの仮想マシンを含むAzureサブスクリプションのセキュリティポスチャを管理します。
Azure Security Centerのセキュアスコアは、SecurityCenterの展示に表示されます。[セキュリティセンター]タブをクリックします。）
Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。[ポリシー]タブをクリックします。）
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。
正解:
説明
リファレンス：
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-acc
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/15

質問: **28**
技術的な要件を満たすには、ContosoとFabrikamのAzureSentinelクエリを実装する必要があります。
ソリューションに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。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenantsこれはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。

ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。
概要
LitwareInc。は再生可能な会社です。
Litwareは、ボストンとシアトルにオフィスを構えています。Litwareには、米国全土にリモートユーザーがいます。クラウドリソースを含むLitwareリソースにアクセスするために、リモートユーザーはいずれかのオフィスへのVPN接続を確立します。

質問: **29**
Microsoft 365 Defenderには、次の高度なハンティングクエリがあります。
過去24時間に、Microsoft Defenderによって管理されているデバイスでプロセスがシステムの復元を無効にした場合は、アラートを受信する必要があります。
実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. 検出ルールを作成します。
B. 抑制ルールを作成します。
C. 追加|タイムスタンプでクエリに並べ替えます。
D. DeviceProcessEventsをDeviceNetworkEventsに置き換えます。
E. クエリの出力にDeviceIdとReportIdを追加します。
正解: **(正解を表示します)**
リファレンス：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

質問: **30**
MicrosoftDefenderを使用するMicrosoft365 E5サブスクリプションと、AzureSentinelを使用するAzureサブスクリプションがあります。
既知の悪意のある電子メール送信者によって送信された電子メール内のファイルを含むすべてのデバイスを識別する必要があります。クエリは、SHA256ハッシュの一致に基づいて行われます。
どのようにクエリを完了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。
正解:

リファレンス：
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: **31**
sub1という名前のAzureサブスクリプションを作成します。
sub1では、workspace1という名前のLogAnalyticsワークスペースを作成します。
Azure Security Centerを有効にし、workspace1を使用するようにSecurityCenterを構成します。
ワークスペース1にレポートするAzure仮想マシンからセキュリティイベントログを収集する必要があります。
あなたは何をするべきか？
A. セキュリティセンターから、データ収集を有効にします
B. sub1にプロバイダーを登録します。
C. セキュリティセンターから、ワークフローの自動化を作成します。
D. workspace1で、ブックを作成します。
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

質問: **32**
あなたの会社はEndpointにMicrosoftDefenderを使用しています。
同社には、マクロを含むMicrosoftWord文書があります。ドキュメントは、会社の経理チームのデバイスで頻繁に使用されます。
既存のセキュリティ体制を維持しながら、アラートキューで誤検知を非表示にする必要があります。実行する必要がある3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：正しい選択はそれぞれ1ポイントの価値があります。
A. アラートを自動的に解決します。
B. アラートを非表示にします。
C. 任意のデバイスを対象とする抑制ルールを作成します。
D. デバイスグループを対象とする抑制ルールを作成します。

E. アラートを生成します。
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

質問: **33**
会社は、すべてのプロジェクトのデータを異なるAzureサブスクリプションに保存します。すべてのサブスクリプションは、同じAzure Active Directory（Azure AD）テナントを使用します。
すべてのプロジェクトは、WindowsServerを実行する複数のAzure仮想マシンで構成されています。仮想マシンのWindowsイベントは、各マシンのそれぞれのサブスクリプションのLogAnalyticsワークスペースに保存されます。
AzureSentinelを新しいAzureサブスクリプションにデプロイします。
すべてのサブスクリプションのすべてのLogAnalyticsワークスペースを検索するには、AzureSentinelでハンティングクエリを実行する必要があります。
実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. セキュリティイベントコネクタをAzureSentinelワークスペースに追加します。
B. workspaceexpressionとunionoperatorを使用するクエリを作成します。
C. aliasstatementを使用します。
D. resourceexpressionとaliasoperatorを使用するクエリを作成します。
E. AzureSentinelソリューションを各ワークスペースに追加します。
正解: **(**正解を表示します**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問: **34**
Cloud Appのセキュリティ要件を満たすには、異常検出ポリシーの設定を変更する必要があります。
どのポリシーを変更する必要がありますか？
A. 疑わしいIPアドレスからのアクティビティ
B. 匿名IPアドレスからのアクティビティ
C. 不可能な旅
D. 危険なサインイン
正解: **(**正解を表示します**)**
説明/参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy Microsoft 365Defender質問セット3を使用して脅威を軽減する

質問: **35**
ビジネス要件を満たすようにDC1を構成する必要があります。
順番に実行する必要がある4つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
説明
中程度の信頼度で自動的に生成されたテキストの説明
手順1 :グローバル管理者としてhttps://portal.atp.azure.comにログインします
ステップ2 :インスタンスを作成する
手順3.インスタンスをActiveDirectoryに接続します
ステップ4.センサーをダウンロードしてインストールします。
リファレンス：
https://docs.microsoft.com/en-us/defender-for-identity/install-step1
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

質問: **36**
通常のアクティビティに対して、Azure SecurityCenterで毎日何千ものアラートを生成するAzureFunctionsアプリがあります。
セキュリティセンターでアラートを自動的に非表示にする必要があります。
セキュリティセンターで順番に実行する必要がある3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：正しい選択はそれぞれ1ポイントの価値があります。
正解:
1-セキュリティポリシーを選択します。
2- [抑制ルール]を選択してから、[新しい抑制ルールの作成]を選択します。
3-エンティティタイプとしてAzureResourceを選択し、IDを指定します。
リファレンス：
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

