Microsoft.SC-200.v2022-04-23.q109

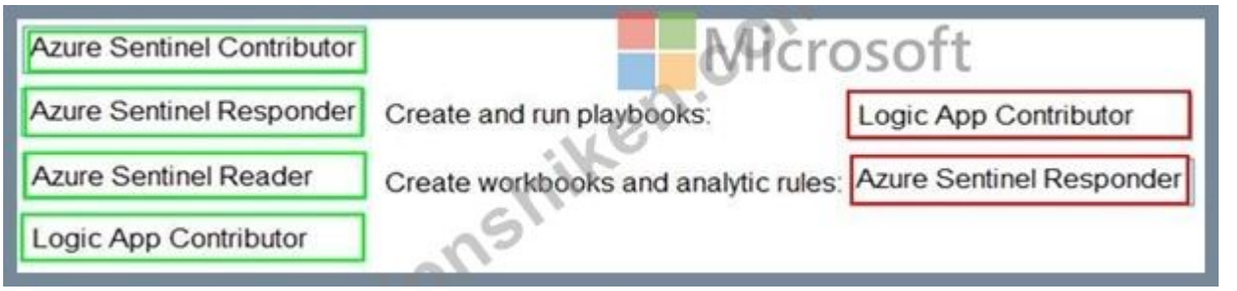
試験コード：	SC-200
試験名称：	Microsoft Security Operations Analyst
認証ベンダー：	Microsoft
無料問題の数：	109
バージョン：	v2022-04-23
ページの閲覧量：	1510
問題集の閲覧量：	39993

https://www.jpnshiken.com/shiken/Microsoft.SC-200.v2022-04-23.q109.html

質問**: 1**
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**: A (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

質問**: 2**
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:



参照：

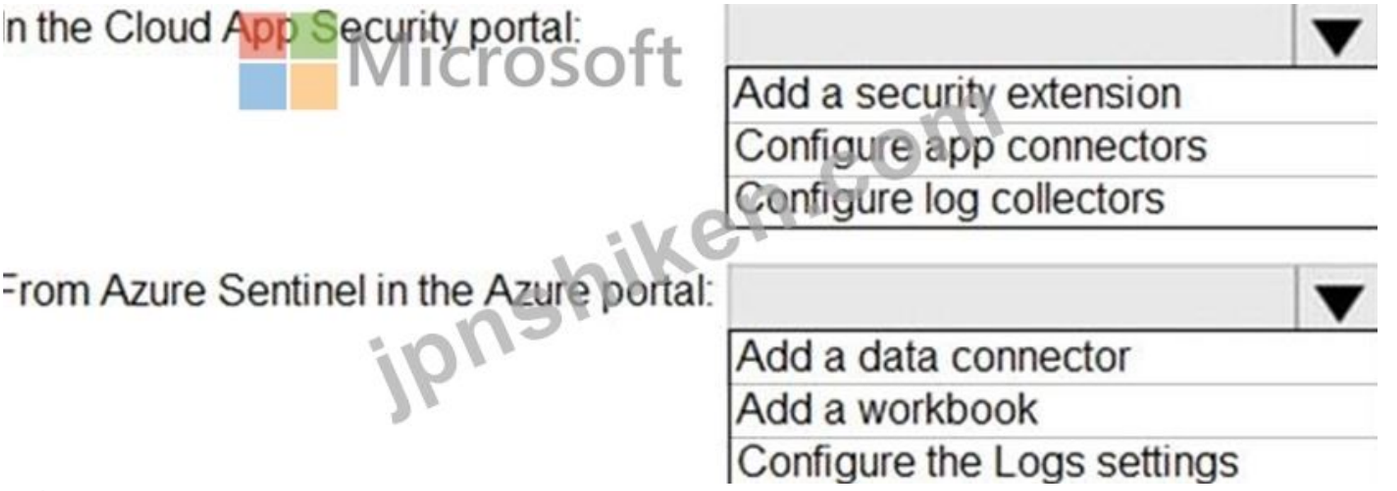
https://docs.microsoft.com/en-us/azure/sentinel/roles

質問: **3**

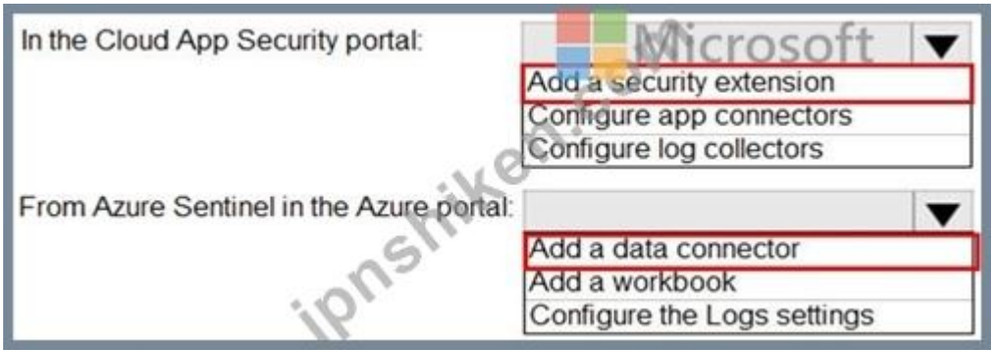
Azure Sentinelの要件を満たすように、AzureSentinel統合を構成する必要があります。

あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択してください。

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:



参照：

https://docs.microsoft.com/en-us/cloud-app-security/siem-sentinel

質問: **4**
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: **C (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

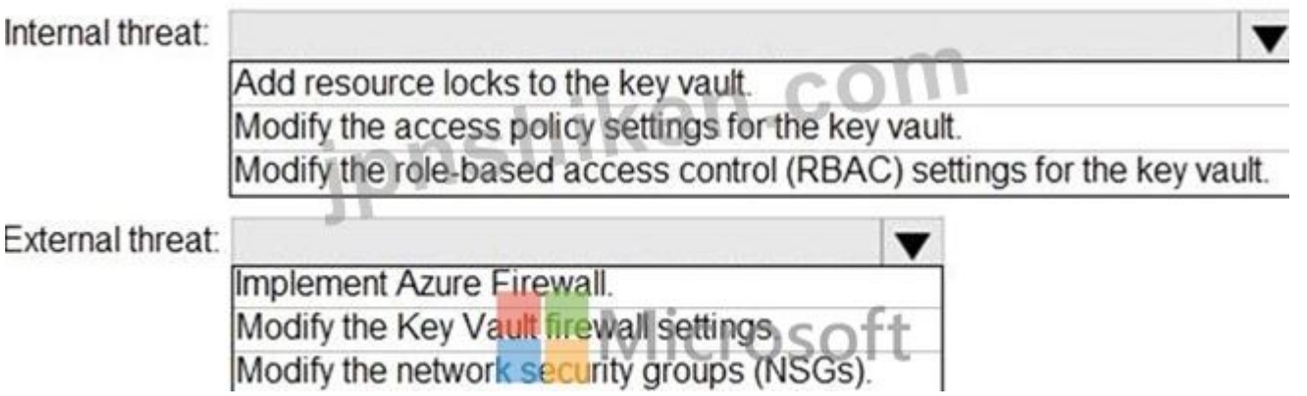
質問: **5**
あなたの会社はAzureSentinelを使用しています。
新しいセキュリティアナリストは、AzureSentinelでインシデントを割り当てて解決できないと報告しています。
アナリストがインシデントを割り当てて解決できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
アナリストにどの役割を割り当てる必要がありますか？
A. Azure Sentinel Responder
B. ロジックアプリコントリビューター
C. AzureSentinelコントリビューター
D. Azure Sentinel Reader
正解: **(**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: **6**
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。

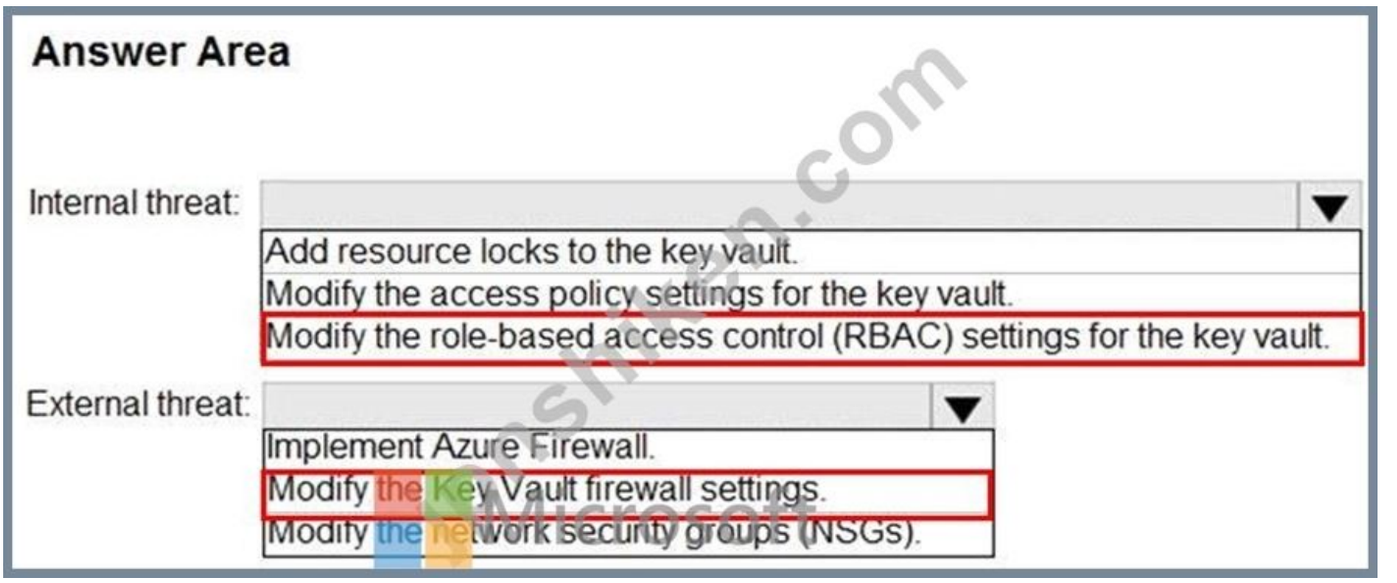
C. マシンにタグを追加します。
D. ランク1の新しいデバイスグループを作成します。
E. 新しい管理者ロールを作成します。
F. ランク4の新しいデバイスグループを作成します。
正解: (正解を表示します)
説明/参照：
https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/

質問: **7**
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: **8**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。
Answer Area



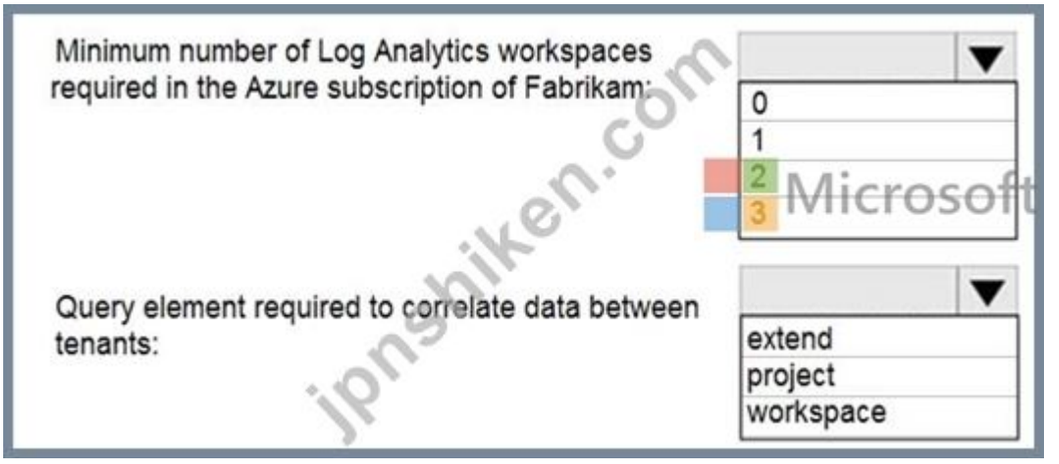
正解:



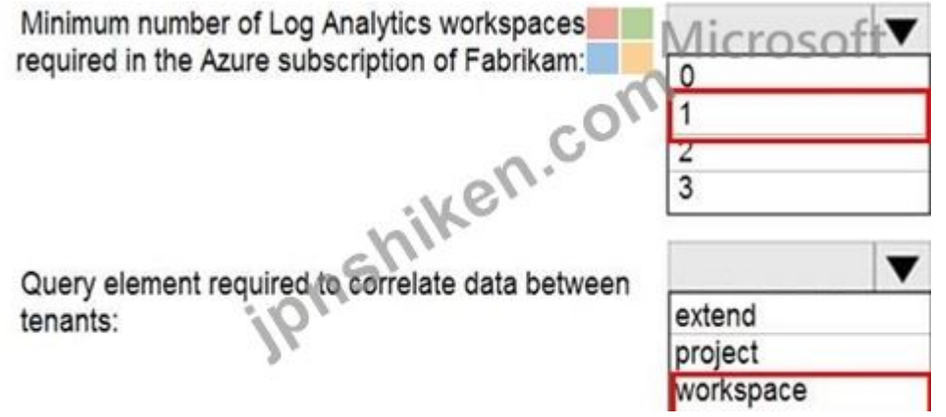
参照：
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

質問: **9**
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. ロジックアプリでトリガーを変更します。
C. AzureSentinelにデータコネクタを追加します。
D. 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。
正解: **(**正解を表示します**)**

質問: **10**
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、回答エリアで適切なオプションを選択してください。
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:



参照：

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。

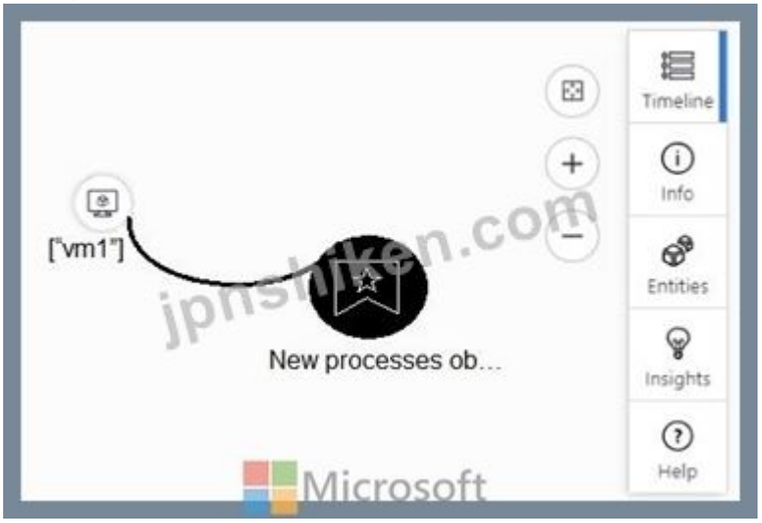
このケーススタディの最後に、レビュー画面が表示されます。この画面では、試験の次のセクションに進む前に、回答を確認して変更を加えることができます。新しいセクションを開始した後は、このセクションに戻ることはできません。

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: **11**
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。

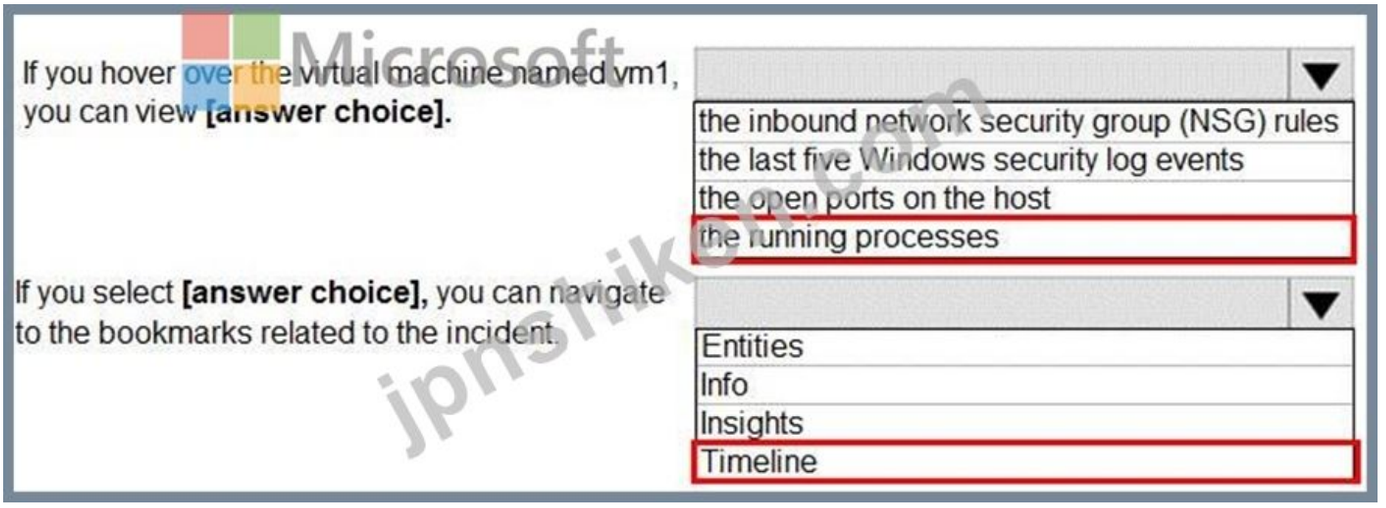
f you hover over the virtual machine named vm1, you can view **[answer choice]**.

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

you select **[answer choice]**, you can navigate o the bookmarks related to the incident.

- Entities
- Info
- Insights
- Timeline

正解:



参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

質問: **12**
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格納します。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)**
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: **13**
MicrosoftDefenderを使用するMicrosoft365E5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。クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

正解:

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

(DeviceId)
(RecipientEmailAddress)
(SenderFromAddress)
(SHA256)

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: **14**
次の環境があります。
AzureSentinel
Microsoft365サブスクリプション
アイデンティティのためのMicrosoftDefender
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 DefenderforIdentity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: **A,D (**コメントを発表する**)**
参照：
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: **15**
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イベントグリッド
B. Azure Data Lake
C. Azureイベントハブ
D. Azure Cosmos DB
正解: **(**正解を表示します**)**

質問: **16**

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: **17**
異常なAzureActiveDirectory（Azure AD）サインインアクティビティを追跡し、その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: **18**
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to
B. a URL/domain indicator that has Action set to
C. a file hash indicator that has Action set to
D. a certificate indicator that has Action set to Alert and block
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

質問**: 19**
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答えた後は、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：各アカウントを機密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**: B (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

質問**: 20**
あなたの会社は、MicrosoftOfficeVBA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.
```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```
B.
```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

C.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC
-AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

D.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

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/attack-surface-reduction

質問: **21**

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答えた後は、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 :クエリからライブストリームを作成します。

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**)**

参照：

https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

質問: **22**

AzureSentinelを構成しています。

サインインリスクイベントを表すインシデントがAzureSentinelでアクティブ化されるたびに、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。

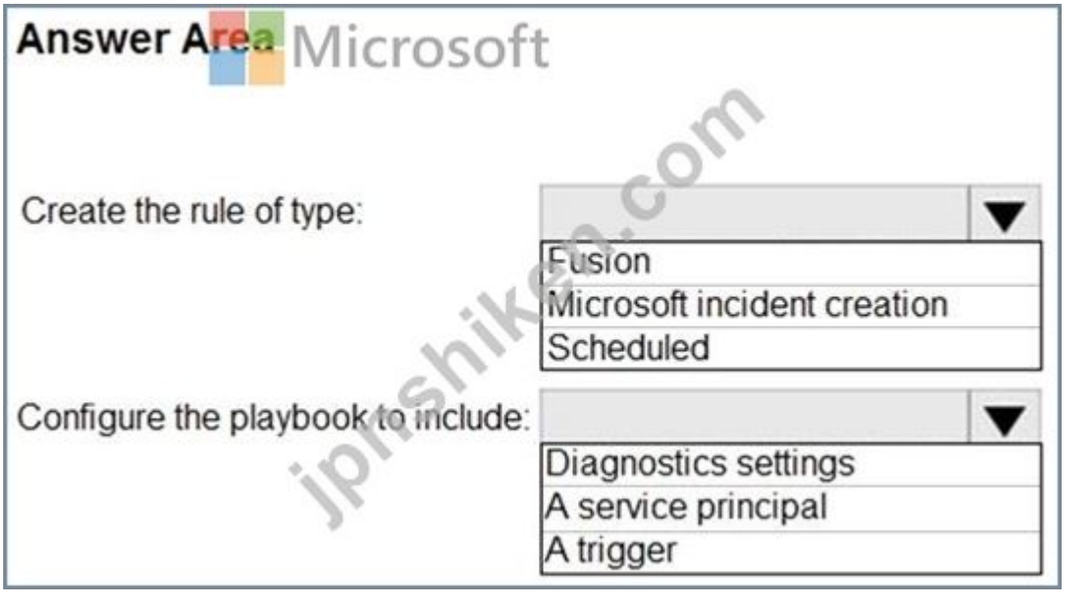
A. エンティティの動作分析を有効にします。

B. インシデントをトリガーした分析ルールにプレイブックを関連付けます。

C. Fusionルールを有効にします。

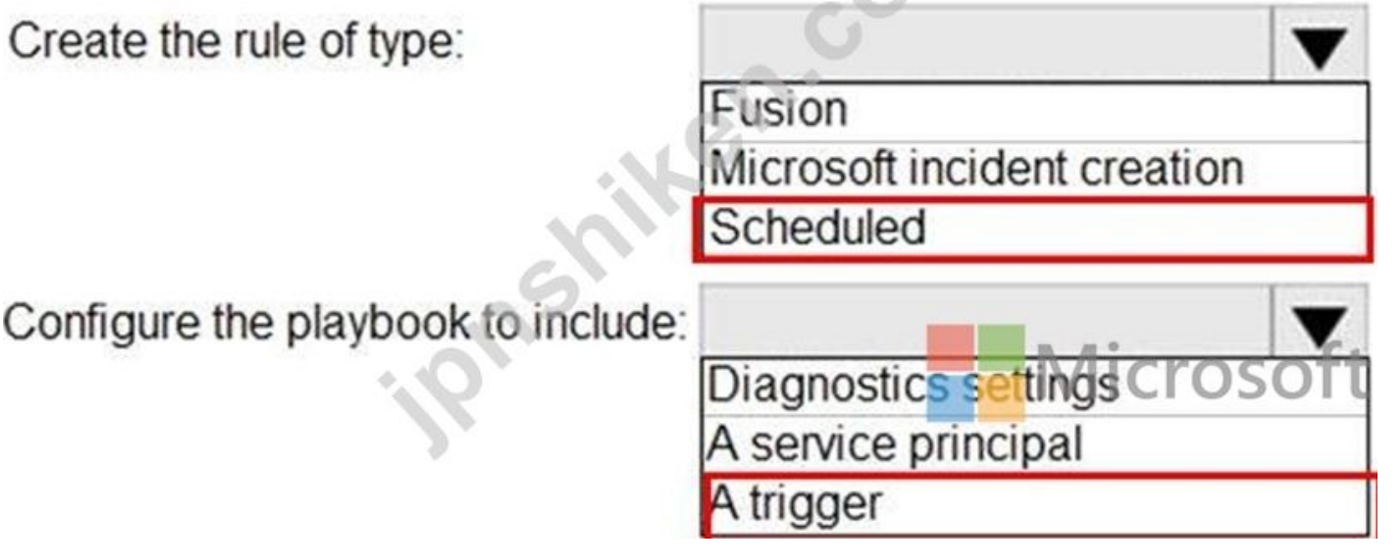
D. プレイブックを追加します。
E. ワークブックを作成します。
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/azure/sentinel/enable-entity-behavior-analytics
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

質問: **23**
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、回答エリアで適切なオプションを選択してください。
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:

Answer Area

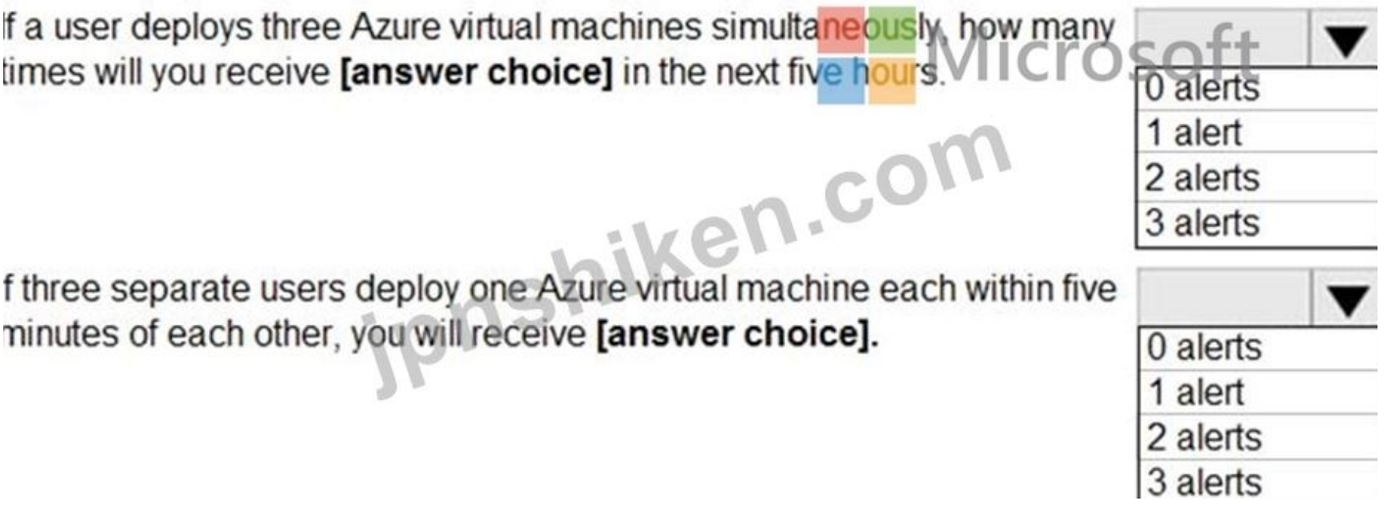


質問: **24**

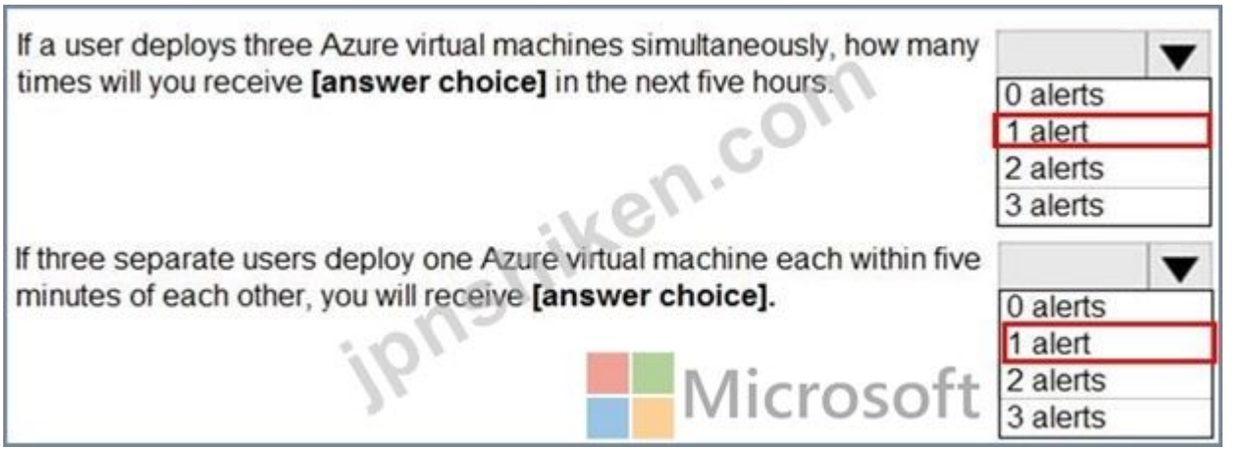
Azure Sentinelを使用して、不規則なAzureアクティビティを監視します。