質問: **37**
vm1とvm2という名前の2つの仮想マシンを含むAzureサブスクリプションのセキュリティポスチャを管理します。
Azure Security Centerのセキュアスコアは、SecurityCenterの展示に表示されます。[セキュリティセンター]タブをクリックします。）
Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。[ポリシー]タブをクリックします。）
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。
正解:
リファレンス：
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

質問: **38**
技術的な要件を満たすには、失敗したサインインのクエリを完了する必要があります。
where句を完成させるための列名はどこにありますか？
A. Azure SecurityCenterのセキュリティアラート
B. Azureのアクティビティログ
C. Azure Advisor
D. LogAnalyticsワークスペースのクエリウィンドウ
正解: **D (**コメントを発表する**)**
これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。
ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。
概要
LitwareInc。は再生可能な会社です。
Litwareは、ボストンとシアトルにオフィスを構えています。Litwareには、米国全土にリモートユーザーがいます。クラウドリソースを含むLitwareリソースにアクセスするために、リモートユーザーはいずれかのオフィスへのVPN接続を確立します。

質問: **39**
新しいAzureサブスクリプション用にAzureSentinelをプロビジョニングします。
セキュリティイベントコネクタを設定しています。
コネクタのテンプレートから新しいルールを作成するときに、イベントごとに新しいアラートを生成することにしました。
次のルールクエリを作成します。
アラートをインシデントにグループ化できる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. ユーザー
B. リソースグループ
C. IPアドレス
D. コンピューター
正解: **(正解を表示します)**
セクション :[なし]

質問: **40**
次の環境があります。
AzureSentinel
Microsoft365サブスクリプション
Microsoft Defender for Identity
Azure Active Directory（Azure AD）テナント
すべてのActiveDirectoryメンバーサーバーとドメインコントローラーからセキュリティログを収集するようにAzureSentinelを構成します。
スタンドアロンセンサーを使用して、Microsoft Defender forIdentityを展開します。
ActiveDirectoryで機密グループが変更されたときに検出できることを確認する必要があります。
実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. ドメインコントローラーの高度な監査ポリシー構成設定を構成します。
B. ドメインコントローラー組織単位（OU）の権限を変更します。
C. Microsoft365コンプライアンスセンターで監査を構成します。
D. ドメインコントローラーでWindowsイベント転送を構成します。
正解: **(正解を表示します)**
リファレンス：
https://docs.microsoft.com/en-us/defender-for-identity/configure-windows-event-collection
https://docs.microsoft.com/en-us/defender-for-identity/configure-event-collection

質問: **41**

あなたの会社は、Microsoft OfficeVBAマクロを含む基幹業務アプリを使用しています。
追加の子プロセスとしてOfficeVBAマクロから追加のペイロードをダウンロードして実行することに対する保護を有効にすることを計画しています。
影響を受ける可能性のあるOfficeVBAマクロを特定する必要があります。
目標を達成するために実行できる2つのコマンドはどれですか？それぞれの正解は完全な解決策を提示します。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解**: (**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

質問**: 42**
FabrikamのAzureDefenderアラートの修正アクションを推奨する必要があります。
各脅威に対して何を推奨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。
正解**:**
リファレンス：
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

質問**: 43**
カスタム分析ルールを作成して、AzureSentinelで脅威を検出します。
ルールが断続的に失敗することがわかります。
失敗の2つの考えられる原因は何ですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. ルールクエリの実行に時間がかかりすぎてタイムアウトします。
B. ターゲットワークスペースが削除されました。
C. ルールクエリのデータソースへのアクセス許可が変更されました。
D. データソースとLogAnalyticsの間に接続の問題があります
正解**: (**正解を表示します**)**
セクション :[なし]
Explanation:
不正解：
B :これにより、断続的にではなく、毎回失敗する可能性があります。
C :これにより、断続的にではなく、毎回失敗する可能性があります。

質問: **44**
あなたの会社はAzureSecurityCenterとAzureDefenderを使用しています。
会社のセキュリティ運用チームは、セキュリティアラートの電子メール通知を受信しないことを通知します。
電子メール通知を有効にするには、セキュリティセンターで何を構成する必要がありますか？
A. セキュリティソリューション
B. セキュリティポリシー
C. 価格と設定
D. セキュリティアラート
E. Azure Defender
正解: **(正解を表示します)**
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

質問: **45**
AzureSentinelワークスペースがあります。
Azureポータルでハンドブックを手動でテストする必要があります。
Azure Sentinelのどこからテストを実行できますか？
A. プレイブック
B. 分析
C. 脅威インテリジェンス
D. インシデント
正解: **(正解を表示します)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

質問: **46**
ドラッグドロップ
Azure Sentinelの要件を満たすには、イベントにメモを追加する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/bookmarks

質問: **47**
Azure Sentinel分析ルールを使用して、Amazon Web Services（AWS）ログで特定の基準を検索し、インシデントを生成する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
1-アマゾンウェブサービスコネクタを追加します
2-AzureSentinelのAnalyticsから。スケジュールされたクエリを使用するカスタム分析ルールを作成する
3-アラートロジックを設定します
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

質問: **48**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
AzureSentinelを構成しています。
悪意のあるIPアドレスからAzure仮想マシンへのサインインが検出された場合は、AzureSentinelでインシデントを作成する必要があります。
解決策 :ハンティングブックマークを作成します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: (正解を表示します)
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

質問: **49**
Azure仮想マシンの技術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必要がありますか？
A. ジャストインタイム（JIT）アクセス
B. Azure Defender
C. Azureファイアウォール
D. Azure Application Gateway
正解: **(正解を表示します)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/azure-defender
質問セット3

質問: **50**
Azure Sentinelの要件を満たすために、テストルールを作成する必要があります。
ルールを作成するときはどうすればよいですか？
A. [ルールロジックの設定]から、抑制をオフにします。
B. Analyticsルールの詳細から、戦術を構成します。
C. [ルールロジックの設定]から、エンティティをマップします。
D. Analyticsルールの詳細から、重大度を構成します。
正解: **(正解を表示します)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **51**
Sub1という名前のAzureサブスクリプションとMicrosoft365サブスクリプションがあります。Sub1は、contoso.comという名前のAzure Active Directory（Azure AD）テナントにリンクされています。
ワークスペース1という名前のAzureSentinelワークスペースを作成します。ワークスペース1で、contoso.com用のAzureADコネクタとMicrosoft365サブスクリプション用のOffice365コネクタをアクティブ化します。
Fusionルールを使用して、contoso.comへの疑わしいサインインとそれに続く異常なMicrosoft Office365アクティビティを含む多段階の攻撃を検出する必要があります。
実行する必要がある2つのアクションはどれですか？それぞれの正解は、ソリューションの一部を表しています。
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. Microsoft Cloud AppSecurityコネクタを作成します。
B. Azure AD IdentityProtectionコネクタを作成します。

C. Office365コネクタテンプレートに基づいてカスタムルールを作成します。
D. Azure SecurityCenterに基づいてMicrosoftインシデント作成ルールを作成します。
正解: **C,D** (コメントを発表する)

質問: **52**
技術的な要件を満たすには、アクティブな攻撃を修正する必要があります。
ソリューションに何を含める必要がありますか？
A. AzureAutomationのRunbook
B. Azure Logic Apps
C. Azure関数
正解: **B** (コメントを発表する)
D AzureSentinelライブストリーム
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

質問: **53**
セキュリティ管理者は、ストレージアカウントにアップロードされた潜在的なマルウェアや、ブルートフォース攻撃の成功の可能性などのアクティビティについて、AzureDefenderから電子メールアラートを受信します。
セキュリティ管理者は、ウイルス対策アクションの失敗や疑わしいネットワークアクティビティなどのアクティビティに関する電子メールアラートを受信しません。アラートはAzureSecurityCenterに表示されます。
セキュリティ管理者がすべてのアクティビティの電子メールアラートを受信することを確認する必要があります。
セキュリティセンターの設定で何を構成する必要がありますか？
A. 電子メール通知の重大度
B. クラウドコネクタ
C. AzureDefenderの計画
D. 脅威検出の統合設定
正解: **A** (コメントを発表する)
リファレンス：
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

質問: **54**
vm1とvm2という名前の2つの仮想マシンを含むAzureサブスクリプションのセキュリティポスチャを管理します。
Azure Security Centerのセキュアスコアは、SecurityCenterの展示に表示されます。[セキュリティセンター]タブをクリックします。）

Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。 [ポリシー]タブをクリックします。）
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。
正解:
リファレンス：
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

質問: **55**
エグゼクティブチームの問題を調査するには、高度なハンティングクエリを作成する必要があります。
どのようにクエリを完了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。
正解:
説明

質問: **56**
新しいAzureサブスクリプションを作成し、AzureMonitorのログの収集を開始します。
疑わしいIPアドレスからAzure仮想マシンへのサインインに関連する可能性のある脅威を検出するようにAzureSecurityCenterを構成する必要があります。ソリューションは構成を検証する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **57**
サポートされているすべてのリソースタイプに対してAzureDefenderが有効になっているAzureサブスクリプションがあります。
LA1という名前のAzureロジックアプリを作成します。
LA1を使用して、Azure SecurityCenterで検出されたセキュリティリスクを自動的に修正することを計画しています。
セキュリティセンターでLA1をテストする必要があります。

あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

質問: **58**
Azure InformationProtectionの要件を実装する必要があります。最初に何を構成する必要がありますか？
A. AzureポータルからのAzure InformationProtectionのコンテンツスキャンジョブ
B. AzureポータルからのAzure InformationProtectionのスキャナークラスター
C. Microsoft Defender SecurityCenterのデバイスヘルスおよびコンプライアンスレポートの設定
D. Microsoft Defender SecurityCenterの設定の高度な機能
正解: **(正解を表示します)**
トピック2、Litwareinc。
既存の環境
アイデンティティ環境
ネットワークには、litware.comという名前のAzure Active Directory（Azure AD）テナントと同期するlitware.comという名前のActiveDirectoryフォレストが含まれています。
Microsoft365環境
Litwareには、litware.com AzureADテナントにリンクされたMicrosoft365E5サブスクリプションがあります。Microsoft Defender for Endpointは、Windows10を実行しているすべてのコンピューターに展開されます。すべてのMicrosoftCloud AppSecurityの組み込みの異常検出ポリシーが有効になっています。
Azure環境
Litwareには、litware.com AzureADテナントにリンクされたAzureサブスクリプションがあります。次の表に示すように、サブスクリプションには米国東部のAzureリージョンのリソースが含まれています。
ネットワーク環境
各Litwareオフィスはインターネットに直接接続し、Azureサブスクリプションの仮想ネットワークへのサイト間VPN接続を備えています。
オンプレミス環境
オンプレミスネットワークには、次の表に示すコンピューターが含まれています。
現在の問題
Cloud App Securityは、ユーザーが両方のオフィスに同時に接続すると、誤検知アラートを頻繁に生成します。
計画された変更
Litwareは、次の変更を実装する予定です。
AzureサブスクリプションでAzureSentinelを作成して構成します。