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。

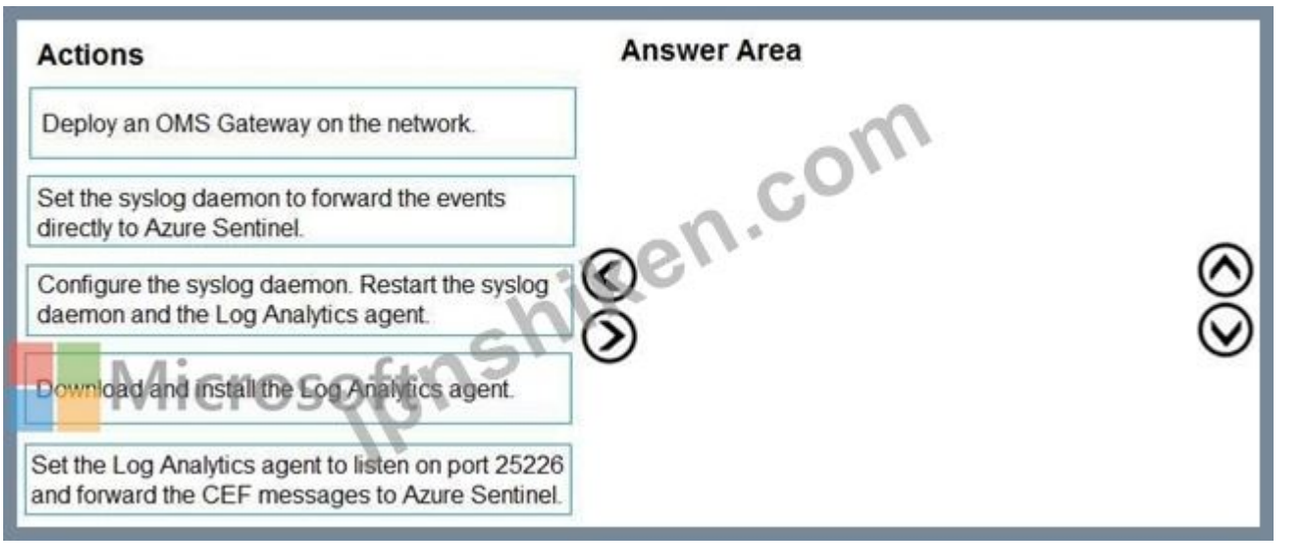


正解:

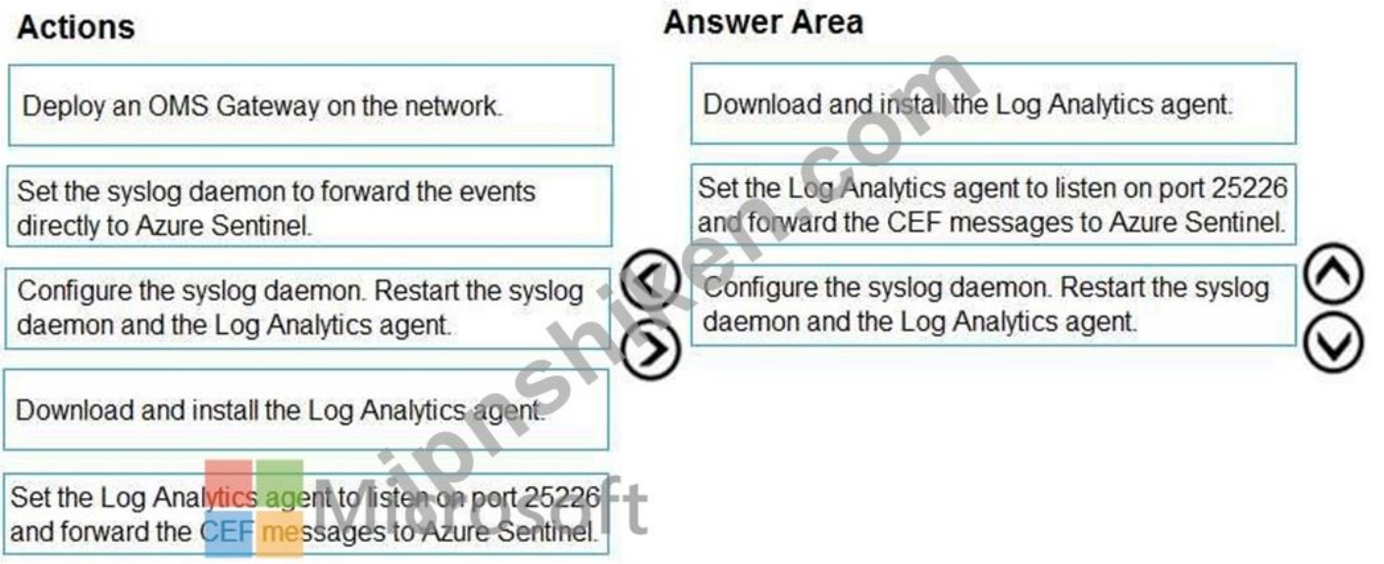


参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **25**
ドラッグドロップ
Common Event Format（CEF）メッセージをAzureSentinelに送信する外部ソリューションを接続することを計画しています。
ログフォワーダーをデプロイ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/connect-cef-agent?tabs=rsyslog

質問: **26**
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. 不可能な旅
B. 匿名IPアドレスからのアクティビティ
C. 疑わしいIPアドレスからのアクティビティ
D. 危険なサインイン
正解: **(正解を表示します)**

質問: **27**
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: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

質問: **28**
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

Configure the GCP Security Command Center.

Enable Security Health Analytics.

Enable the GCP Security Command Center API.

Create a dedicated service account and a private key.

From Azure Security Center, add cloud connectors.

参照：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

質問: **29**
ブックのクエリを作成する必要があります。クエリは次の要件を満たしている必要があります。
すべてのインシデントをインシデント番号別に一覧表示します。
各インシデントの最新のログのみを含めます。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

正解:

```
SecurityIncident
| [project / sort / summarize] [arg_max / limit / top] (LasModifiedTime,*) by IncidentNumber
```

参照：
https://www.drware.com/whats-new-soc-operational-metrics-now-available-in-sentinel/

質問: **30**
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)**
参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios
トピック1、Contoso Ltd
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
Contoso Ltd.という名前の会社には、北米全体に本社と5つの支社があります。
本社はシアトルにあります。支社はトロント、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持つ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 CloudAppSecurity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の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 MicrosoftSharePointOnline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: **31**
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: **B (**コメントを発表する**)**
参照：
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.comAzureAD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MicrosoftCloudAppSecurity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.comAzureAD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。

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

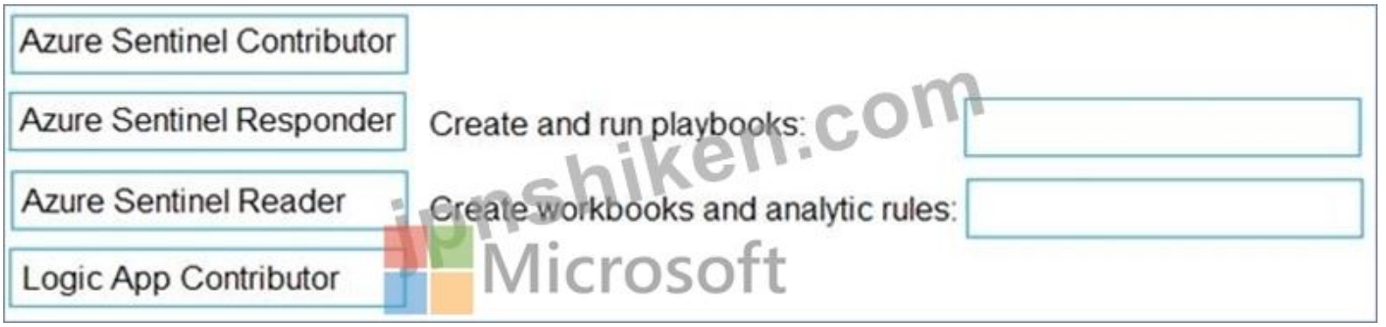
現在の問題
Cloud App Securityは、ユーザーが両方のオフィスに同時に接続すると、誤検知アラートを頻繁に生成します。
計画された変更
Litwareは、次の変更を実装する予定です。
*AzureサブスクリプションでAzureSentinelを作成および構成します。
* Azure ADテストユーザーアカウントを使用して、AzureSentinelの機能を検証します。
ビジネス要件
Litwareは、次のビジネス要件を識別します。
*可能な限り、最小特権の原則を使用する必要があります。
*他のすべての要件が満たされている限り、コストを最小限に抑える必要があります。
* Log Analytics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 DefenderforIdentityを使用して保護する必要があります。
AzureInformationProtection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、AzureInformationProtection-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CloudAppSecurityの認可されていないアプリは、Microsoft DefenderforEndpoint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。

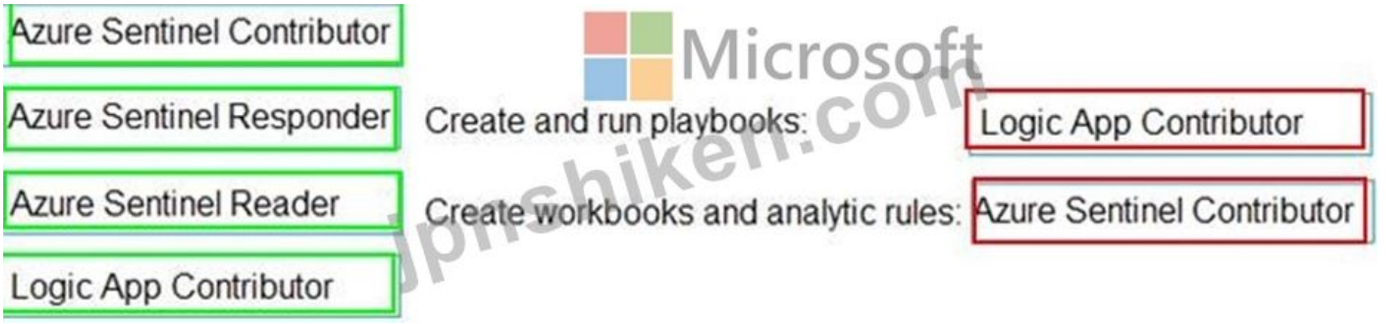
質問: **32**
AzureInformationProtectionの要件を実装する必要があります。最初に何を構成する必要がありますか？
A. Microsoft DefenderSecurityCenterのデバイスヘルスおよびコンプライアンスレポートの設定
B. AzureポータルからのAzureInformationProtectionのスキャナークラスター
C. AzureポータルからのAzureInformationProtectionのコンテンツスキャンジョブ

D. Microsoft DefenderSecurityCenterの設定の高度な機能
正解: **(**正解を表示します**)**
説明
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview

質問: **33**
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:



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

質問: **34**
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ドキュメントがあります。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**)**
説明/参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

質問**: 35**
You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?
A. a URL/domain indicator that has Action set to Alert only
B. アクションがアラートおよびブロックに設定されているURL/ドメインインジケーター
C. アクションがアラートおよびブロックに設定されているファイルハッシュインジケーター
D. アクションがアラートおよびブロックに設定されている証明書インジケーター
正解**: C (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

質問**: 36**
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答えた後は、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。
AzureSecurityCenter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: **(**正解を表示します**)**
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。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

質問: **37**
KeyVaultのAzureDefender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**)**
参照：
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

質問: **38**
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。

Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

General | Set rule logic | Incident settings | Automated response | Review and create

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every *

5 | Minutes

Lookup data from the last * ⓘ

5 | Hours

Alert threshold

Generate alert when number of query results *

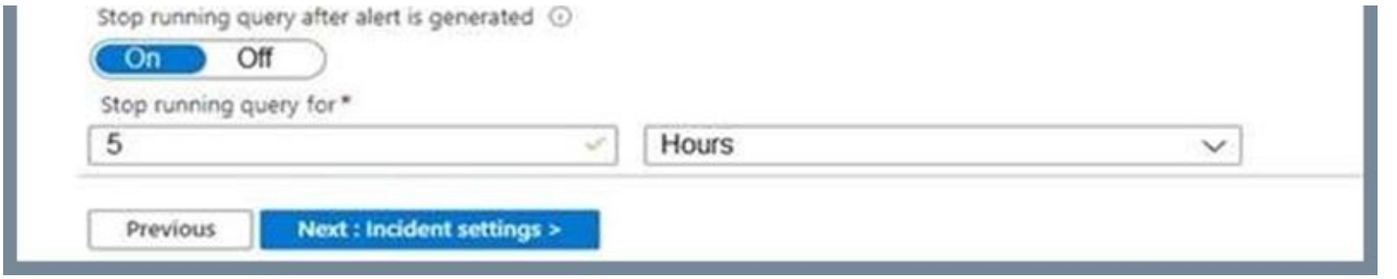
Is greater than | 2

Event grouping

Configure how rule query results are grouped into alerts

- (•) Group all events into a single alert
- ( ) Trigger an alert for each event

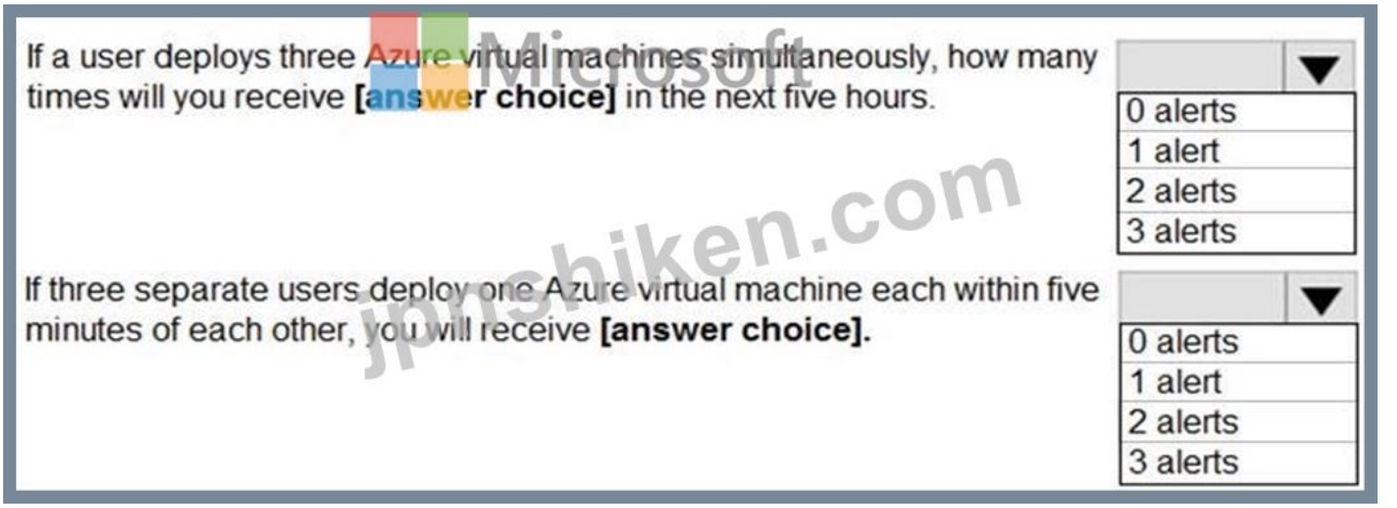
Suppression



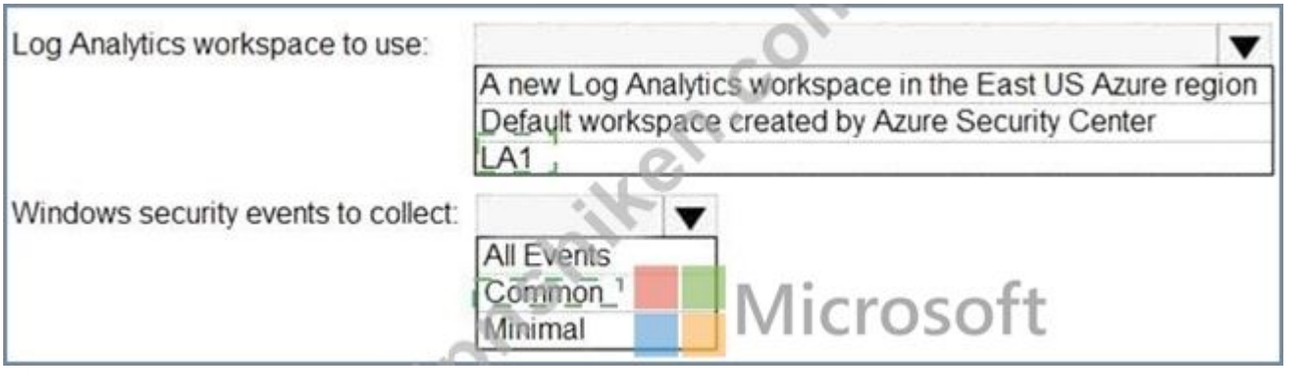
ルール定義の一部としてインシデント設定を定義しないでください。

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。

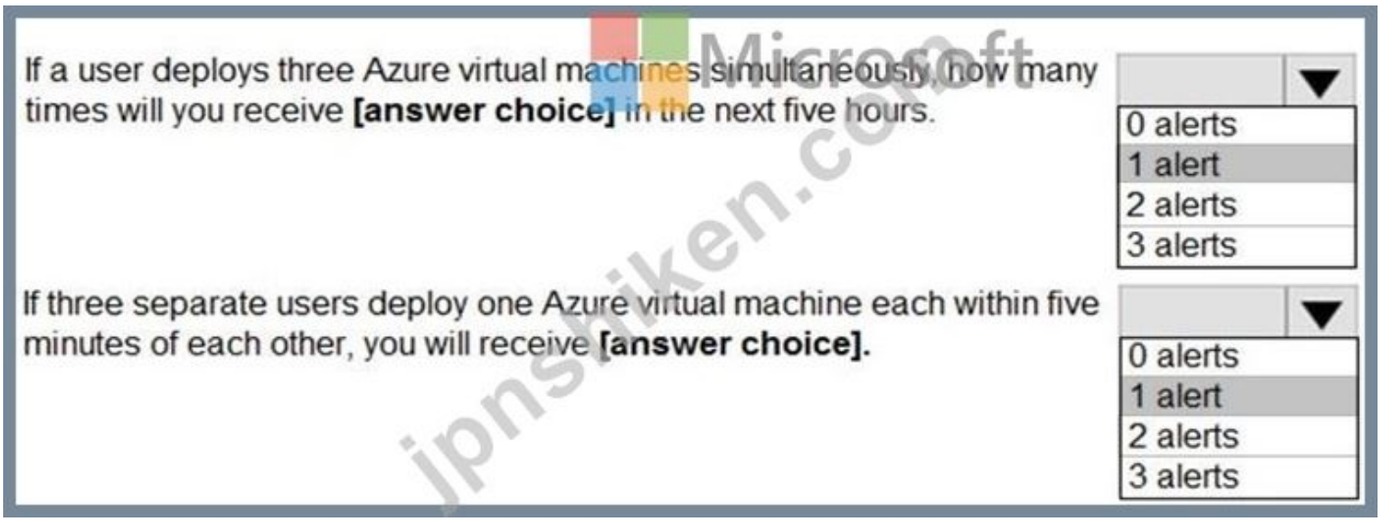


正解:



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、電子メール説明が自動的に生成されます



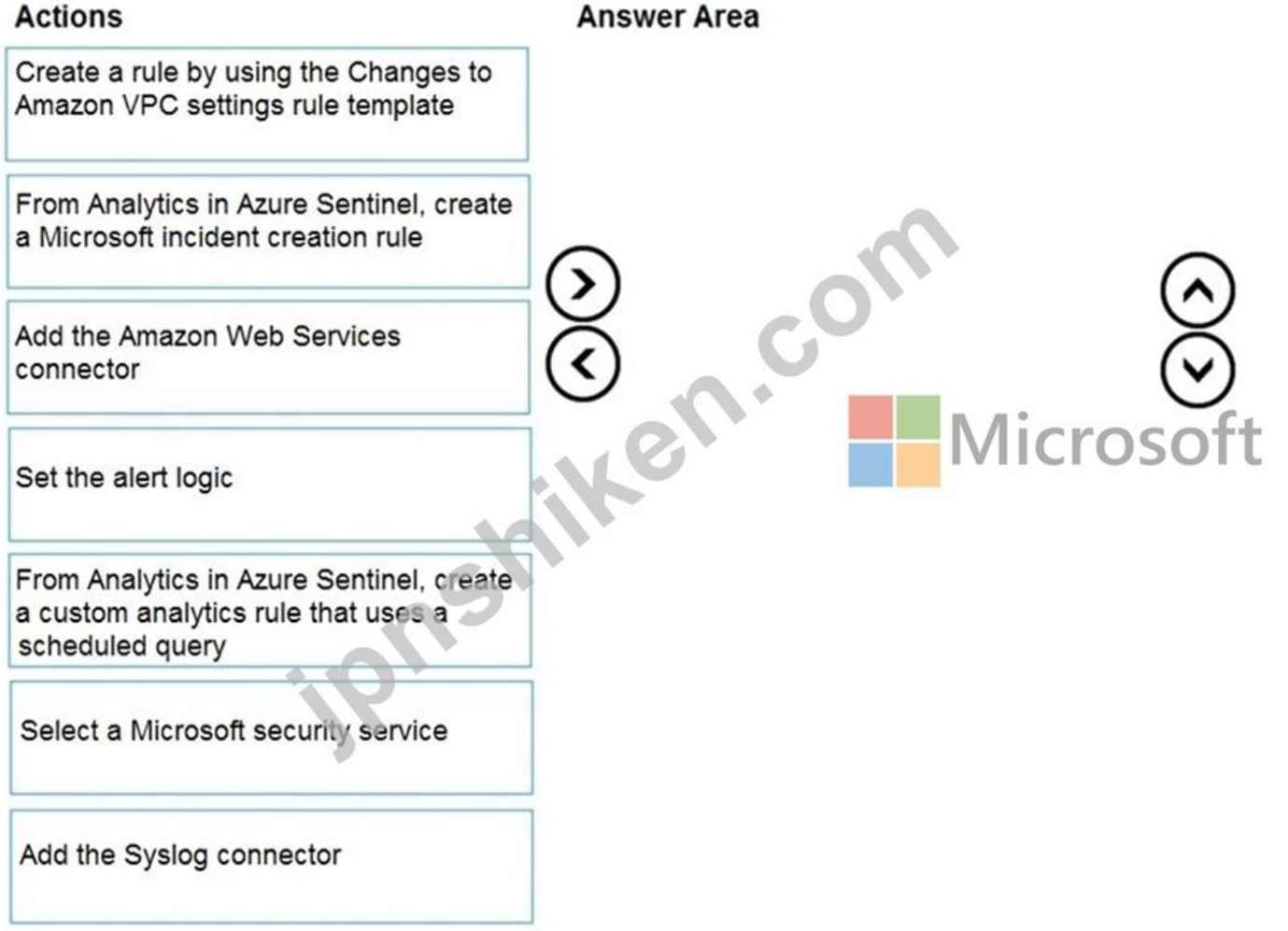
参照：

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

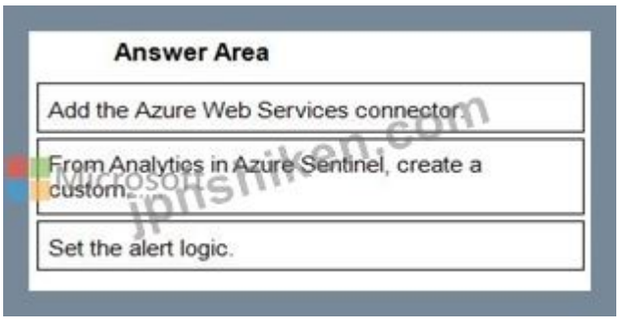
質問: 39

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-AzureWebServicesコネクタを追加します。
2-Azure SentinelのAnalyticsから、カスタムを作成します.....
3-アラートロジックを設定します。
参照：
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

質問: **40**
Microsoft 365 Defenderには、次の高度なハンティングクエリがあります。

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

過去24時間に、Microsoft Defenderによって管理されているデバイスで、プロセスによってシステムの復元が無効になった場合は、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)**
参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

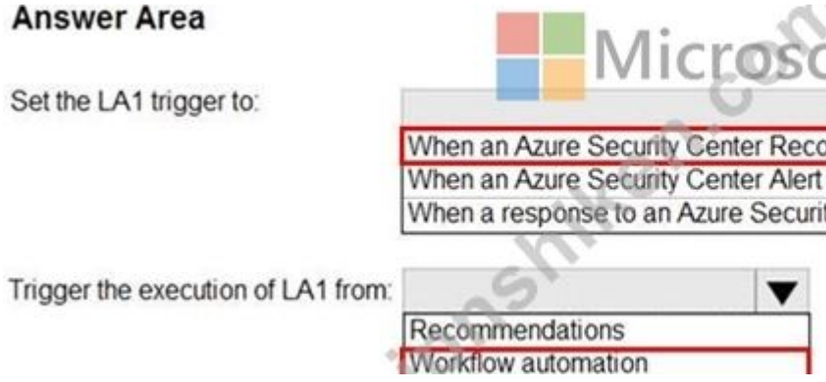
質問: **41**
イメージファイルを使用する潜在的な攻撃に関するセキュリティ情報を受け取ります。
攻撃を防ぐには、Microsoft Defender for Endpointで侵入の痕跡（IoC）を作成する必要があります。
どのインジケータータイプを使用する必要がありますか？
A. アクションがアラートのみに設定されているURL/ドメインインジケーター
B. アクションがアラートおよびブロックに設定されているURL/ドメインインジケーター

C. アクションがアラートおよびブロックに設定されているファイルハッシュインジケーター
D. アクションがアラートおよびブロックに設定されている証明書インジケーター
正解: **C** (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/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

質問: **42**
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: **B,D** (コメントを発表する)
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/livestream

質問: **43**
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、AzureSecurityCenter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、回答エリアで適切なオプションを選択してください。
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:



参照：
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

質問: **44**

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答えた後は、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Microsoftインシデント作成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

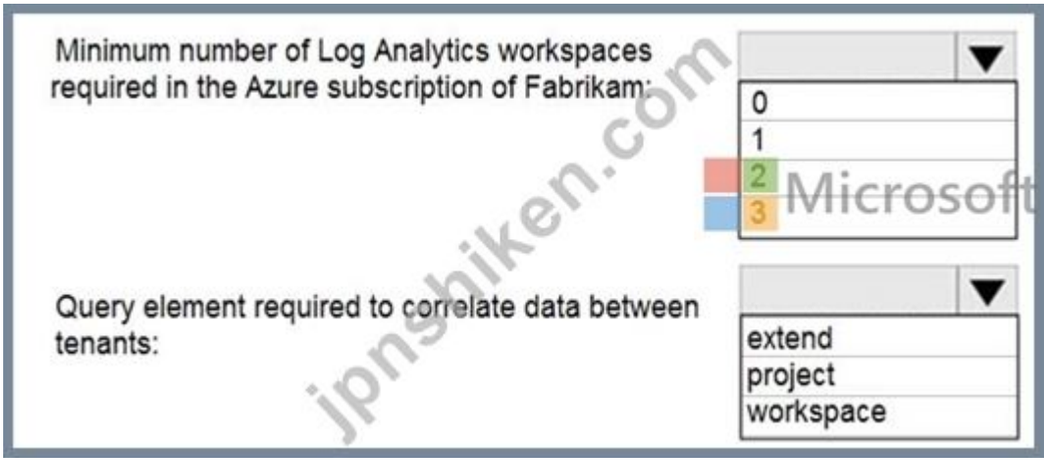
正解: **(**正解を表示します**)**

セクション :[なし]

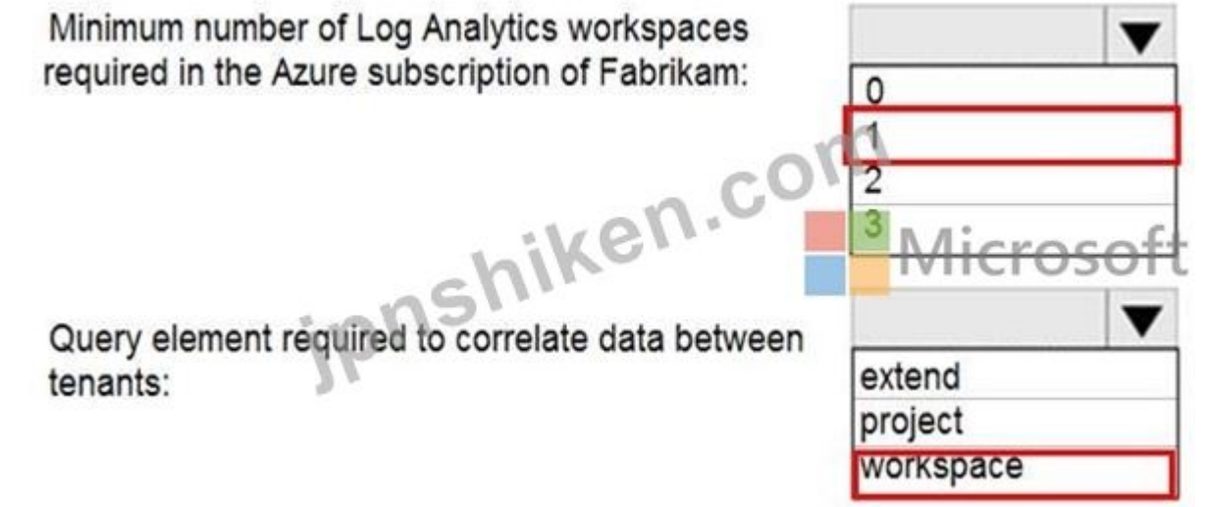
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