Azure ADテストユーザーアカウントを使用して、AzureSentinelの機能を検証します。
ビジネス要件
Litwareは、次のビジネス要件を識別します。
* Azure情報保護の要件
*セキュリティラベルが付いていてWindows10コンピューターに保存されているすべてのファイルは、Azure InformationProtection-データ検出ダッシュボードから利用できる必要があります。
*エンドポイント要件のためのMicrosoftDefender
*すべてのCloudApp Securityの認可されていないアプリは、Microsoft Defender forEndpointを使用してWindows10コンピューターでブロックする必要があります。
Microsoftクラウドアプリのセキュリティ要件
Cloud App Securityは、テナントレベルのデータに基づいて、ユーザー接続が異常であるかどうかを識別する必要があります。
AzureDefenderの要件
すべてのサーバーは、同じLogAnalyticsワークスペースにログを送信する必要があります。
AzureSentinelの要件
Litwareは、次のAzureSentinel要件を満たしている必要があります。
AzureSentinelとCloudAppSecurityを統合します。
admin1という名前のユーザーがAzureSentinelプレイブックを構成できることを確認します。
カスタムクエリに基づいてAzureSentinel分析ルールを作成します。ルールは、プレイブックの実行を自動的に開始する必要があります。
特定のIPアドレスからのデータアクセスを表すイベントにメモを追加して、ハンティング中に調査グラフをナビゲートするときにIPアドレスを参照できるようにします。
AzureADテストユーザーアカウントによるMicrosoftOffice365へのインバウンドアクセスが検出されたときにアラートを生成するテストルールを作成します。ルールによって生成されたアラートは、テストユーザーアカウントごとに1つのインシデントを使用して、個々のインシデントにグループ化する必要があります。

質問: **59**
技術的な要件を満たすには、アクティブな攻撃を修正する必要があります。
ソリューションに何を含める必要がありますか？
A. AzureAutomationのRunbook
B. Azure Logic Apps
C. Azure関数
D AzureSentinelライブストリーム
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

質問: **60**
AzureSentinelを使用します。

Azure Storageアカウントキーが列挙されるたびに、すぐにアラートを受信する必要があります。
実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. ライブストリームを作成する
B. データコネクタを追加します
C. 分析ルールを作成する
D. ハンティングクエリを作成します。
E. ブックマークを作成します。
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/livestream

質問: **61**
Azure Defender for KeyVaultアラートに対応するのはユーザーの責任です。
アラートの調査中に、Tor出口ノードからキーボールトに不正にアクセスしようとしていることがわかりました。
脅威を軽減するために何を構成する必要がありますか？
A. 主要なVaultファイアウォールと仮想ネットワーク
B. Azure Active Directory（Azure AD）のアクセス許可
C. キーボールトの役割ベースのアクセス制御（RBAC）
D. キーボールトのアクセスポリシー設定
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

質問: **62**
Azure Sentinelの要件とビジネス要件を満たすには、admin1に役割ベースのアクセス制御（RBAC）の役割を割り当てる必要があります。
どの役割を割り当てる必要がありますか？
A. 自動化オペレーター
B. 自動化Runbookオペレーター

C. AzureSentinelコントリビューター
D. ロジックアプリの貢献者
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/roles

質問: **63**
米国東部のAzureリージョンにAzureSentinelをデプロイしています。
米国西部のAzureリージョンにLogsWestという名前のLogAnalyticsワークスペースを作成します。
LogsWestへのクエリに基づいてアラートを生成するには、既存のAzureSentinelデプロイメントでスケジュールされた分析ルールを使用できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. Azureデータカタログを米国西部のAzureリージョンにデプロイします。
B. 既存のAzureSentinelデプロイメントのワークスペース設定を変更します
C. AzureSentinelをワークスペースに追加します。
D. AzureSentinelでデータコネクタを作成します。
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問: **64**
あなたは、新しいランサムウェア株を展開する潜在的な攻撃を調査しています。
機密情報を含む非常に価値のあるマシンのグループで自動化されたアクションを実行することを計画しています。
3つのカスタムデバイスグループがあります。
デバイスでアクションを実行するには、マシンを一時的にグループ化できる必要があります。実行する必要がある3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：正しい選択はそれぞれ1ポイントの価値があります。
A. デバイスグループにタグを追加します。
B. デバイスユーザーを管理者ロールに追加します。
C. マシンにタグを追加します。
D. ランク1の新しいデバイスグループを作成します。
E. 新しい管理者ロールを作成します。
F. ランク4の新しいデバイスグループを作成します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

質問: **65**
新しいAzureサブスクリプション用にAzureSentinelをプロビジョニングします。セキュリティイベントコネクタを設定しています。
コネクタのテンプレートから新しいルールを作成するときに、イベントごとに新しいアラートを生成することにしました。次のルールクエリを作成します。
アラートをインシデントにグループ化できる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. ユーザー
B. コンピューター
C. IPアドレス
D. リソースグループ
正解: **(正解を表示します)**

質問: **66**
LogAnalytics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。
Azureリソースのジャストインタイム（JIT）VMアクセスとネットワーク検出を有効にする必要があります。
Azure Defenderをどこで有効にする必要がありますか？
A. サブスクリプションレベル
B. ワークスペースレベル
C. リソースレベルで
正解: **A (コメントを発表する)**
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

質問: **67**
エグゼクティブチームの問題を調査するには、高度なハンティングクエリを作成する必要があります。
どのようにクエリを完了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。
正解:

質問: **68**
Cloud Appのセキュリティ要件を満たすには、異常検出ポリシーの設定を変更する必要があります。
どのポリシーを変更する必要がありますか？
A. 疑わしいIPアドレスからのアクティビティ
B. 匿名IPアドレスからのアクティビティ