質問: **45**

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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

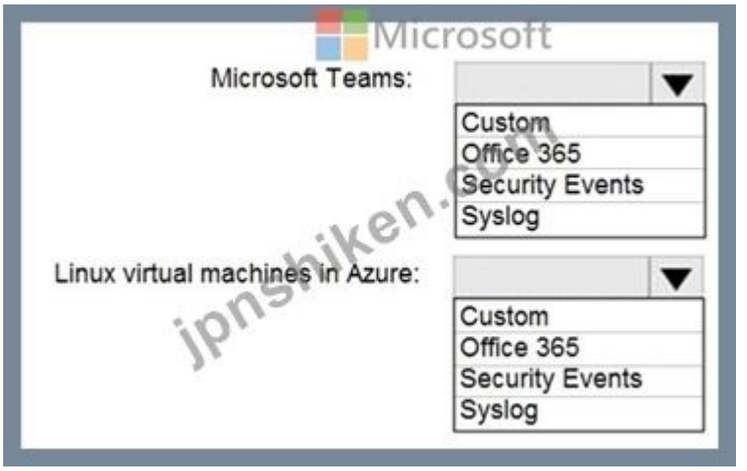


正解:



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

質問: **46**
AzureSentinelをデプロイします。
AzureでMicrosoftTeamsとLinux仮想マシンを監視するには、AzureSentinelにコネクタを実装する必要があります。ソリューションは、管理作業を最小限に抑える必要があります。
各ワークロードにどのデータコネクタタイプを使用する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
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:

参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

質問: **47**
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、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

Create the rule of type:

- Fusion
- Microsoft incident creation
- Scheduled

Configure the playbook to include:

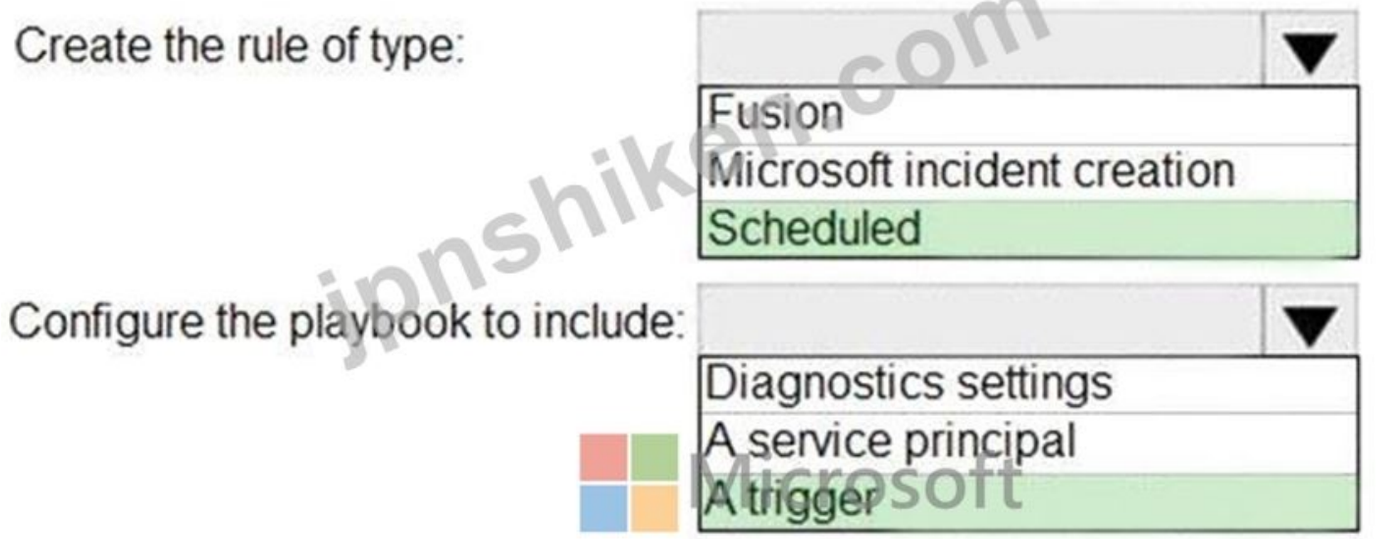
- Diagnostics settings
- A service principal
- A trigger

正解:

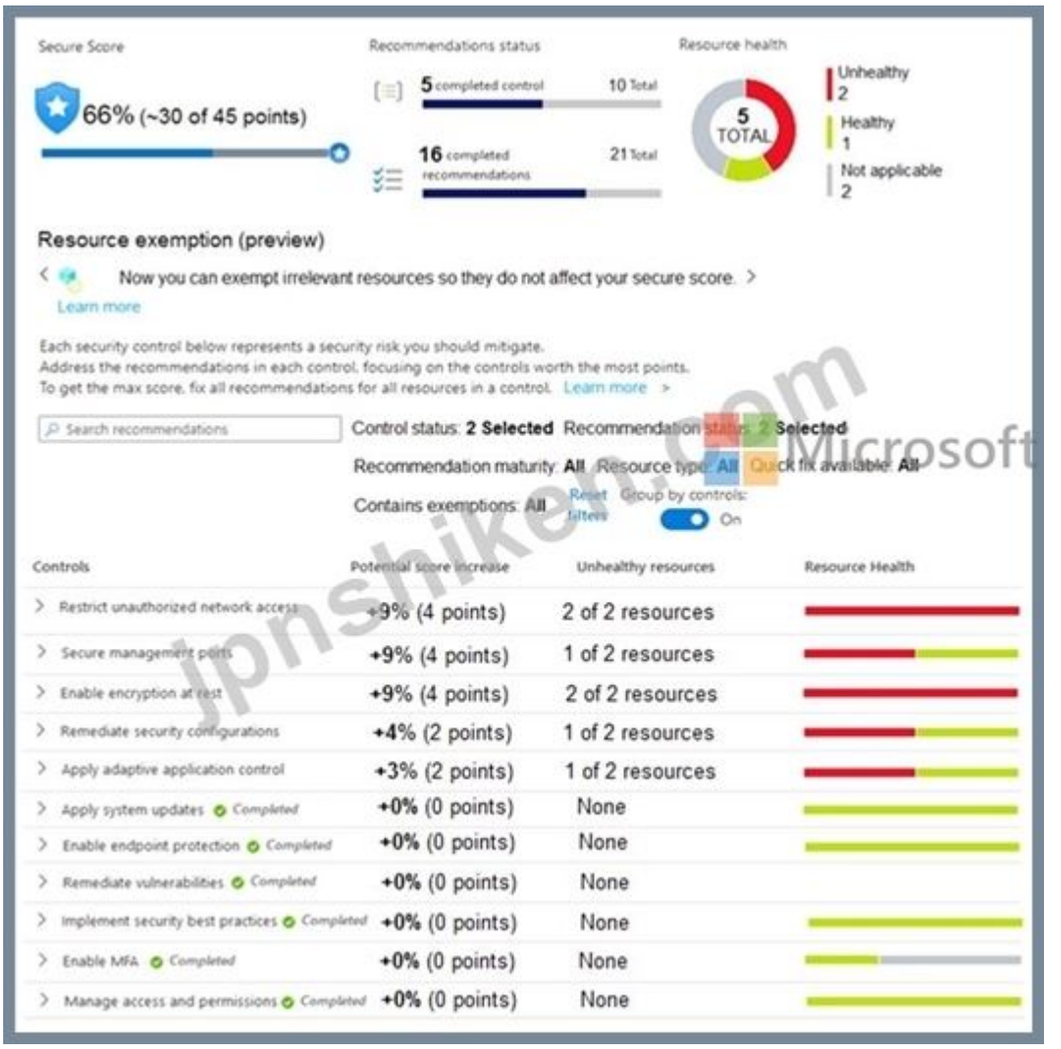
```
"resources": [
  {
    "type": "[Microsoft.Automation | Microsoft.Logic | Microsoft.Security]/automations",
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameters('location')]",
    "properties": {
      "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '[Microsoft.Automation | Microsoft.Logic | Microsoft.Security]/workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ],
```

説明

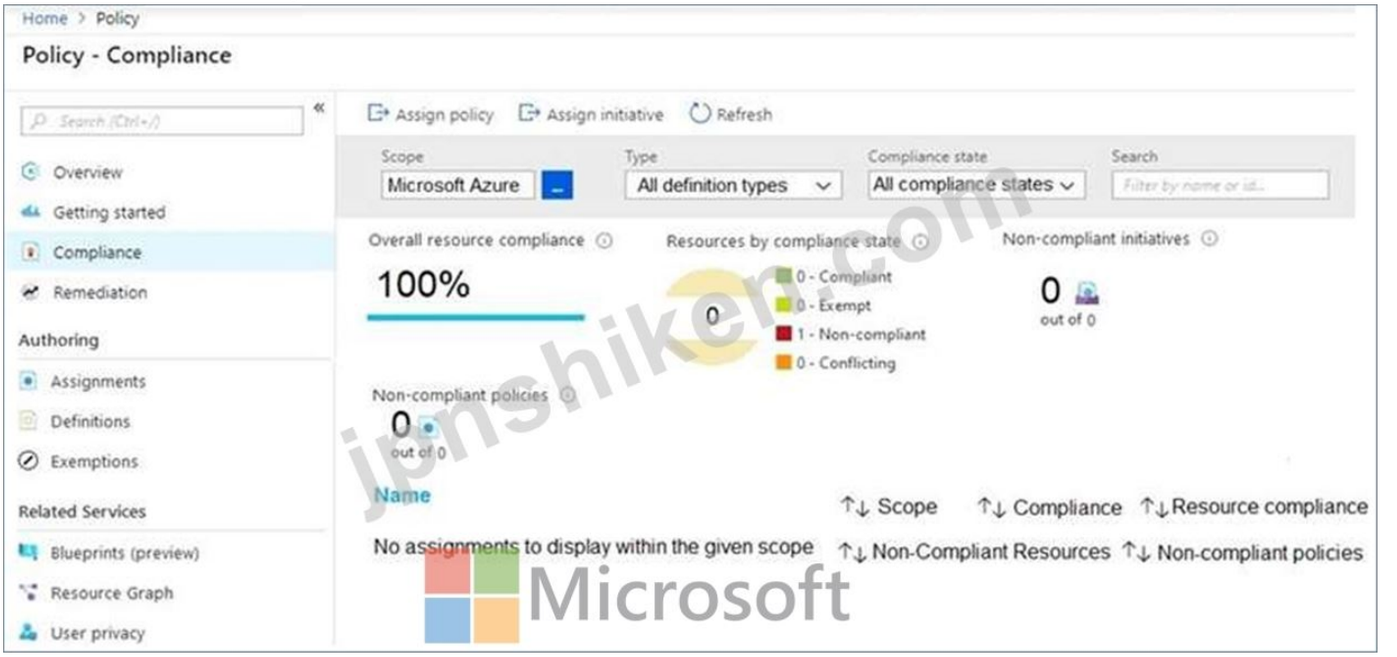
Answer Area



質問: **48**
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。）

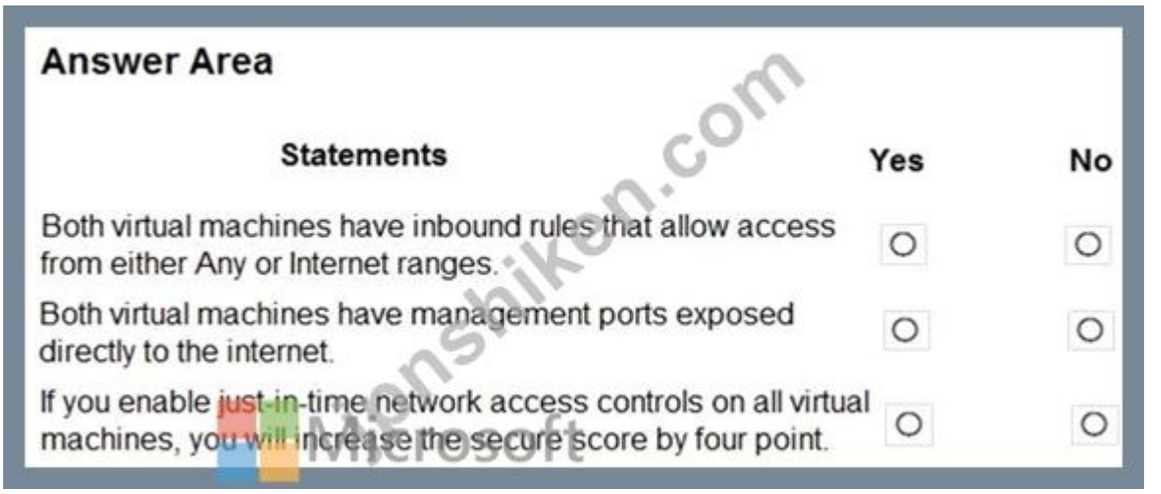


Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。[ポリシー]タブをクリックします。）



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。

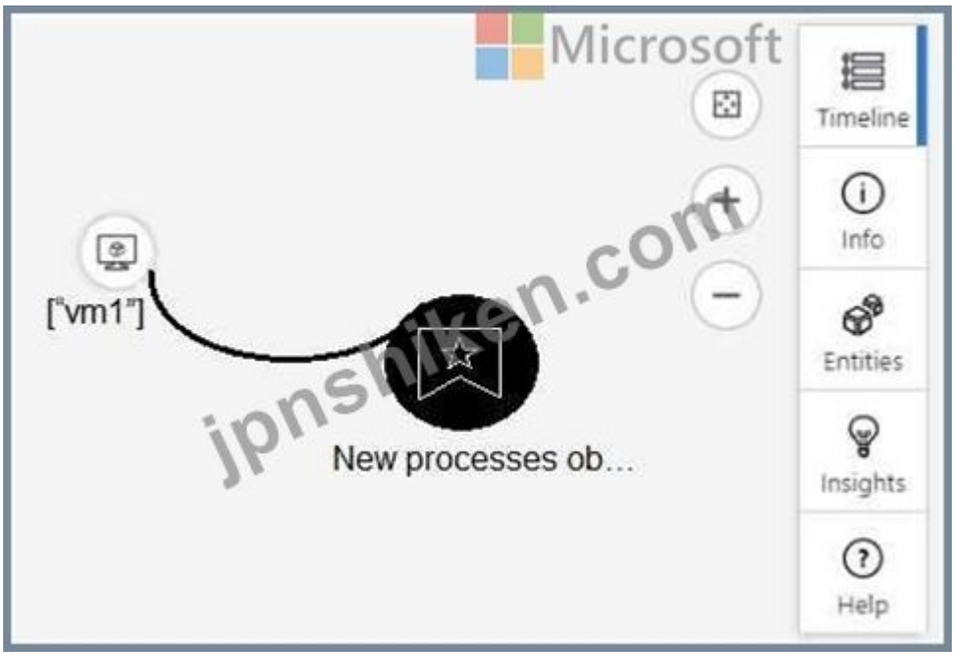
注：正しい選択はそれぞれ1ポイントの価値があります。



正解:

参照：
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: **49**
ホットスポット
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。

ホットエリア：

Answer Area

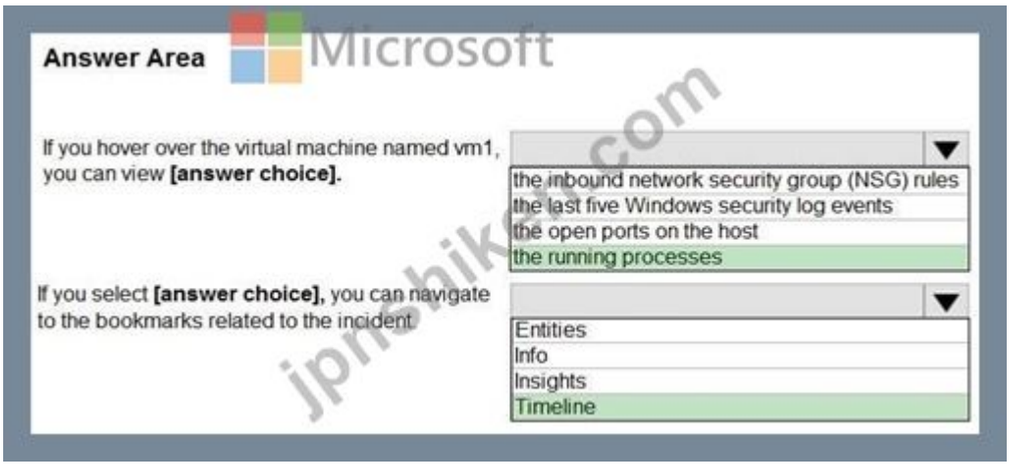
If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the bookmarks related to the incident.

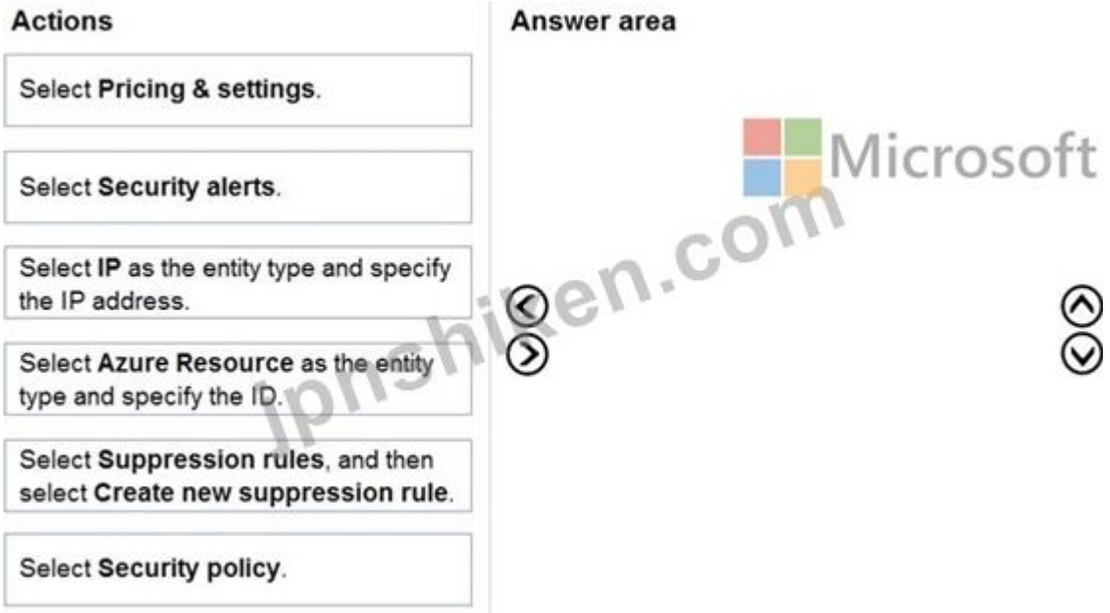
- Entities
- Info
- Insights
- Timeline

正解:

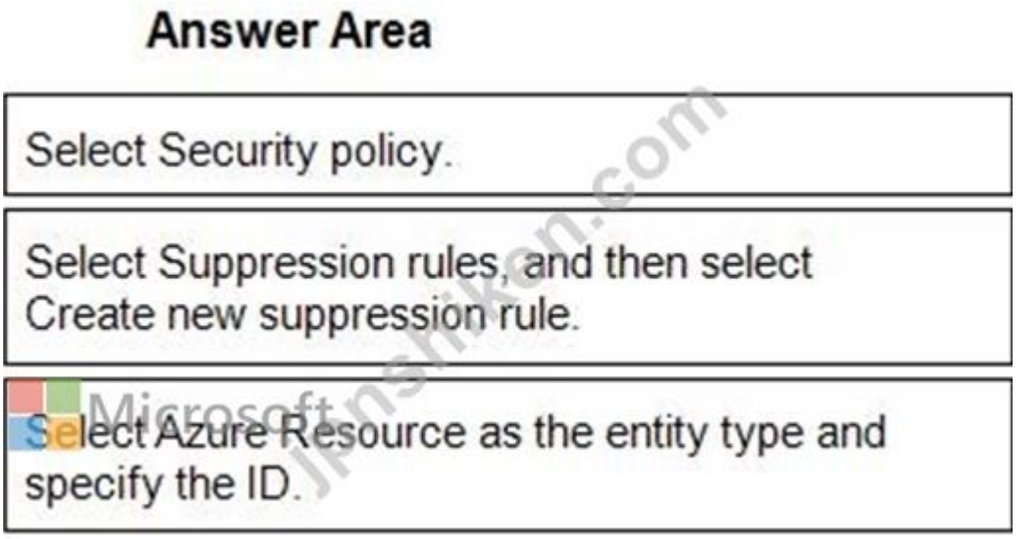


セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep- dive

質問: **50**
通常のアクティビティに対して、AzureSecurityCenter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。
参照：
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

質問: **51**
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: **C** (コメントを発表する)
参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

質問: **52**
AzureDefenderを使用するMicrosoft365サブスクリプションがあります。
RG1という名前のリソースグループに100台の仮想マシンがあります。
SecAdmin1という名前の新しいユーザーにセキュリティ管理者の役割を割り当てます。
SecAdmin1がAzureDefenderを使用して、仮想マシンにクイックフィックスを適用できることを

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。
SecAdmin1にどの役割を割り当てる必要がありますか？
A. サブスクリプションのセキュリティリーダーの役割
B. サブスクリプションの寄稿者
C. RG1のコントリビューターの役割
D. RG1の所有者の役割
正解: **C** (コメントを発表する)
セクション :[なし]

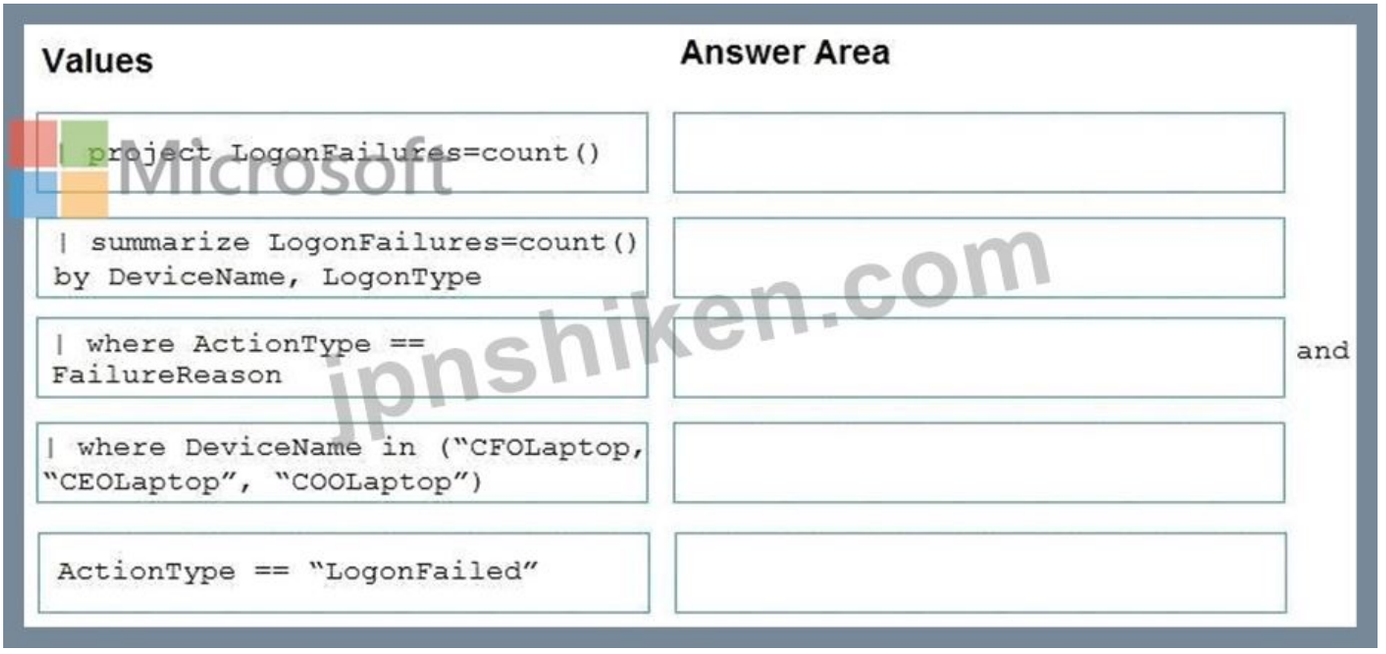
質問: **53**
会社はAzureSentinelを使用しています。
自動化された脅威応答を作成する必要があります。
何を使うべきですか？
A. データコネクタ
B. プレイブック
C. ワークブック
D. Microsoftインシデント作成ルール
正解: **B** (コメントを発表する)
参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **54**
米国東部のAzureリージョンにAzureSentinelを展開しています。
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展開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. 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
B. AzureSentinelをワークスペースに追加します。
C. AzureSentinelでデータコネクタを作成します。
D. 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。
正解: **B** (コメントを発表する)

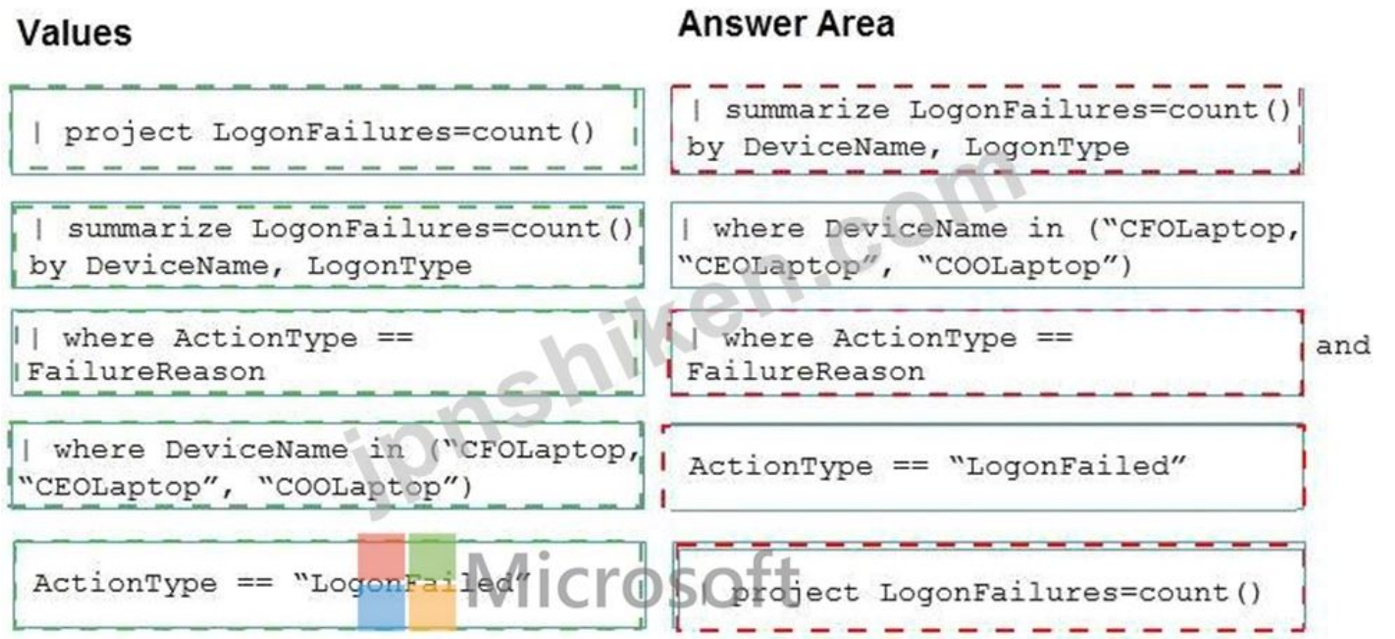
質問: **55**
組織内の他のユーザーがサインインに使用したことのない場所からユーザーがサインインしようとすると、セキュリティアラートを受信する必要があります。
どの異常検出ポリシーを使用する必要がありますか？
A. 不可能な旅
B. 匿名IPアドレスからのアクティビティ