C. 不可能な旅
D. 危険なサインイン
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

質問: **69**
環境に影響を与える新しいCommonVulnerability and Exposures（CVE）の脆弱性が通知されます。文書化されたアクティブなエクスプロイトが利用可能な場合は、Microsoft Defender Security Centerを使用して、影響を受けるシステムを担当するチームに修復を要求する必要があります。順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
リファレンス：
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

質問: **70**
Azure Resource Managerテンプレートを使用して、特定のセキュリティアラートがAzure SecurityCenterによって受信されたときに自動修復をトリガーするワークフローの自動化を作成する必要があります。
必要なAzureリソースをプロビジョニングするテンプレートの部分をどのように完成させ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。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

質問: **71**
異常なAzureActive Directory（Azure AD）サインインアクティビティを追跡し、アクティビティを日ごとに集計されたタイムチャートとして表示するカスタムAzureSentinelクエリを作成することを計画しています。
タイムチャートを表示するために使用されるクエリを作成する必要があります。クエリには何を含める必要がありますか？
A. 拡張
B. ビン
C. メイクセット
D. ワークスペース
正解: **B (**コメントを発表する**)**

リファレンス：
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

質問: **72**
Azure Sentinelを使用して、不規則なAzureアクティビティを監視します。
次の展示に示すように、脅威を検出するためのカスタム分析ルールを作成します。
ルール定義の一部としてインシデント設定を定義しないでください。
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了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **73**
環境に影響を与える新しいCommonVulnerability and Exposures（CVE）の脆弱性が通知されます。
文書化されたアクティブなエクスプロイトが利用可能な場合は、Microsoft Defender Security Centerを使用して、影響を受けるシステムを担当するチームに修復を要求する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
説明
リファレンス：
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps

質問: **74**
エグゼクティブチームの問題を調査するには、高度なハンティングクエリを作成する必要があります。
どのようにクエリを完了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。
正解:
これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する

詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。
ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。

質問: **75**
Azure Active Directory（Azure AD）ユーザーをブロックするために使用される既存のAzureロジックアプリがあります。ロジックアプリは手動でトリガーされます。
AzureSentinelをデプロイします。
AzureSentinelのプレイブックとして既存のロジックアプリを使用する必要があります。
あなたは最初に何をすべきですか？
A. そして新しいスケジュールされたクエリルール。
B. AzureSentinelにデータコネクタを追加します。
C. AzureSentinelでカスタム脅威インテリジェンスコネクタを構成します。
D. ロジックアプリでトリガーを変更します。
正解: **(**正解を表示します**)**
説明/参照：

質問: **76**
Azure Defenderの要件とビジネス要件を満たすには、AzureDefenderを実装する必要があります。ソリューションに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。
正解:

質問: **77**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
AzureSentinelを構成しています。
悪意のあるIPアドレスからAzure仮想マシンへのサインインが検出された場合は、AzureSentinelでインシデントを作成する必要があります。
解決策 :データコネクタのスケジュールされたクエリルールを作成します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

質問: **78**
Microsoft Defender for Office365を使用するMicrosoft365サブスクリプションがあります。
機密文書を含むMicrosoftSharePointOnlineサイトがあります。ドキュメントには、それぞれ32文字の英数字で構成される顧客アカウント番号が含まれています。
機密文書を保護するには、データ損失防止 (DLP)ポリシーを作成する必要があります。どのドキュメントが機密であるかを検出するために何を使用する必要がありますか？
A. SharePoint検索
B. Microsoft 365Defenderでのハンティングクエリ
C. Azure Information Protection
D. 正規表現パターンマッチング
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

質問: **79**
127を超えるアラートを含むAzureSentinelのインシデントを調査しています。
インシデントで、さらに調査が必要な8つのアラートを発見しました。
アラートを別のAzureSentinel管理者にエスカレーションする必要があります。

管理者にアラートを提供するにはどうすればよいですか？
A. Microsoftインシデント作成ルールを作成します
B. インシデントURLを共有する
C. スケジュールされたクエリルールを作成します
D. インシデントを割り当てます
正解**: D (**コメントを発表する**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

質問**: 80**
ドラッグドロップ
ビジネス要件を満たすようにDC1を構成する必要があります。
順番に実行する必要がある4つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解**:**
セクション :[なし]
Explanation:
手順1 :グローバル管理者としてhttps://portal.atp.azure.comにログインします
ステップ2 :インスタンスを作成する
手順3.インスタンスをActiveDirectoryに接続します
ステップ4.センサーをダウンロードしてインストールします。
リファレンス：
https://docs.microsoft.com/en-us/defender-for-identity/install-step1
https://docs.microsoft.com/en-us/defender-for-identity/install-step4
質問セット3

質問**: 81**
Microsoft Defender for Endpointを使用して解決できるチームの問題は？
A. エグゼクティブ
B. 販売
C. マーケティング
正解**: B (**コメントを発表する**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios
ケーススタディ

これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。
あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。
ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、[次へ]ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであることに注意してください。質問に答える準備ができたら、[質問]ボタンをクリックして質問に戻ります。
概要
Contoso Ltd.という名前の会社には、北米全体に本社と5つの支店があります。
本社はシアトルにあります。支店はトロント、マイアミ、ヒューストン、ロサンゼルス、バンクーバーにあります。
Contosoには、ニューヨークとサンフランシスコにオフィスを構えるFabrikam、Ltd。という名前の子会社があります。
既存の環境
エンドユーザー環境
Contosoのすべてのユーザーは Windows10デバイスを使用しています。各ユーザーは Microsoft365のライセンスを取得しています。さらに、iOSデバイスはContosoの営業チームのメンバーに配布されます。
クラウドとハイブリッドインフラストラクチャ
すべてのContosoアプリケーションはAzureにデプロイされます。
Microsoft Cloud AppSecurityを有効にします。
ContosoとFabrikamには、異なるAzure Active Directory（Azure AD）テナントがあります。Fabrikamは最近Azureサブスクリプションを購入し、サポートされているすべてのリソースタイプに対してAzureDefenderを有効にしました。
現在の問題