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、最近ではない場所、または組織内のどのユーザーも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。
参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

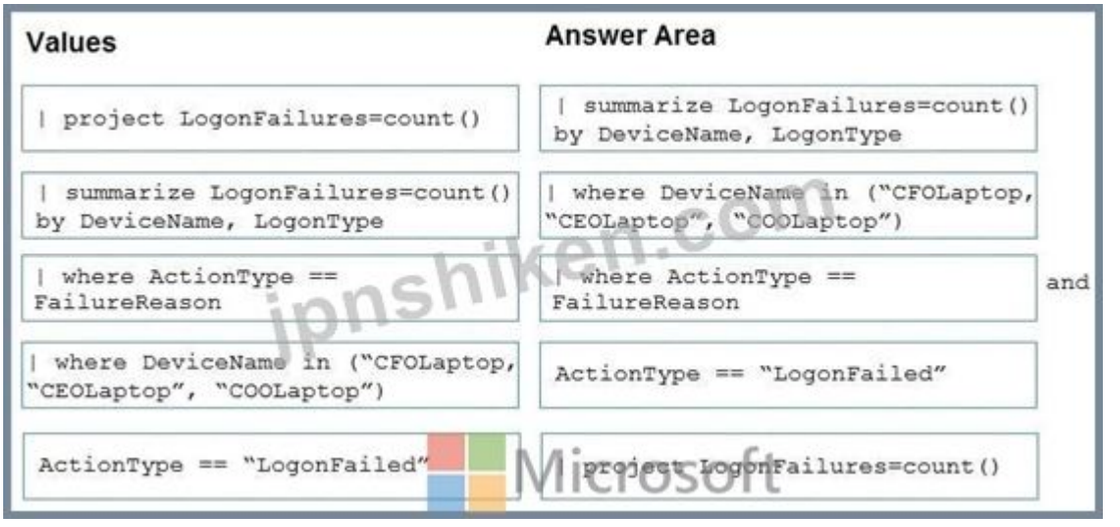
質問: **56**
Microsoft365Defenderを使用してインシデントを調査しています。
CFOLaptop、CEOLaptop、およびCOOLaptopという名前の3つのデバイスで失敗したサインイン認証を検出するには、高度なハンティングクエリを作成する必要があります。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。



正解:



説明



質問: **57**

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。

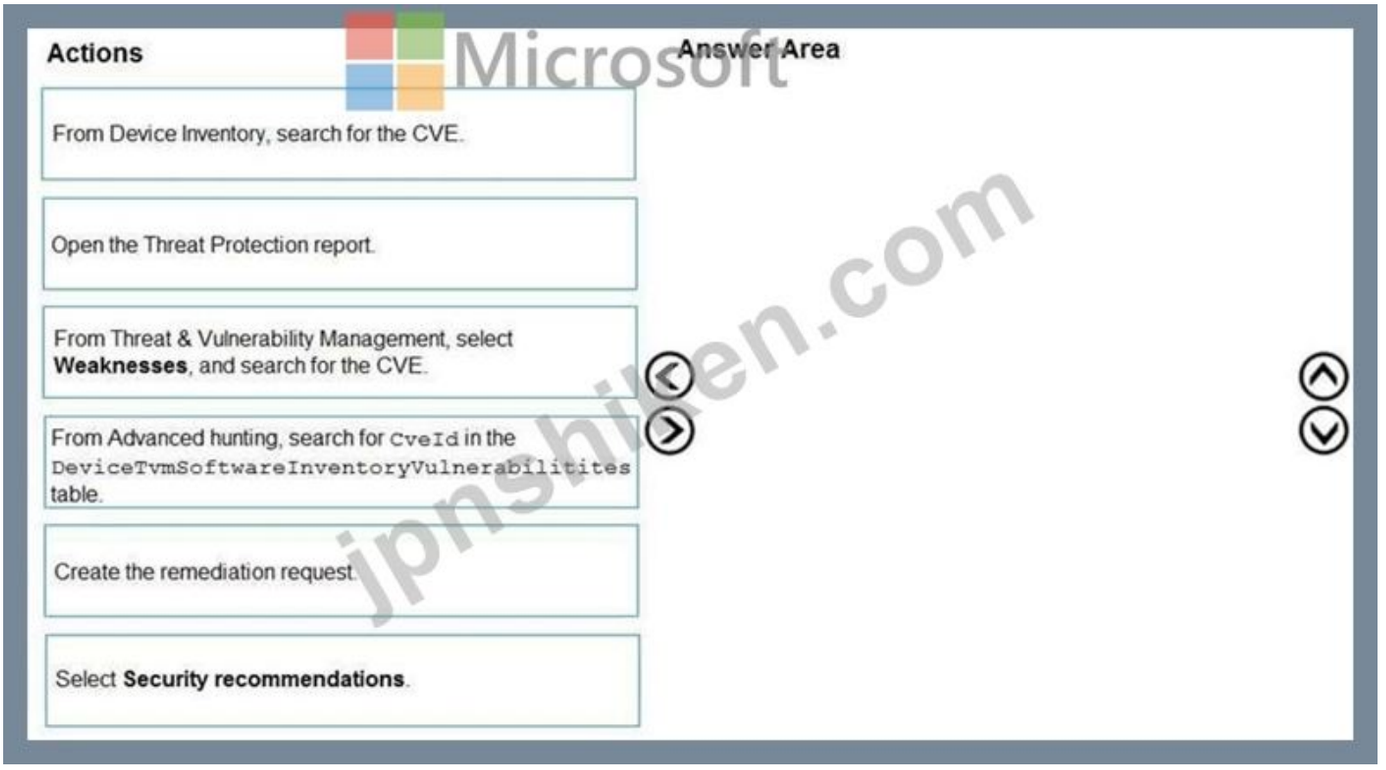
E. フュージョンルールを有効にします。

正解: **A,B** (コメントを発表する)

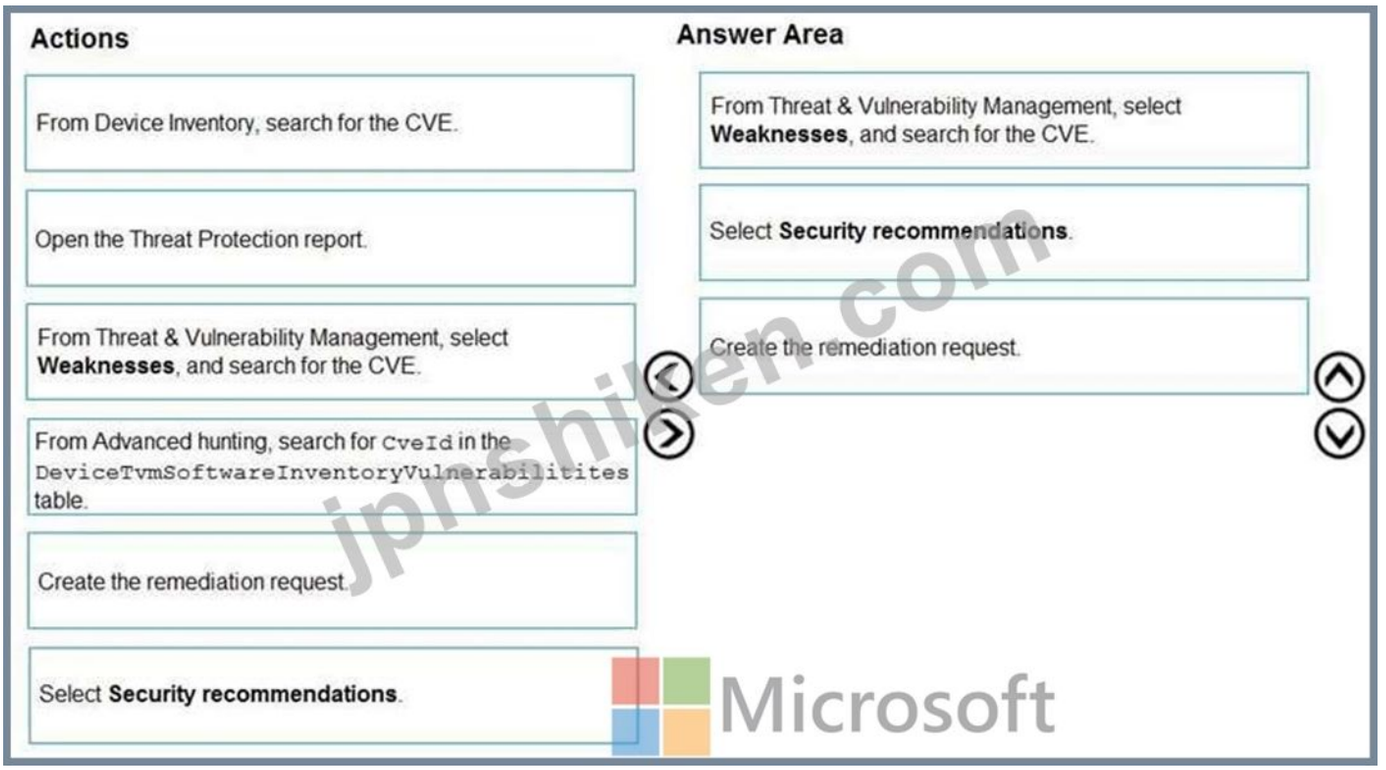
説明/参照：

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **58**
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: **59**
AzureSecurityCenter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: **C** (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/azure-monitor/visualize/workbooks-chart-visualizations

質問: **60**
安全な添付ファイルポリシーをMicrosoftDefenderforOffice365に実装します。
ユーザーから、添付ファイルを含む電子メールメッセージの受信に予想よりも時間がかかるとの報告がありました。
セキュリティを損なうことなく、添付ファイルを含むメッセージの配信にかかる時間を短縮する

必要があります。添付ファイルでマルウェアをスキャンし、マルウェアを含むメッセージをブロックする必要があります。
セーフアタッチメントポリシーで何を構成する必要がありますか？
A. 動的配信
B. 置換
C. リダイレクトをブロックして有効にする
D. リダイレクトを監視して有効にする
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

質問: **61**
AzureSentinelにプレイブックがあります。
プレイブックをトリガーすると、配布グループに電子メールが送信されます。
配布グループではなくリソースの所有者に電子メールを送信するように、プレイブックを変更する必要があります。
あなたは何をするべきか？
A. パラメータを追加し、トリガーを変更します。
B. カスタムデータコネクタを追加し、トリガーを変更します。
C. 条件を追加し、アクションを変更します。
D. パラメータを追加し、アクションを変更します。
正解: **(**正解を表示します**)**
参照：
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

質問: **62**
Microsoft Defender forOffice365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. Microsoft365Defender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**)**

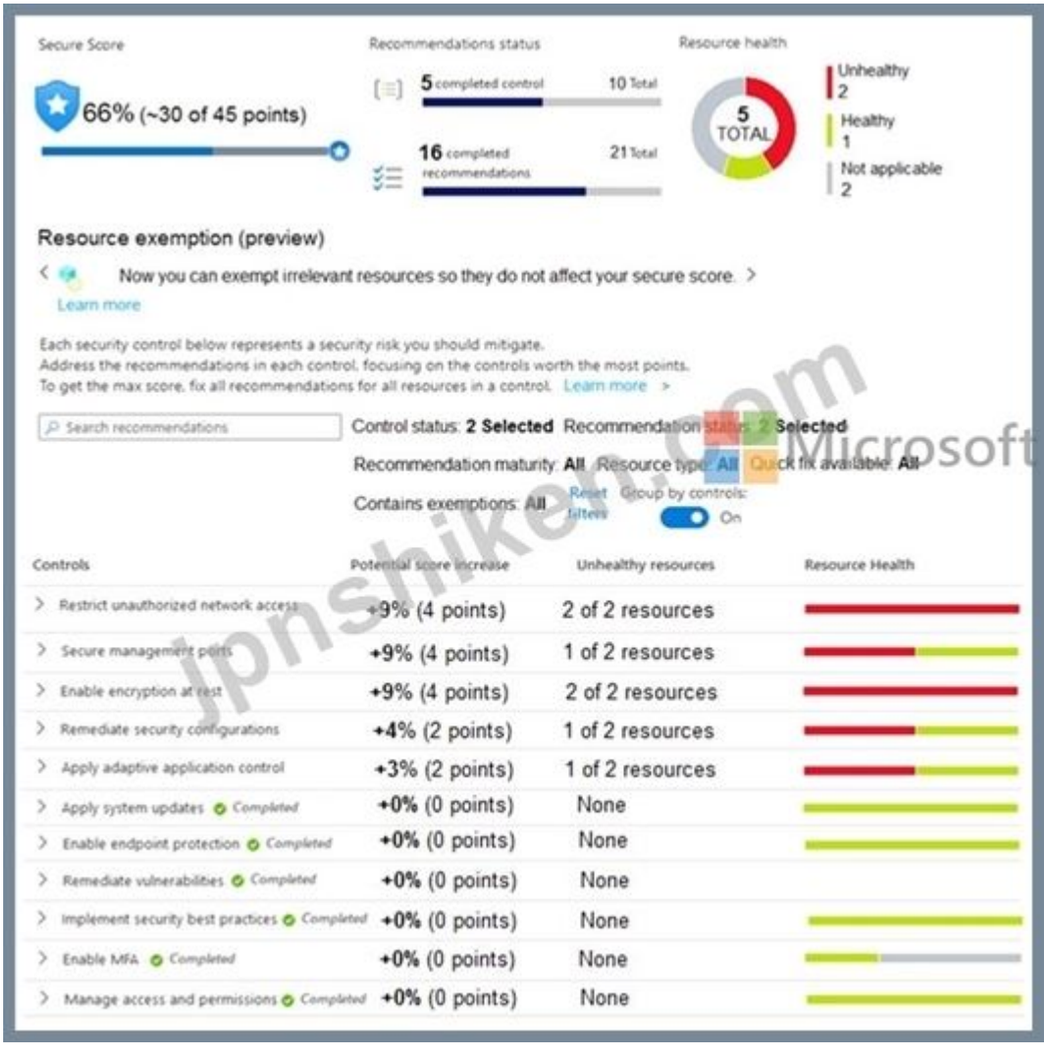
参照：

https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

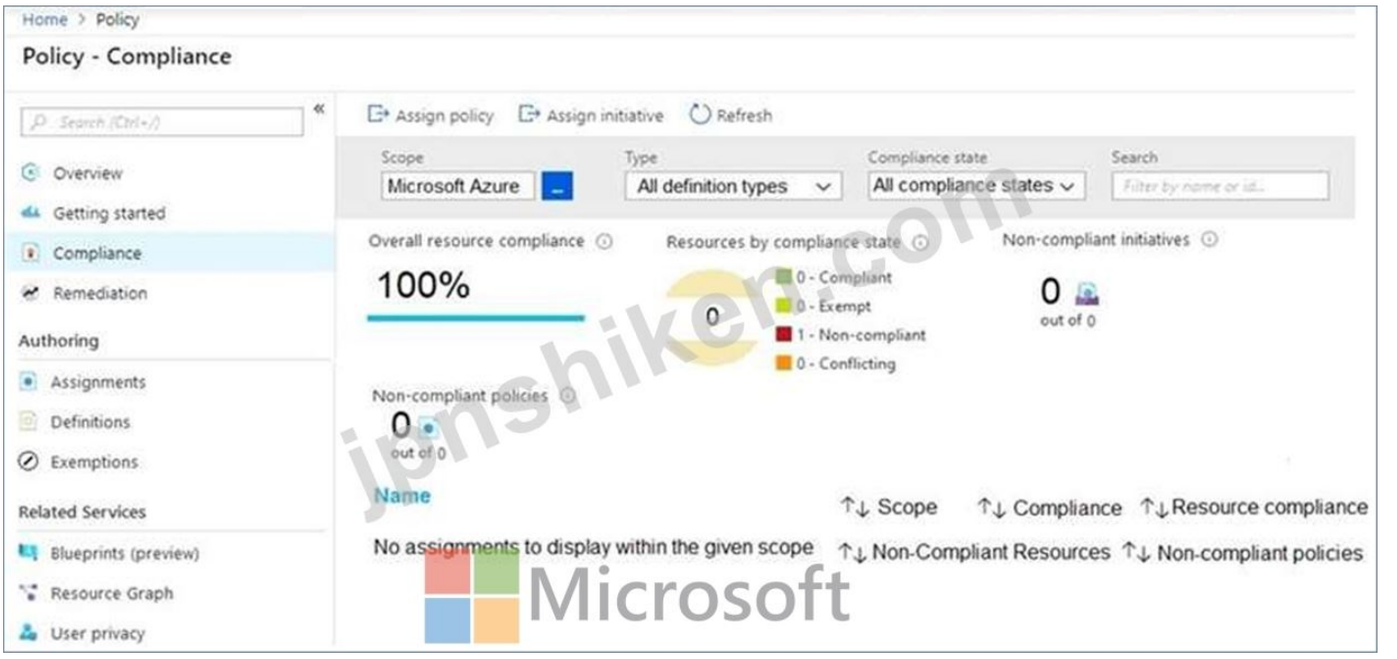
質問**: 63**

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。）

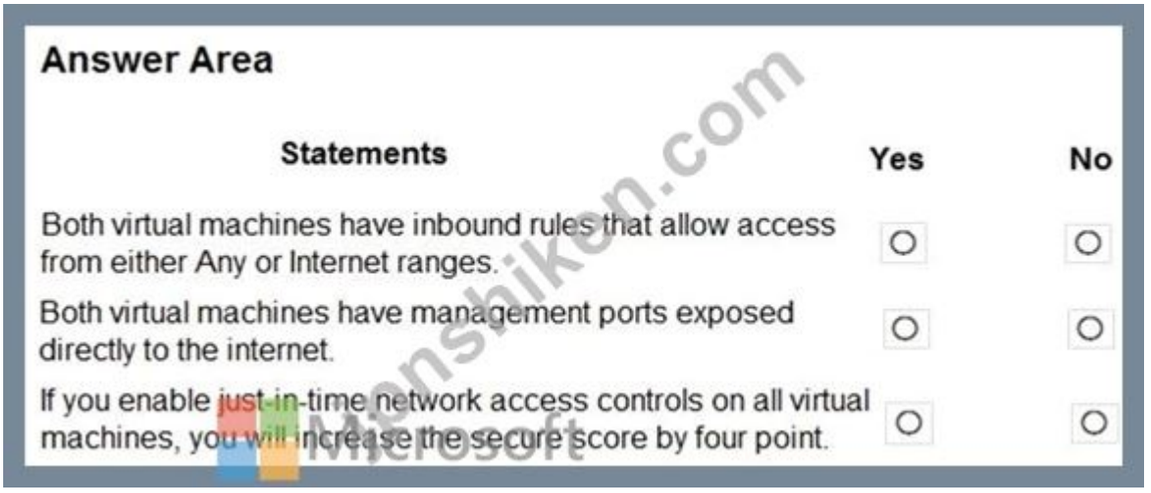


Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。[ポリシー]タブをクリックします。）

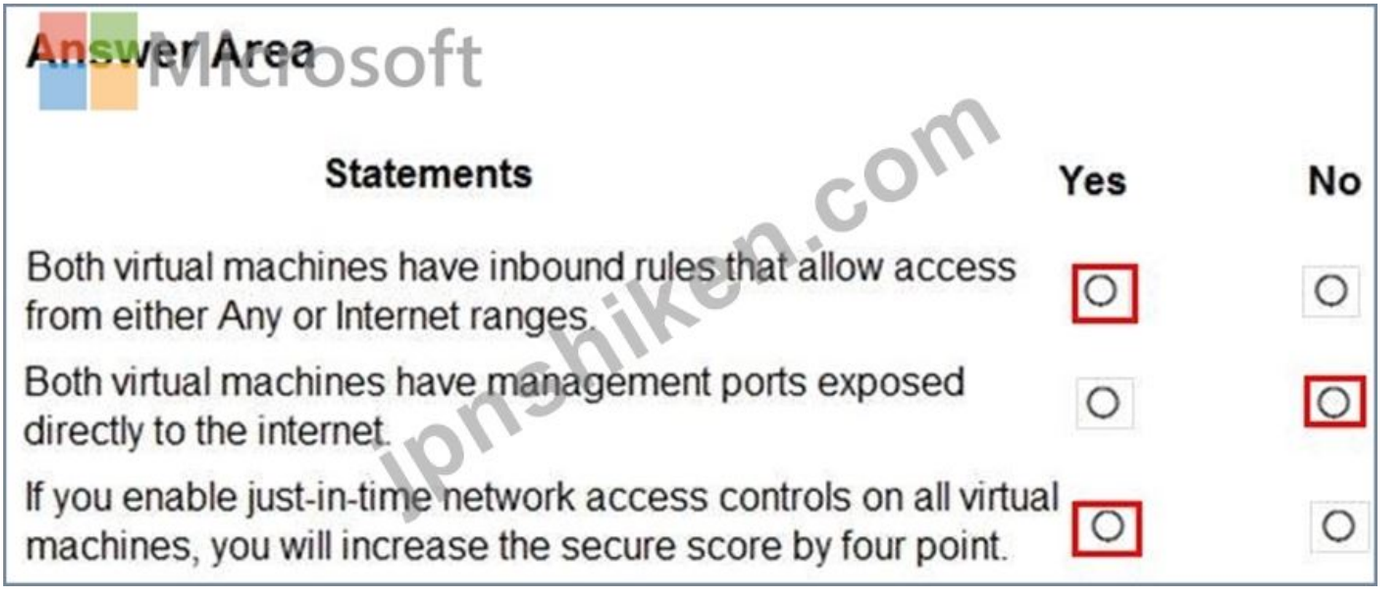


次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

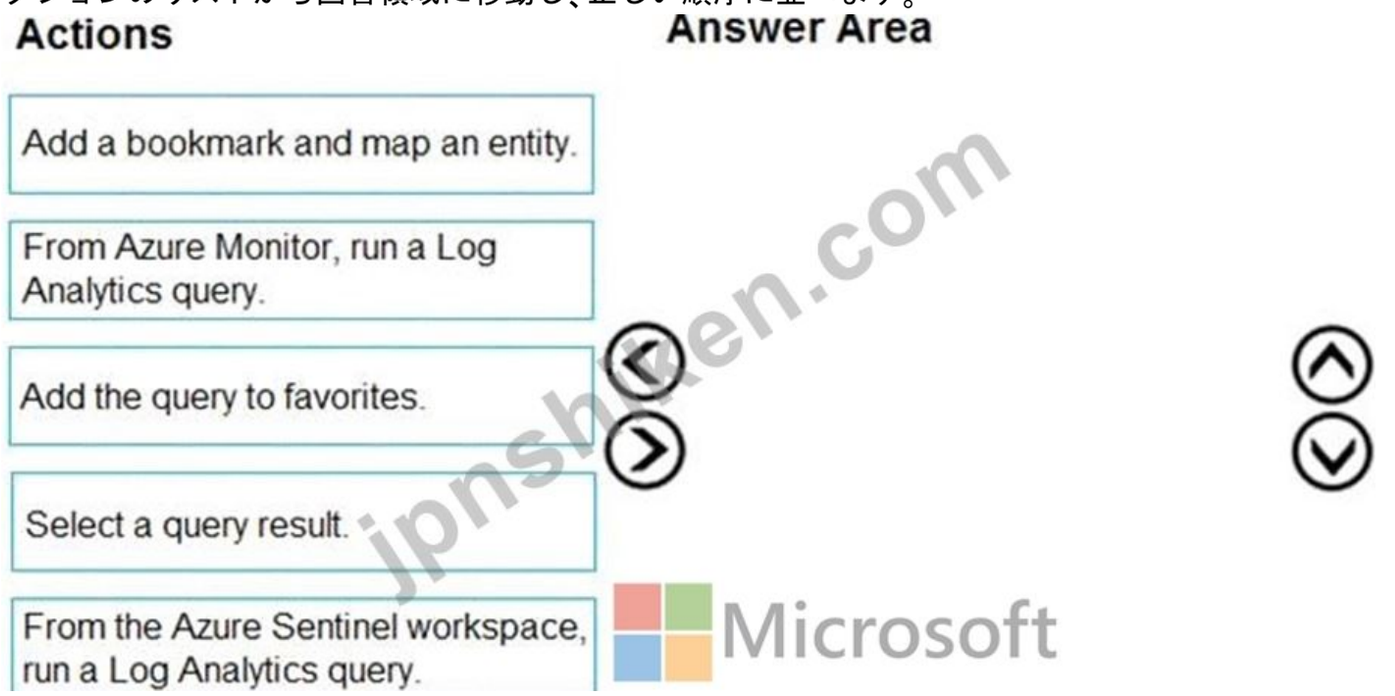


正解:

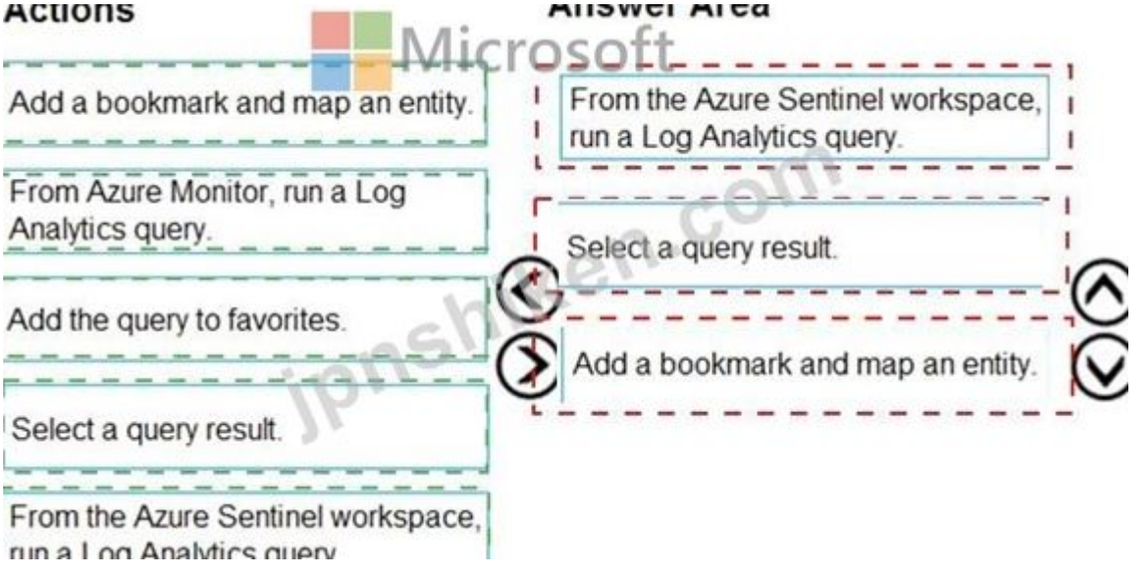


参照：
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

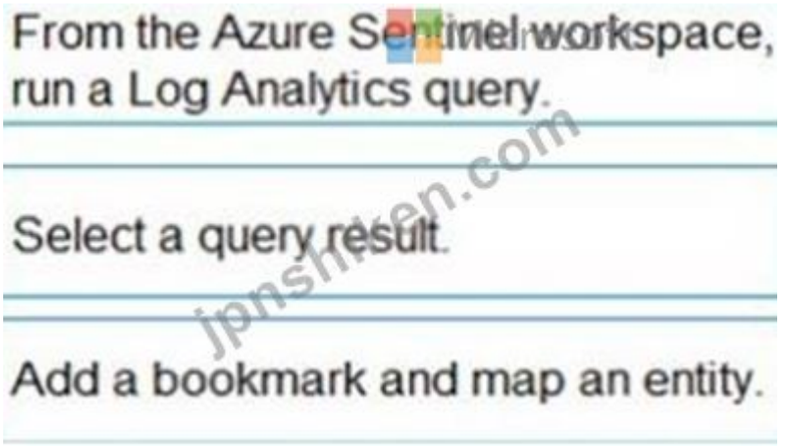
質問: **64**
Azure Sentinelの要件を満たすには、イベントにメモを追加する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。



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



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

質問: **65**
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: **A,B (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **66**
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**)**
参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios
トピック2、Litwareinc。
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.comAzureAD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MicrosoftCloudAppSecurity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.comAzureAD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。

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

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。

* AzureInformationProtectionの要件

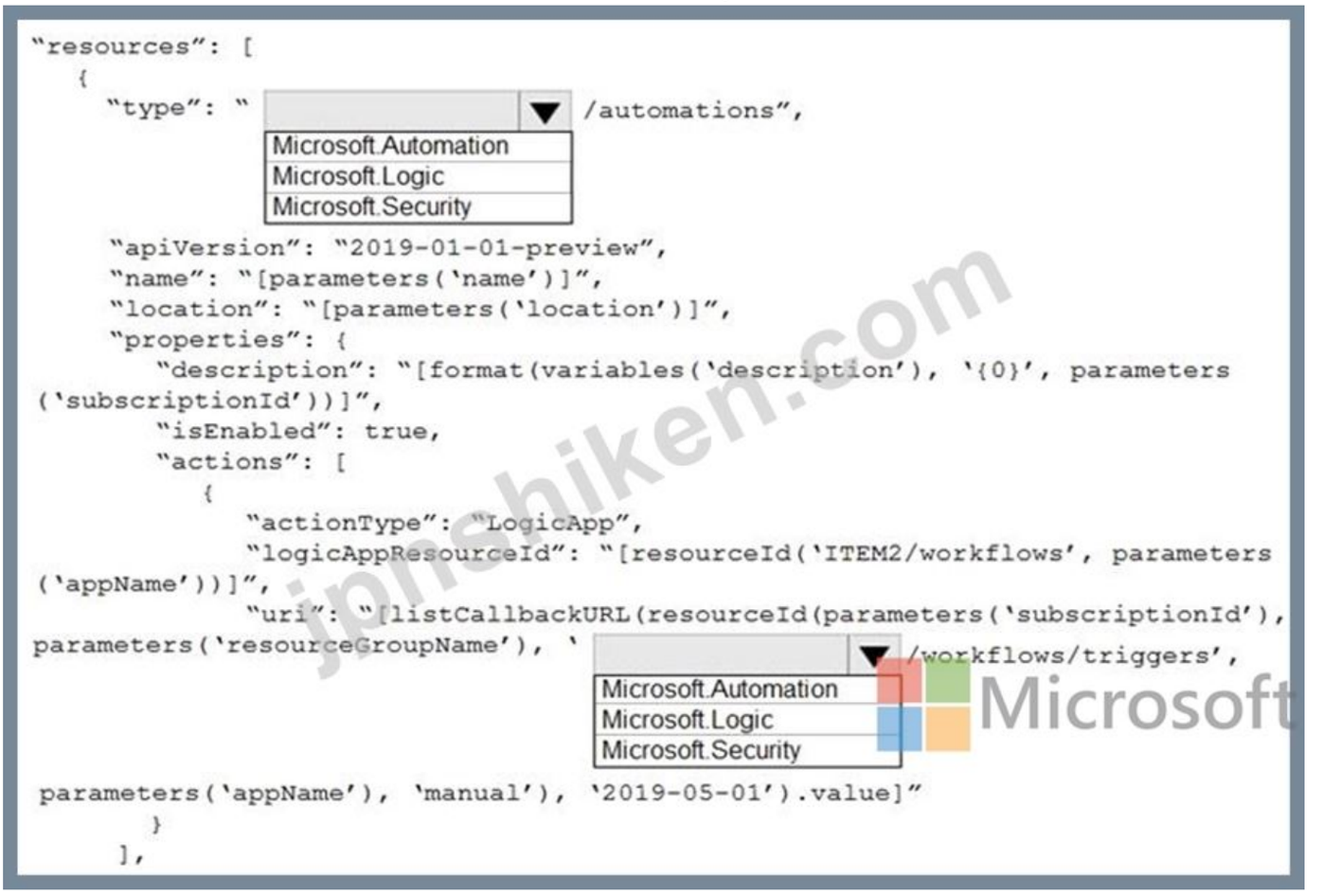
*セキュリティラベルが付いていてWindows10コンピューターに保存されているすべてのファイルは、Azure Information*Protection-データ検出ダッシュボードから利用できる必要があります。

*エンドポイント要件のためのMicrosoftDefender
すべてのCloudAppSecurityの認可されていないアプリは、Microsoft DefenderforEndpoint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: **67**
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。
SIEMソリューションがAzureActiveDirectory（Azure AD）サインイベントのアラートをほぼリアルタイムで生成できることを確認する必要があります。
イベントをSIEMソリューションにルーティングするにはどうすればよいですか？
A. セキュリティイベントコネクタを持つAzureSentinelワークスペースを作成します。
B. イベントハブにストリーミングするようにAzureADの診断設定を構成します。
C. AzureActiveDirectoryコネクタを持つAzureSentinelワークスペースを作成します。
D. ストレージアカウントにアーカイブするようにAzureADの診断設定を構成します。
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

質問: **68**
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AzureSecurityCenter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、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。

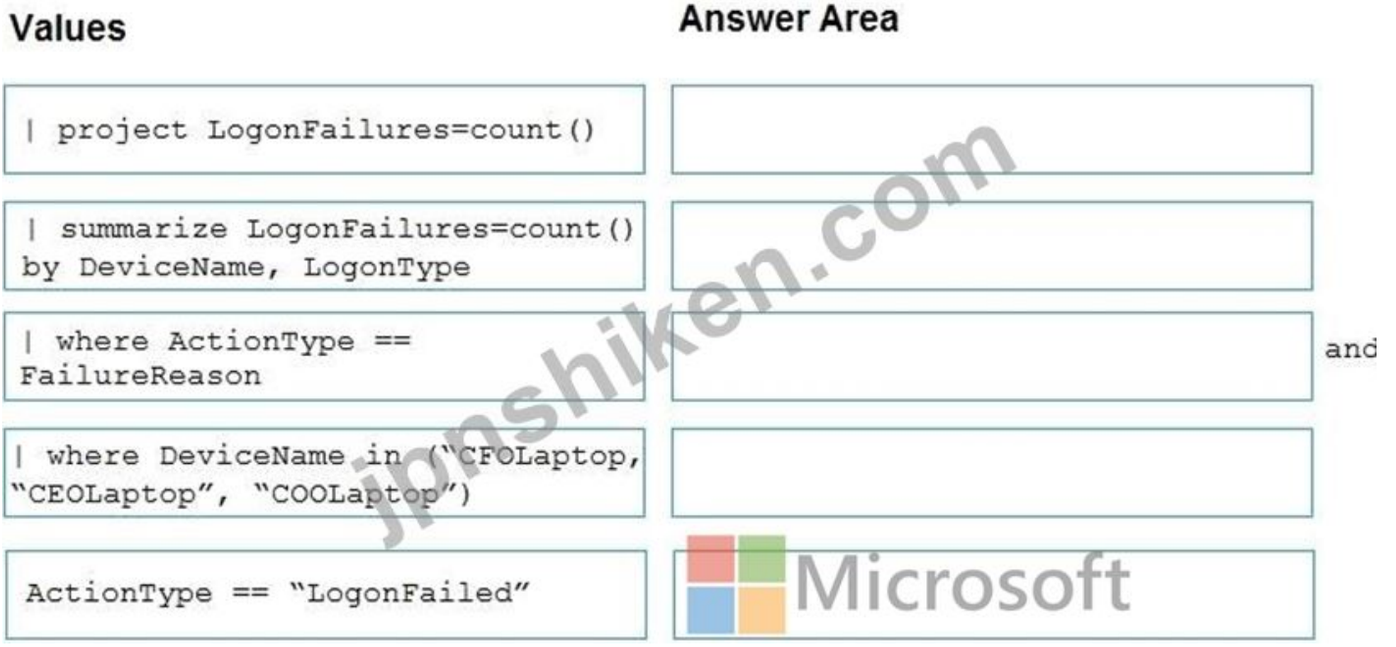


正解:

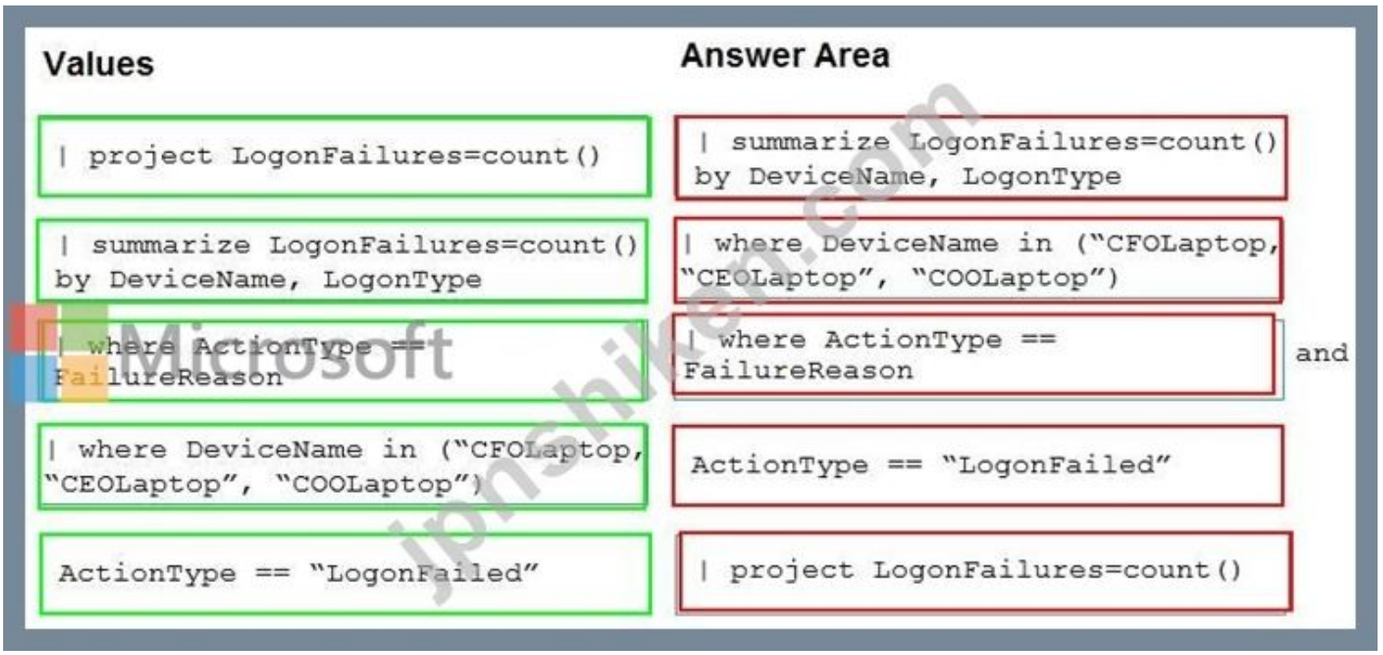
参照：
https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

質問: **69**
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**)**
参照：
https://docs.microsoft.com/en-us/azure/sentinel/livestream

質問: **70**
Microsoft365Defenderを使用してインシデントを調査しています。
CFOLaptop、CEOLaptop、およびCOOLaptopという名前の3つのデバイスで失敗したサインイン認証を検出するには、高度なハンティングクエリを作成する必要があります。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
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: **71**
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格納します。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. ワークスペース式と共用体演算子を使用するクエリを作成します。
C. エイリアスステートメントを使用します。
D. リソース式とエイリアス演算子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)**
参照：
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問: **72**
あなたの会社は、MicrosoftOfficeVBA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. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

B. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

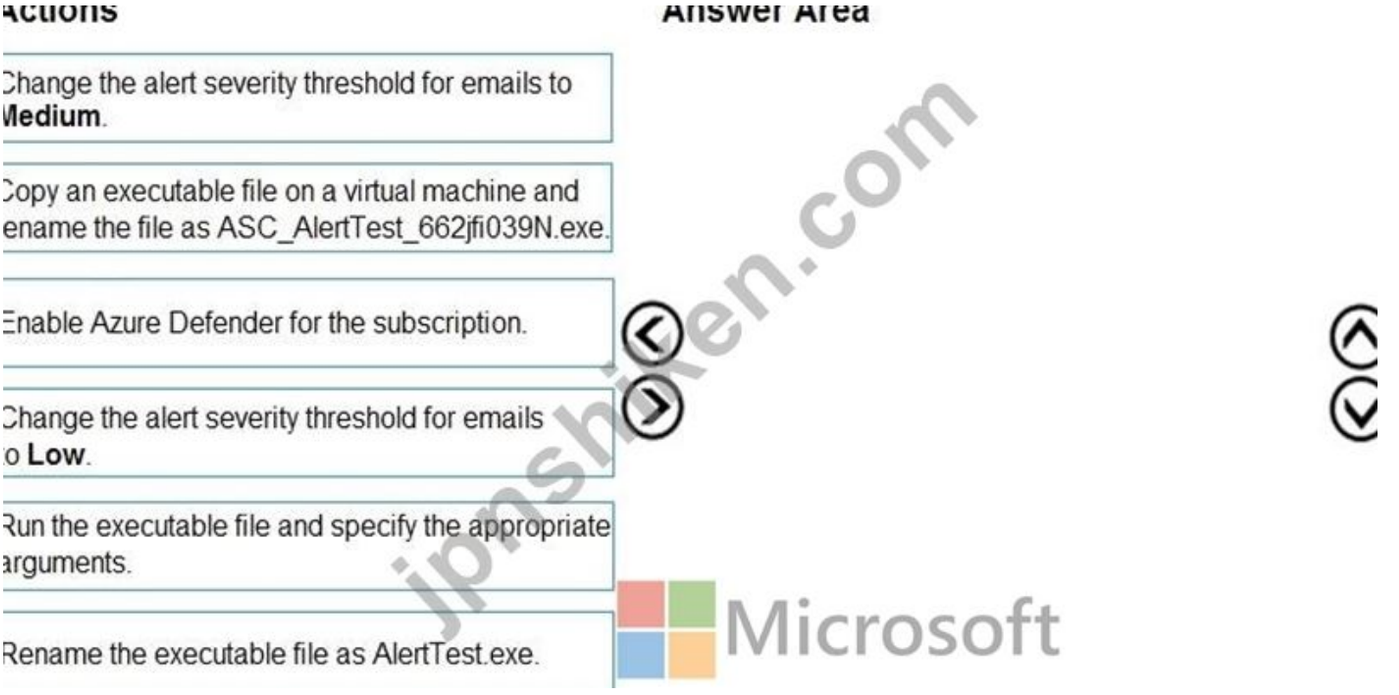
C. Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode

D. Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

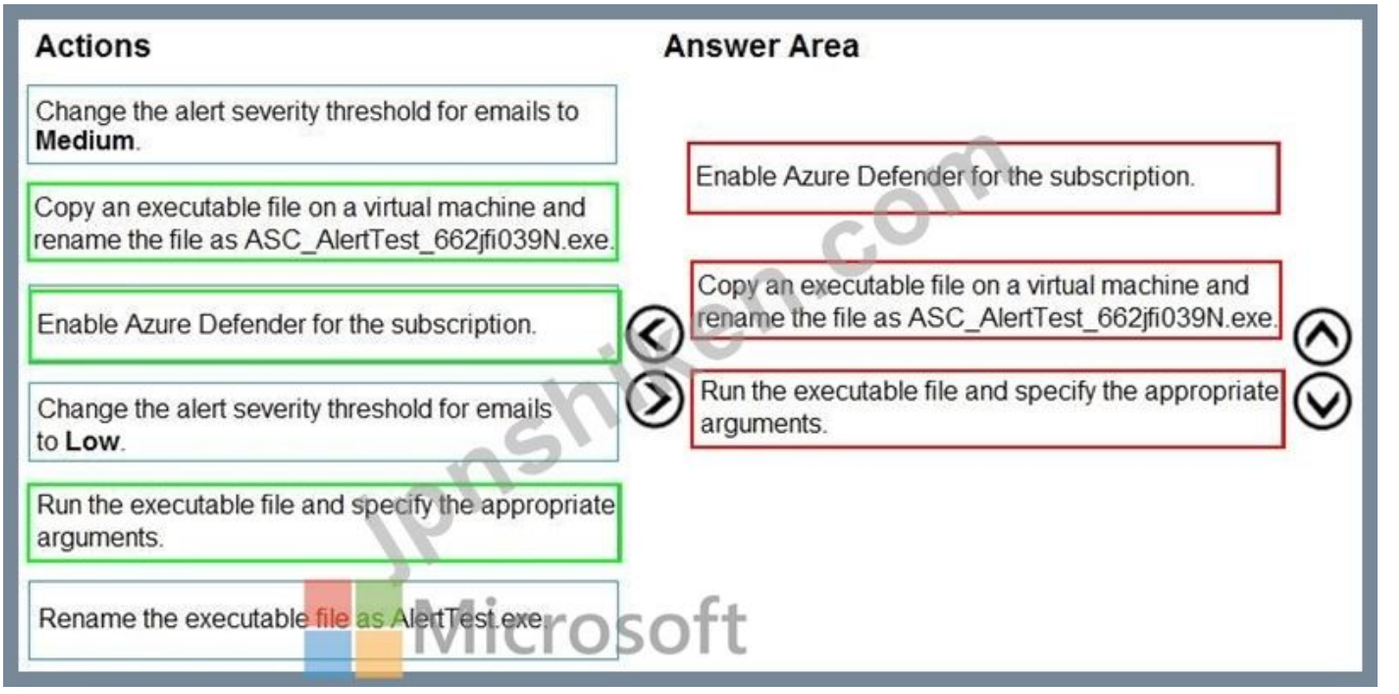
A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

質問: **73**
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**)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

質問: **74**
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:



参照：

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **75**

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

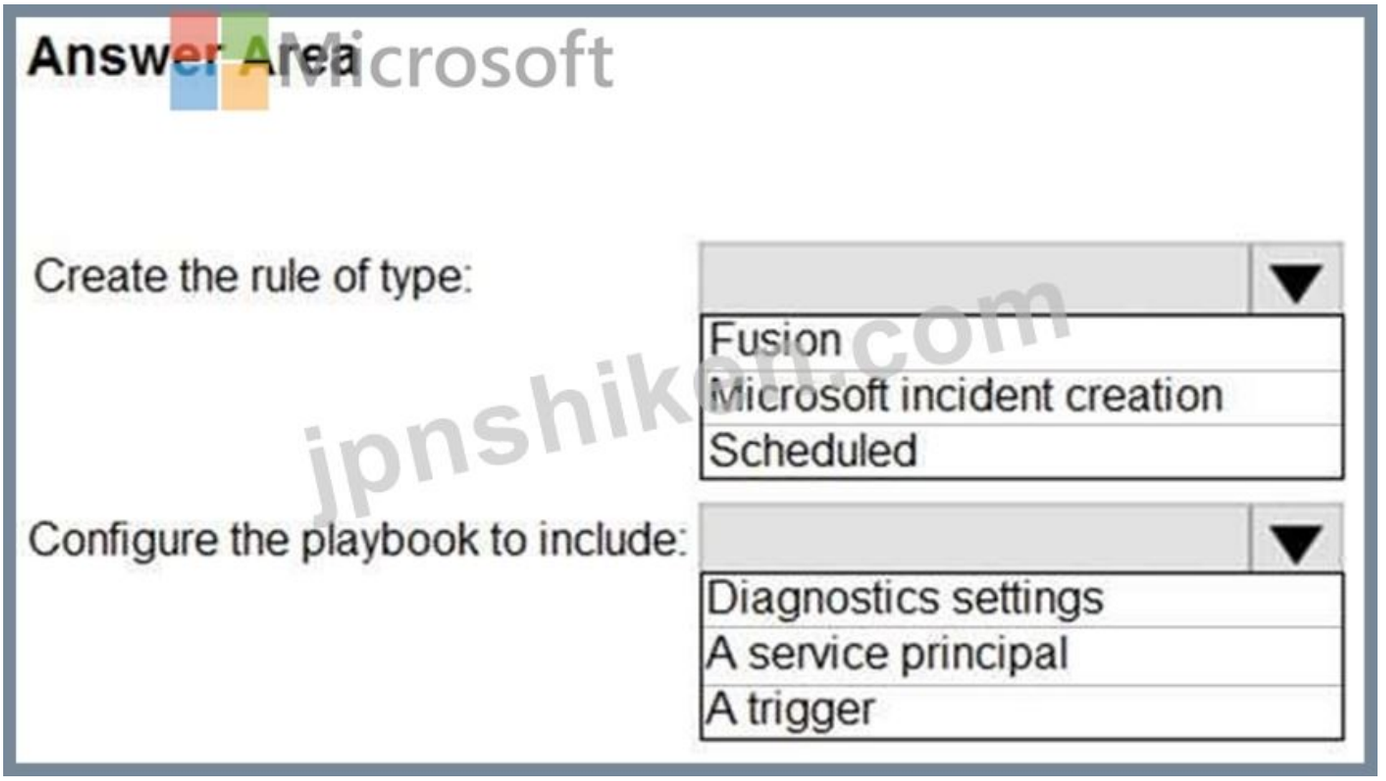
B. 分析

C. 脅威インテリジェンス

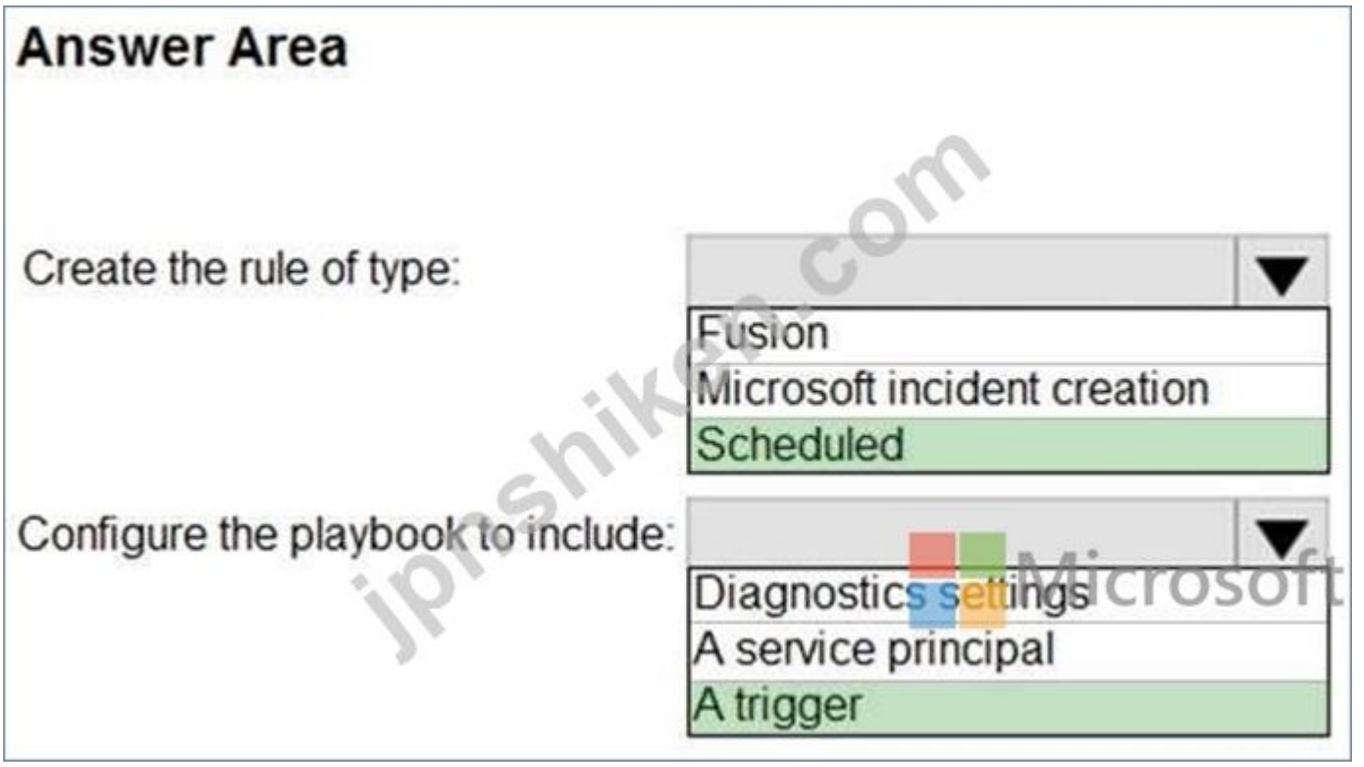
D. インシデント

正解: **D** (コメントを発表する)
参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

質問: **76**
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、回答エリアで適切なオプションを選択してください。
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：



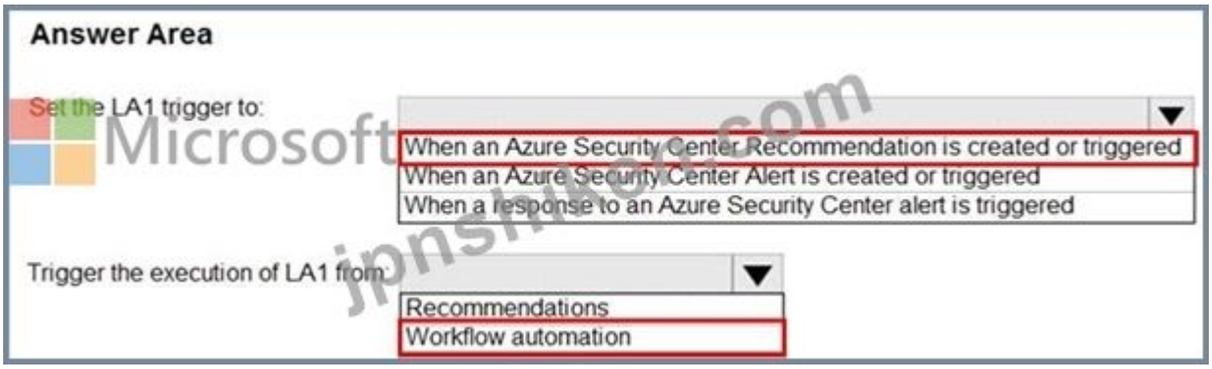
正解:



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: **77**
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、AzureSecurityCenter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、回答エリアで適切なオプションを選択してください。
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:

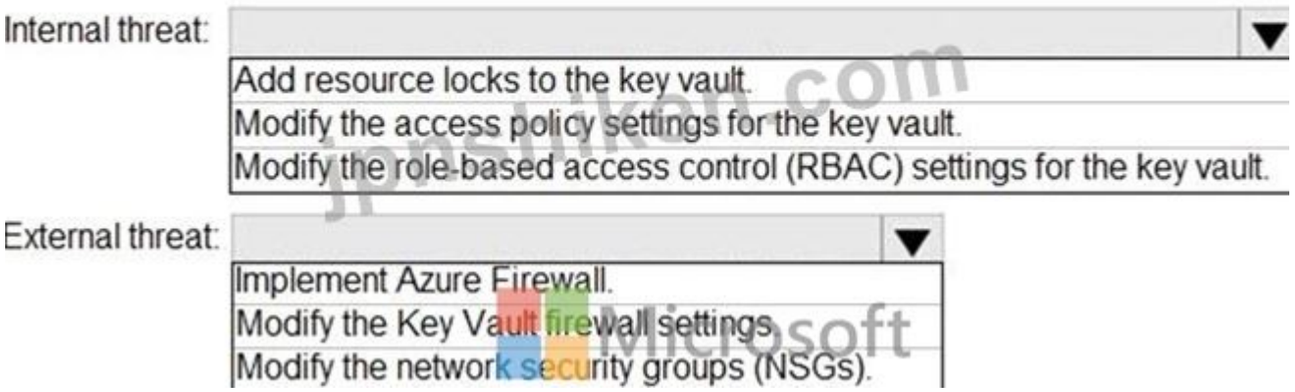


参照：
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

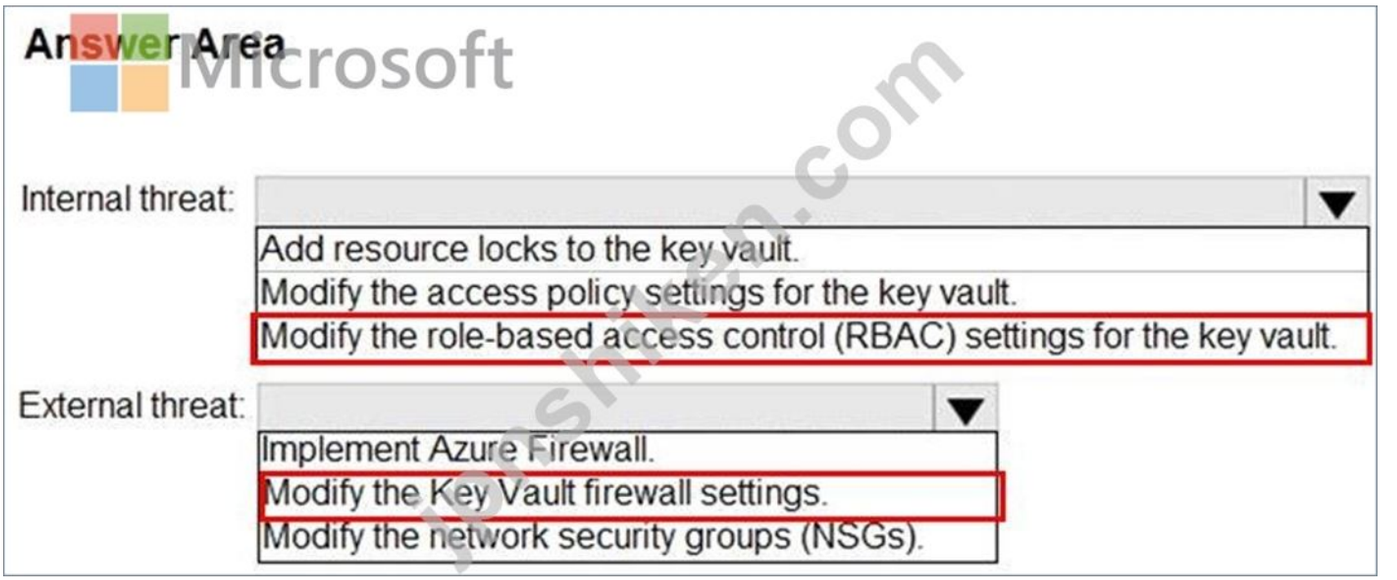
質問: **78**

You need to recommend remediation actions for the Azure Defender alerts for Fabrikam.
What should you recommend for each threat? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