Contosoのセキュリティチームは、多数のサイバーセキュリティアラートを受信します。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威であり、どれがそうでないかを特定するのに多くの時間を費やしています。
Contosoの営業チームはiOSデバイスのみを使用しています。営業チームのメンバーは、さまざまなサードパーティツールを使用して顧客とファイルを交換します。過去に、営業チームはデバイスに対してさまざまな攻撃を経験しました。
Contosoのマーケティングチームには、外部ベンダーと協力するためのMicrosoft SharePointOnlineサイトがいくつかあります。マーケティングチームには、ベンダーがマルウェアを含むファイルをアップロードするという事件がいくつかありました。
Contosoのエグゼクティブチームは、セキュリティ違反を疑っています。エグゼクティブチームは、Microsoft Cloud App Securityで保護されたアプリケーションのデータアクセス、ダウンロード、削除など、過去48時間に5つを超えるアクティビティがあったファイルを特定するように要求します。
要件
計画された変更
Contosoは、両社のセキュリティ運用を統合し、すべてのセキュリティ運用を一元管理することを計画しています。
技術要件
Contosoは、次の技術要件を識別します。
* Azure仮想マシンがブルートフォース攻撃を受けている場合にアラートを受信します。
* Azure Sentinelを使用して、環境に対するアクティブな攻撃を迅速に修正することにより、組織のリスクを軽減します。
* ContosoとFabrikamのAzureADテナント間でデータを相互に関連付けるAzureSentinelクエリを実装します。
*外部の攻撃者や独自のAzureADアプリケーションの潜在的な侵害が発生した場合に、FabrikamのKeyVaultアラート用のAzureDefenderを修正する手順を開発します。
*特定の国から初めてAzureリソースにサインインできなかったユーザーのすべてのケースを特定します。ジュニアセキュリティ管理者は、次の不完全なクエリを提供します。
BehaviorAnalytics
| ここで、ActivityType == "FailedLogOn"
| ここで、_____ == True

質問: **82**
あなたの会社はイスタンブールに単一のオフィスとMicrosoft365サブスクリプションを持っています。
同社は、条件付きアクセスポリシーを使用して、多要素認証（MFA）を実施することを計画しています。
リモートで作業するすべてのユーザーにMFAを適用する必要があります。
ソリューションに何を含める必要がありますか？

A. 詐欺の警告
B. ユーザーリスクポリシー
C. 名前付きの場所
D. サインインユーザーポリシー
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

質問: **83**
サポートされているすべてのリソースタイプに対してAzureDefenderが有効になっているAzureサブスクリプションがあります。
LA1という名前のAzureロジックアプリを作成します。
LA1を使用して、Azure SecurityCenterで検出されたセキュリティリスクを自動的に修正することを計画しています。
セキュリティセンターでLA1をテストする必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
正解:
説明
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-whe

質問: **84**
異常なAzureActive Directory（Azure AD）サインインアクティビティを追跡し、アクティビティを日ごとに集計されたタイムチャートとして表示するカスタムAzureSentinelクエリを作成することを計画しています。
タイムチャートを表示するために使用されるクエリを作成する必要があります。
クエリには何を含める必要がありますか？
A. 拡張
B. ビン
C. メイクセット
D. ワークスペース
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

質問: **85**
新しいAzureサブスクリプションを作成し、AzureMonitorのログの収集を開始します。

疑わしいIPアドレスからAzure仮想マシンへのサインインに関連する可能性のある脅威を検出するようにAzureSecurityCenterを構成する必要があります。ソリューションは構成を検証する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
説明
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **86**
Azure SecurityCenterによって生成されたセキュリティアラートの視覚的表現を提供するカスタムAzureSentinelクエリを作成することを計画しています。
棒グラフを表示するために使用されるクエリを作成する必要があります。クエリには何を含める必要がありますか？
A. 拡張
B. ビン
C. カウント
D. ワークスペース
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-chart-visualizations

質問: **87**
ホットスポット
Azure Sentinelの要件を満たすには、分析ルールを作成する必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。
ホットエリア：
正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and- create-the-rule
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook質問セット3

質問: **88**
AzureとGoogleクラウドにリソースがあります。
Google Cloud Platform（GCP）データをAzureDefenderに取り込む必要があります。

アクションを実行する順序はどれですか。回答するには、すべてのアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
説明
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

質問: **89**
AzureSentinelを構成しています。
疑わしいIPアドレスからのサインインが検出されるたびに、MicrosoftTeamsメッセージをチャネルに送信する必要があります。
Azure Sentinelで実行する必要がある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：正しい選択はそれぞれ1ポイントの価値があります。
A. プレイブックを追加します。
B. プレイブックをインシデントに関連付けます。
C. エンティティの動作分析を有効にします。
D. ワークブックを作成します。
E. フュージョンルールを有効にします。
正解: **(**正解を表示します**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **90**
ドラッグドロップ
AzureとGoogleクラウドにリソースがあります。
Google Cloud Platform（GCP）データをAzureDefenderに取り込む必要があります。
アクションを実行する順序はどれですか。回答するには、すべてのアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
選択して配置：
正解:
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