正解:



Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault

質問: **79**
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：

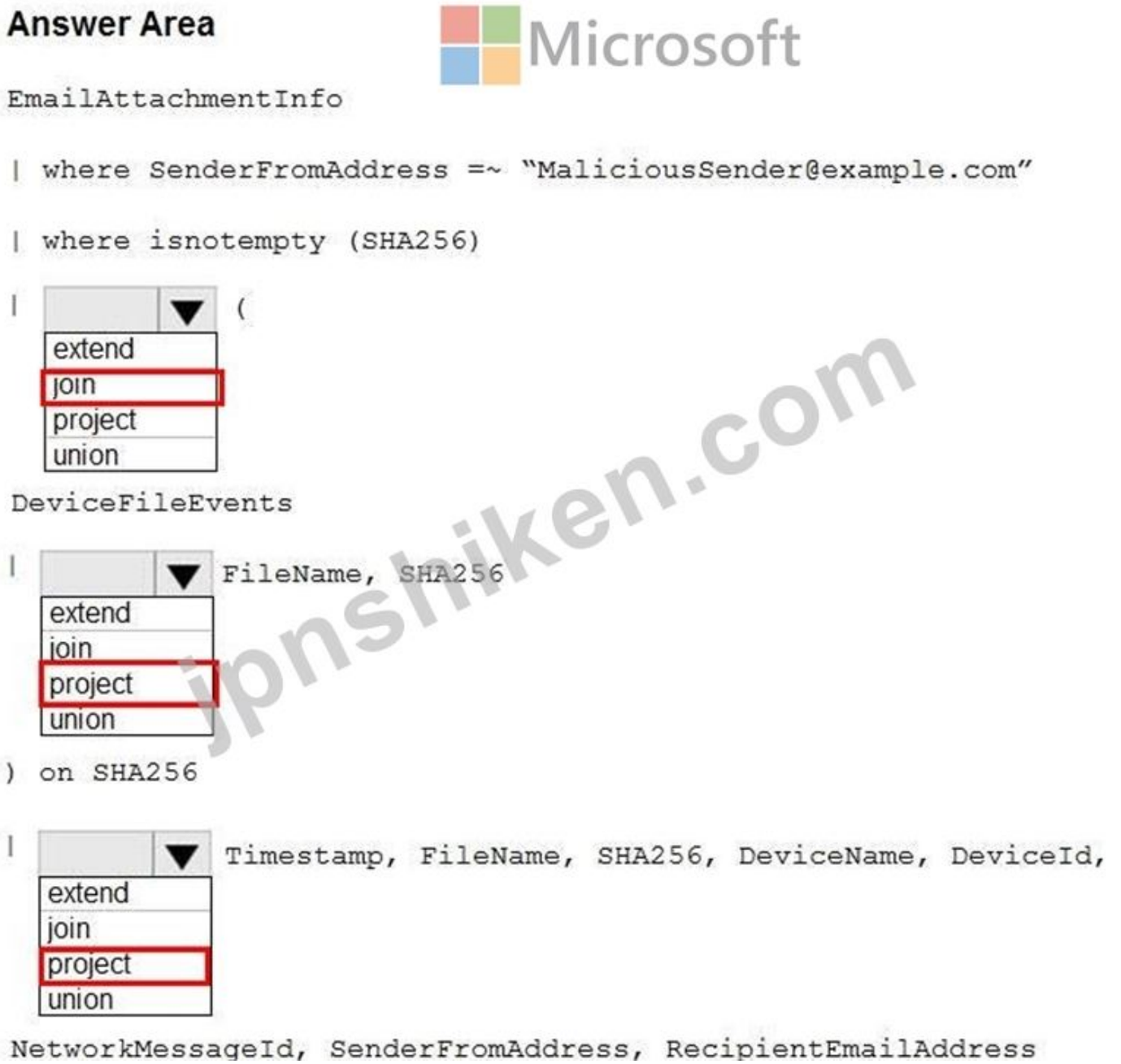
質問: **80**
Microsoft365E5サブスクリプションがあります。
Microsoft365Defenderを使用してクロスドメイン調査を実行することを計画しています。
悪意のある電子メールの添付ファイルの影響を受けるデバイスを特定するには、高度なハンティングクエリを作成する必要があります。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [extend / join / project / union] (
    DeviceFileEvents
    | [extend / join / project / union] FileName, SHA256
    ) on SHA256
| [extend / join / project / union] Timestamp, FileName, SHA256, DeviceName, DeviceId
```


正解:

Answer Area



参照：
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: **81**
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答えた後は、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。
AzureSecurityCenter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、[脅威の軽減]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: **(正解を表示します)**
説明/参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts Azure SentinelTestlet1を使用して脅威を軽減する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
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.comAzureAD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MicrosoftCloudAppSecurity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.comAzureAD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。

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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。

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

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 DefenderforIdentityを使用して保護する必要があります。

AzureInformationProtection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、AzureInformationProtection-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CloudAppSecurityの認可されていないアプリは、Microsoft DefenderforEndpoint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: **82**
米国東部のAzureリージョンにAzureSentinelを展開しています。
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展開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. Modify the workspace settings of the existing Azure Sentinel deployment
C. Add Azure Sentinel to a workspace.
D. Create a data connector in Azure Sentinel.
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

質問: **83**
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答えた後は、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。
AzureSecurityCenter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: **(**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-managing-and-responding-alerts

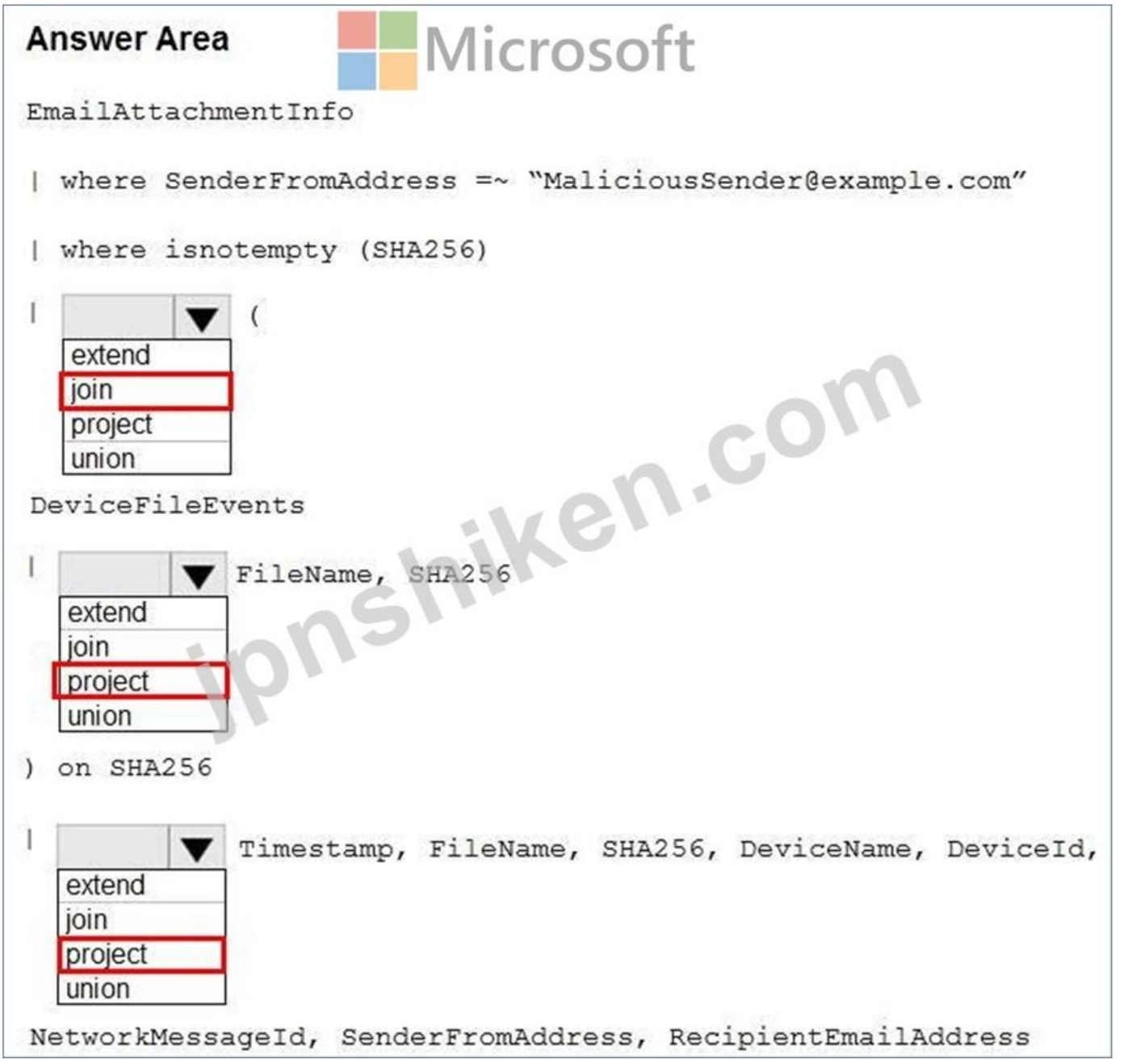
質問: **84**
新しいAzureサブスクリプションでLinux仮想マシンをプロビジョニングします。
Azure Defenderを有効にして、仮想マシンをAzureDefenderにオンボードします。
仮想マシンへの攻撃がAzureDefenderでアラートをトリガーすることを確認する必要があります。
仮想マシンで実行する必要がある2つのBashコマンドはどれですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. cp / bin / echo ./asc_alerttest_662jfi039n
B. ./ alerttest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: **A,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/security-center/security-center-alert-validation#simulate-alerts-on-your- azure-vms-linux-

質問: **85**
Microsoft365E5サブスクリプションがあります。
Microsoft365Defender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。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [extend / join / project / union] (
    DeviceFileEvents
    | [extend / join / project / union] FileName, SHA256
    ) on SHA256
| [extend / join / project / union] Timestamp, FileName, SHA256, DeviceName, DeviceId
```

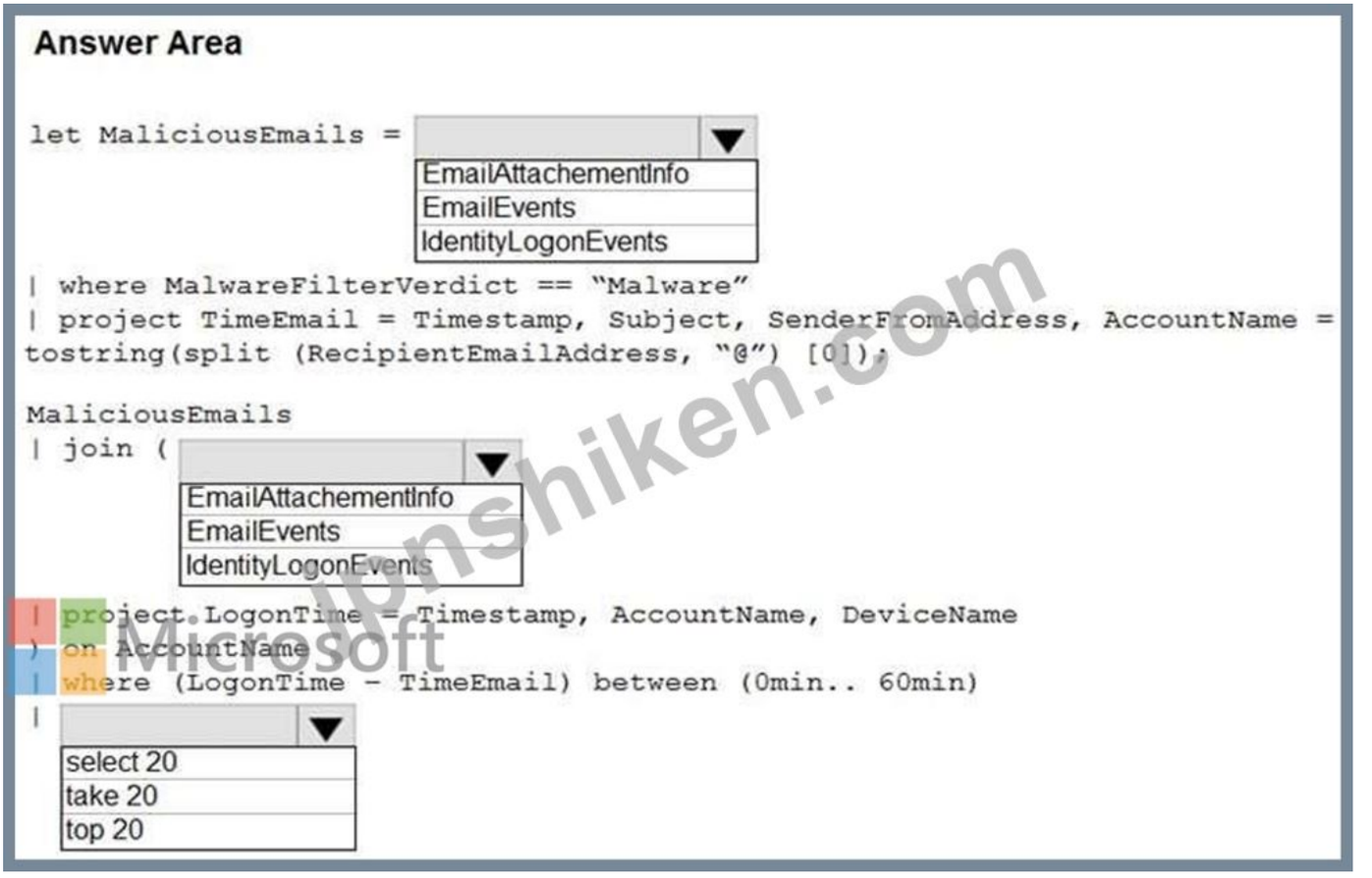

正解:



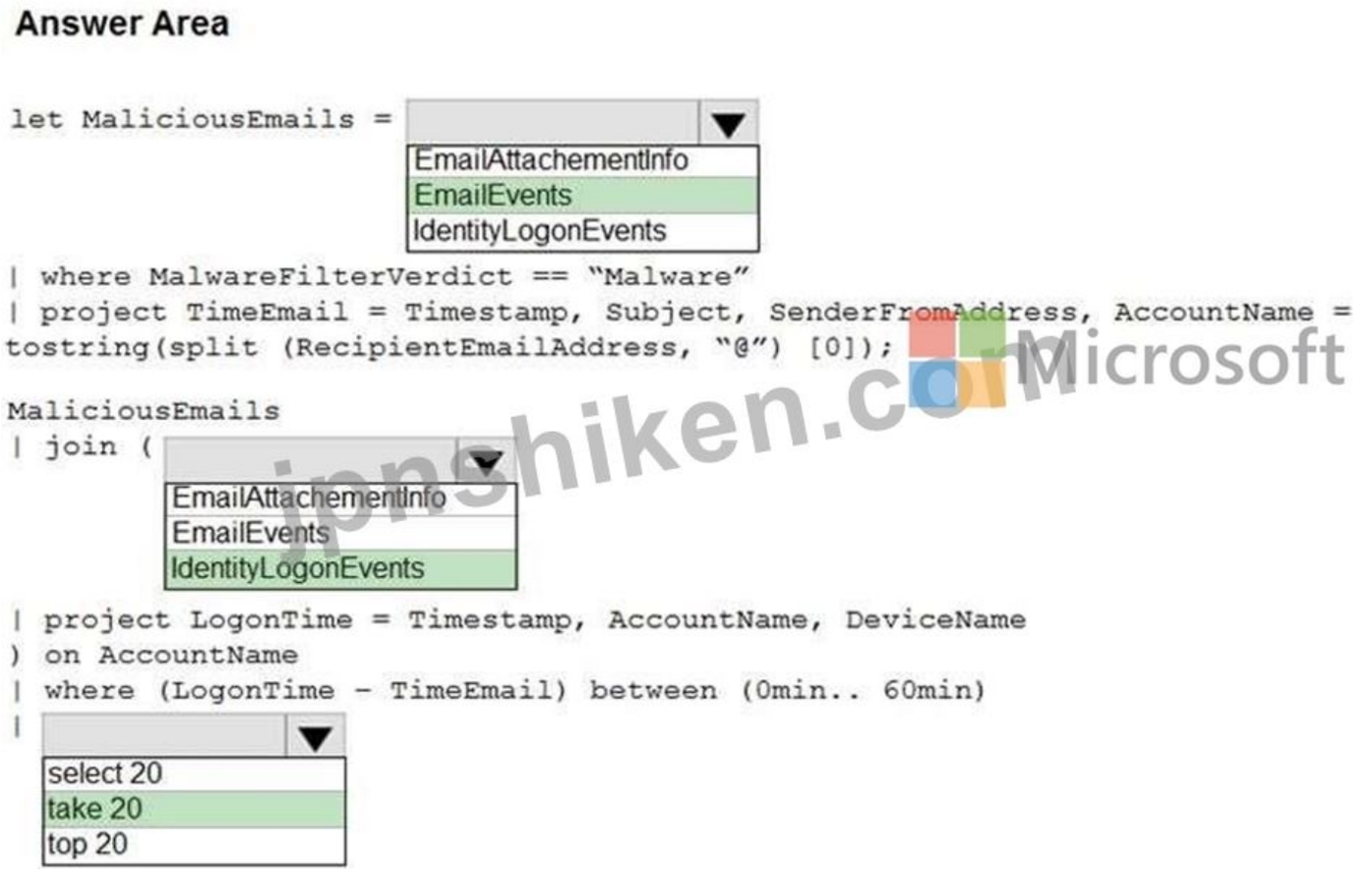
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: **86**
ホットスポット
ユーザーが受信する悪意のある電子メールの増加が通知されます。
電子メール受信者のアカウントが侵害されたかどうかを識別するために、Microsoft365Defenderで高度なハンティングクエリを作成する必要があります。クエリは、既知の悪意のある電子メールを受信してから1時間以内に受信者が実行した最新の20のサインインを返す必要があります。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
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：



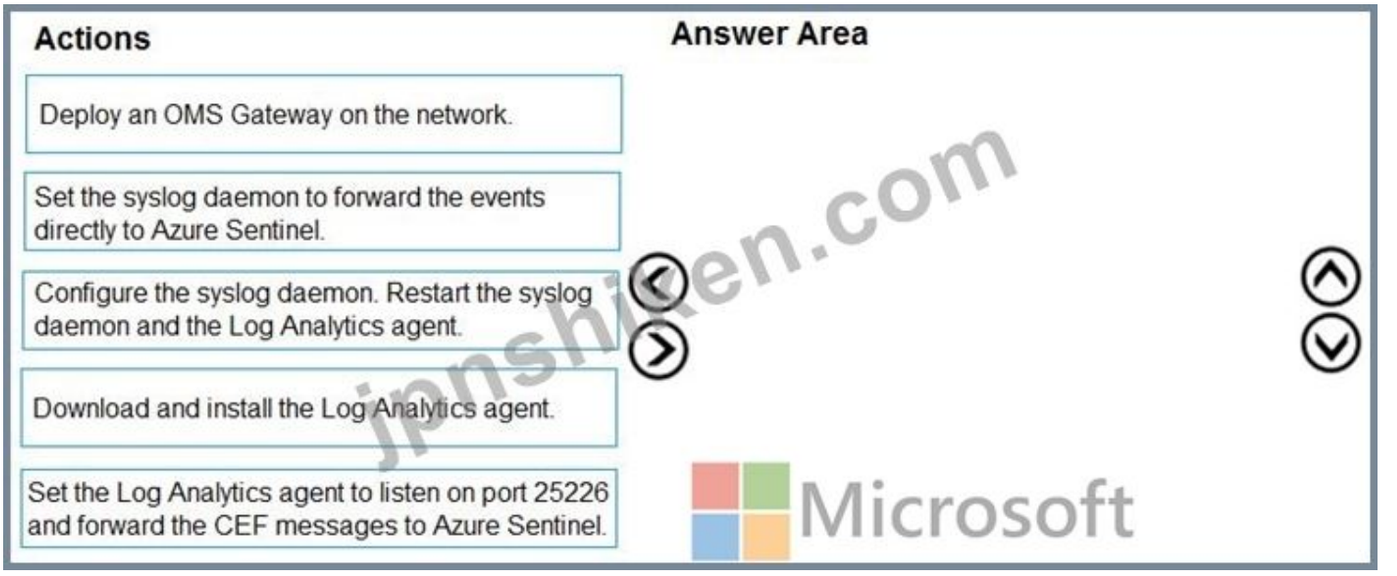
正解:



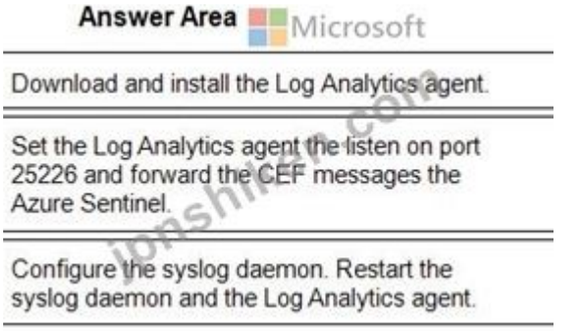
セクション :[なし]
説明/参照：

https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices？
view=o365-全世界

質問: **87**
Common Event Format（CEF）メッセージをAzureSentinelに送信する外部ソリューションを接続することを計画しています。
ログフォワーダーをデプロイ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。

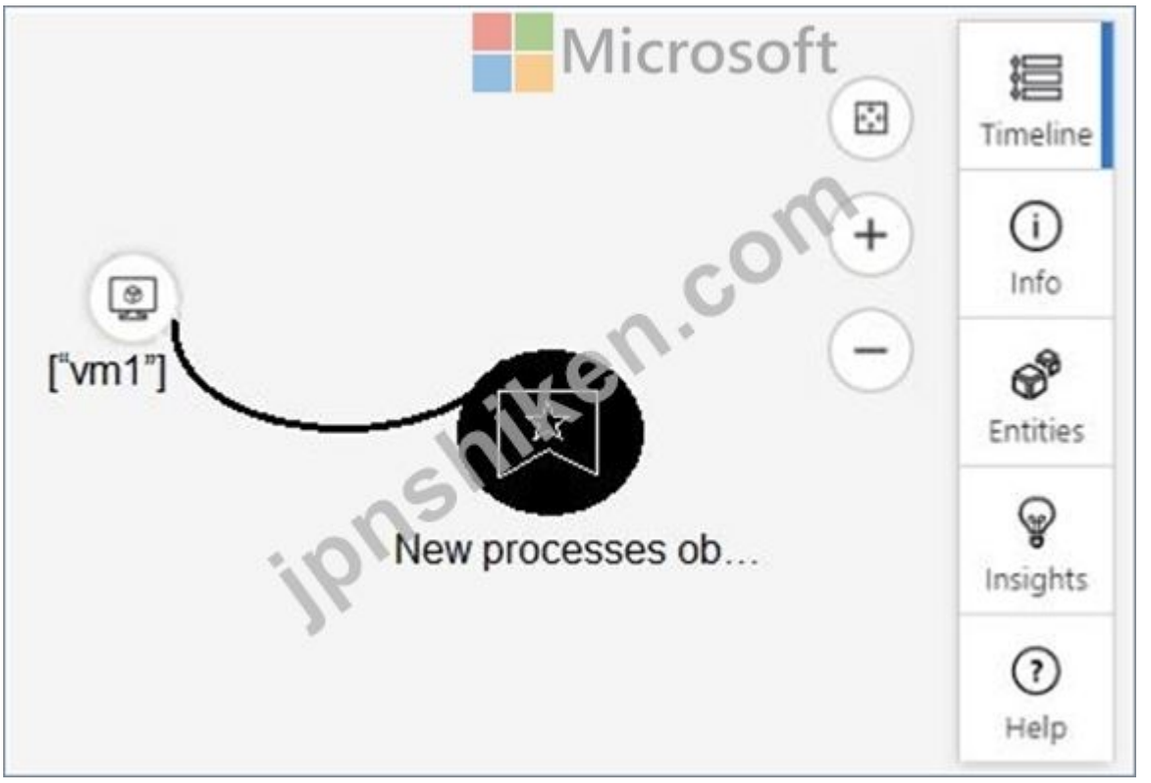


正解:



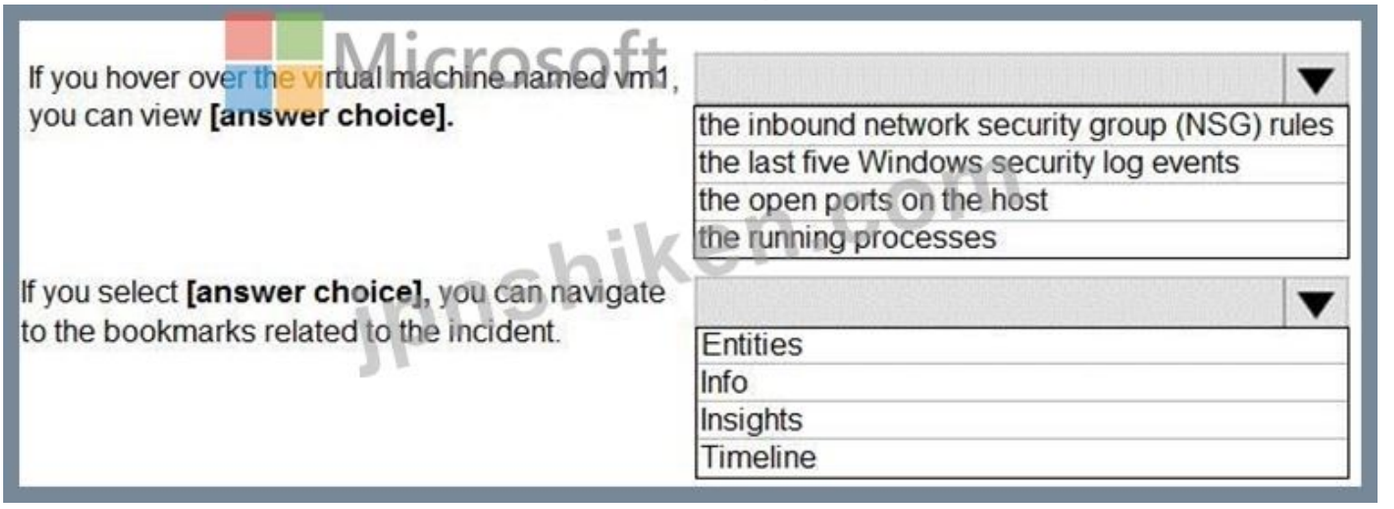
1-LogAnalyticsエージェントをダウンロードしてインストールします。
2-Log Analyticsエージェントをポート25226でリッスンするように設定し、CEFメッセージをAzureSentinelに転送します。
3-syslogデーモンを構成します。syslogデーモンとLogAnalyticsエージェントを再起動します。
参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

質問: **88**
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。



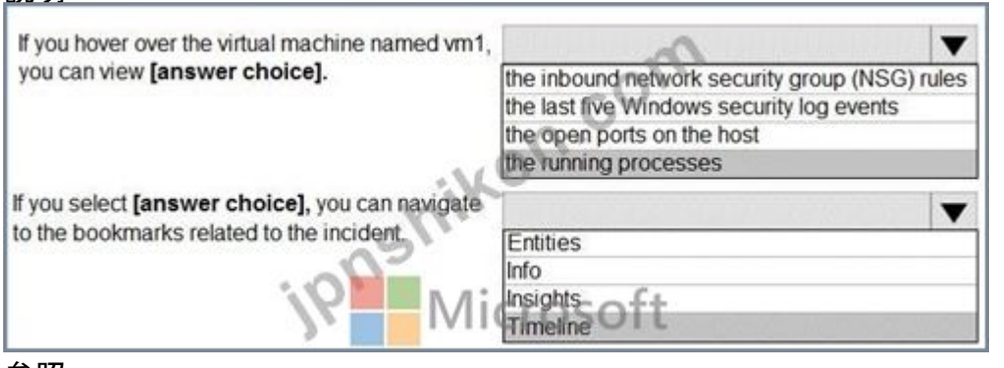
ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。

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

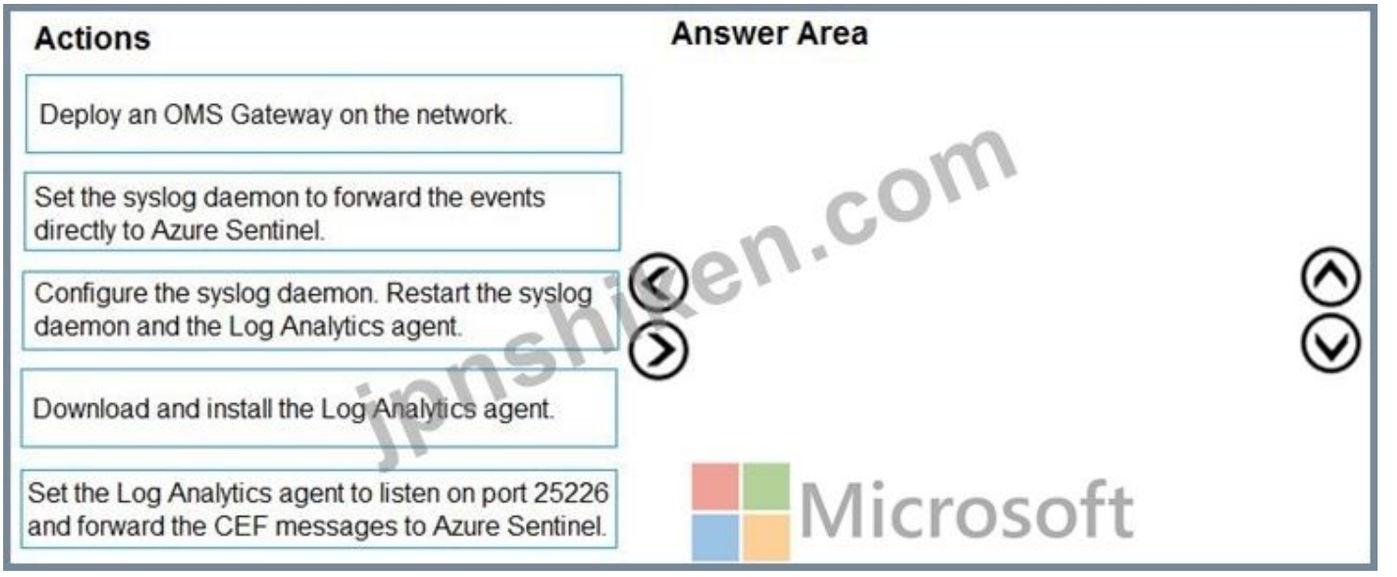


参照：

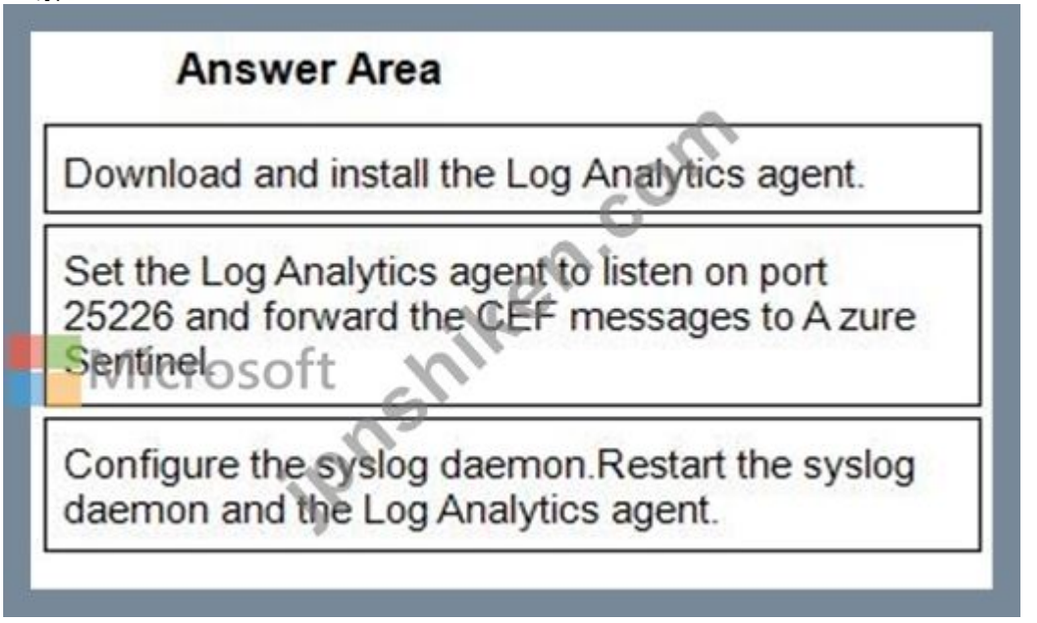
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-

graph-to-deep-di

質問: **89**
Common Event Format（CEF）メッセージをAzureSentinelに送信する外部ソリューションを接続することを計画しています。
ログフォワーダーをデプロイ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。



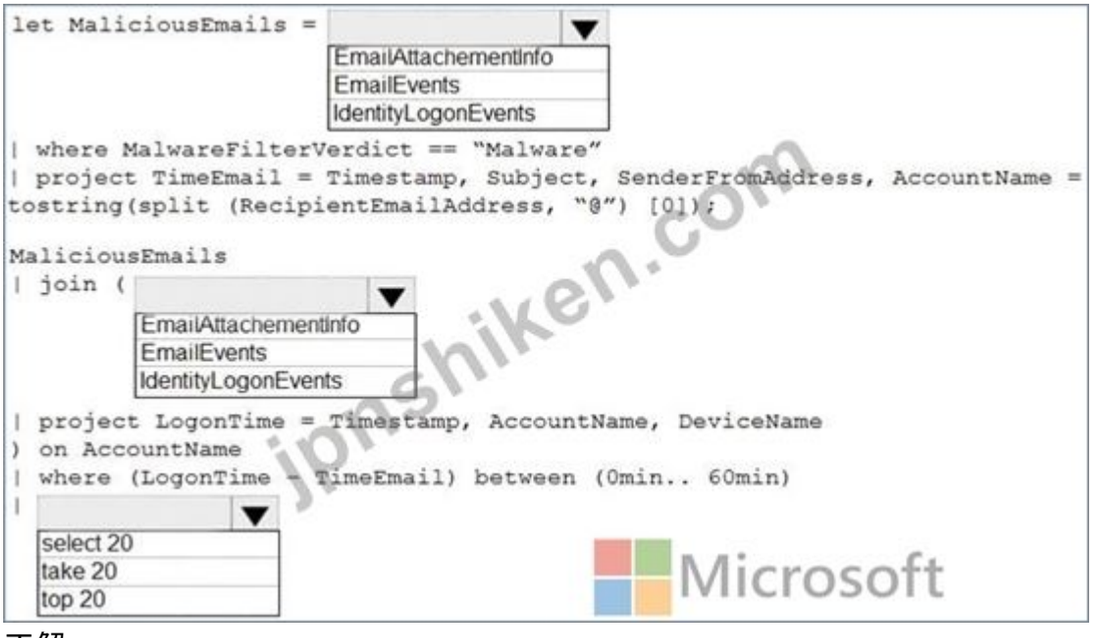
正解:



1-LogAnalyticsエージェントをダウンロードしてインストールします。
2-ポート25226でリッスンし、CEFメッセージをAzureSentinelに転送するようにLogAnalyticsエージェントを設定します。
3-syslogデーモンを構成します。syslogデーモンとLogAnalyticsエージェントを再起動します。
参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

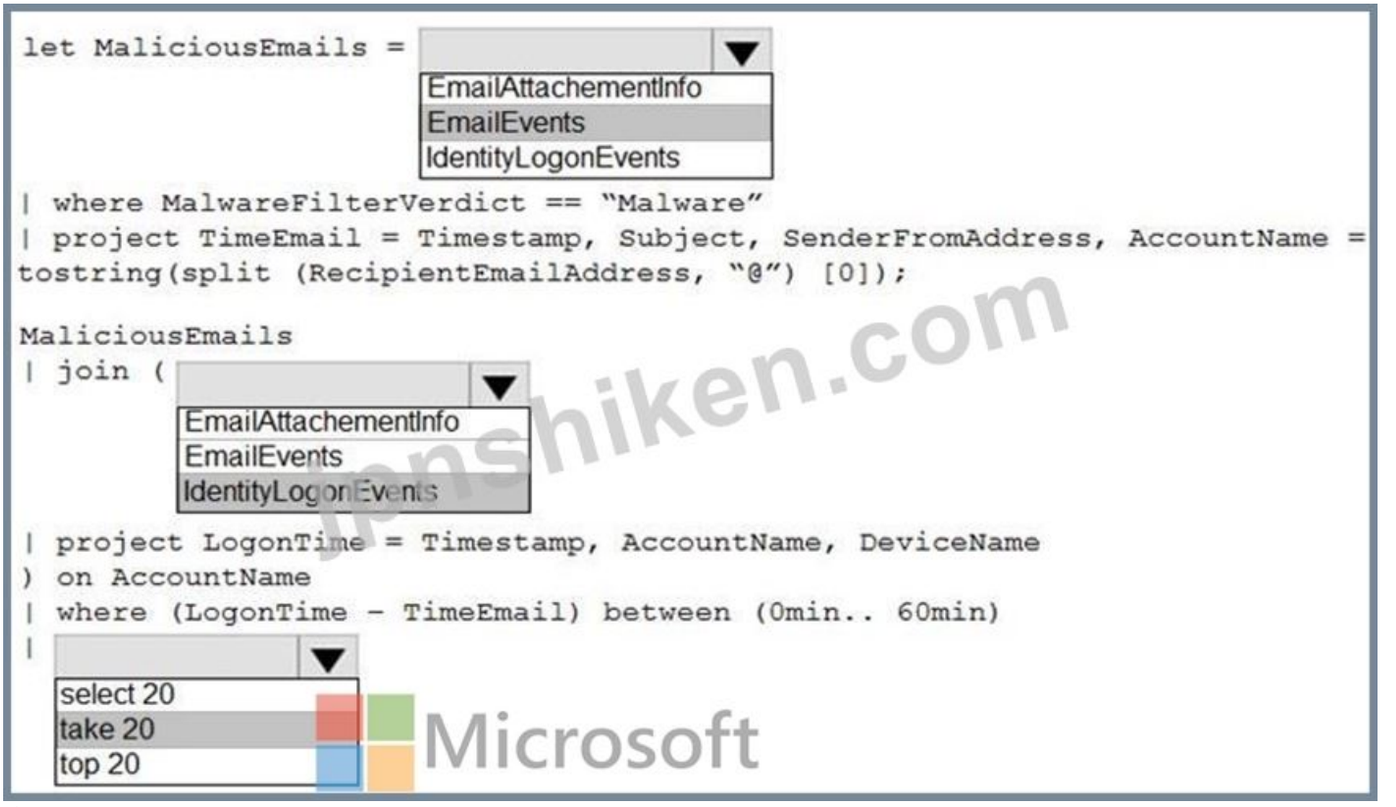
質問: **90**
AzureSentinelを構成しています。
疑わしいIPアドレスからのサインインが検出されるたびに、MicrosoftTeamsメッセージをチャネルに送信する必要があります。
Azure Sentinelで実行する必要がある2つのアクションはどれですか？それぞれの正解は、解決策の一部を示しています。
注：正しい選択はそれぞれ1ポイントの価値があります。
A. プレイブックを追加します。
B. プレイブックをインシデントに関連付けます。
C. エンティティの動作分析を有効にします。
D. ワークブックを作成します。
E. フュージョンルールを有効にします。
正解: **(正解を表示します)**
セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **91**
ユーザーが受信する悪意のある電子メールの増加が通知されます。
電子メール受信者のアカウントが侵害されたかどうかを識別するために、Microsoft365Defenderで高度なハンティングクエリを作成する必要があります。クエリは、既知の悪意のある電子メールを受信してから1時間以内に受信者が実行した最新の20のサインインを返す必要があります。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
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、電子メール説明が自動的に生成されます



参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view

質問: **92**
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たり却下したりすることはできないと報告しています。アナリストの問題を解決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. ロジックアプリコントリビューター
C. AzureSentinelコントリビューター
D. Azure Sentinel Reader

正解: **A** (コメントを発表する)
参照：
https://docs.microsoft.com/en-us/azure/sentinel/roles
トピック2、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 CloudAppSecurity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の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 MicrosoftSharePointOnline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: **93**
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。

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```


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. コンピューター
B. リソースグループ
C. ユーザー
D. IPアドレス
正解: **(**正解を表示します**)**

質問: **94**
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: **C (**コメントを発表する**)**
説明/参照：

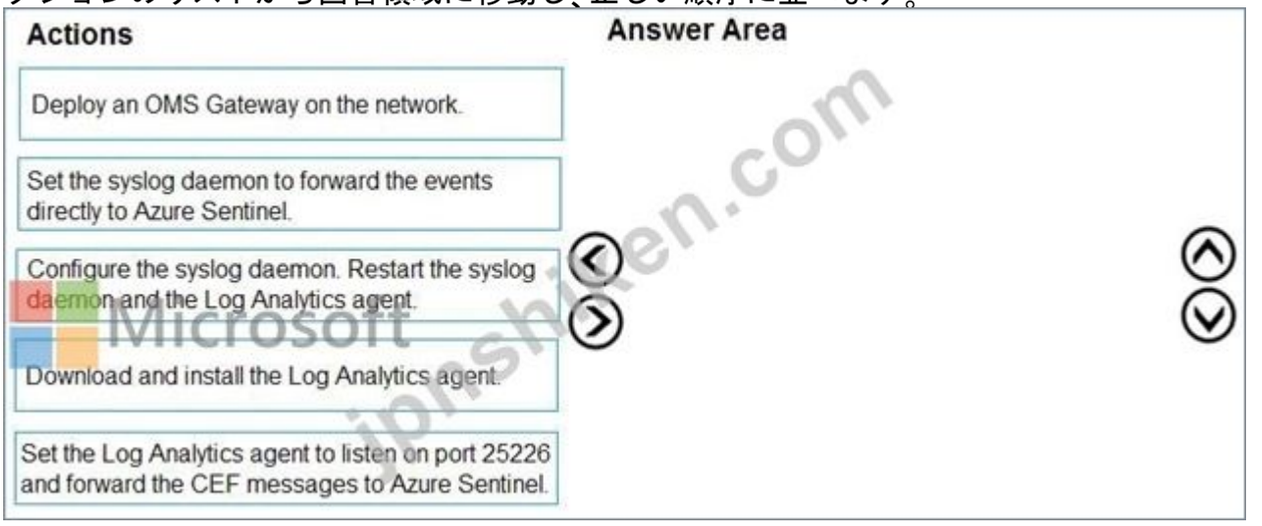
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-customAzureSentinel質問セット2を使用して脅威を軽減する

質問: **95**
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: **(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/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

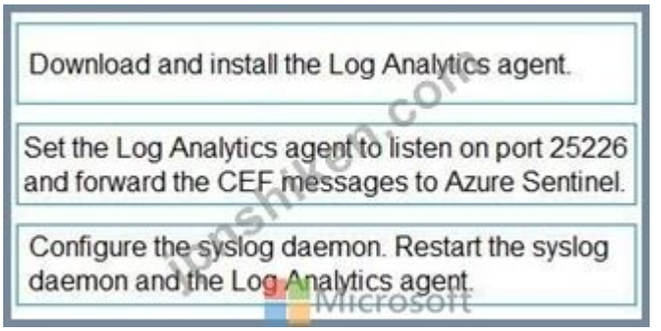
質問: **96**
組織内の他のユーザーがサインインに使用したことのない場所からユーザーがサインインしようとすると、セキュリティアラートを受信する必要があります。
どの異常検出ポリシーを使用する必要がありますか？
A. 不可能な旅
B. 匿名IPアドレスからのアクティビティ
C. 頻度の低い国からの活動
D. マルウェアの検出
正解: **(正解を表示します)**
説明
悪意のある活動を示す可能性のある国/地域からの活動。このポリシーは、環境のプロファイルを作成し、最近ではない場所、または組織内のどのユーザーもアクセスしたことがない場所からアクティビティが検出されたときにアラートをトリガーします。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。

参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

質問: **97**
Common Event Format（CEF）メッセージをAzureSentinelに送信する外部ソリューションを接続することを計画しています。
ログフォワーダーをデプロイ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



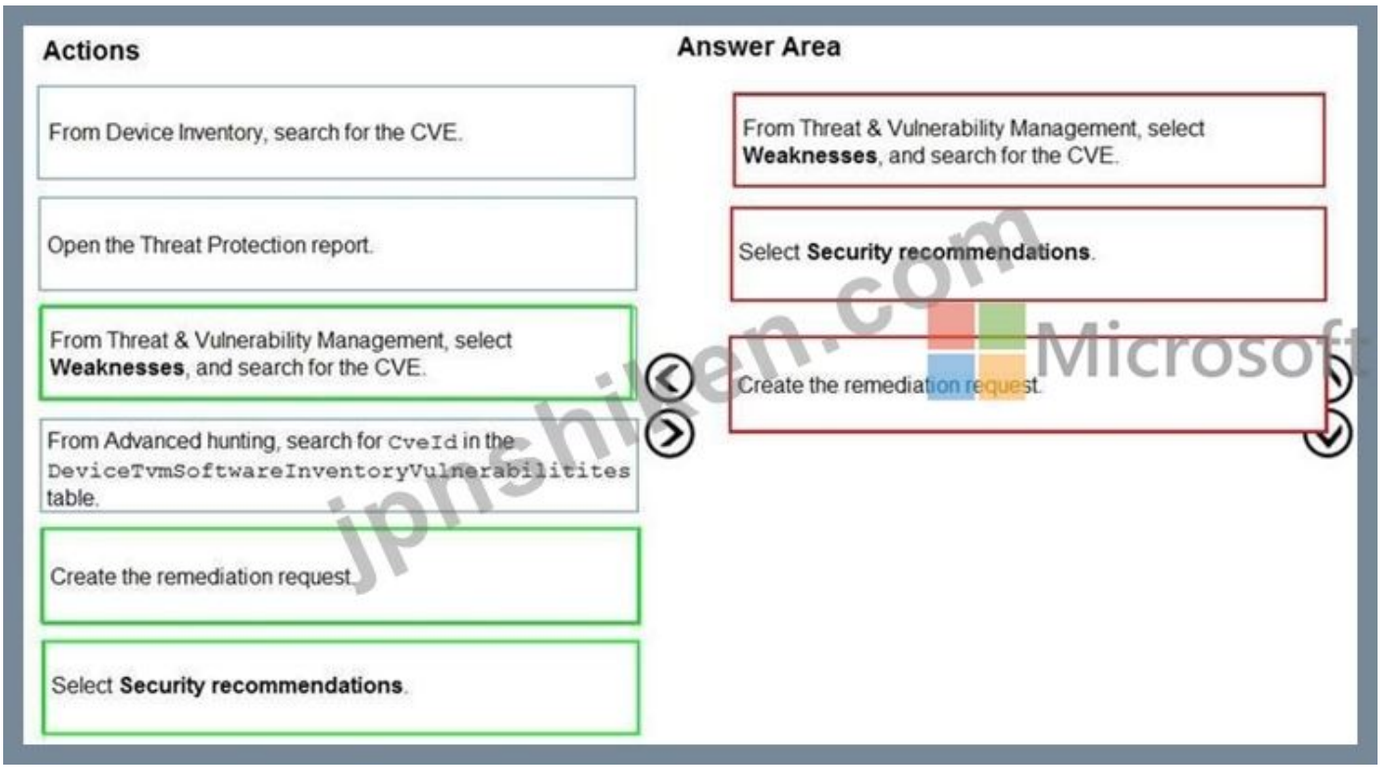
参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

質問: **98**
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**: 99**
環境に影響を与える新しいCommonVulnerabilityand 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**:**



参照：
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

質問**: 100**

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答えた後は、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。

AzureSecurityCenter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]

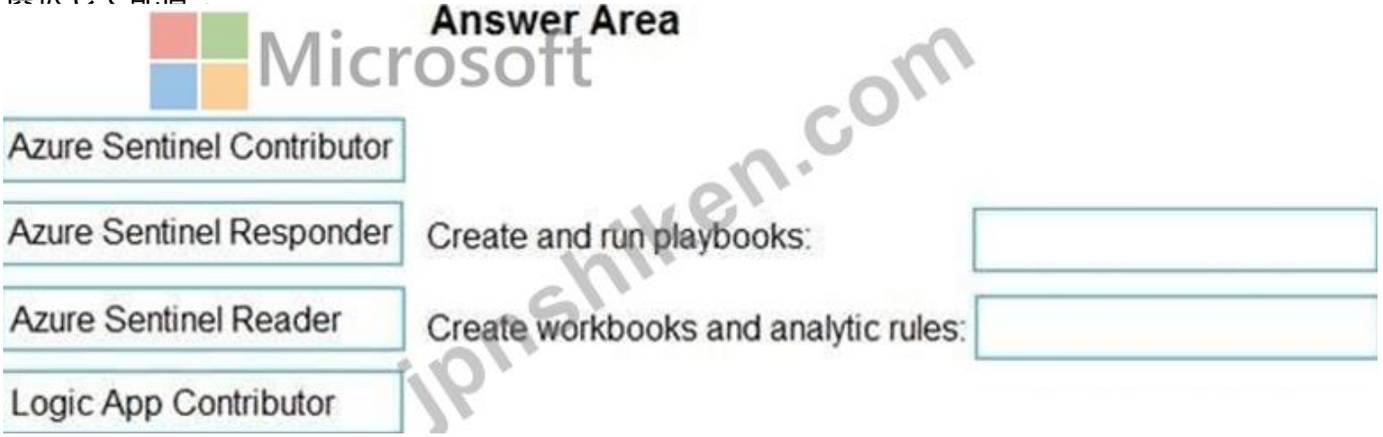
Explanation:

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。

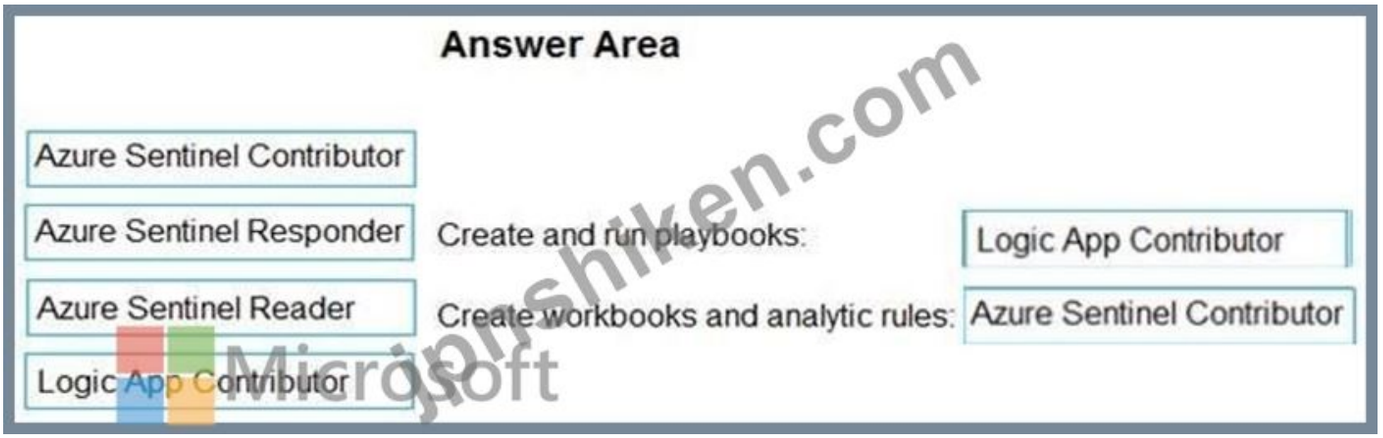
参照：

https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

質問: **101**
ドラッグドロップ
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。
選択して配置：



正解:

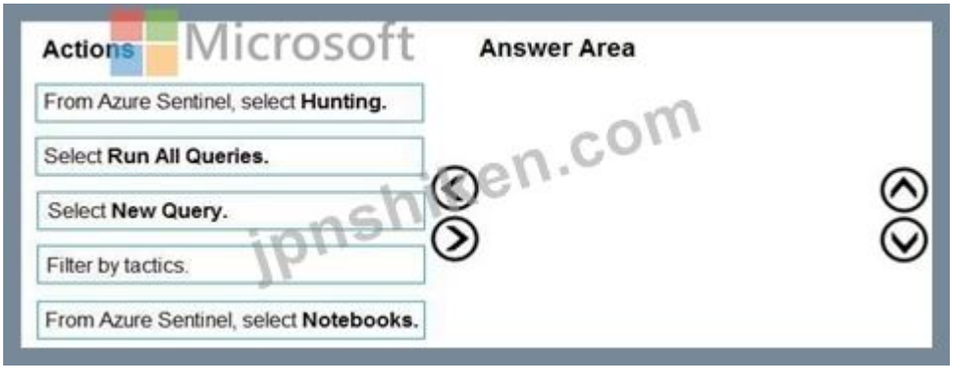


セクション :[なし]
説明/参照：
https://docs.microsoft.com/en-us/azure/sentinel/roles

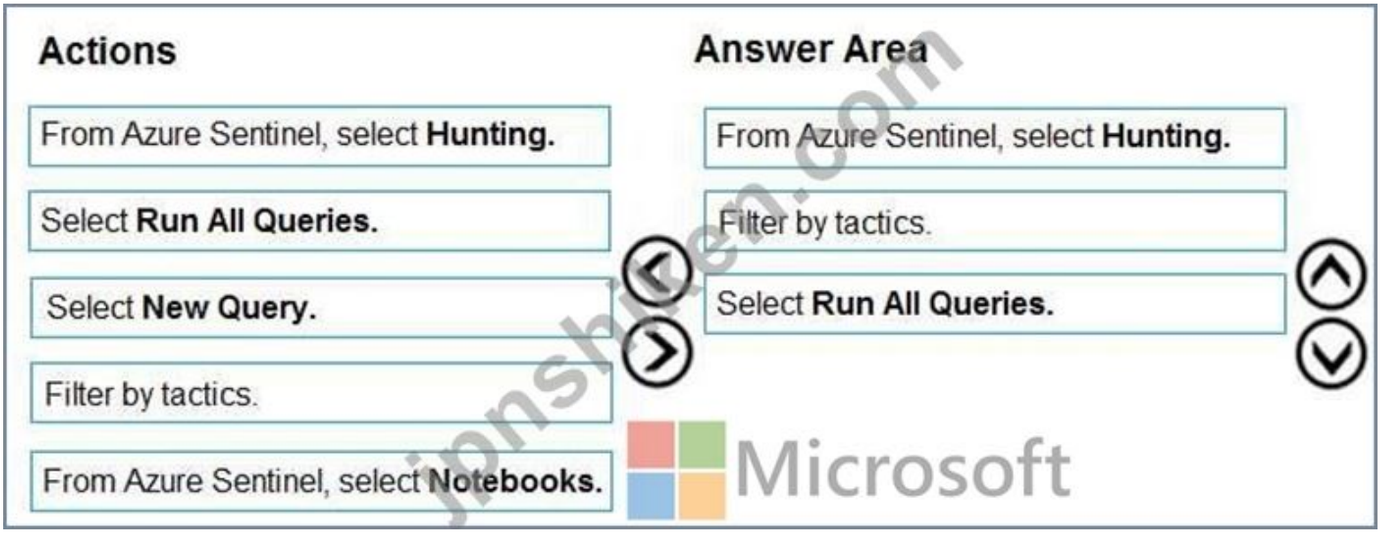
質問: **102**

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**)**
セクション :[なし]