質問: **91**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryとのID統合のためにMicrosoftDefenderを構成しています。
Microsoft Defender for Identityポータルから、攻撃者が悪用できるようにいくつかのアカウントを構成する必要があります。
解決策 :エンティティタグから、アカウントをハニートークンアカウントとして追加します。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

質問: **92**
sub1という名前のAzureサブスクリプションを作成します。
sub1では、workspace1という名前のLogAnalyticsワークスペースを作成します。
Azure Security Centerを有効にし、workspace1を使用するようにSecurityCenterを構成します。
SecurityCenterがworkspace1にレポートするAzure仮想マシンからのイベントを処理することを確認する必要があります。
あなたは何をするべきか？
A. workspace1にソリューションをインストールします。
B. sub1にプロバイダーを登録します。
C. セキュリティセンターから、ワークフローの自動化を作成します。
D. workspace1で、ブックを作成します。
正解: **(**正解を表示します**)**
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

質問: **93**
Azure InformationProtectionの要件を実装する必要があります。
最初に何を構成する必要がありますか？

A. Microsoft Defender SecurityCenterのデバイスヘルスおよびコンプライアンスレポートの設定
B. AzureポータルからのAzure InformationProtectionのスキャナークラスター
C. AzureポータルからのAzure InformationProtectionのコンテンツスキャンジョブ
D. Microsoft Defender SecurityCenterの設定の高度な機能
正解**: (**正解を表示します**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview

質問**: 94**
Azure仮想マシンの技術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必要がありますか？
A. ジャストインタイム（JIT）アクセス
B. Azure Defender
C. Azureファイアウォール
D. Azure Application Gateway
正解**: (**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/azure-defender
トピック2、Litwareinc。
ケーススタディ
これはケーススタディです。ケーススタディは個別にタイミングが調整されていません。各ケースを完了するのに必要なだけの試験時間を使用できます。ただし、この試験には追加のケーススタディとセクションがある場合があります。あなたはあなたが提供された時間内にこの試験に含まれるすべての質問を完了することができることを確実にするためにあなたの時間を管理しなければなりません。
ケーススタディに含まれている質問に答えるには、ケーススタディで提供されている情報を参照する必要があります。ケーススタディには、ケーススタディで説明されているシナリオに関する詳細情報を提供する展示やその他のリソースが含まれている場合があります。このケーススタディでは、各質問は他の質問から独立しています。
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。
ケーススタディを開始するには
このケーススタディの最初の質問を表示するには、ボタンをクリックします。質問に答える前に、左側のペインのボタンを使用して、ケーススタディの内容を調べてください。これらのボタンをクリックすると、ビジネス要件、既存の環境、問題の説明などの情報が表示されます。ケーススタディに[すべての情報]タブがある場合、表示される情報は後続のタブに表示される情報と同じであ

ることに注意してください。質問に答える準備ができたら、ボタンをクリックして質問に戻ります。
概要
LitwareInc。は再生可能な会社です。
Litwareは、ボストンとシアトルにオフィスを構えています。Litwareには、米国全土にリモートユーザーがいます。クラウドリソースを含むLitwareリソースにアクセスするために、リモートユーザーはいずれかのオフィスへのVPN接続を確立します。
既存の環境
アイデンティティ環境
ネットワークには、litware.comという名前のAzure Active Directory（Azure AD）テナントと同期するlitware.comという名前のActiveDirectoryフォレストが含まれています。
Microsoft365環境
Litwareには、litware.com AzureADテナントにリンクされたMicrosoft365E5サブスクリプションがあります。Microsoft Defender for Endpointは、Windows10を実行しているすべてのコンピューターに展開されます。すべてのMicrosoftCloud AppSecurityの組み込みの異常検出ポリシーが有効になっています。
Azure環境
Litwareには、litware.com AzureADテナントにリンクされたAzureサブスクリプションがあります。次の表に示すように、サブスクリプションには米国東部のAzureリージョンのリソースが含まれています。
ネットワーク環境
各Litwareオフィスはインターネットに直接接続し、Azureサブスクリプションの仮想ネットワークへのサイト間VPN接続を備えています。
オンプレミス環境
オンプレミスネットワークには、次の表に示すコンピューターが含まれています。
現在の問題
Cloud App Securityは、ユーザーが両方のオフィスに同時に接続すると、誤検知アラートを頻繁に生成します。
計画された変更
Litwareは、次の変更を実装する予定です。
* AzureサブスクリプションでAzureSentinelを作成および構成します。
* Azure ADテストユーザーアカウントを使用して、AzureSentinelの機能を検証します。
ビジネス要件
Litwareは、次のビジネス要件を識別します。
*可能な限り、最小特権の原則を使用する必要があります。
*他のすべての要件が満たされている限り、コストを最小限に抑える必要があります。
* Log Analyticsによって収集されたログは、ユーザーアクティビティの完全な監査証跡を提供する必要があります。

*すべてのドメインコントローラーは、Microsoft Defender forIdentityを使用して保護する必要があります。
Azure InformationProtectionの要件
セキュリティラベルがあり、Windows 10コンピューターに保存されているすべてのファイルは、Azure InformationProtection-データ検出ダッシュボードから利用できる必要があります。
エンドポイント要件のためのMicrosoftDefender
すべてのCloudApp Securityの認可されていないアプリは、Microsoft Defender forEndpointを使用してWindows10コンピューターでブロックする必要があります。
Microsoft CloudAppのセキュリティ要件
Cloud App Securityは、テナントレベルのデータに基づいて、ユーザー接続が異常であるかどうかを識別する必要があります。
AzureDefenderの要件
すべてのサーバーは、同じLogAnalyticsワークスペースにログを送信する必要があります。
AzureSentinelの要件
Litwareは、次のAzureSentinel要件を満たしている必要があります。
* AzureSentinelとCloudAppSecurityを統合します。
* admin1という名前のユーザーがAzureSentinelプレイブックを構成できることを確認します。
*カスタムクエリに基づいてAzureSentinel分析ルールを作成します。ルールは、プレイブックの実行を自動的に開始する必要があります。
*特定のIPアドレスからのデータアクセスを表すイベントにメモを追加して、ハンティング中に調査グラフをナビゲートするときにIPアドレスを参照できるようにします。
* AzureADテストユーザーアカウントによるMicrosoftOffice365へのインバウンドアクセスが検出されたときにアラートを生成するテストルールを作成します。ルールによって生成されたアラートは、テストユーザーアカウントごとに1つのインシデントを使用して、個々のインシデントにグループ化する必要があります。