質問: **103**
ドラッグドロップ
AzureSentinelがデプロイされています。
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。
選択して配置：



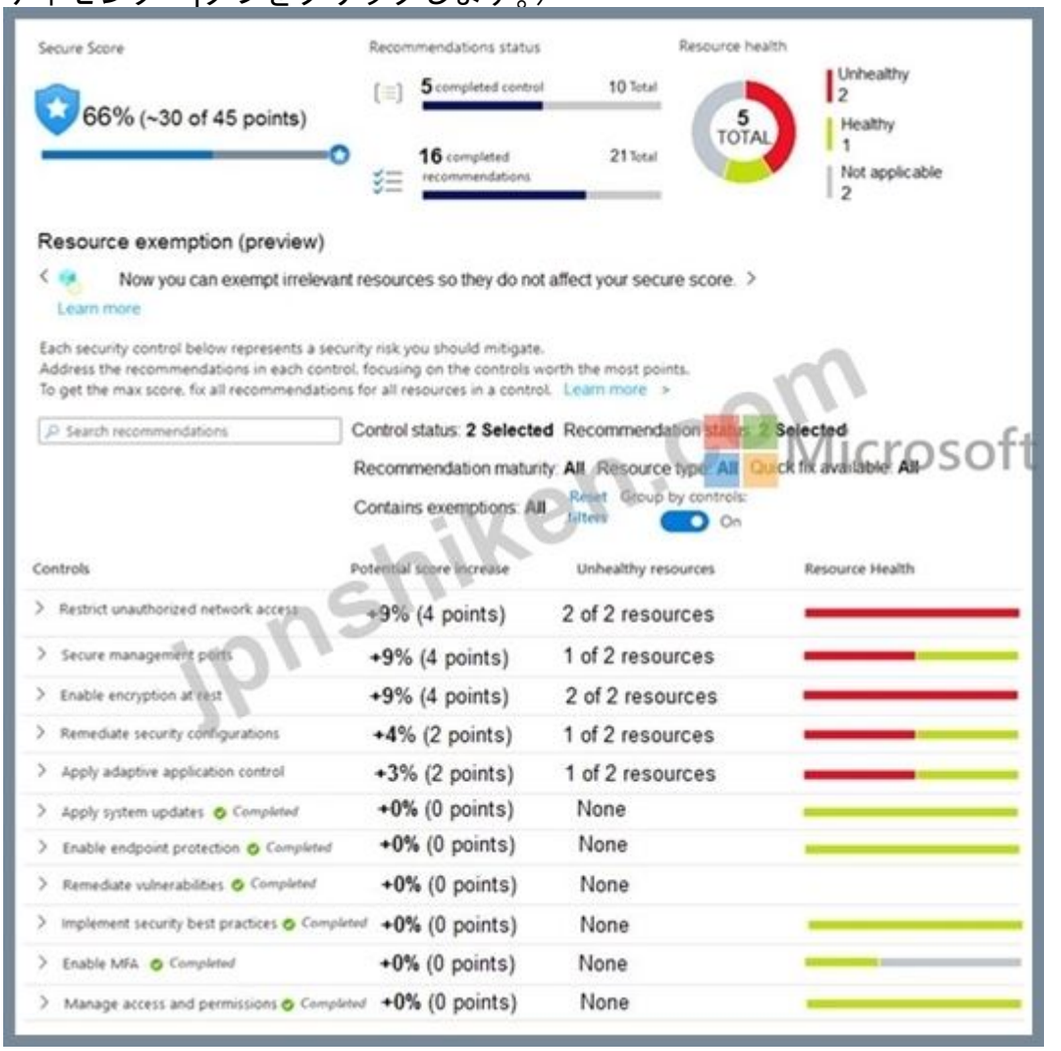
正解:



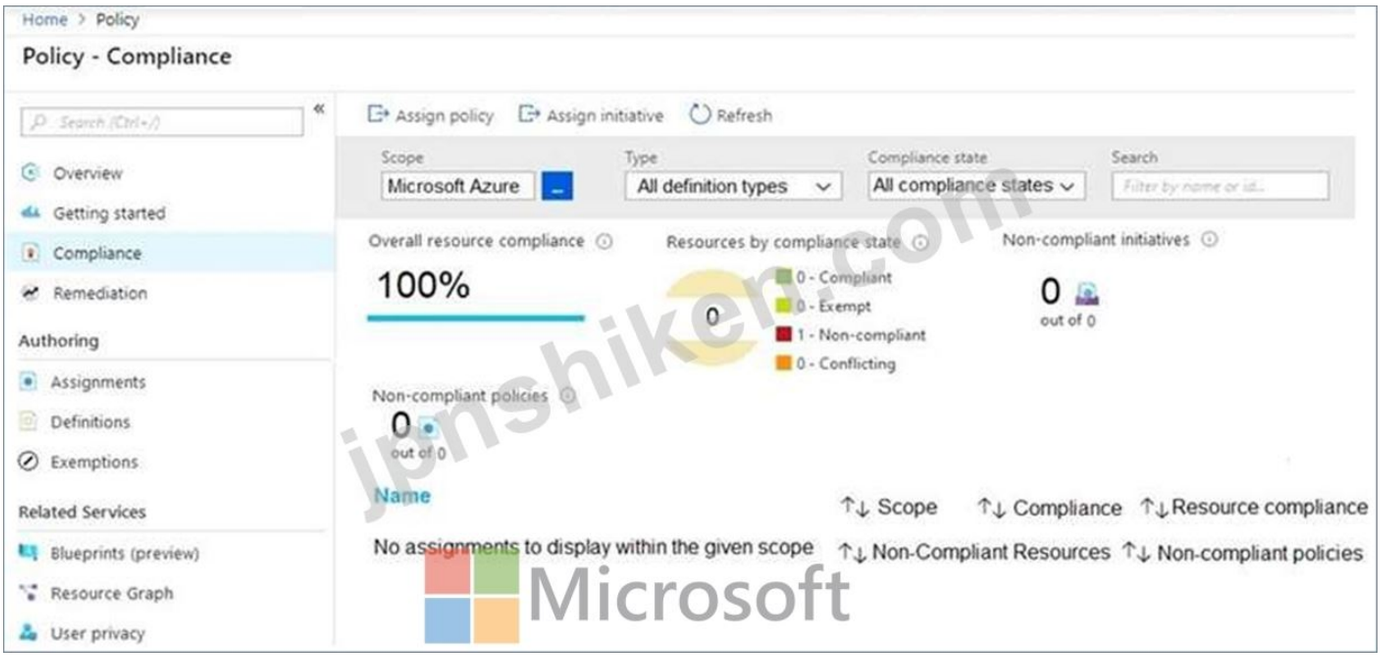
セクション :[なし]
説明/参照：

https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/

質問**: 104**
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。）

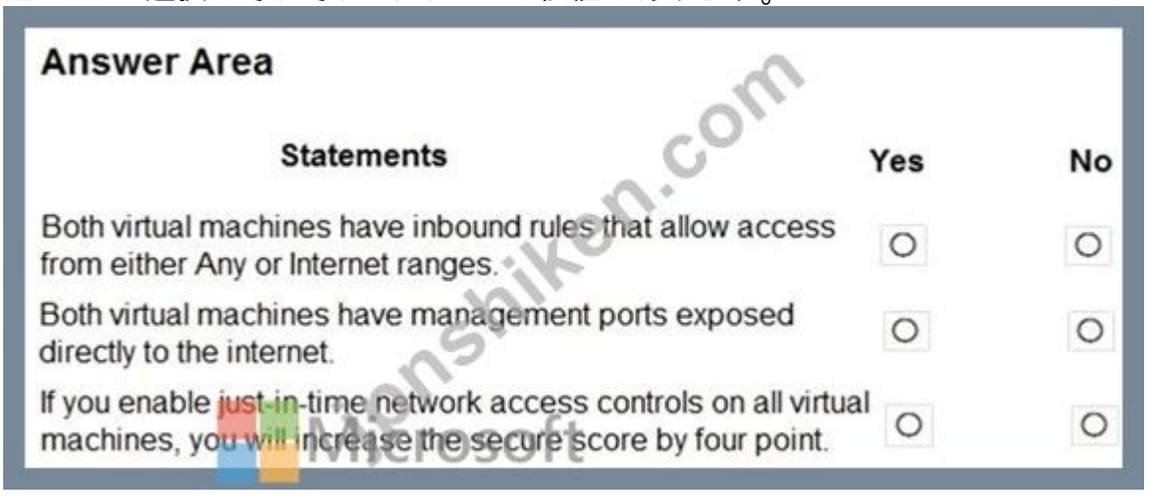


Azureポリシーの割り当ては、ポリシーの展示に示されているように構成されます。[ポリシー]タブをクリックします。）

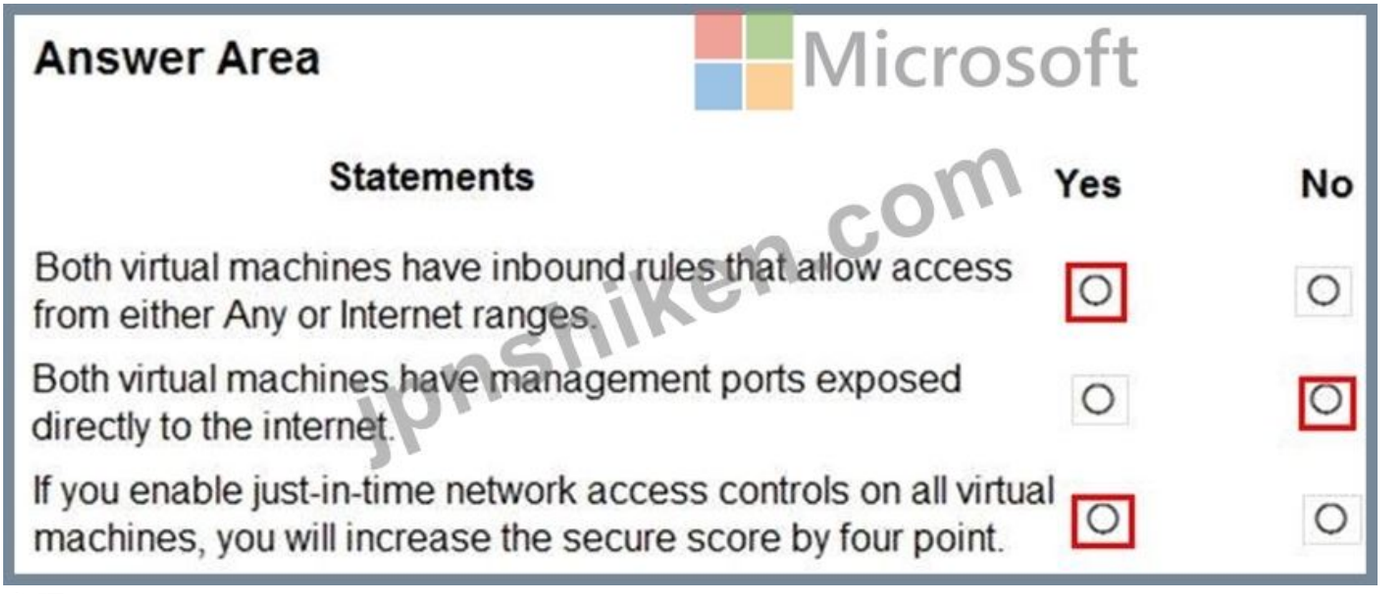


次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。

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:

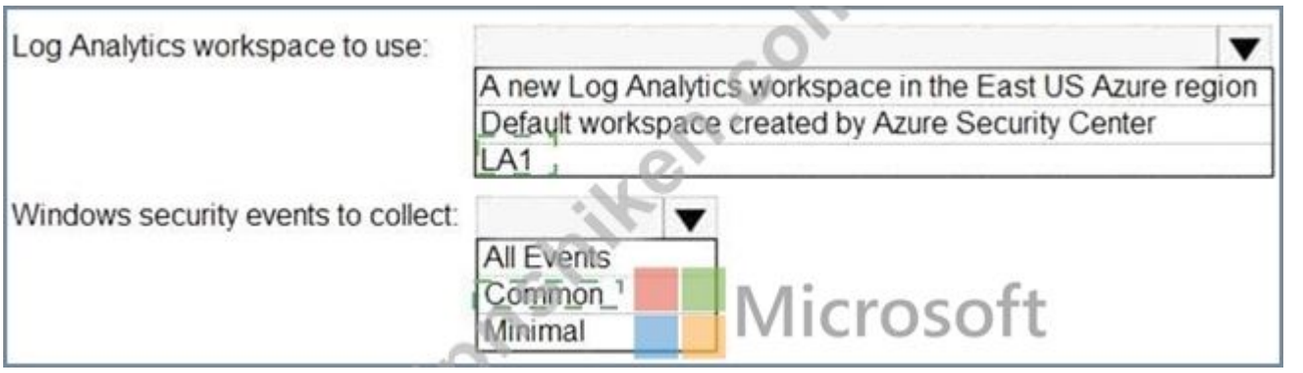


参照：

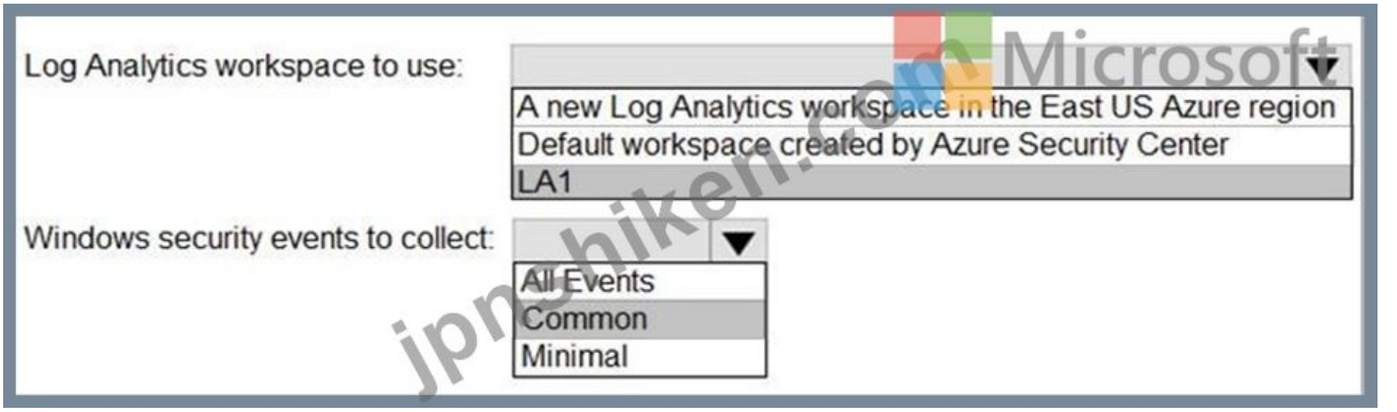
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

質問: **105**
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、回答エリアで適切なオプションを選択してください。
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:



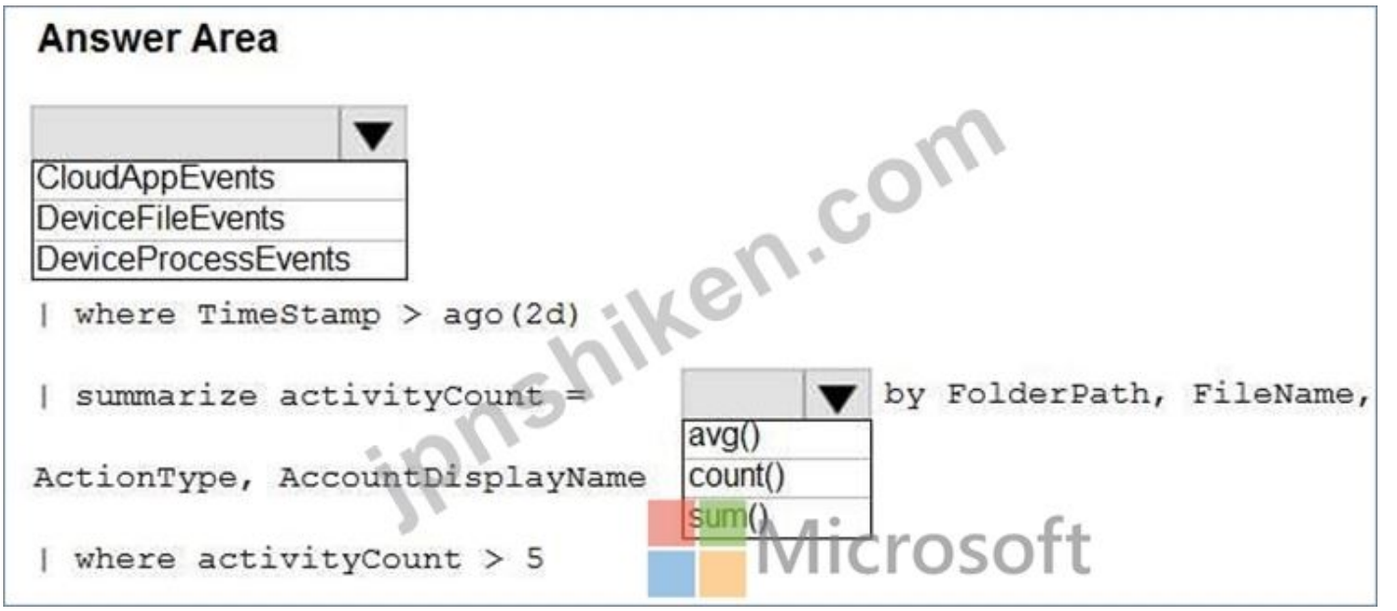
説明
グラフィカルユーザーインターフェイス、アプリケーションの説明が自動的に生成されます



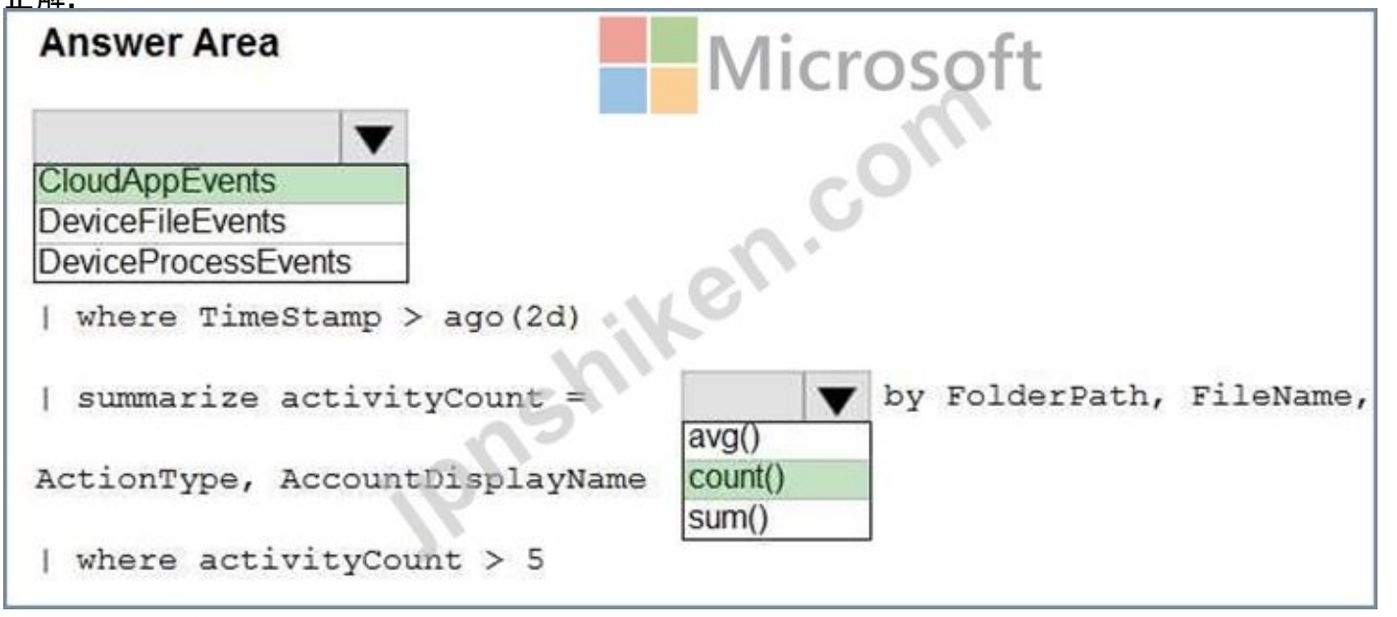
質問: **106**
あなたの会社は次のサービスを展開しています。

*アイデンティティのためのMicrosoftDefender
*エンドポイント用のMicrosoftDefender
*Office365用のMicrosoftDefender
セキュリティアナリストにMicrosoft365セキュリティセンターを使用する機能を提供する必要があります。アナリストは、Microsoft DefenderforEndpointによって生成された保留中のアクションを承認および拒否できる必要があります。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。
アナリストに割り当てる必要がある2つの役割はどれですか？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. Azure Active Directory（Azure AD）のコンプライアンスデータ管理者
B. Microsoft DefenderforEndpointでのアクティブな修復アクションの役割
C. Azure Active Directory（Azure AD）のセキュリティ管理者の役割
D. Azure Active Directory（Azure AD）でのセキュリティリーダーの役割
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/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

質問: **107**
ホットスポット
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。
クエリをどのように完了する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。
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：

テストレット2

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
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.comAzureAD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MicrosoftCloudAppSecurity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.comAzureAD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。

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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。

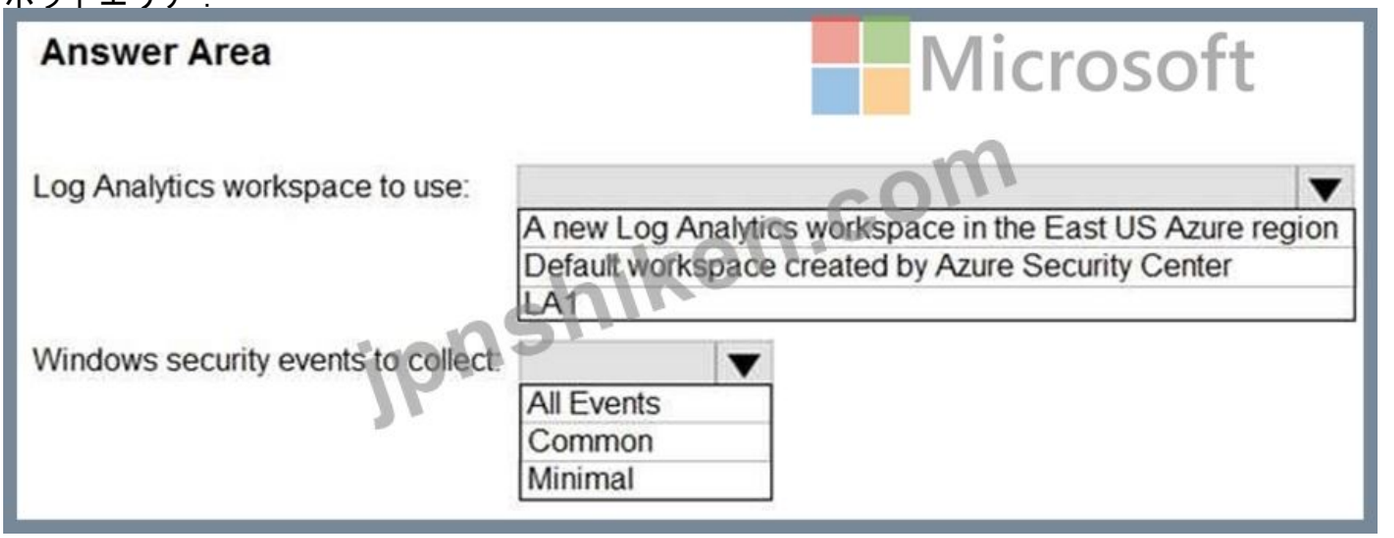
Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

現在の問題

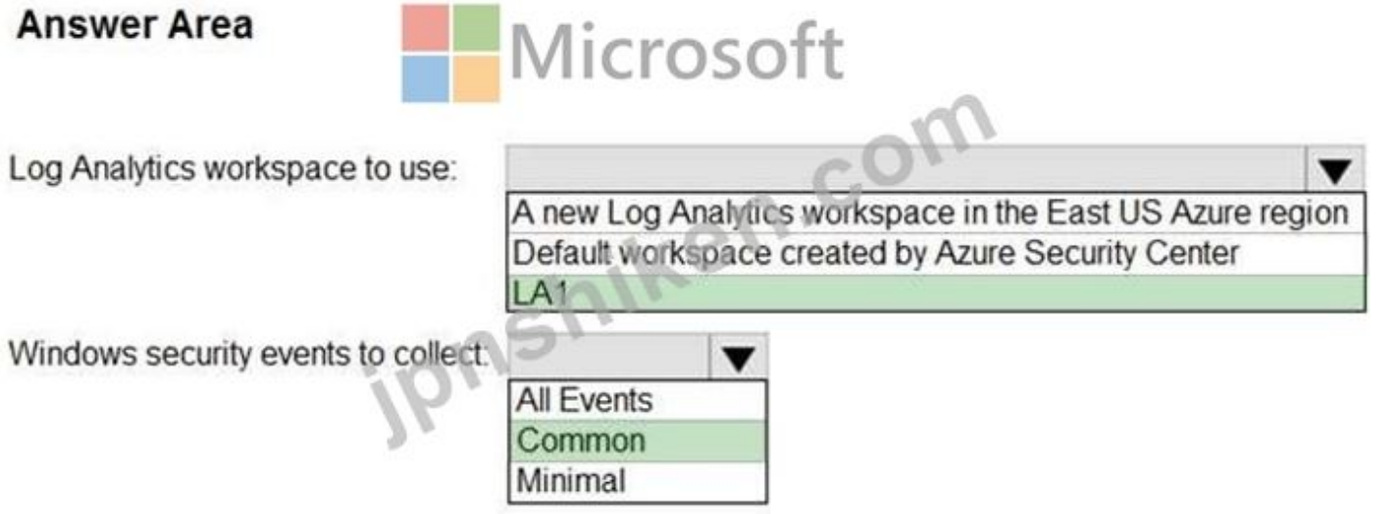
Cloud App Securityは、ユーザーが両方のオフィスに同時に接続すると、誤検知アラートを頻繁に生成します。
計画された変更
Litwareは、次の変更を実装する予定です。
*AzureサブスクリプションでAzureSentinelを作成および構成します。
* Azure ADテストユーザーアカウントを使用して、AzureSentinelの機能を検証します。
ビジネス要件
Litwareは、次のビジネス要件を識別します。
*可能な限り、最小特権の原則を使用する必要があります。
*他のすべての要件が満たされている限り、コストを最小限に抑える必要があります。
* Log Analytics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 DefenderforIdentityを使用して保護する必要があります。
AzureInformationProtection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、AzureInformationProtection-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CloudAppSecurityの認可されていないアプリは、Microsoft DefenderforEndpoint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: **108**
ホットスポット

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、回答エリアで適切なオプションを選択してください。
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：
テストレット2
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つの支社があります。
本社はシアトルにあります。支社はトロント、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持つ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 CloudAppSecurity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の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MicrosoftSharePointOnline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。
*外部および内部の脅威が発生した場合に、ContosoのKeyVaultアラート用のAzureDefenderを修正する手順を開発します。このソリューションでは、主要なボールトコンテンツにアクセスするための正当な試みへの影響を最小限に抑える必要があります。
*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: **109**
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**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

有効的な**SC-200**問題集はJPNTest.com提供され、**SC-200**試験に合格することに役に立ちます！JPNTest.comは今最新**SC-200**試験問題集を提供します。JPNTest.com SC-200試験問題集はもう更新されました。ここで**SC-200**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/SC-200-mondaishu　**370**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」