質問: **95**
Microsoft Defender for Endpointを使用して解決できるチームの問題は？
A. エグゼクティブ
B. 販売
C. マーケティング
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

質問: **96**
新しいAzureサブスクリプションでLinux仮想マシンをプロビジョニングします。
Azure Defenderを有効にして、仮想マシンをAzureDefenderにオンボードします。

仮想マシンへの攻撃がAzureDefenderでアラートをトリガーすることを確認する必要があります。
仮想マシンで実行する必要がある2つのBashコマンドはどれですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. cp / bin / echo ./asc_alerttest_662jfi039n
B. ./ alerttestテストeicarパイプ
C. cp / bin / echo ./alerttest
D. ./ asc_alerttest_662jfi039neicarパイプのテスト
正解: **(正解を表示します)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your- azure-vms-linux-

質問: **97**
Azure Sentinelデータを視覚化し、サードパーティのデータソースを使用してデータを強化し、侵入の痕跡（IoC）を特定する必要があります。
何を使うべきですか？
A. AzureSentinelのノートブック
B. Microsoftクラウドアプリのセキュリティ
C. Azureモニター
D. AzureSentinelでのクエリのハンティング
正解: **(正解を表示します)**
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

質問: **98**
米国東部のAzureリージョンにAzureSentinelをデプロイしています。
米国西部のAzureリージョンにLogsWestという名前のLogAnalyticsワークスペースを作成します。
LogsWestへのクエリに基づいてアラートを生成するには、既存のAzureSentinelデプロイメントでスケジュールされた分析ルールを使用できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. Azureデータカタログを米国西部のAzureリージョンにデプロイします。
B. 既存のAzureSentinelデプロイメントのワークスペース設定を変更します。
C. AzureSentinelをワークスペースに追加します。
D. AzureSentinelでデータコネクタを作成します。
正解: **(正解を表示します)**
セクション :[なし]

説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問: **99**
Azure Security Centerには、テストに使用される10台の仮想マシンに対する抑制ルールがあります。仮想マシンはWindowsServerを実行します。
仮想マシンの問題のトラブルシューティングを行っています。
セキュリティセンターでは、過去5日間に仮想マシンによって生成されたアラートを表示する必要があります。
あなたは何をするべきか？
A. 抑制ルールのルール有効期限を変更します。
B. 抑制ルールの状態を無効に変更します。
C. セキュリティアラートページのフィルターを変更します。
D. 仮想マシンのWindowsイベントログを表示します。
正解: **B (**コメントを発表する**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

質問: **100**
AzureとGoogleクラウドにリソースがあります。
Google Cloud Platform（GCP）データをAzureDefenderに取り込む必要があります。
アクションを実行する順序はどれですか。回答するには、すべてのアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

質問: **101**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成す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あ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した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure SecurityCenterを使用します。
セキュリティセンターでセキュリティアラートを受け取ります。
セキュリティセンターでアラートを解決するには、推奨事項を表示する必要があります。
解決策 :[セキュリティアラート]から、アラートを選択し、[アクションの実行]を選択して、[今後の攻撃の防止]セクションを展開します。
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**)**
セクション :[なし]
Explanation:
将来のアラートを防ぐのではなく、既存のアラートを解決する必要があります。したがって、 脅威を軽減する」オプションを選択する必要があります。
リファレンス：
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

質問: **102**
AzureSentinelのデプロイがあります。
疑わしいすべての資格情報アクセスアクティビティを照会する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。
正解:
1-Azure Sentinelから、[ハンティング]を選択します。
2-戦術でフィルタリングします。
3- [すべてのクエリを実行]を選択します。

質問: **103**
組織内の他のユーザーがサインインに使用したことのない場所からユーザーがサインインしようとすると、セキュリティアラートを受信する必要があります。
どの異常検出ポリシーを使用する必要がありますか？
A. 不可能な旅
B. 匿名IPアドレスからのアクティビティ
C. 頻度の低い国からの活動
D. マルウェアの検出
正解: **(**正解を表示します**)**
悪意のある活動を示す可能性のある国/地域からの活動。このポリシーは、環境のプロファイルを作成し、組織内のユーザーが最近アクセスしたことがない、またはアクセスしたことがない場所からアクティビティが検出されたときにアラートをトリガーします。2つの場所間の予想移動時間よりも短い期間内の、異なる場所での同じユーザーからのアクティビティ。これは、資格情報の侵害を示している可能性がありますが、VPNを使用するなどして、ユーザーの実際の場所がマスクされている可能性もあります。
リファレンス：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

質問: **104**

技術的な要件を満たすには、アクティブな攻撃を修正する必要があります。
ソリューションに何を含める必要がありますか？
A. AzureAutomationのRunbook
B. Azure Logic Apps
C. Azure関数
D. AzureSentinelライブストリーム
正解: **(**正解を表示します**)**
リファレンス：
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks