Microsoft.SC-200.v2026-07-10.q128

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：	128
バージョン：	v2026-07-10
ページの閲覧量：	102
問題集の閲覧量：	1304

https://www.jpnshiken.com/shiken/Microsoft.SC-200.v2026-07-10.q128.html

質問: **1**

あなたはAzureサブスクリプションをお持ちです。

Microsoft Sentinelワークスペースを導入する予定です。1日あたり20GBのセキュリティログデータを取り込むことを想定しています。

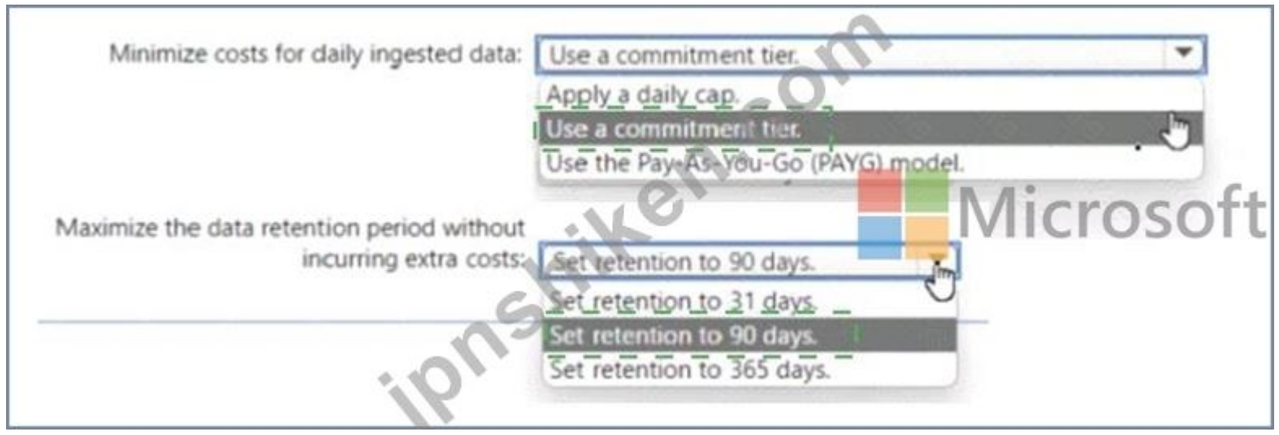
ワークスペースのストレージを設定する必要があります。ソリューションは以下の要件を満たす必要があります。

* 日々取り込むデータにかかるコストを最小限に抑える。

追加費用をかけずにデータ保持期間を最大限に延ばす。

各要件に対して、どのような対応を取るべきですか？回答欄で適切な選択肢を選んでください。注：正解ごとに1ポイントが加算されます。

正解:



Explanation:

質問: **2**

Microsoft Sentinelワークスペースには、以下のAdvanced Security Information Model（ASIM）パーサーが含まれています。

* _Im_ProcessCreate
* InProcessCreate

vimProcessCreate という名前の、ソース固有の新しいパーサーを作成します。

以下の要件を満たすようにパーサーを修正する必要があります。

* すべての ProcessCreate パーサーを呼び出します。
* フィールドをプロセススキーマに標準化する。

各要件を満たすために、どのパーサーを変更する必要がありますか？回答するには、適切なパーサーを正しい要件にドラッグしてください。各パーサーは、1回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の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：正解ごとに1ポイントが加算されます。

正解:

Explanation:

質問: **3**

お客様は、Microsoft Defender for Endpointを使用するMicrosoft 365 E5サブスクリプションをご利用中です。

以下の表に示すオンプレミスデバイスがあります。

Name	Management state	Operating system
Device1	Onboarded to and managed by using Microsoft Defender for Endpoint	Windows Server 2022
Device2	Discovered by Microsoft Defender for Endpoint and unmanaged	Linux

マルウェアに感染したデバイスに対するインシデント対応計画を作成しています。以下の要件を満たす対応策を推奨する必要があります。

・マルウェアが管理対象デバイスと通信したり、デバイスに感染したりするのを阻止します。

* 管理対象デバイスの制御機能には影響を与えません。

各デバイスに対して、どのような操作を行うべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

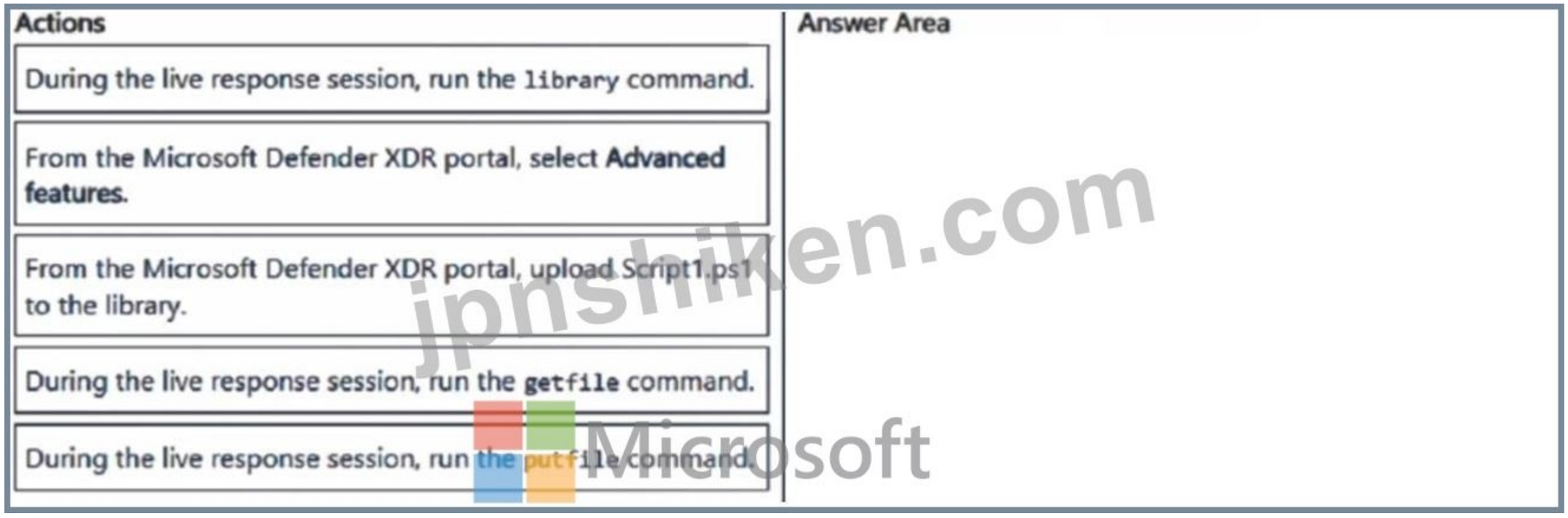
正解:

Explanation:

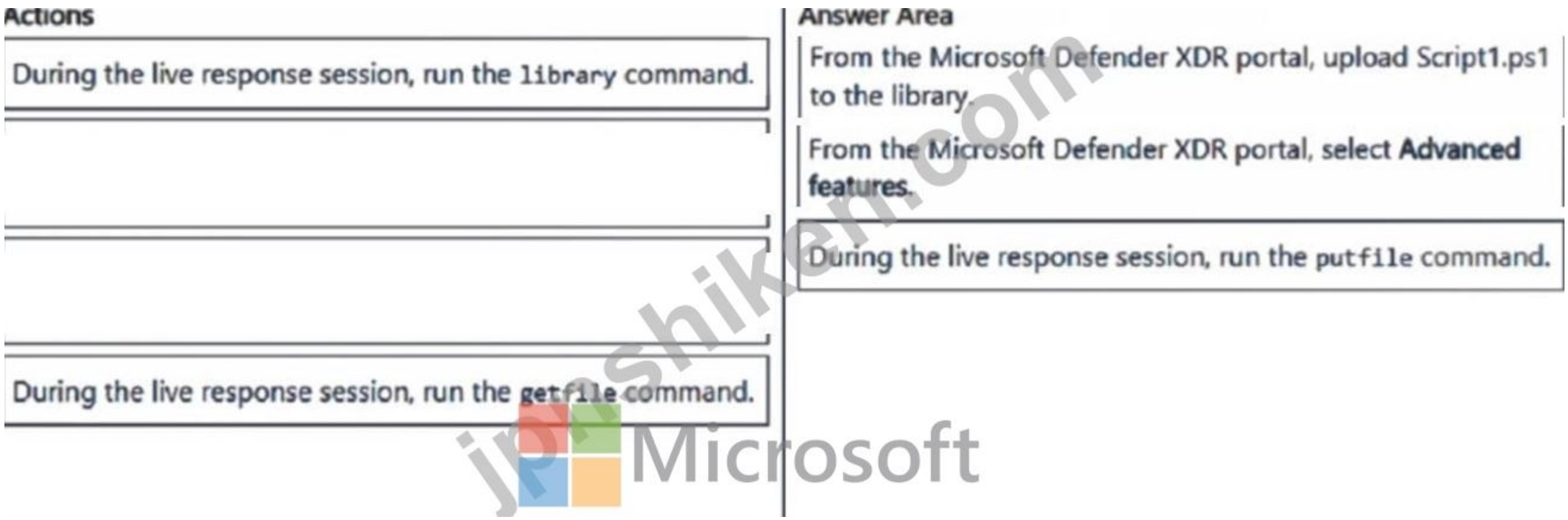
質問: 4

ドラッグアンドドロップ問題

お客様は、Device1という名前のWindows 11デバイスを含むMicrosoft 365 E5サブスクリプションをご利用中です。
デバイス1はMicrosoft Defender XDRに登録されました。
あなたは以下の操作を実行します。
- Script1.ps1という名前のPowerShellスクリプトを作成します。
Microsoft Defender XDR ポータルから、ライブレスポンスを確立します。
デバイス1へのセッション。
Device1上でScript1.ps1を実行できることを確認する必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。

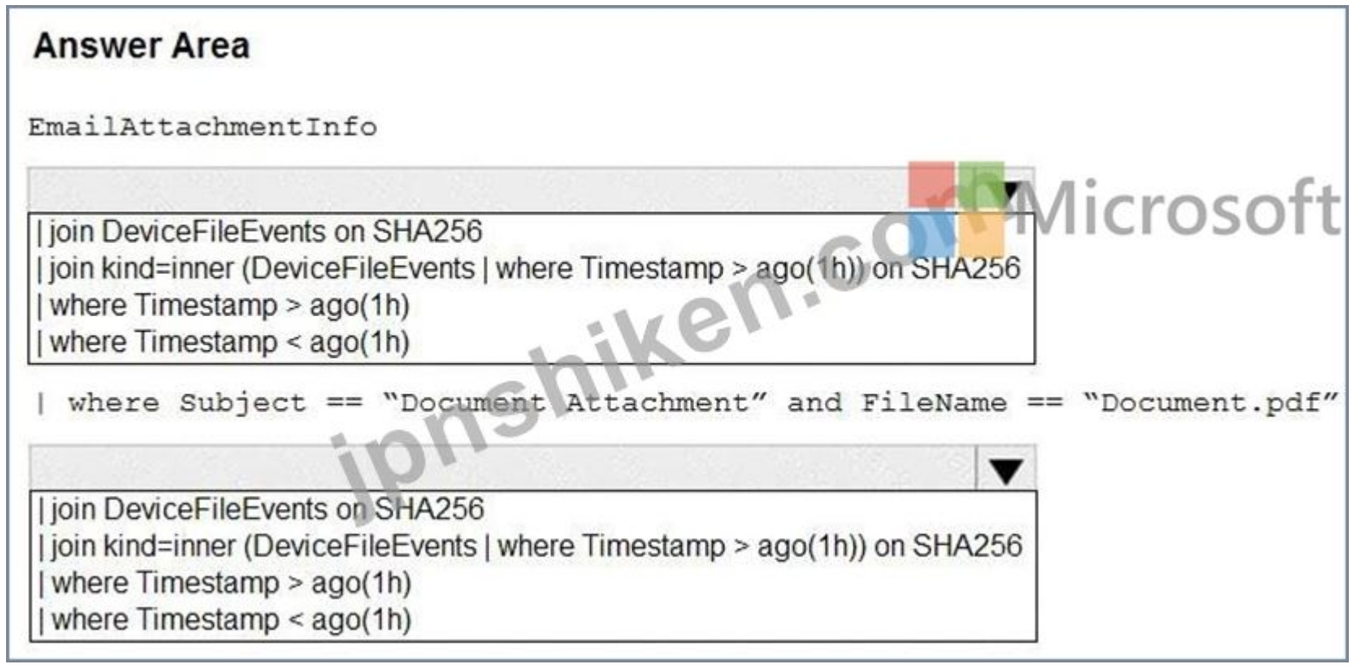


正解:

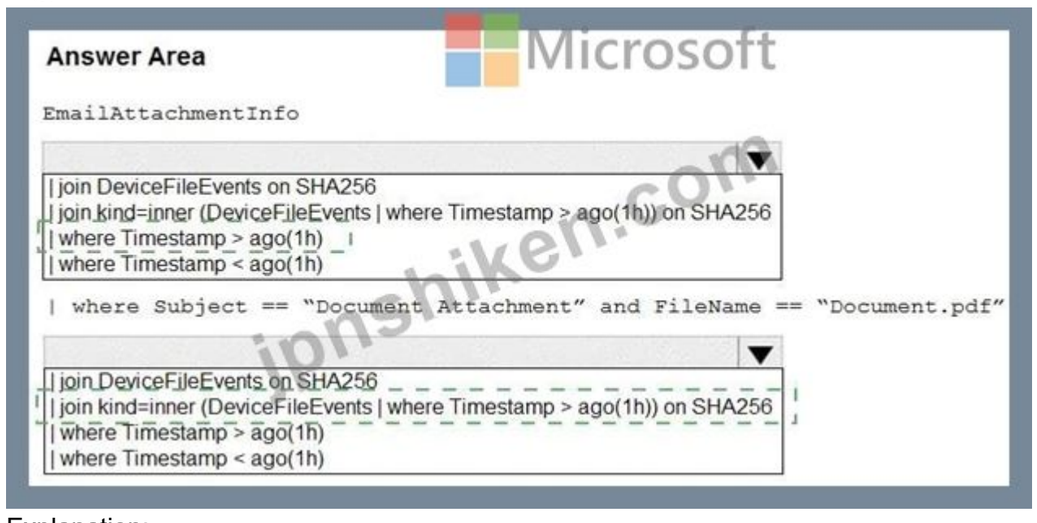


Explanation:
参照：
https://learn.microsoft.com/en-us/defender-endpoint/live-response

質問: **5**
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
「Document」という名前の添付ファイルを含むすべてのメールを返す検索クエリを作成する必要があります。
PDFファイル。クエリは以下の要件を満たす必要があります。
* 過去1時間以内に送信されたメールのみを表示します。
* クエリのパフォーマンスを最適化します。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。注：
正解ごとに1ポイント獲得できます。



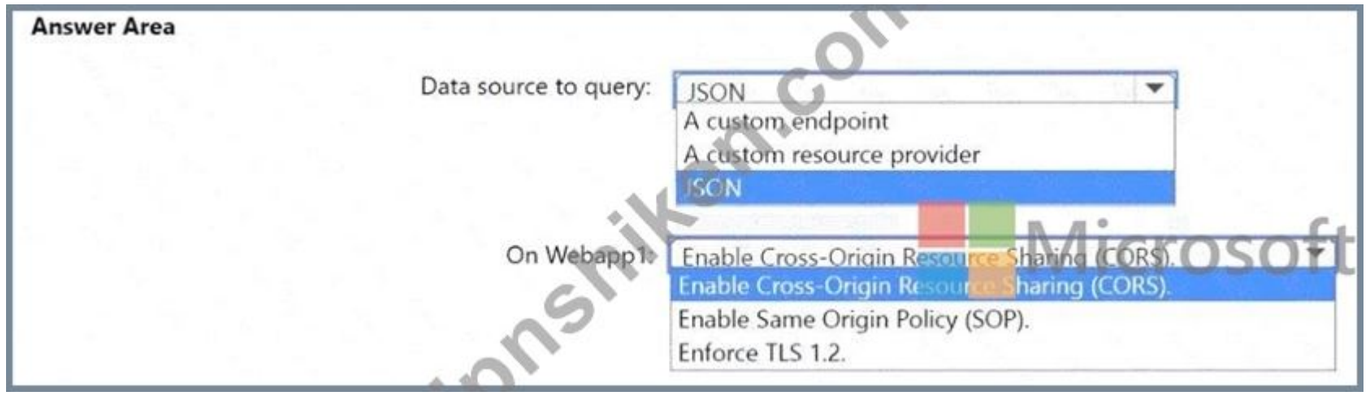
正解:



Explanation:

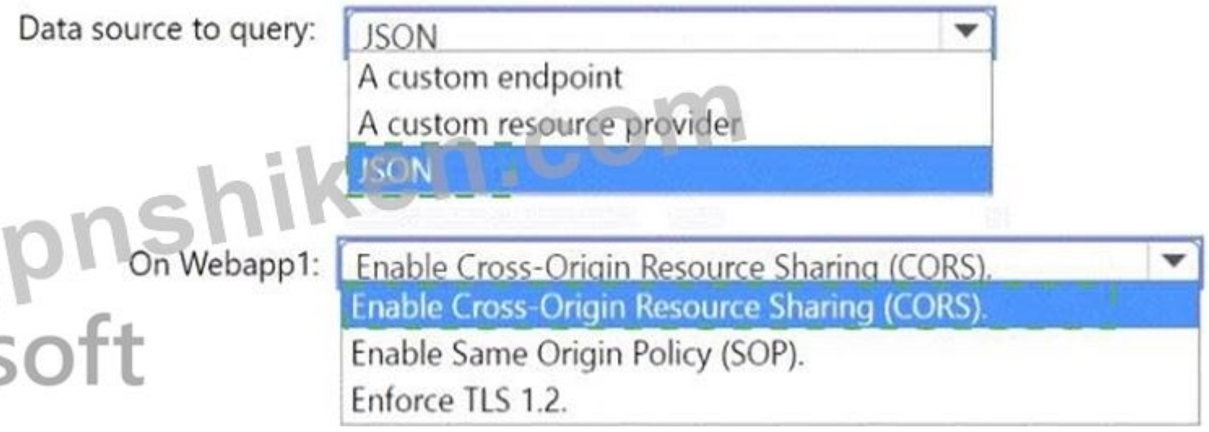
質問: 6

Workbook1とWebapp1のクエリを実装する必要があります。ソリューションはMicrosoft Sentinelの要件を満たす必要があります。クエリはどのように構成すればよいですか？回答するには、回答領域で適切なオプションを選択してください。注：正解ごとに1ポイントが加算されます。



正解:

Answer Area



Explanation:

Microsoft Sentinel ワークブックで外部 Web サービスからライブ データを取得するには、ワークブックに組み込まれている JSON データ ソースを使用します。ワークブックは、JSON を返す REST エンドポイントにクエリを実行し、結果をビジュアルに動的にレンダリングできます。ワークブックが実行される Azure ポータルは、オンプレミス/パブリック Web app1 とは異なるオリジンであるため、エンドポイントが明示的に許可しない限り、ブラウザーはこれらのクロス オリジン リクエストをブロックします。したがって、外部サービスでは CORS を有効にして、ポータルのオリジンが JSON を取得できるようにする必要があります。これは、ワークブックが HTTP/HTTPS JSON エンドポイントにクエリを実行できること、および外部エンドポイントが Azure ポータルからのクライアント側呼び出しに対してクロス オリジン リクエストを許可する必要があるという Microsoft のガイダンスと一致しています。Webapp1 で CORS を強制することで、セキュリティ モデルを満たしつつ、ワークブックがビュー時にデータを取得できるようになり、「Webapp1 からデータを動的に取得する」という要件を満たします。ここでは「カスタムエンドポイント」や「カスタムリソースプロバイダー」といったオプションは不要であり、SOPを有効にしたりTLS 1.2のみを強制したりしても、ブラウザのクロスオリジンポリシーによる呼び出しのブロックには対処できません。

質問: **7**
お客様は、Microsoft Defender for Endpointを使用するMicrosoft 365サブスクリプションをご利用で、以下の表に示すデバイスが含まれています。

Name	Operating system
Device1	Windows
Device2	Windows
Device3	Linux
Device4	macOS

各デバイス上でライブレスポンスセッションを開始します。
各デバイスからDefender for Endpointの調査パッケージを収集する必要があります。
コマンドラインインターフェース（CLI）から高度なライブレスポンスコマンドを実行することで、どのデバイスでパッケージを収集できますか？
A. デバイス1とデバイス2のみ
B. デバイス1、デバイス2、およびデバイス3のみ
C. デバイス3とデバイス4のみ
D. デバイス1、デバイス2、デバイス3、およびデバイス4
正解: **(**正解を表示します**)**
Microsoft Defender for Endpoint (MDE) では、ライブレスポンスセッションにより、セキュリティアナリストがオンボーディング済みのデバイスにリモート接続し、調査コマンドを実行できます。利用可能な主要コマンドの 1 つは、イベントログ、レジストリハイブ、実行中のプロセス、ネットワーク接続などのフォレンジックアーティファクトを含む調査パッケージを収集する機能です。
Microsoftの公式Defender for Endpointドキュメントによると、次のとおりです。
「スクリプトの実行や調査パッケージの収集など、高度なライブレスポンス機能は、WindowsおよびLinuxデバイスでサポートされています。macOSデバイスは、基本的なライブレスポンスコマンドのみをサポートしています。」これは、Windows（Device1およびDevice2）とLinux（Device3）デバイスは高度なライブレスポンス機能（collect investigation_packageを含む）を完全にサポートしているのに対し、macOS（Device4）デバイスは現在、基本的なファイルおよびディレクトリ操作といった限られたコマンドのみをサポートしており、調査パッケージを収集する機能は備えていないことを意味します。
したがって：
* デバイス1 (Windows) # サポート対象
* デバイス2 (Windows) # サポート対象
* デバイス3 (Linux) # サポート対象
* Device4 (macOS) # サポートされていません
# 最終回答: B. デバイス1、デバイス2、およびデバイス3のみ

質問: **8**
以下のSQLクエリがあります。

```
let IPList = _GetWatchlist('Bad_IPs');
Event
   | where Source == "Microsoft-Windows-Sysmon"
   | where EventID == 3
   | extend EvData = parse_xml(EventData)
   | extend EventDetail = EvData.DataItem.EventData.Data
   | extend SourceIP = EventDetail.[9].["#text"], DestinationIP = EventDetail.[14].["#text"]
   | where SourceIP in (IPList) or DestinationIP in (IPList)
   | extend IPMatch = case( SourceIP in (IPList), "SourceIP", DestinationIP in (IPList), "DestinationIP", "None")
   | extend timestamp = TimeGenerated, AccountCustomEntity = UserName, HostCustomEntity = Computer, '
```

Answer Area

Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

正解:

Answer Area

Statements	Yes	No
The UserName field is set as the account entity.	○	○
The watchlist cannot be updated after it is created.	○	○
The IPList variable is set as the IP address entity.	○	○

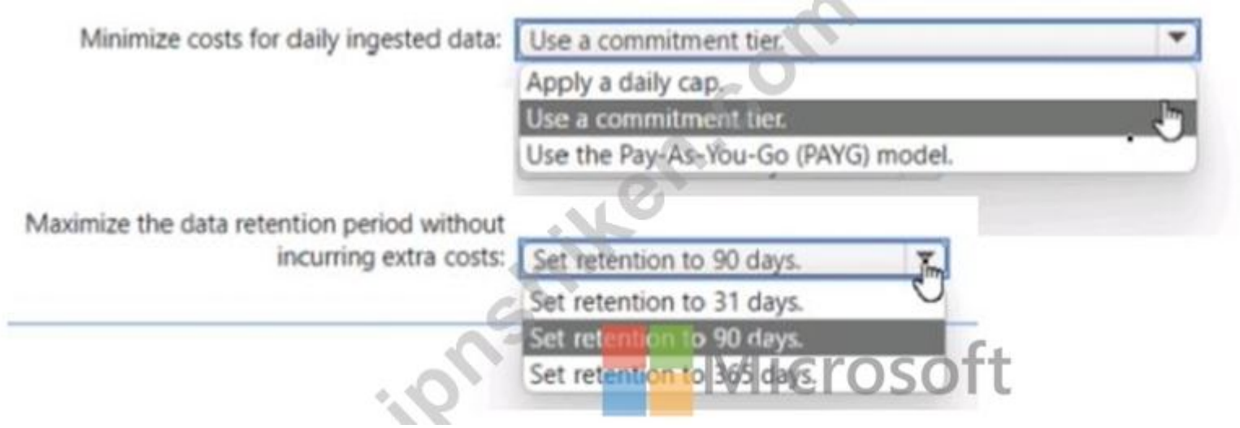
Explanation:

Answer Area

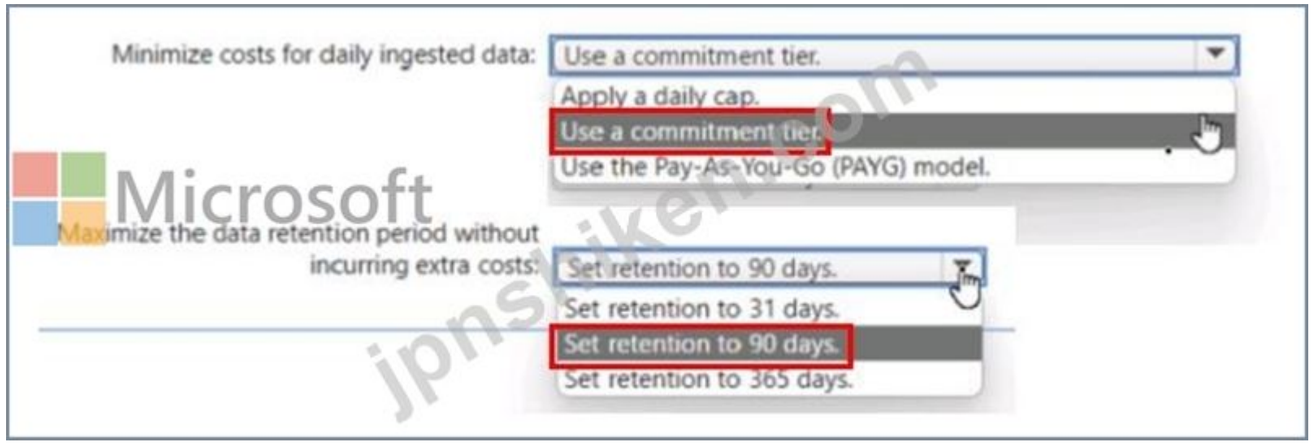
Statements	Yes	No
The UserName field is set as the account entity.	○	●
The watchlist cannot be updated after it is created.	○	●
The IPList variable is set as the IP address entity.	○	●

質問: **9**
お客様は、Microsoft Defender for Endpointを使用するAzureサブスクリプションをお持ちです。
ユーザーが指定したIPアドレスとURLの範囲を許可またはブロックできることを確認する必要があります。
Microsoft 365 Defender ポータルのエンドポイント設定にある高度な機能で、最初に有効にすべき機能は何ですか？
A. ウェブコンテンツフィルタリング
B. ブロックモードのエンドポイント検出および応答（EDR）
C. サーバーへのリアルタイム応答
D. カスタムネットワークインジケーター
正解: **(**正解を表示します**)**

質問: **10**
あなたはAzureサブスクリプションをお持ちです。
Microsoft Sentinelワークスペースを導入する予定です。1日あたり20GBのセキュリティログデータを取り込むことを想定しています。
ワークスペースのストレージを設定する必要があります。ソリューションは以下の要件を満たす必要があります。
* 日々取り込むデータにかかるコストを最小限に抑える。
追加費用をかけずにデータ保持期間を最大限に延ばす。
各要件に対して何をすべきですか? 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: 正解ごとに 1 ポイントが加算されます。



正解:



質問: **11**

あなたはMicrosoft 365 Defenderを使用してインシデントを調査しています。

CFOLaptop、CEOLaptop、COOLaptopという名前の3つのデバイスで、サインイン認証の失敗を検出するために、高度なハンティングクエリを作成する必要があります。

質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

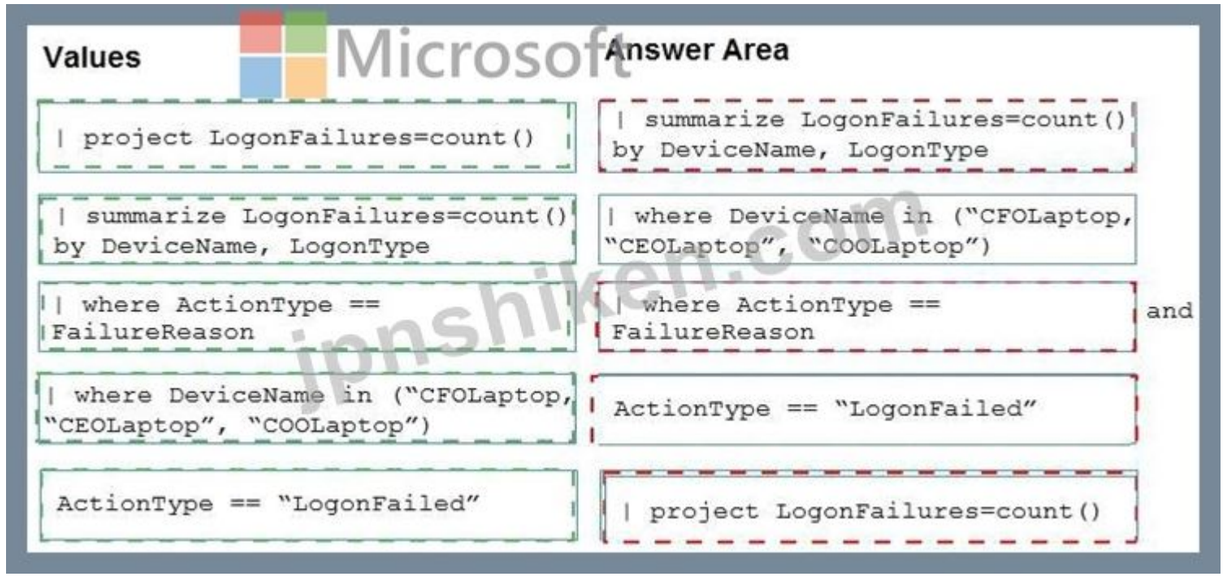
Values

```
| project LogonFailures=count()
| summarize LogonFailures=count()
by DeviceName, LogonType
| where ActionType ==
FailureReason
| where DeviceName in ("CFOLaptop,
"CEOLaptop", "COOLaptop")
ActionType == "LogonFailed"
```

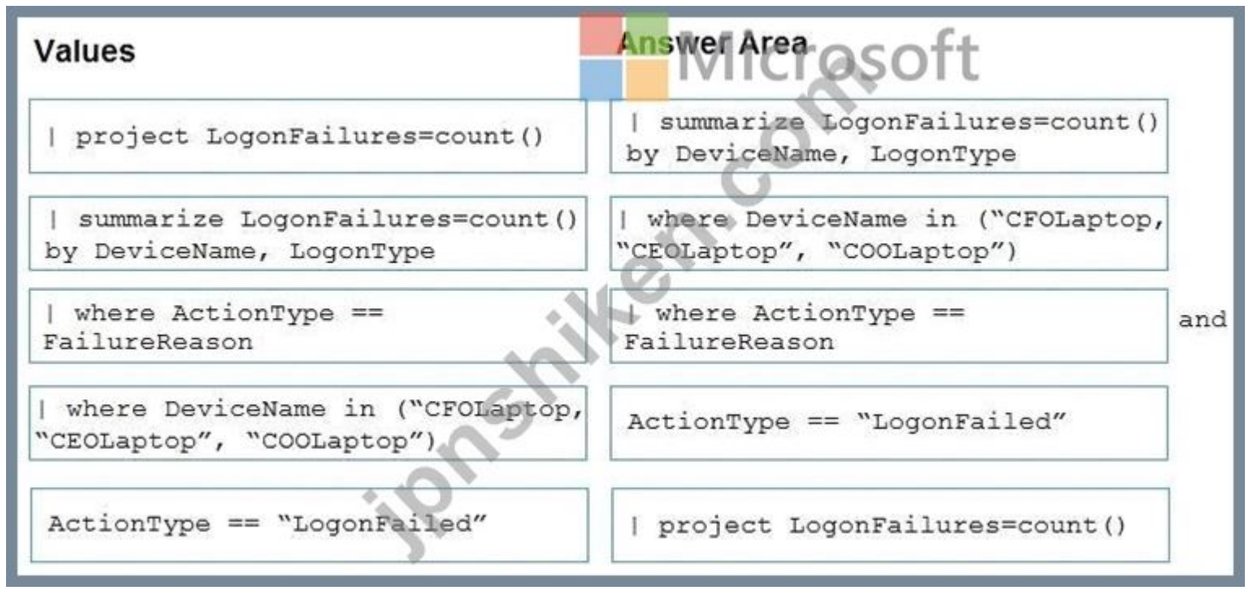
Answer Area

anc

正解:



説明



質問: **12**

Microsoft Defender for Cloud の要件を満たすには、Account! にネイティブ クラウド コネクタをデプロイする必要があります。Account! で最初に行うべきことは何ですか？

A. Defender for Cloud 用の AWS ユーザーを作成します。

B. Defender for Cloud 用のアクセス制御 (1AM) ロールを作成します。

C. AWS Security Hubを設定します。

D. AWS Systems Manager (SSM) エージェントをデプロイする

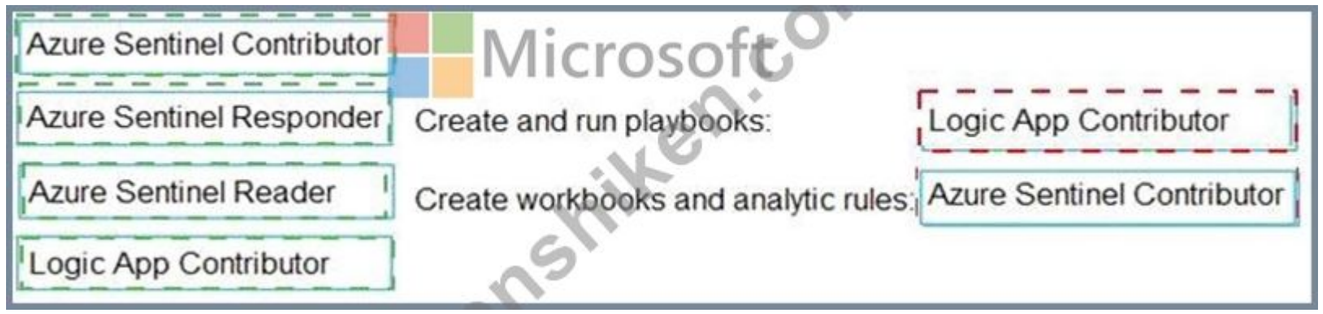
正解: **(**正解を表示します**)**

質問: **13**

Microsoft Sentinelワークスペースをお持ちです。
監査ログとサインインログを使用して、ユーザーおよびエンティティの動作分析 (UFBA) を有効にします。Azure AD テナントでは、次のエンティティが検出されます。
* アプリ名: App1
* IPアドレス: 192.168.1.2
* コンピュータ名: Device1
* 使用したクライアントアプリ: Microsoft Edge
* メールアドレス :user1@company.com
* サインインURL: https://www.company.com
UEBAを使用して調査できるエンティティは何ですか？
A. アプリ名、コンピューター名、IPアドレス、メールアドレス、および使用クライアントアプリのみ
B. IPアドレスとメールアドレスのみ
C. 使用クライアントアプリとアプリ名のみ
D. IPアドレスのみ
正解: **B** (コメントを発表する)
Microsoft Sentinel UEBA (ユーザーおよびエンティティ行動分析)は、ユーザーとホスト (デバイス)に焦点を当て、コンテキスト情報でデータを強化します。
UEBAを監査ログとサインインログで有効にした場合、調査対象としてサポートされるエンティティは以下のとおりです。
* ユーザーアカウント (メールアドレス)
* ホストまたはデバイス (IPアドレスを含む)
アプリ名、使用クライアントアプリ、サインインURLなどのその他の値は、ログデータの属性ではありますが、UEBA調査で追跡されるエンティティではありません。

質問: **14**
貴社はAzure Sentinelを導入します。
Azure Sentinelの管理を複数のグループに委任する予定です。
以下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。
解決策は、最小権限の原則に基づかなければならない。
各タスクにはどの役割を割り当てるべきでしょうか？回答するには、適切な役割を正しいタスクにドラッグしてください。各役割は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の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：正解ごとに1ポイントが加算されます。

正解:



Explanation:

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

質問: 15
Microsoft Defender for Endpointを使用することで、どのチームの問題を解決できますか？
A. エグゼクティブ
B. 売上
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、コントソ社
事例研究
これはケーススタディです。ケーススタディには個別の時間制限はありません。各ケースを完了するために、試験時間を自由に使うことができます。ただし、この試験には追加のケーススタディやセクションが含まれる場合があります。与えられた時間内に試験に含まれるすべての問題を完了できるよう、時間配分をしっかり行う必要があります。
ケーススタディに含まれる質問に答えるには、ケーススタディに記載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図表やその他の資料が含まれている場合があります。各質問は、このケーススタディ内の他の質問とは独立しています。
このケーススタディの最後に、確認画面が表示されます。この画面では、解答を確認し、次のセクションに進む前に修正することができます。新しいセクションを開始すると、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てください。質問に答える前に、左側のペインにあるボタンを使ってケーススタディの内容を確認してください。これらのボタンをクリックすると、ビジネス要件、既存環境、問題記述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、そこに表示される情報は以降のタブに表示される情報と同一です。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ってください。
概要
Contoso Ltd.という会社は、本社と北米各地に5つの支店を構えている。
本社はシアトルにあります。支店はトロント、マイアミ、ヒューストン、ロサンゼルス、バンクーバーにあります。
コントソ社は、ニューヨークとサンフランシスコにオフィスを構えるファブリカム社という子会社を所有している。
既存の環境

エンドユーザー環境
Contosoの全ユーザーはWindows 10デバイスを使用しています。各ユーザーはMicrosoft 365のライセンスを取得しています。さらに、Contosoの営業チームのメンバーにはiOSデバイスが配布されています。
クラウドおよびハイブリッドインフラストラクチャ
Contosoのすべてのアプリケーションは Azureにデプロイされています。
Microsoft Cloud App Securityを有効にします。
ContosoとFabrikamは、それぞれ異なるAzure Active Directory (Azure AD) テナントを使用しています。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Azure Defenderを有効にしました。
現在の問題点
Contosoのセキュリティチームは、大量のサイバーセキュリティ警告を受け取っています。セキュリティチームは、どの警告が正当な脅威で、どれがそうでないかを判断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製ツールを使用して顧客とファイルをやり取りしています。過去には、営業チームのデバイスがさまざまな攻撃を受けたことがあります。
Contoso社のマーケティングチームは、外部ベンダーとの連携のために複数のMicrosoft SharePoint Onlineサイトを運用しています。しかし、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態が何度か発生しています。
Contosoの経営陣は、セキュリティ侵害が発生した疑いがあると見ています。経営陣は、Microsoft Cloud App Securityで保護されているアプリケーションにおいて、過去48時間以内にデータアクセス、ダウンロード、削除などの操作が5回以上行われたファイルを特定していただくようお願いしています。
要件
計画されている変更
Contosoは、両社のセキュリティ業務を統合し、すべてのセキュリティ業務を一元的に管理する計画だ。
技術要件
Contoso社は、以下の技術要件を特定しました。
* 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 を使用すると、環境に対するアクティブな攻撃を迅速に修復することで、組織のリスクを軽減できます。
* ContosoとFabrikamのAzure ADテナント間でデータを関連付けるAzure Sentinelクエリを実装する。
* 外部からの攻撃や、Fabrikam自身のAzure ADアプリケーションが侵害される可能性が発生した場合に、Azure Defender for Key VaultのアラートをFabrikam向けに修復するための手順を開発する。
* 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。下級セキュリティ管理者が、以下の不完全なクエリを提供します。
行動分析
| ActivityType == "FailedLogOn"
| ただし、_____ == True

質問: **16**
あなたは、新たなランサムウェアの亜種を仕掛ける可能性のある攻撃を調査しています。
あなたは、機密情報を含む非常に価値の高い機器群に対して、自動化された操作を実行する計画を立てています。
カスタムデバイスグループが3つあります。
デバイスに対して操作を実行するには、マシンを一時的にグループ化する必要があります。実行すべき操作を3つ挙げてください。正解はそれぞれ、解決策の一部を示しています。注：正解ごとに1ポイントが加算されます。
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. 機械にタグを追加します。
D. ランク1の新しいデバイスグループを作成します。
E. 新しい管理者ロールを作成します。
F. ランク4の新しいデバイスグループを作成します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

質問: **17**
お客様は、Microsoft Purview を使用する Microsoft 365 サブスクリプションを所有しており、その中に Site1 という名前の Microsoft SharePoint Online サイトが含まれています。Site1 には、次の表に示すファイルが含まれています。

Name	Author
File1.docx	User1
File2.docx	User2
File3.xlsx	User3

Microsoft Purview から、次の表に示すコンテンツ検索クエリを作成します。

Name	Query
Search1	Author:"User1" FileExtension:xlsx
Search2	Author:"User*" and FileExtension:*
Search3	Author:("User1..3")

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
Search1 will return File3.	○	○
Search2 will return File1.	○	○
Search3 will return File2.	○	○

正解:

Explanation:

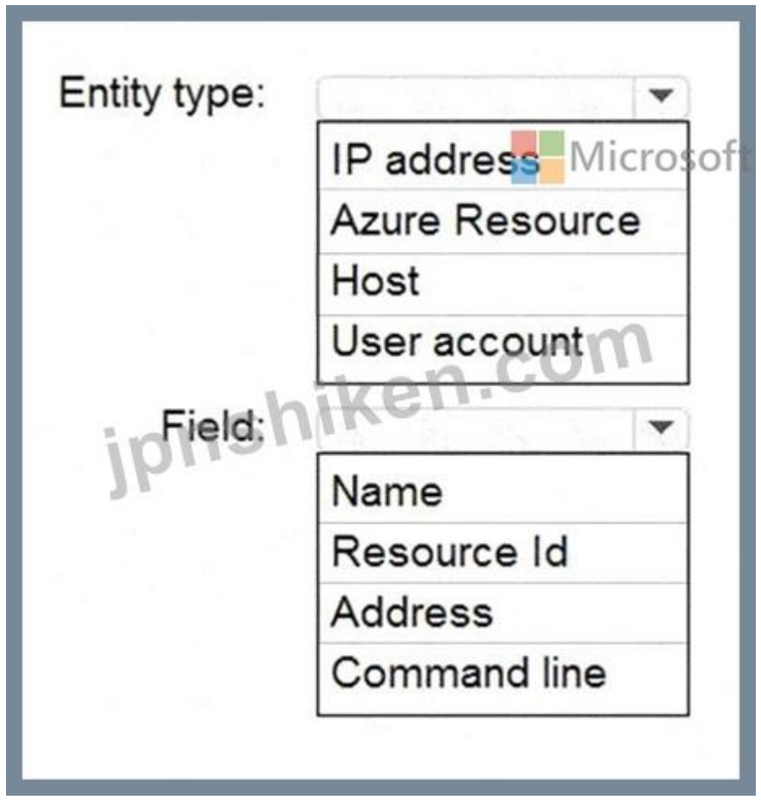
質問: 18

アプリケーション開発中に複数のAzure Functionsアプリからアクセスされるストレージアカウントをお持ちです。

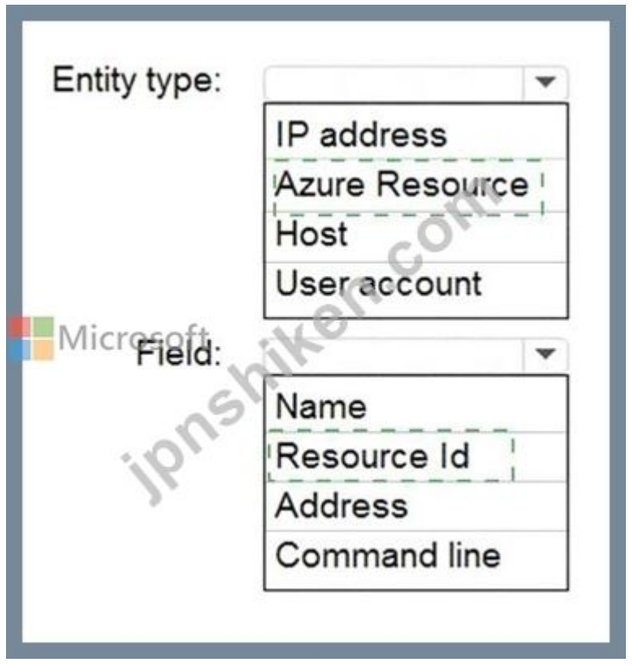
ストレージアカウントに関するAzure Defenderのアラートを非表示にする必要があります。

抑制ルールでは、どのエンティティタイプとフィールドを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。

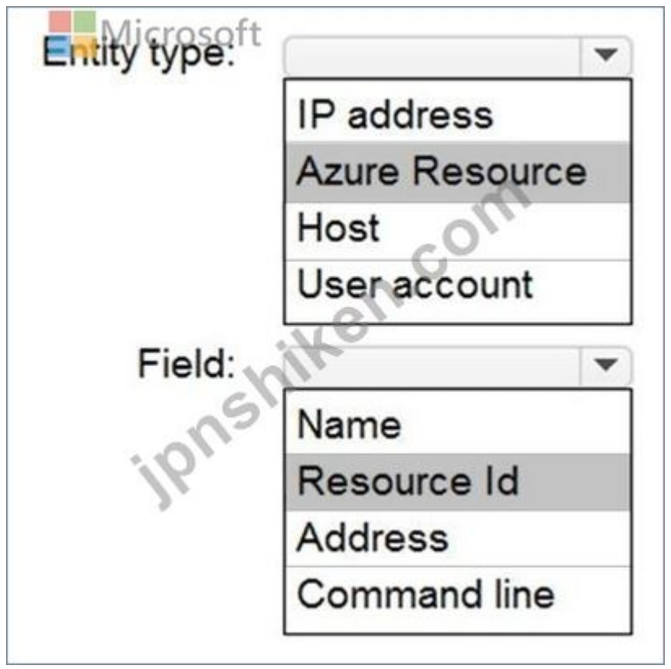
注：正解ごとに1ポイントが加算されます。



正解:



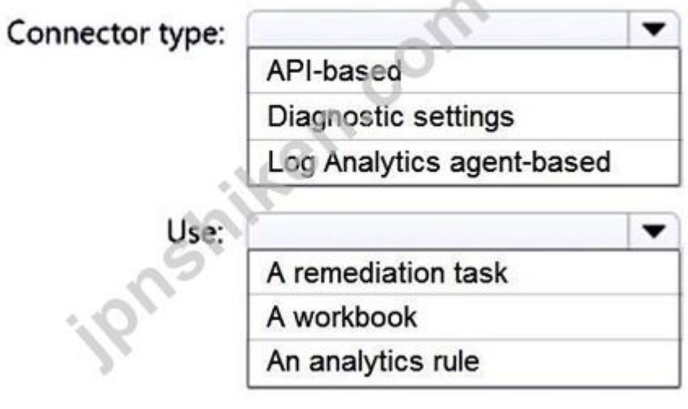
Explanation:



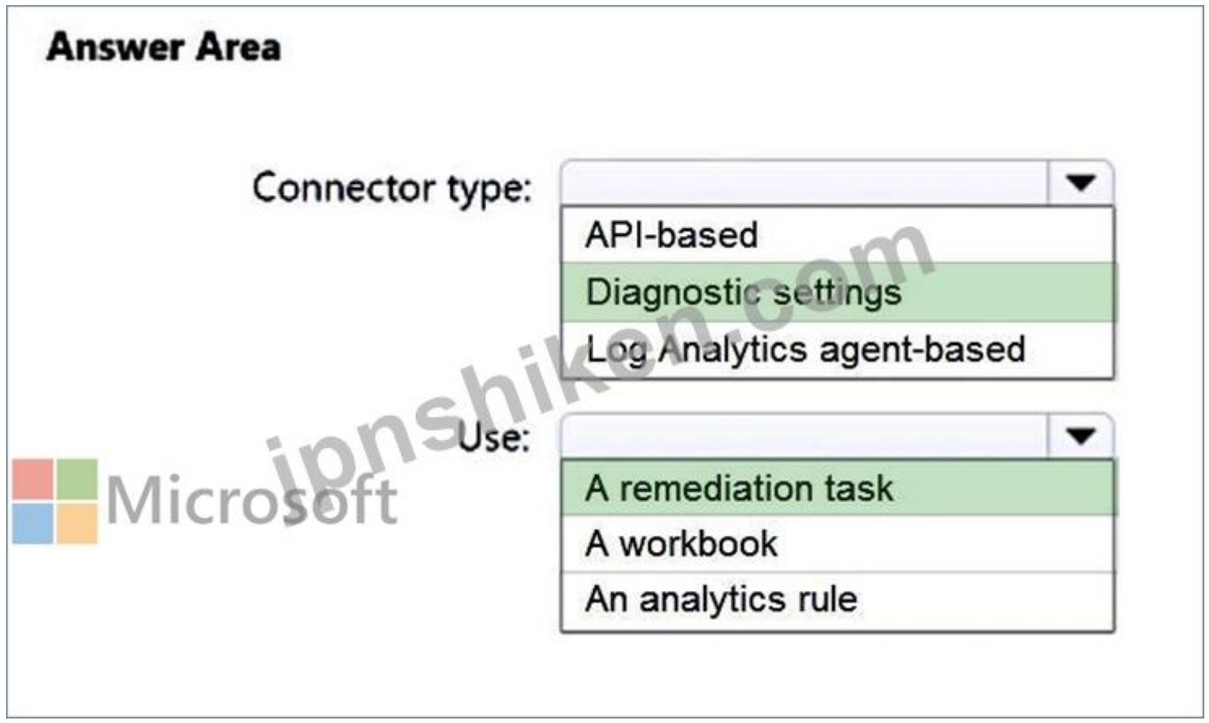
参照：
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

質問: **19**
ホットスポットに関する質問
お客様は4つのAzureサブスクリプションをお持ちです。そのうちの1つのサブスクリプションには、Microsoft Sentinelワークスペースが含まれています。
Azure Policy を使用してサブスクリプションからデータを収集するには、Microsoft Sentinel データコネクタをデプロイする必要があります。このソリューションでは、ポリシーがサブスクリプション内の新規リソースと既存リソースの両方に適用されることを保証する必要があります。
どのタイプのコネクタをプロビジョニングすべきか、また、すべてのリソースが監視されるようにするには何を使用すべきか。回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:



質問: 20

Microsoft Defender for Endpointの要件を満たすには、CLIENT1上で実行されるクラウドアプリを制限する必要があります。

どの2つの設定を変更すべきでしょうか？それぞれの正解は、解決策の一部を示しています。

注：正解ごとに1ポイントが加算されます。

A. Microsoft Defender Security Center のデバイス管理にあるオンボーディング設定

B. クラウドアプリセキュリティ異常検知ポリシー

C. Microsoft Defender セキュリティ センターの 「設定」にある高度な機能

D. クラウドアプリセキュリティのクラウド検出設定

正解: **(**正解を表示します**)**

Windows 10 コンピューターでは、Microsoft Defender for Endpoint を使用して、Cloud App Security によって承認されていないすべてのアプリをブロックする必要があります。

参照：

https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

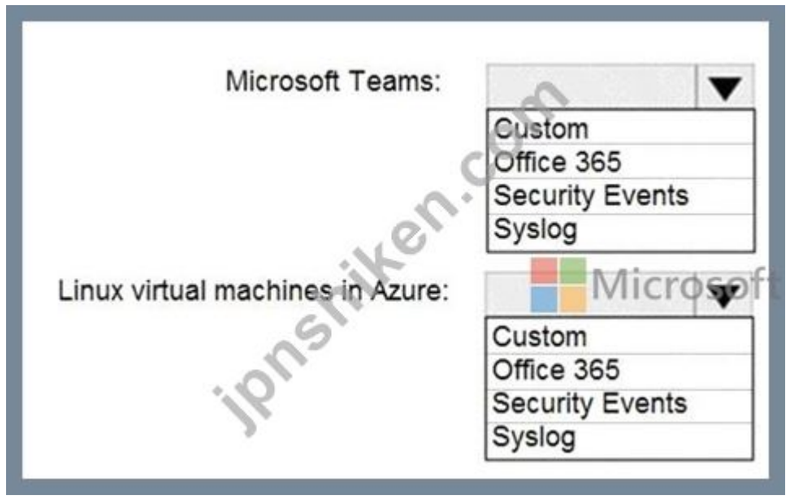
質問: 21

Azure Sentinelをデプロイします。

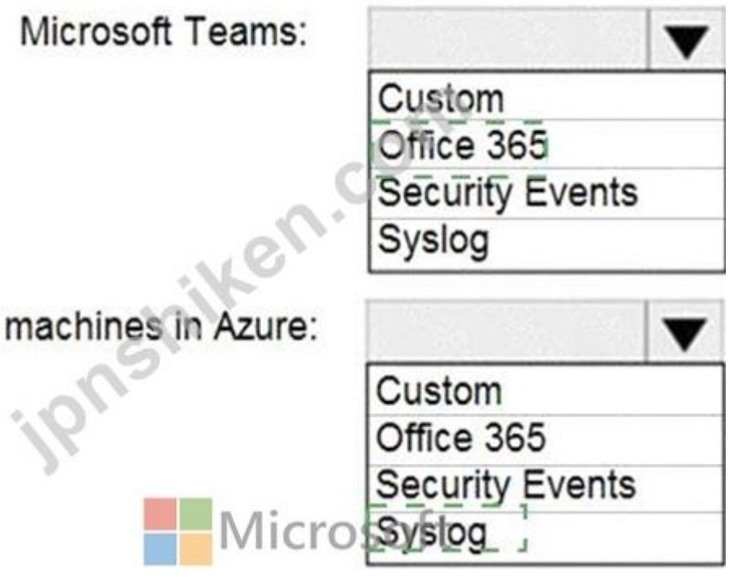
Azure Sentinelにコネクタを実装して、Azure上のMicrosoft TeamsとLinux仮想マシンを監視する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。

各ワークロードには、どのデータコネクタタイプを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。

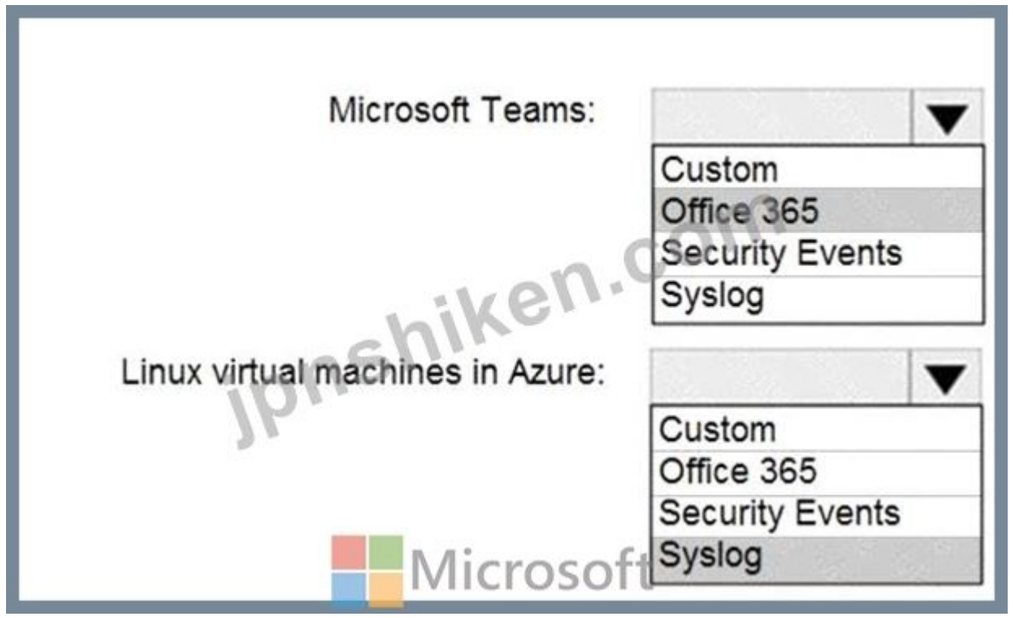
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



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: 22

Azure Sentinel を使用すると、Azure の異常なアクティビティを監視できます。
次の図に示すように、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

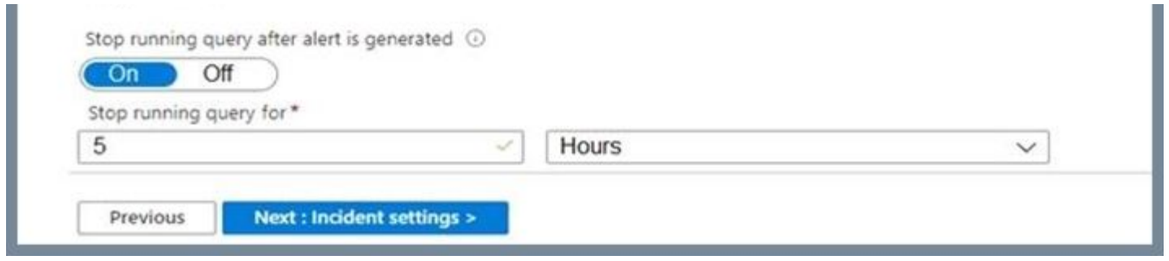
Generate alert when number of query results *: Is greater than 2

Event grouping

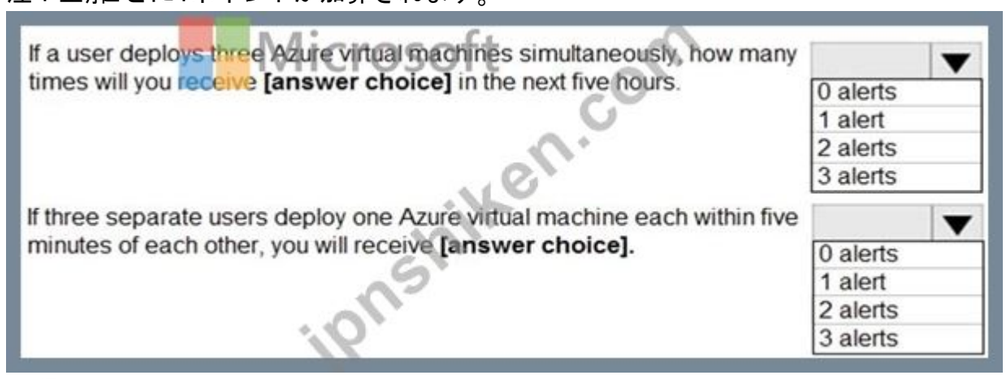
Configure how rule query results are grouped into alerts

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

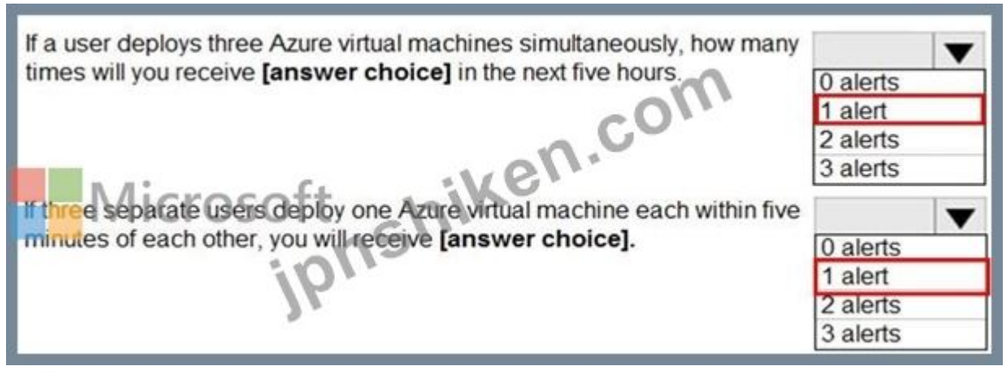
Suppression



ルール定義の一部として、インシデント設定を定義する必要はありません。
図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。

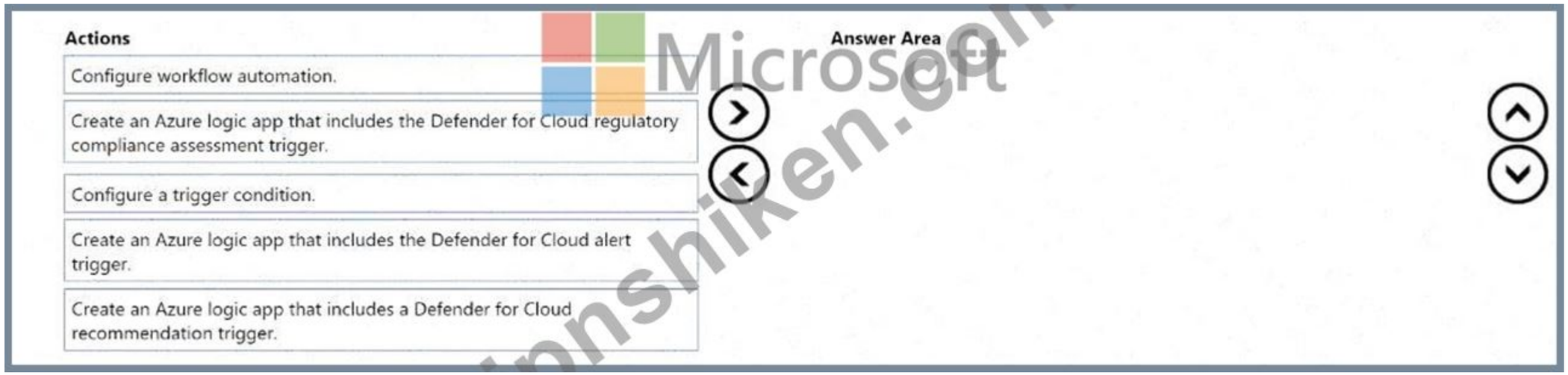


正解:

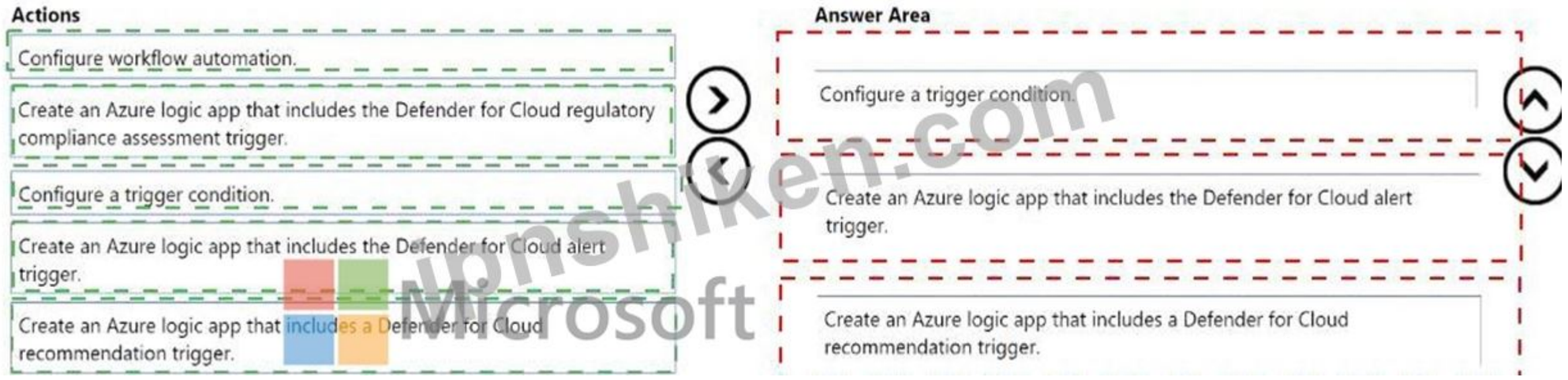


参照：
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

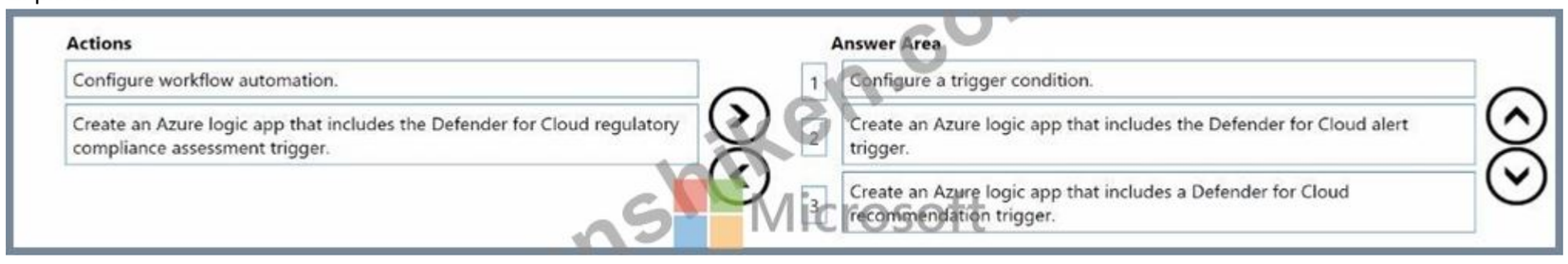
質問: **23**
お客様は、Microsoft Defender for Cloudを使用するAzureサブスクリプションをお持ちです。
新しいMicrosoft Secure Scoreアクションが生成された際に、会社のIT部門にMicrosoft Teamsメッセージを送信するワークフローを作成する必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:



質問: **24**

Server1 のイベント監視を設定する必要があります。ソリューションは Microsoft Sentinel の要件を満たす必要があります。最初に何を作成すればよいでしょうか？

A. Azure Event Grid トピック

B. Microsoft Sentinel スケジュール済みクエリ ルール

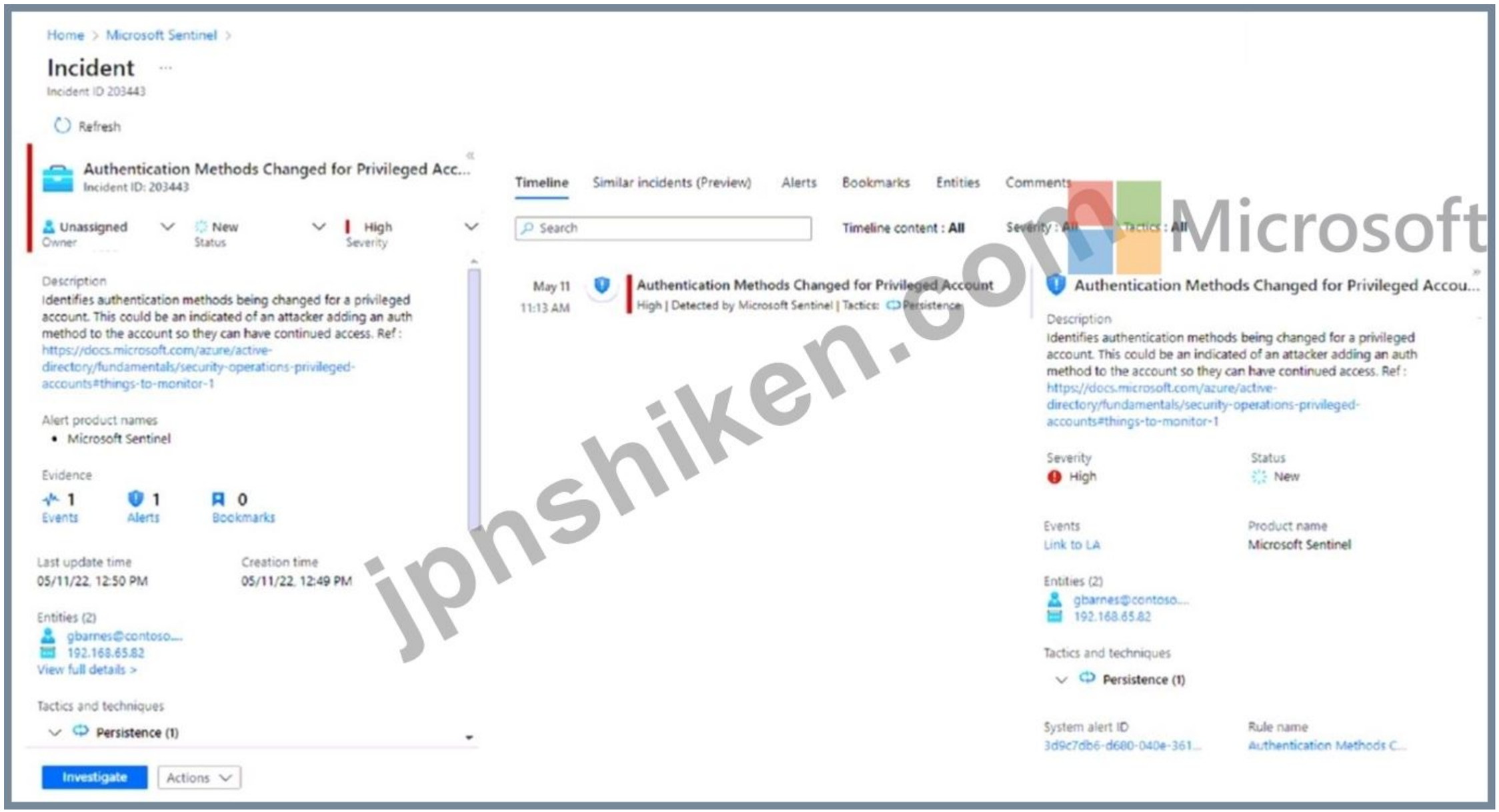
C. データ収集ルール（DCR）

D. Microsoft Sentinelの自動化ルール

正解: **C** (コメントを発表する)

質問: **25**
Microsoft Defender for Endpoint を使用する Microsoft 365 E5 サブスクリプションをご利用の場合、マルウェア警告をトリガーしたデバイスを特定し、警告に関連する証拠を収集する必要があります。このソリューションは、収集した結果を使用して、影響を受けたデバイスの隔離を開始できることを保証する必要があります。
Microsoft 365 Defender ポータルでは何を使用すべきですか？
A. 事件
B. 調査
C. 高度な狩猟
D. 修復
正解: **(**正解を表示します**)**
Microsoft Defender for Endpoint では、調査 (自動調査および対応 (AIR) とも呼ばれます) がアラートに関連する証拠を収集し、デバイスの動作を分析し、デバイスの隔離、ファイルの隔離、修復などの対応アクションを有効にします。
インシデントは単一の攻撃チェーンに対する複数のアラートを集約する機能であり、高度なハンティングはカスタムKQLクエリに使用されますが、調査はトリガーされたマルウェアアラートに対する証拠収集と分析を自動化するために特別に設計されています。
調査結果に基づき、アナリストはポータル上で影響を受けるエンドポイントの隔離を直接開始することができます。
回答: B. 調査

質問: **26**
ホットスポットに関する質問
Microsoft Sentinelワークスペースをお持ちです。
Microsoft Sentinelインシデントは、以下の図に示すように生成されます。



図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

Explanation:
https://learn.microsoft.com/en-us/azure/sentinel/investigate-cases

質問: **27**
ユーザー User1 という名前のユーザーを含む Microsoft 365 B5 サブスクリプションをお持ちです。このサブスクリプションは Microsoft を使用しています。
365 Copilot for Security。Copilot for SecurityはSentinelプラグインを使用します。User1にはCopilot Contributorロールが割り当てられています。
調査中に、ユーザー1がプロンプトを送信すると、セキュリティコンピューティングユニット $CU）の使用量がプロビジョニングされた容量制限に近づいているため、Copilot for Securityが要求に応答できないという通知を受け取ります。
User1がCopilot for Securityを使用して正常な応答を生成できることを確認する必要があります。
ユーザー1は何をすべきでしょうか？
A. プロビジョニングされたSCUを更新します。
B. 2つ目の Copilot for Security セッションを開き、プロンプトを送信します。
C. Microsoft Sentinel 最適化ワークブックを実行します。
D. 1時間待ってからプロンプトを再送信してください。
正解: **A (**コメントを発表する**)**

質問: **28**

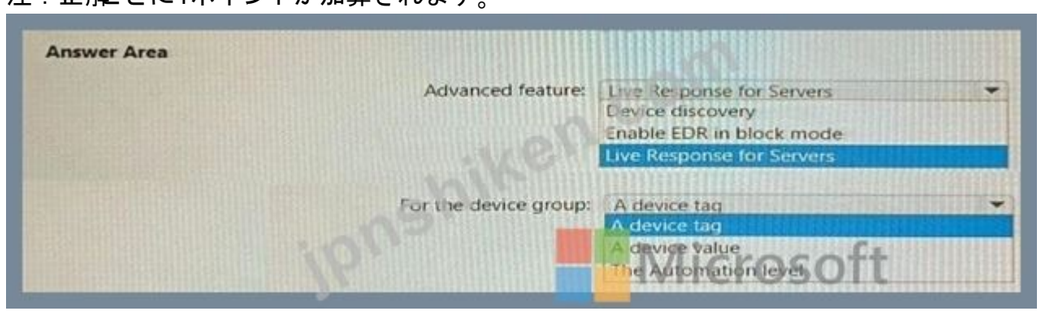
お客様は、Microsoft 365 Defender for Endpointを使用するMicrosoft 365 E5サブスクリプションをご利用中です。

Microsoft を使用して Windows サーバーへのリモート シェル接続を開始できることを確認する必要があります

365 Defenderポータル。

何を設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。



正解:

Explanation:

Microsoft Defender for Endpoint の Live Response 機能を使用すると、セキュリティアナリストは Microsoft 365 Defender ポータルから直接、セキュア シェル セッションを介してデバイス (サーバーを含む) にリモート接続できます。この機能により、デバイスへの直接的なネットワークアクセスを必要とせずに、リアルタイムでの調査、証拠収集、および修復コマンドを実行できます。

Windowsサーバーでこの機能を有効にするには、まずDefender for Endpointの設定で 『サーバーのライブレスポンス」という高度な機能を有効にする必要があります。Microsoftのドキュメントには、この設定により、オンボードされたWindows Serverデバイスへのリモートシェルアクセスが可能になると明記されています。この機能は、セキュリティ上の理由からデフォルトでは無効になっています。

高度なd機能が有効になると、Live Responseのアクセス許可と機能はデバイスグループレベルで管理されます。Defender for Endpointのデバイスグループは通常、エンドポイントを分類および整理するデバイスタグを使用して構成されます（部門OSの種類、役割など）。タグベースのグループ化により、管理者はポリシーや機能（Live Responseなど）を、本番サーバーのみなど、特定のデバイスセットに効率的に適用できます。

『自動化レベル」や 『デバイス値」といった代替オプションは無関係です。自動化レベルは自動修復を制御し、デバイス値はアラートの優先順位付けにおける重要度を割り当てます。

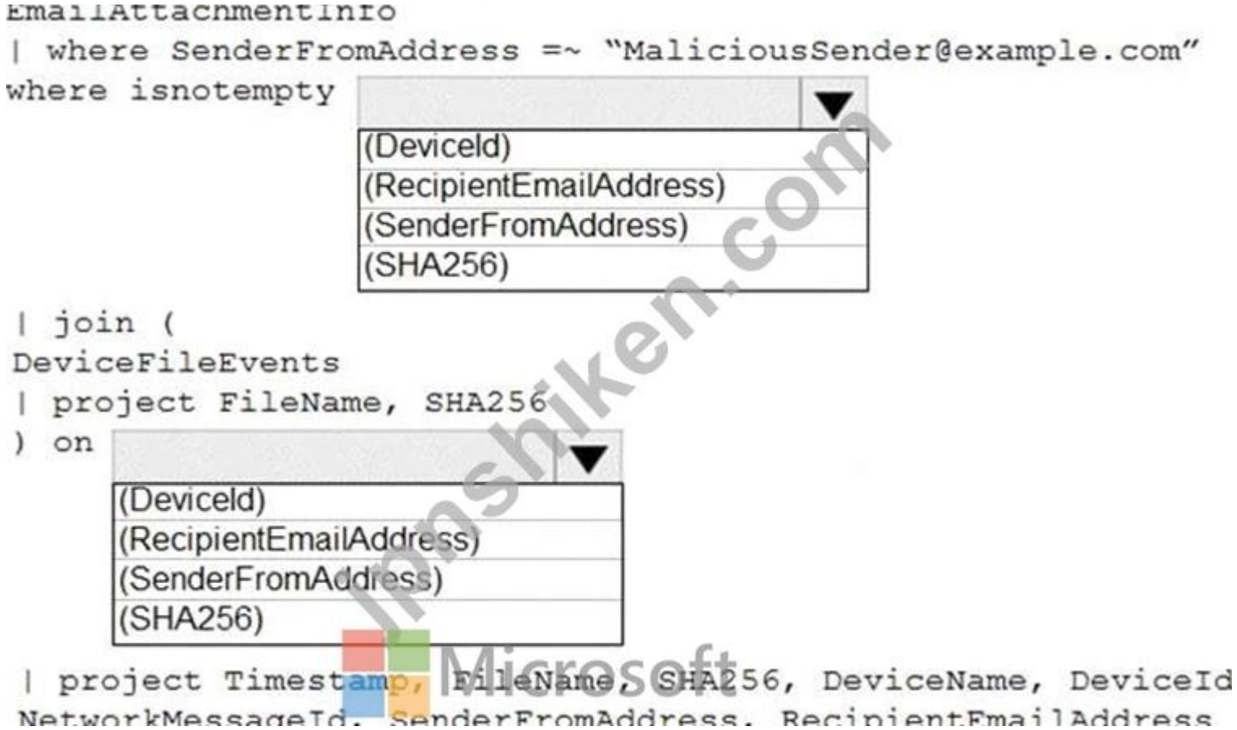
したがって、正しい設定手順は次のとおりです。

* 高度な機能でライブレスポンスを有効にします。

* デバイスタグで識別されるターゲットデバイスグループに構成を適用します。

最終回答:
* 高度な機能 :サーバーのリアルタイム応答
* デバイスグループの場合 :デバイスタグ

質問: **29**
お客様は、Microsoft Defenderを使用するMicrosoft 365 E5サブスクリプションと、Azure Sentinelを使用するAzureサブスクリプションをお持ちです。
既知の悪意のあるメール送信者から送信されたメールに含まれるファイルを持つすべてのデバイスを特定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実行されます。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



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
```

Explanation:

```
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：

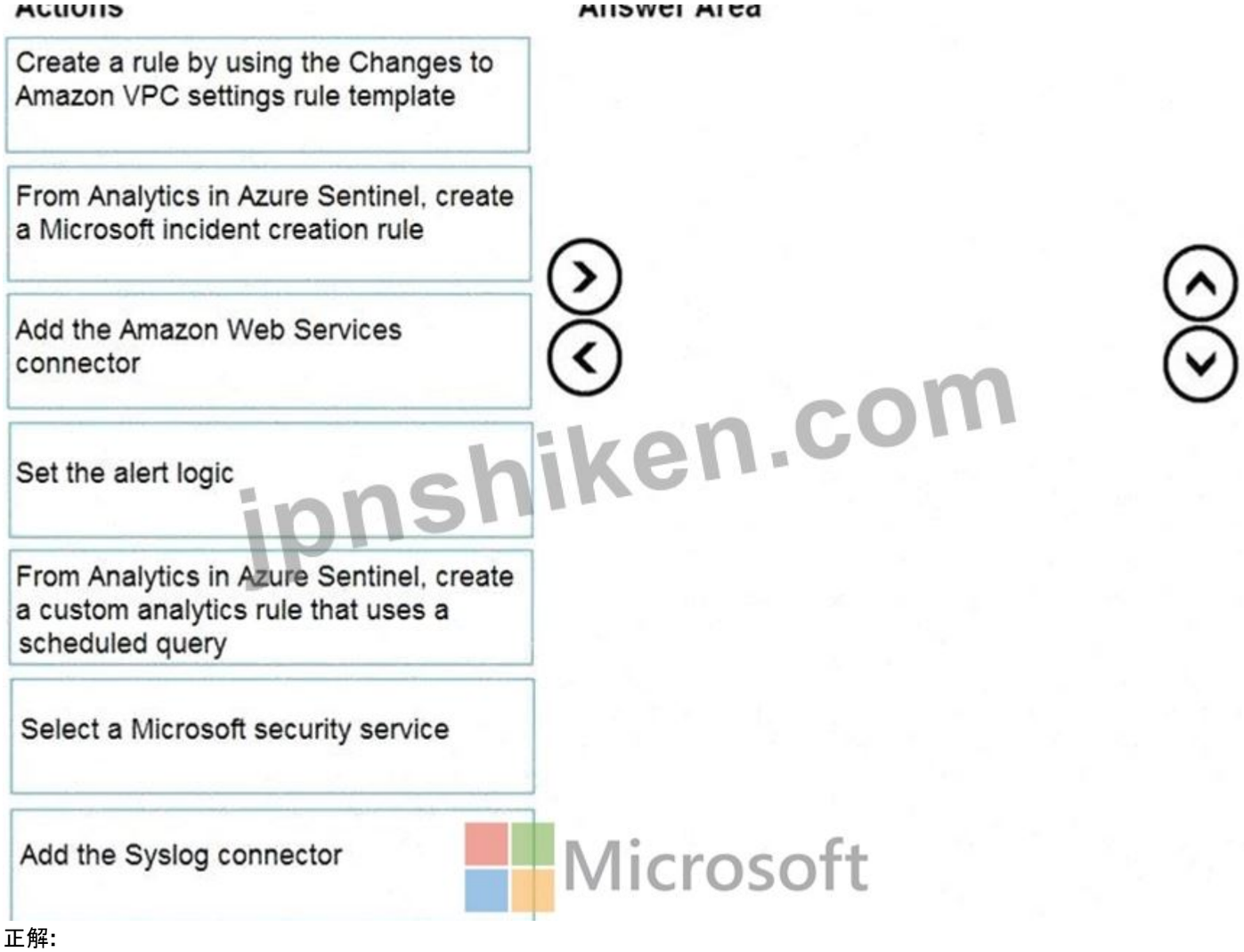
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: 30

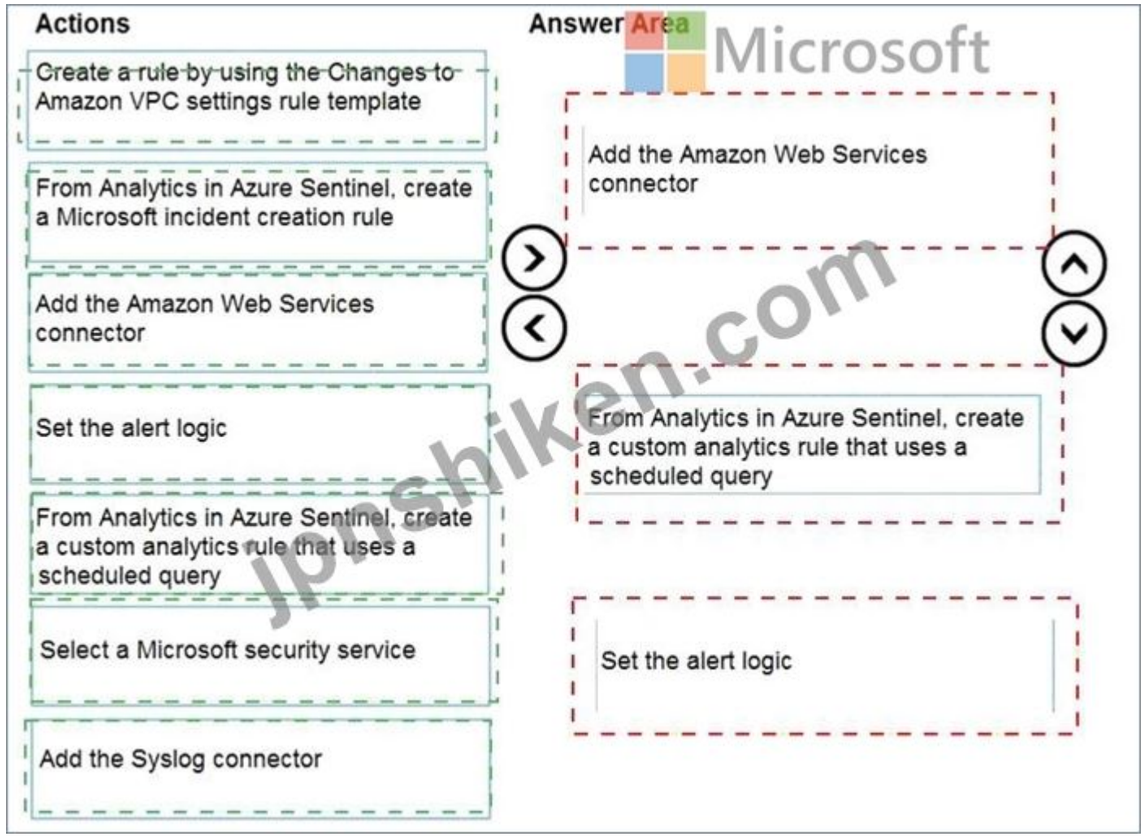
Defender for Cloudの要件を満たす必要があります。
Server2にはどのような設定が必要ですか？

A. Azureリソースロック
B. Windows 用 Azure Automanage マシン構成拡張機能
C. Microsoft Antimalware拡張機能
D. Azureリソースタグ
正解: **(**正解を表示します**)**

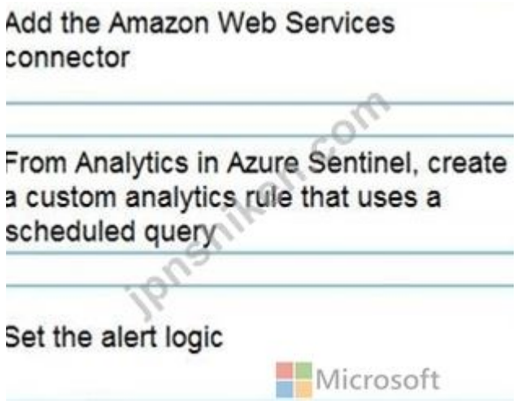
質問: **31**
Amazon Web Services (AWS) のログから特定の条件を検索し、インシデントを生成するには、Azure Sentinel の分析ルールを使用する必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。
Microsoft 365 E5



正解:



Explanation:

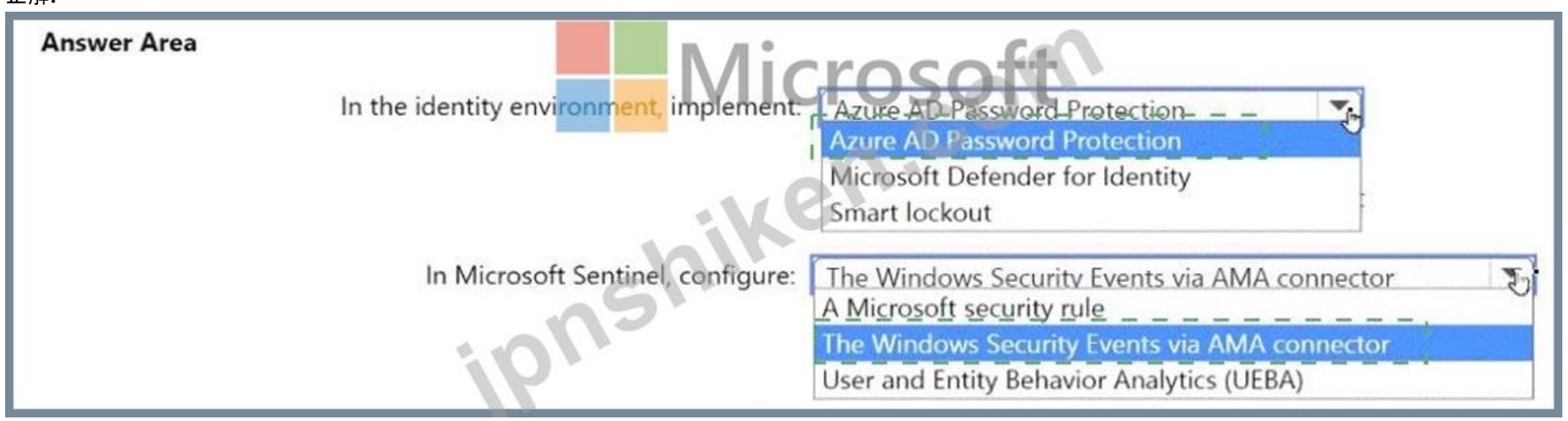


マイクロソフトのセキュリティ運用 $ecOps)に関するすべてのドキュメントを含む、包括的かつ詳細な説明：
Amazon Web Services (AWS) のログから特定の条件を検索し、Microsoft Sentinel を使用してインシデントを生成するには、Microsoft Sentinel のドキュメントと AWS 統合のための Azure Sentinel プレイブックに従って、構造化された手順で構成プロセスを実行します。
* Amazon Web Services (AWS) コネクタを追加する
Sentinel で AWS データを分析するには、まず Amazon Web Services データ コネクタを使用して AWS ログを統合する必要があります。このコネクタは、AWS CloudTrail やその他の AWS ログ データを Sentinel ワークスペースにストリーミングします。Microsoft のドキュメントには、 Amazon Web Services (AWS) コネクタを使用して、CloudTrail イベントとセキュリティ ログを Microsoft Sentinel にストリーミングし、分析とアラートを実行します」と記載されています。
* このコネクタがないと、Sentinel は AWS 固有のアクティビティを照会または検出できません。

* スケジュールされたクエリを使用するカスタム分析ルールを作成する
* データ取り込みが確立されたら、スケジュールされたクエリを使用して、特定の条件（不正アクセス試行、VPC設定の変更など）を継続的に検索する分析ルールをSentinelで作成します。
* マイクロソフトは次のように説明しています。「カスタム分析ルールは、スケジュールに基づいてKQLクエリを実行し、取り込まれたデータソース全体にわたる特定のパターンや異常を検出します。」
アラートロジックを設定する
ルールを定義した後、Sentinelがアラートまたはインシデントをトリガーするタイミングを決定するアラートロジックを設定します。これには、しきい値、イベントの頻度、重大度レベル、およびエンティティマッピングの設定が含まれます。
* Microsoft Sentinel の公式ガイダンスノート：「アラートロジックは、クエリ結果からアラートが生成される条件を定義します。」

質問: **32**
パスワードのリセットを監視する必要があります。ソリューションは、Microsoft Sentinelの要件を満たしている必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

正解:



Explanation:

トピック4、その他の質問
ファブリカム社は金融サービス会社です。
同社はニューヨーク、ロンドン、シンガポールに支社を構えている。Fabrikamには世界中にリモートユーザーがおり、これらのユーザーはVPN接続を介して支社にアクセスすることで、クラウドサービスを含む社内リソースにアクセスする。
このネットワークには、fabrikam.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれており、fabrikam.com という名前の Azure AD テナントと同期しています。フォレストを同期するために、Fabrikam はパススルー認証を有効にし、パスワード ハッシュ同期を無効にした Azure AD Connect を使用しています。
fabrikam.comのフォレストには、Group1とGroup2という2つのグローバルグループが含まれています。
Fabrikamの全ユーザーには、Microsoft 365 E5ライセンスとAzure Active Directory Premium Plan 2ライセンスが割り当てられています。Fabrikamは、Microsoft Defender for IdentityとMicrosoft Defender for Cloud Appsを導入し、ログコレクターを有効にしています。
Fabrikamは、以下の表に示すリソースを含むAzureサブスクリプションを保有しています。

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

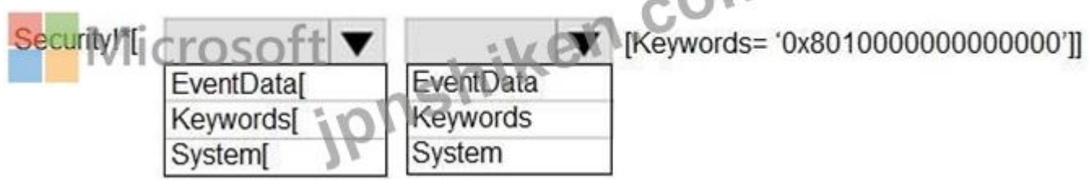
Fabrikamは、Account1という名前のAmazon Web Services（AWS）アカウントを所有しています。Account1には、カスタムWindows Server 2022を実行する100個のAmazon Elastic Compute Cloud（EC2）インスタンスが含まれています。このイメージにはMicrosoft SQL Server 2019が含まれていますが、エージェントはインストールされていません。
ユーザーが VPN 接続を使用すると、Microsoft 365 Defender は、誤検知である「あり得ない旅行」アラートを大量に発生させます。また、Defender for Identity は、誤検知である「疑わしい DCSync 攻撃」アラートを大量に発生させます。
Fabrikamは以下のサービスを導入する予定です。
* Microsoft Defender for Cloud
* マイクロソフトセンチネル
Fabrikamは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則を適用する。
管理業務の手間を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloud Appsの要件として以下の点を挙げています。
* 渡航不可能な場合の警告ポリシーは、各ユーザーの過去の活動に基づいていることを確認してください。
* 誤検知による、あり得ない旅行に関する警告の数を減らす。
誤検知アラートの調査に必要な管理上の労力を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloudに関して以下の要件を特定しました。

* グループ2のメンバーがセキュリティポリシーを変更できることを確認してください。
* Group1のメンバーがAzureサブスクリプションレベルで規制遵守ポリシーのイニシアチブを割り当てられるようにします。
* Azure Arc対応サーバー向けAzure Connected Machineエージェントのデプロイを、Account1の既存および将来のリソースに自動化します。
誤検知アラートの調査に必要な管理作業を最小限に抑える。
Fabrikamは、Microsoft Sentinelに関する以下の要件を特定しました。
* 組み込みの高度セキュリティ情報モデル（ASIM）統合パーサーを使用して、過去7日間のNXDOMAIN DNSリクエストを照会します。
* AWS EC2インスタンスから、ローカルグループメンバーシップの変更を含むWindowsセキュリティイベントログエントリを収集します。
* ユーザーおよびエンティティ行動分析（UEBA）を使用して、Azure ADユーザーの異常なアクティビティを特定します。
* UEBAを使用して、侵害されたAzure ADユーザー認証情報の潜在的な影響を評価します。
* App1がMicrosoft Sentinelの自動化ルールで使用できることを確認してください。
* 過去30日間に発生したインシデントについて、トリアージにかかる平均時間を特定する。
* 過去30日間に発生したインシデントをクローズするまでの平均時間を特定します。
* グループ1のメンバーがプレイブックを作成および実行できることを確認する。
* グループ1のメンバーが分析ルールを管理できることを確認してください。
* Jupyterノートブックを使用して、Pool! でハンティングクエリを実行します。
* グループ2のメンバーがインシデントを管理できることを確認する。
* データクエリのパフォーマンスを最大化する。
収集するデータ量を最小限に抑える。

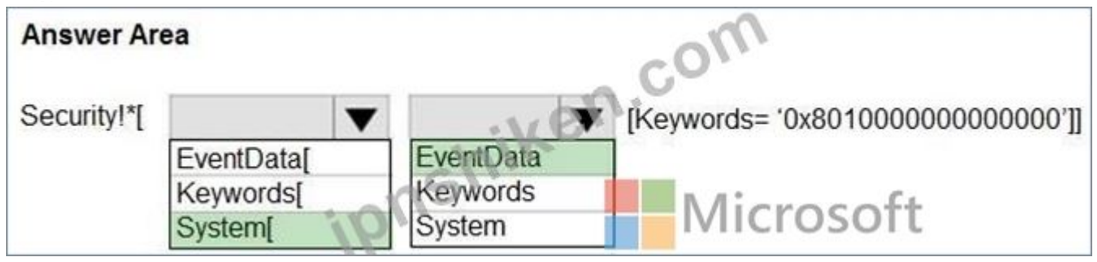
質問: **33**
Microsoft Defender for Office 365で、安全な添付ファイルポリシーを実装します。
ユーザーからは、添付ファイル付きのメールの受信に予想以上に時間がかかるとの報告が寄せられている。
セキュリティを損なうことなく、添付ファイル付きメッセージの配信時間を短縮する必要があります。添付ファイルはマルウェアスキャンを行い、マルウェアを含むメッセージはすべてブロックする必要があります。
安全な添付ファイルに関するポリシーでは、どのような設定を行うべきですか？
A. ダイナミックデリバリー
B. 交換
C. リダイレクトをブロックおよび有効化
D. 監視とリダイレクトの有効化
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-world

質問: **34**
ホットスポットに関する質問
Sub1 という名前の Azure サブスクリプションがあります。Sub1 には、SW1 という名前の Microsoft Sentinel ワークスペースと、Windows Server を実行する VM1 という名前の仮想マシンが含まれています。SW1 は、AMA コネクタを介して Windows セキュリティ イベントを使用して、VM1 からセキュリティ ログを収集します。
VM1から収集するイベントの範囲を制限する必要があります。ソリューションは、監査失敗イベントのみが収集されるようにする必要があります。
コネクタのフィルタ式はどのように完成させるべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:



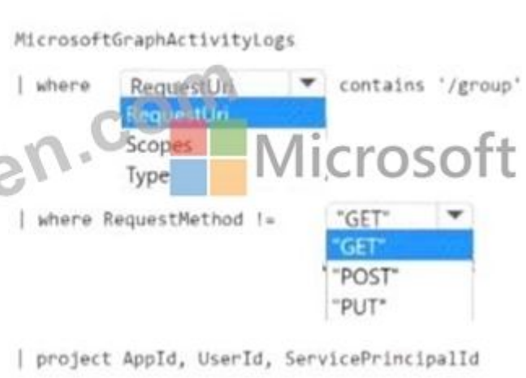
質問: **35**

あなたはMicrosoft 365のサブスクリプションをお持ちです。

グループの変更または削除を要求したすべてのセキュリティプリンシパルを特定する必要があります。KQLクエリはどのように作成すればよいでしょうか？回答するには、回答領域で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area



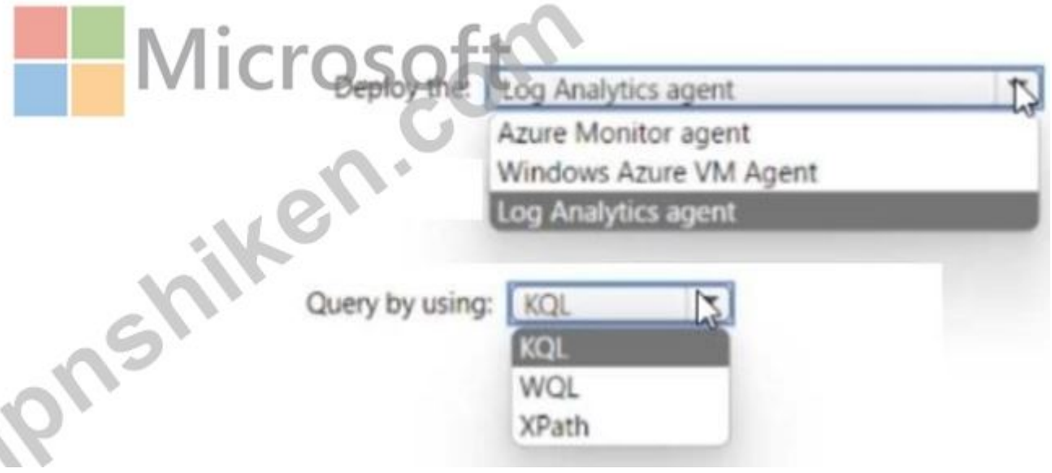
正解:

Explanation:

質問: 36

Windows セキュリティ イベント ログを収集するには、Microsoft Sentinel の要件を満たす必要があります。どうすればよいですか? 回答するには、回答エリア a から適切なオプションを選択してください。注: 正解ごとに 1 ポイントが加算されます。

Answer Area

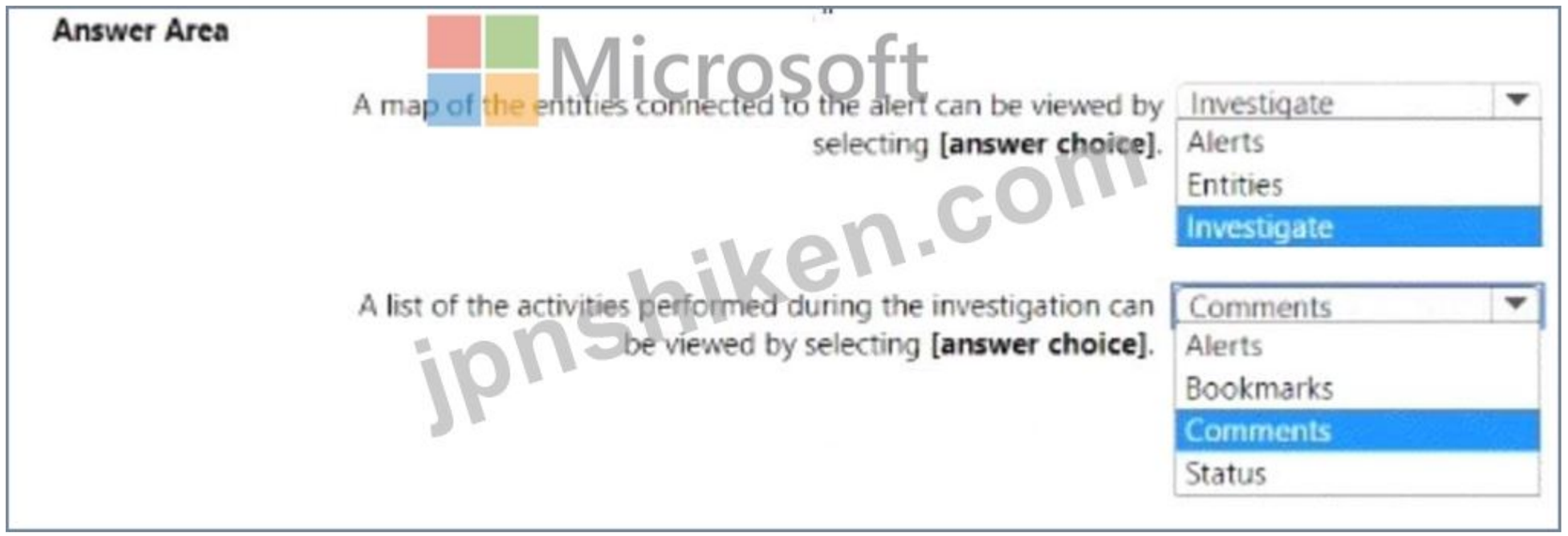


正解:

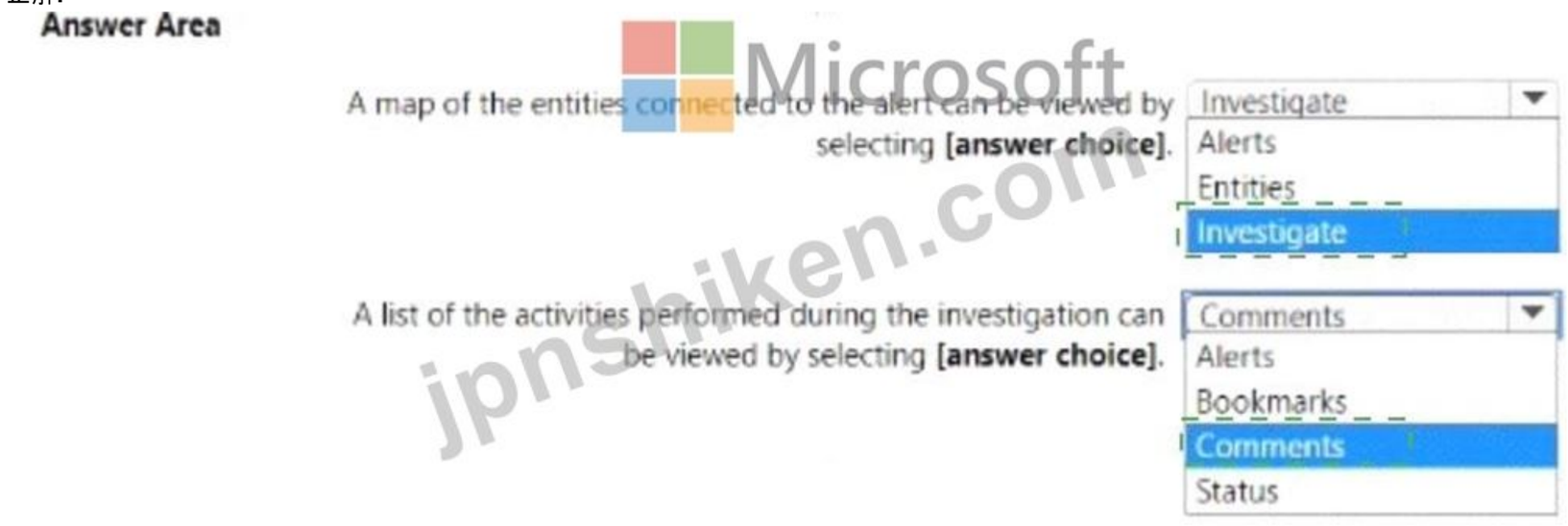
Answer Area

質問: **37**
Microsoft Sentinelワークスペースをお持ちです。
Microsoft Sentinelインシデントは、以下の図に示すように生成されます。

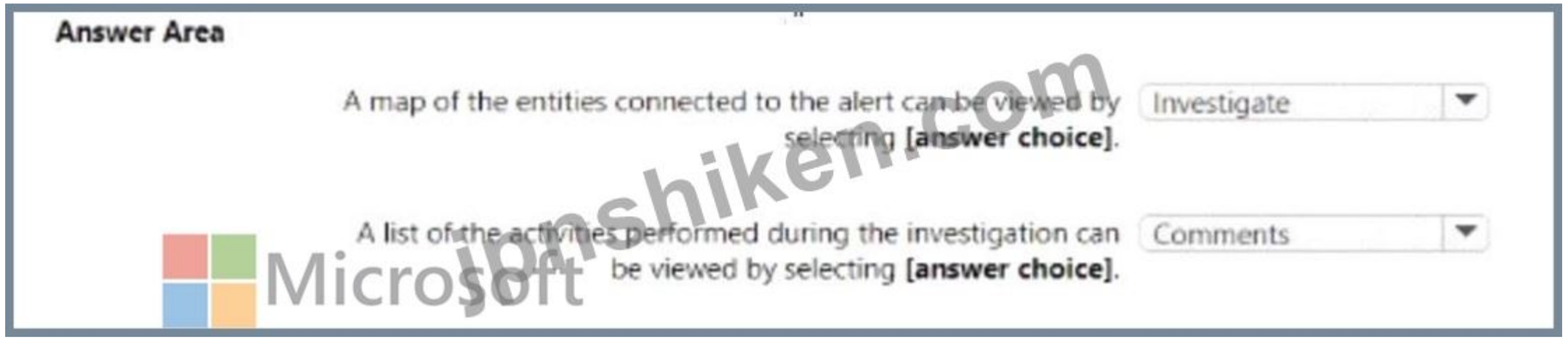
図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



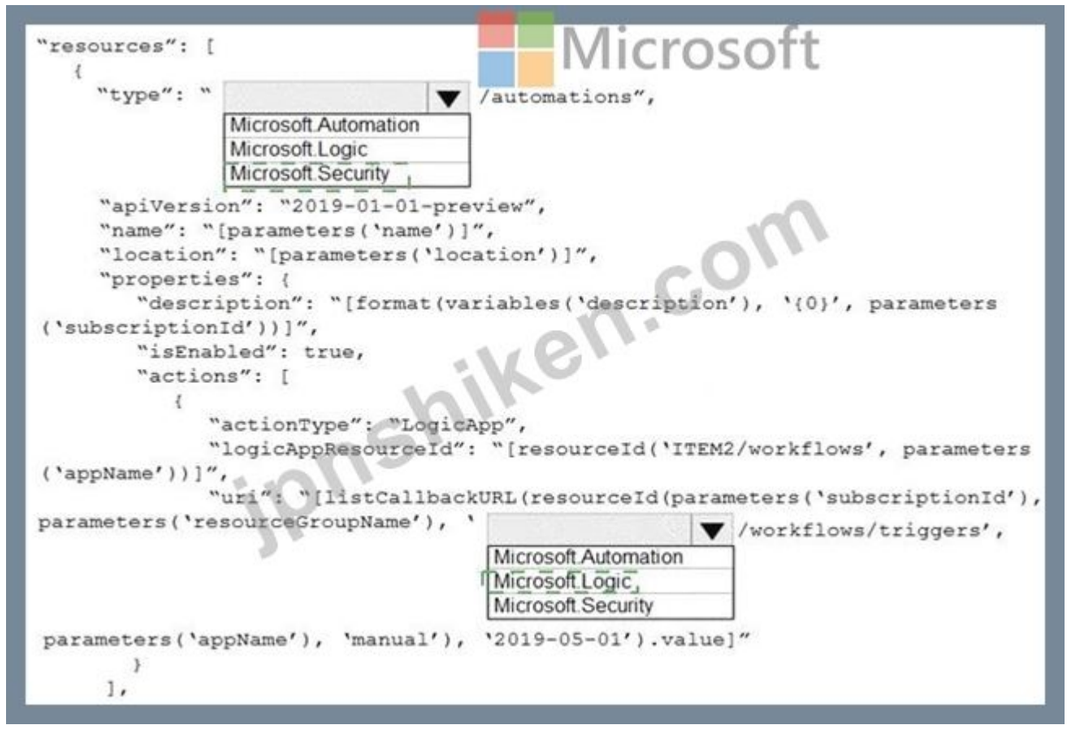
質問: 38

Azure Security Center が特定のセキュリティ警告を受信したときに自動的に修復処理をトリガーするワークフロー自動化を作成するには、Azure Resource Manager テンプレートを使用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はどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

```
"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]"
        }
      ],
```



Explanation:

```
"resources": [
   {
     "type": "                    /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'), '                    /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
         }
       ],
```

- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

- Microsoft.Automation
- Microsoft.Logic
- Microsoft.Security

Azure Security Center (現在は Microsoft Defender for Cloud) では、ワークフロー自動化は Microsoft.Security/automations 型の ARM リソースとしてプロビジョニングされます。自動化リソースは 1 つ以上のアクションを定義し、アクションが Logic App の場合、actionType は LogicApp に設定され、アクションはリソース ID で Logic App を参照する必要があります。ARM では、Logic App の正しいプロバイダー名前空間は Microsoft.Logic であるため、テンプレートでは resourceId(' Microsoft.Logic/workflows ' , < logicAppName >) を使用して logicAppResourceId を設定します。
セキュリティ アラートで Logic App をトリガーできるようにするには、オートメーション アクションに Logic App の手動トリガーへのコールバック URL を含める必要があります。ARM では、これはトリガー リソース ID に対して listCallbackURL() を使用して取得されます。このリソース ID には Microsoft.Logic プロバイダーも使用する必要があります。つまり、resourceId(< subscriptionId > 、< resourceGroupName > 、' Microsoft.Logic/workflows/triggers ' 、< logicAppName > 、' manual ') で、Logic Apps API バージョンは 2019-05-01 などです。これは、Security Center ワークフロー オートメーションのドキュメント化されたパターンです。Microsoft.Security/automations の下にオートメーションを定義し、LogicApp タイプのアクションを指定し、Microsoft.Logic でワークフローを参照し、Microsoft.Logic/workflows/triggers の listCallbackURL を介して手動トリガーのコールバックを取得します。この配線により、指定されたセキュリティ アラートが受信されたときに、オートメーションが Logic App を呼び出して、一致するアラートごとに自動修復が実行されるようになります。

質問: **39**
あなたは、Microsoft 365 Defenderを使用するMicrosoft 365サブスクリプションを所有しており、そのサブスクリプションにはUser1という名前のユーザーが含まれています。
ユーザー1のアカウントが侵害されたことをお知らせします。
User1がログインしたデバイスで発生したアラートを確認する必要があります。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

```
DeviceInfo
| where LoggedOnUsers contains 'user1'
| distinct DeviceId
|  kind=inner AlertEvidence on DeviceId
| project AlertId
| join AlertInfo on AlertId
|  AlertId, Timestamp, Title, Severity, Category
```

extend
join
project

project
summarize
take

正解:

```
 where LoggedOnUsers contains 'user1'
 distinct DeviceId
```

kind=inner AlertEvidence on DeviceId

extend
join
project

```
project AlertId
join AlertInfo on AlertId
```

AlertId, Timestamp, Title, Severity, Category

project
summarize
take

Explanation:
ボックス1：参加する
内側の接合部。
このクエリでは、kind=inner を使用して内部結合を指定しており、DeviceId の左側の値の重複排除を防いでいます。
このクエリは DeviceInfo テーブルを使用して、侵害の可能性のあるユーザー (<アカウント名>) がデバイスにログインしたかどうかを確認し、それらのデバイスでトリガーされたアラートを一覧表示します。
デバイス情報

//侵害された可能性のあるアカウントがログインしたデバイスを照会します
| LoggedOnUsers に '<account-name>' が含まれる場合
| 個別のデバイスID
//デバイスをAlertEvidenceテーブルとAlertInfoテーブルのアラートレコードと照合します
| join kind=inner AlertEvidence on DeviceId
| プロジェクトアラートID
//ユーザーがログインしたデバイス上のすべてのアラートを一覧表示します
| AlertId で AlertInfo に参加
| プロジェクトアラートID、タイムスタンプ、タイトル、重要度、カテゴリ
デバイス情報 ログインユーザー アラート証拠 "project AlertID"
ボックス2 :プロジェクト
参考資料 :https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

質問: **40**
Defender for Cloudの要件を満たす必要があります。
Group1にはどのサブスクリプションレベルの役割を割り当てるべきですか？
A. セキュリティ管理者
B. オーナー
C. セキュリティ評価貢献者
D. 貢献者
正解: **(**正解を表示します**)**
トピック4、混合問題
混合質問
このケーススタディにおけるSC-200混合問題
ファブリカム社は金融サービス会社です。
同社はニューヨーク、ロンドン、シンガポールに支社を構えている。Fabrikamには世界中にリモートユーザーがおり、これらのユーザーはVPN接続を介して支社にアクセスすることで、クラウドサービスを含む社内リソースにアクセスする。
このネットワークには、fabrikam.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれており、fabrikam.com という名前の Azure AD テナントと同期しています。フォレストを同期するために、Fabrikam はパススルー認証を有効にし、パスワード ハッシュ同期を無効にした Azure AD Connect を使用しています。
fabrikam.comのフォレストには、Group1とGroup2という2つのグローバルグループが含まれています。
Fabrikamの全ユーザーには、Microsoft 365 E5ライセンスとAzure Active Directory Premium Plan 2ライセンスが割り当てられています。Fabrikamは、Microsoft Defender for IdentityとMicrosoft Defender for Cloud Appsを導入し、ログコレクターを有効にしています。
Fabrikamは、以下の表に示すリソースを含むAzureサブスクリプションを保有しています。

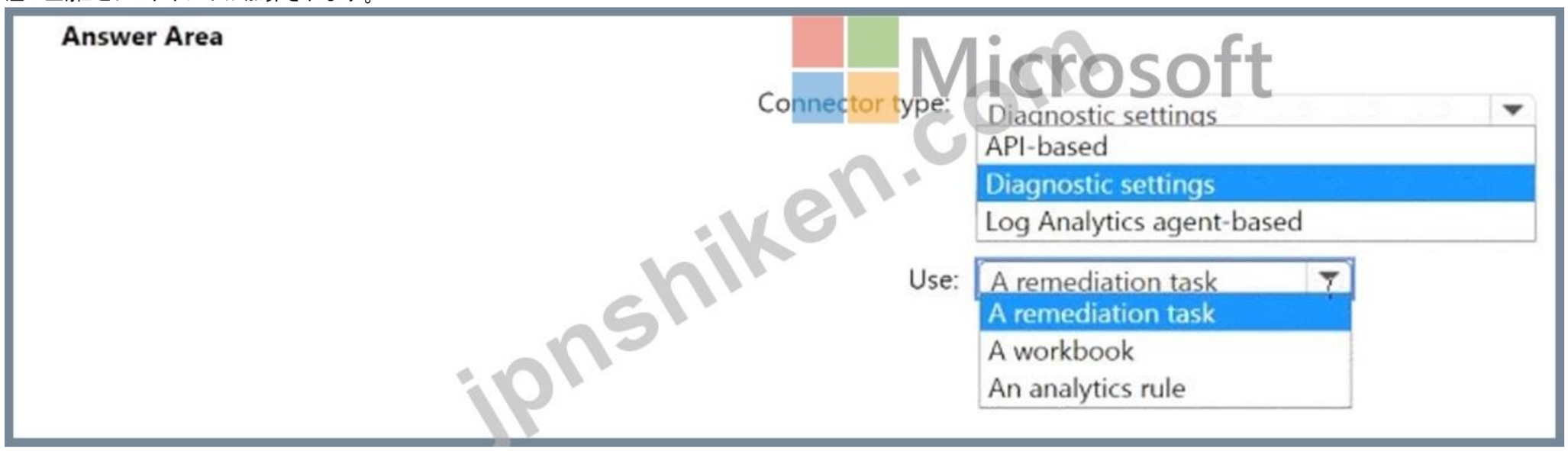
Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Fabrikamは、Account1という名前のAmazon Web Services（AWS）アカウントを所有しています。Account1には、カスタムWindows Server 2022を実行する100個のAmazon Elastic Compute Cloud（EC2）インスタンスが含まれています。このイメージにはMicrosoft SQL Server 2019が含まれていますが、エージェントはインストールされていません。
ユーザーが VPN 接続を使用すると、Microsoft 365 Defender は、誤検知である「あり得ない旅行」アラートを大量に発生させます。また、Defender for Identity は、誤検知である「疑わしい DCSync 攻撃」アラートを大量に発生させます。
Fabrikamは以下のサービスを導入する予定です。
* Microsoft Defender for Cloud
* マイクロソフトセンチネル
Fabrikamは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則を適用する。
♦ 管理業務の手間を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloud Appsの要件として以下の点を挙げています。
* 渡航不可能な場合の警告ポリシーは、各ユーザーの過去の活動に基づいていることを確認してください。
* 誤検知による、あり得ない旅行に関する警告の数を減らす。
誤検知アラートの調査に必要な管理上の労力を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloudに関して以下の要件を特定しました。
* グループ2のメンバーがセキュリティポリシーを変更できることを確認してください。
* Group1のメンバーがAzureサブスクリプションレベルで規制遵守ポリシーのイニシアチブを割り当てられるようにします。
* Azure Arc対応サーバー向けAzure Connected Machineエージェントのデプロイを、Account1の既存および将来のリソースに自動化します。
誤検知アラートの調査に必要な管理作業を最小限に抑える。
Fabrikamは、Microsoft Sentinelに関する以下の要件を特定しました。
* 組み込みの高度セキュリティ情報モデル（ASIM）統合パーサーを使用して、過去7日間のNXDOMAIN DNSリクエストを照会します。
* AWS EC2インスタンスから、ローカルグループメンバーシップの変更を含むWindowsセキュリティイベントログエントリを収集します。
* ユーザーおよびエンティティ行動分析（UEBA）を使用して、Azure ADユーザーの異常なアクティビティを特定します。
* UEBAを使用して、侵害されたAzure ADユーザー認証情報の潜在的な影響を評価します。
* App1がMicrosoft Sentinelの自動化ルールで使用できることを確認してください。
* 過去30日間に発生したインシデントについて、トリアージにかかる平均時間を特定する。
* 過去30日間に発生したインシデントをクローズするまでの平均時間を特定します。
* グループ1のメンバーがプレイブックを作成および実行できることを確認する。
* グループ1のメンバーが分析ルールを管理できることを確認してください。
* Jupyterノートブックを使用して、Pool! でハンティングクエリを実行します。

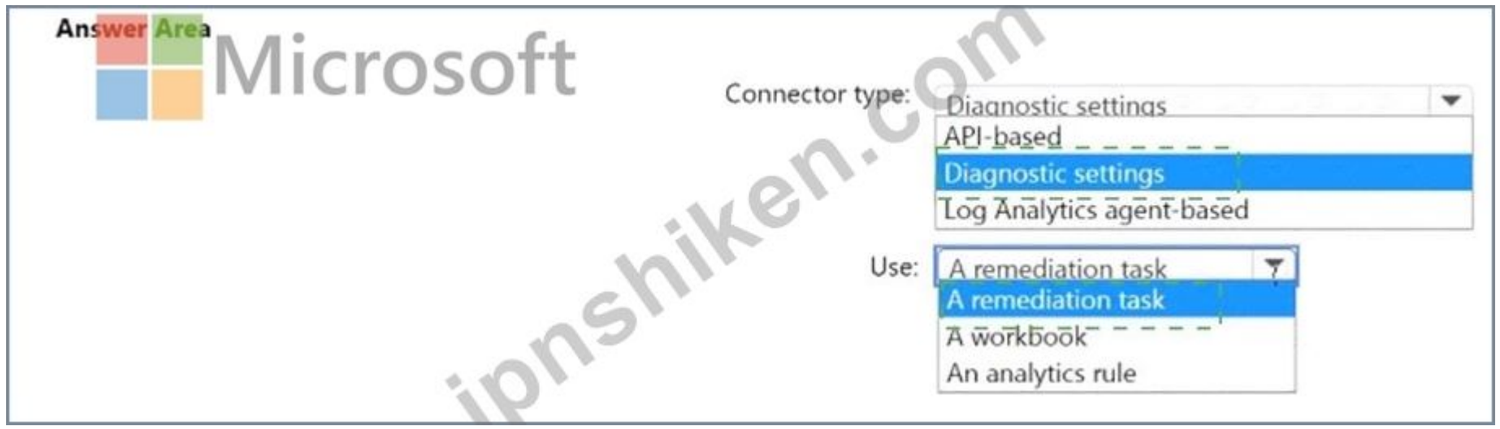
* グループ2のメンバーがインシデントを管理できることを確認する。
* データクエリのパフォーマンスを最大化する。
収集するデータ量を最小限に抑える。

質問: **41**
高度な機能設定で、サードパーティ製のウイルス対策ソフトが使用されている場合でもファイルをブロックするには、どの設定をオンにする必要がありますか？
A. EDRをブロックモードでオンにします。
B. 自動調査
C. ファイルを許可またはブロックします
D. 上記のすべて
正解: **(**正解を表示します**)**
オプションAが正解です。ブロックモードのEDRは、サードパーティ製のウイルス対策ソフトと併用できます。
オプションBは誤りです。「ファイルの許可またはブロック」機能を使用するには、Defender AVが必要です。
選択肢Cは誤りです。自動調査ではファイルはブロックされません。
参照：
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-compatibility?view=o365-worldwide

質問: **42**
お客様は4つのAzureサブスクリプションをお持ちです。そのうちの1つのサブスクリプションには、Microsoft Sentinelワークスペースが含まれています。
Azure Policy を使用してサブスクリプションからデータを収集するには、Microsoft Sentinel データコネクタをデプロイする必要があります。このソリューションでは、ポリシーがサブスクリプション内の新規リソースと既存リソースの両方に適用されることを保証する必要があります。
どのタイプのコネクタをプロビジョニングすべきか、また、すべてのリソースが監視されるようにするには何を使用すべきか。回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



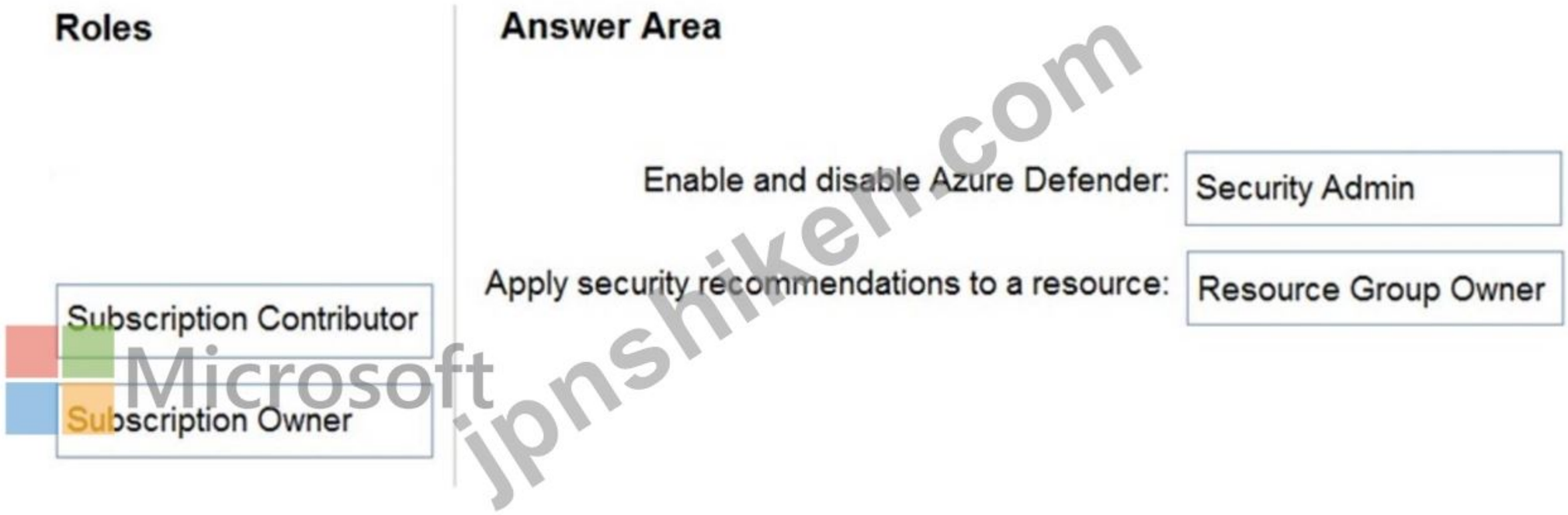
正解:



Explanation:

質問: **43**
ドラッグアンドドロップ問題
あなたはAzureサブスクリプションをお持ちです。
以下の要件を満たすためには、権限を委任する必要があります。
Azure Defenderを有効化および無効化します。
- リソースにセキュリティに関する推奨事項を適用する。
解決策は、最小権限の原則に基づかなければならない。
各要件に対して、どの Azure Security Center ロールを使用すべきでしょうか？回答するには、適切なロールを該当する要件にドラッグしてください。各ロールは、1 回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の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：正解ごとに1ポイントが加算されます。

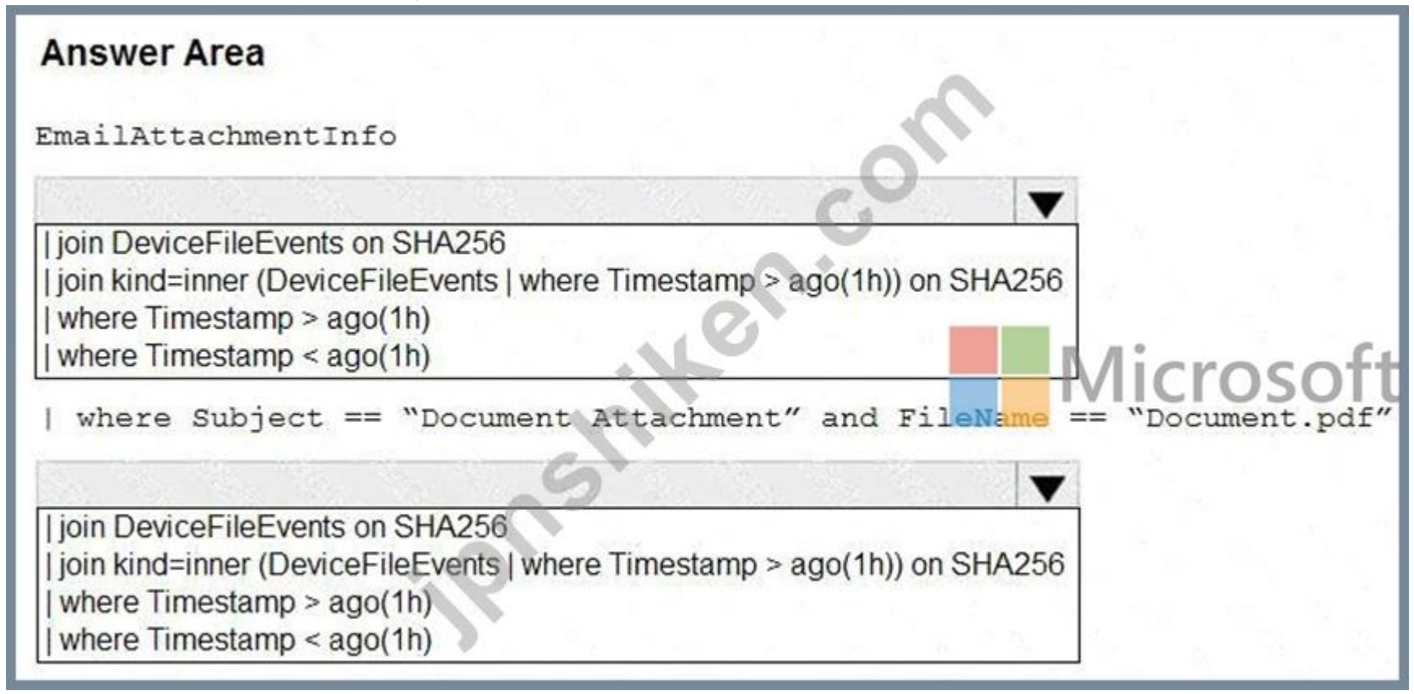
正解:



Explanation:
ボックス1 :セキュリティ管理者
ボックス2 :リソースグループの所有者
これは購読者よりも権限が低いものの、セキュリティに関する推奨事項を適用することは可能です。
参照 :
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

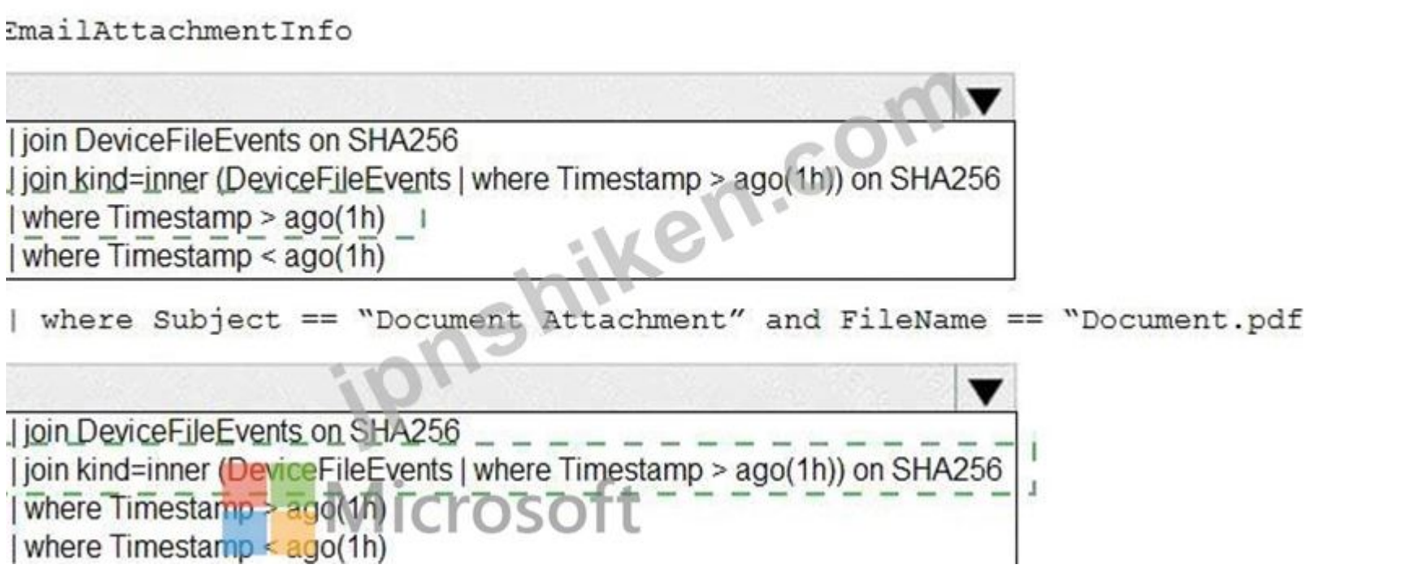
質問: 44

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
Document」という名前の添付ファイルを含むすべてのメールを返す検索クエリを作成する必要があります。
PDFファイル。クエリは以下の要件を満たす必要があります。
* 過去1時間以内に送信されたメールのみを表示します。
* クエリのパフォーマンスを最適化します。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。注：
正解ごとに1ポイント獲得できます。



正解:

Answer Area



Explanation:

質問: 45

あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。

あなたはMicrosoft 365 Defenderを使用して、ドメインをまたいだ調査を実施する予定です。

悪意のあるメール添付ファイルの影響を受けた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。

質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

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


正解:

Answer Area

```
EmailAttachmentInfo

| where SenderFromAddress =~ "MaliciousSender@example.com"

| where isnotempty (SHA256)

| [ ▼ ] (
```

- extend
- join
- project
- union

```
DeviceFileEvents

| [ ▼ ] FileName, SHA256
```

- extend
- join
- project
- union

```
) on SHA256

| [ ▼ ] Timestamp, FileName, SHA256, DeviceName, DeviceId,
```

- extend
- join
- project
- union

```
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```


説明

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,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

参照：
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o36

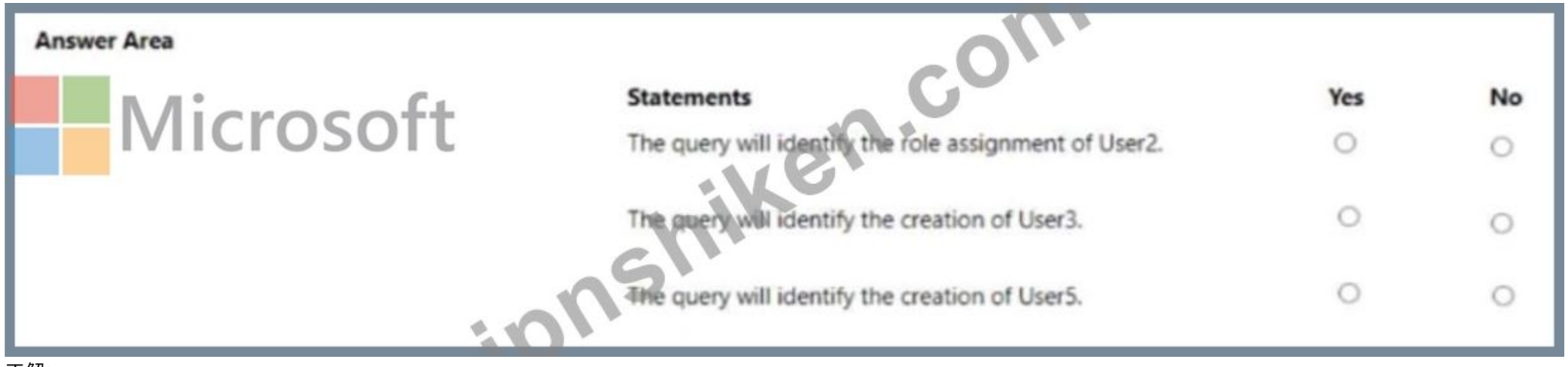
質問: **46**
Microsoft 365 E5 サブスクリプションには、User! と User2 という名前の 2 人のユーザーが含まれています。次の図に示すようなハンティングクエリがあります。

ユーザーは以下の陰イオンを実行します。

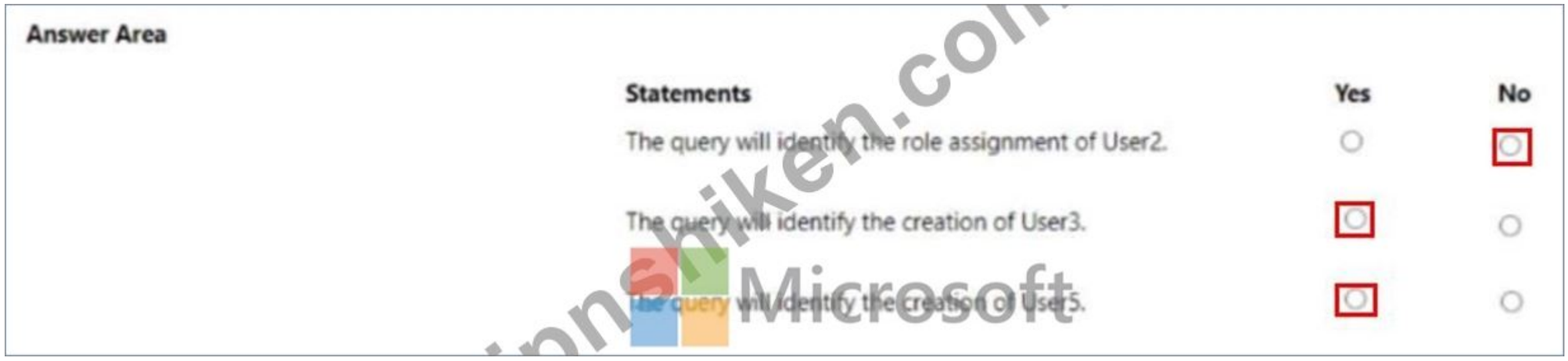
* User1がUser2にグローバル管理者ロールを割り当てます。
* User1はUser3という名前の新しいユーザーを作成し、そのユーザーにMicrosoft Teamsのライセンスを割り当てます。
* User2 は User4 という名前の新しいユーザーを作成し、そのユーザーにセキュリティ閲覧者の役割を割り当てます。
* User2はUser5という名前の新しいユーザーを作成し、そのユーザーにセキュリティオペレーターの役割を割り当てます。

以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



正解:



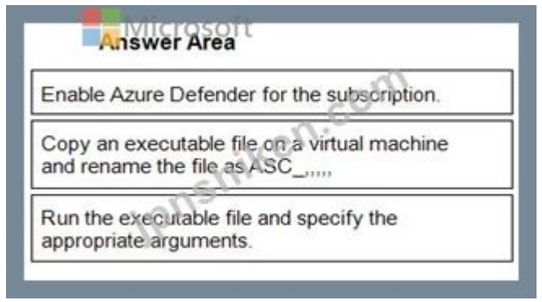
質問: **47**

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

Azure Security Center を構成して、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潜在的な脅威を検出できるようにする必要があります。ソリューションは、この構成を検証する必要があります。

3つの行動を順番に実行する必要があります。回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。

正解:

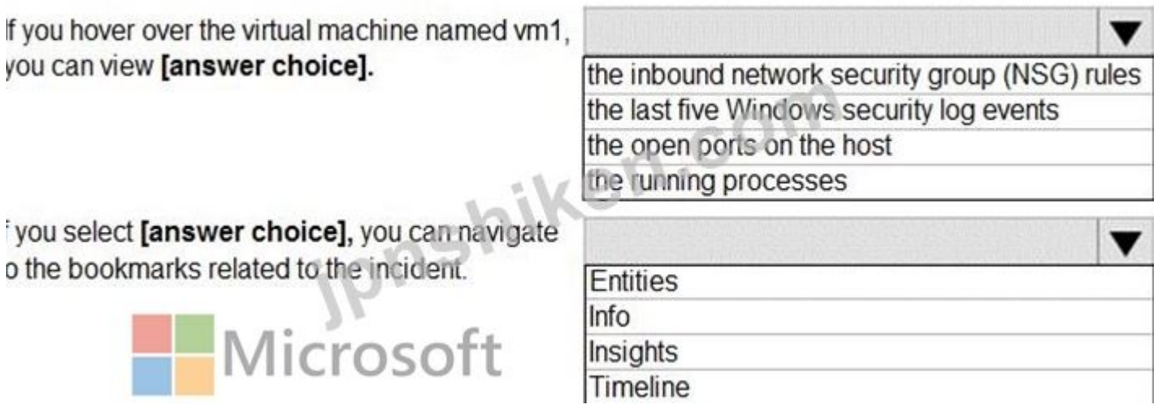


1 - サブスクリプションで Azure Defender を有効にします。
2 - 仮想マシンに実行可能ファイルをコピーし、ファイル名を ASC_,,,,, に変更します。
3 - 実行可能ファイルを実行し、適切な引数を指定します。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

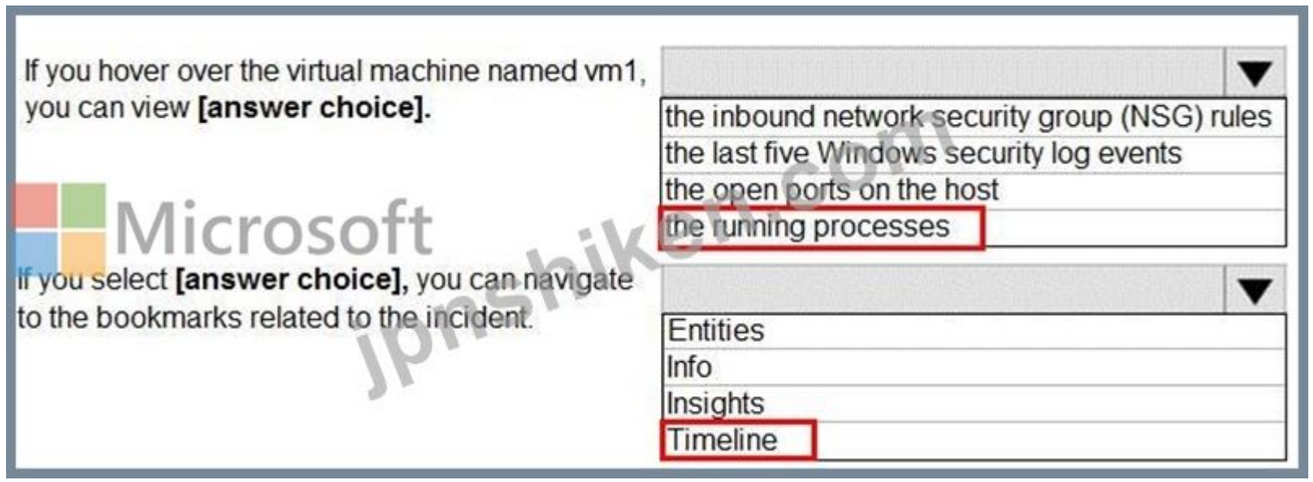
質問: **48**
Azure Active Directory (Azure AD) ユーザーをブロックするために使用されている既存の Azure ロジック アプリがあります。このロジック アプリは手動で起動されます。
Azure Sentinelをデプロイします。
Azure Sentinel で既存のロジック アプリをプレイブックとして使用する必要があります。最初に何をすべきでしょうか？
A. 新しいスケジュール済みクエリルール。
B. Azure Sentinel にデータ コネクタを追加します。
C. Azure Sentinel でカスタム脅威インテリジェンスコネクタを構成します。
D. ロジックアプリのトリガーを変更します。
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **49**
Azure Sentinel から、次の図に示すように、重大度の高いインシデントの調査ペインを開きます。

図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。



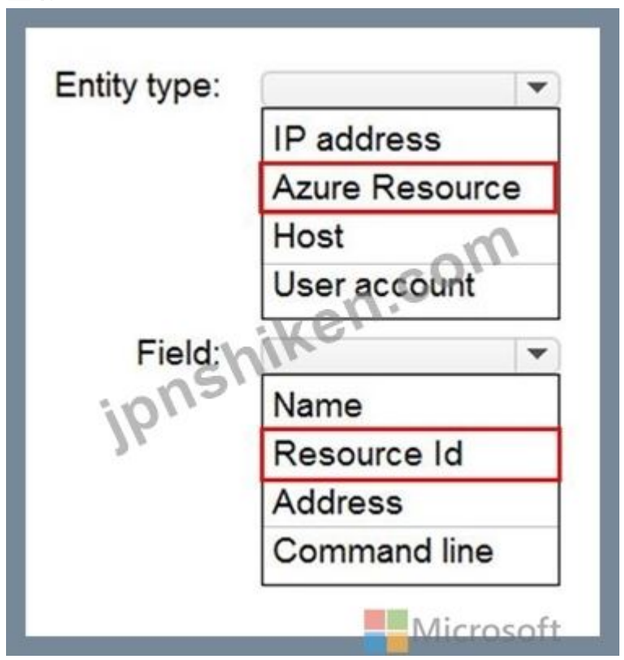
正解:



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

質問: **50**
アプリケーション開発中に複数のAzure Functionsアプリからアクセスされるストレージアカウントをお持ちです。
ストレージアカウントに関するAzure Defenderのアラートを非表示にする必要があります。
抑制ルールでは、どのエンティティタイプとフィールドを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

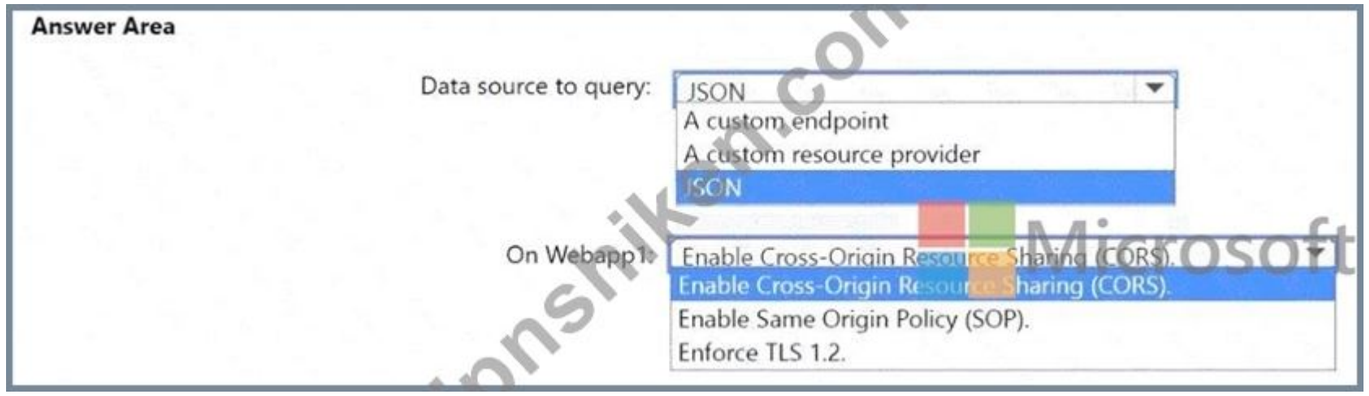


参照：
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

質問: **51**
貴社では、各プロジェクトのデータをそれぞれ異なるAzureサブスクリプションに保存しています。すべてのサブスクリプションは同じMicrosoft Entraテナントを使用しています。
各プロジェクトは、Windows Server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内のLog Analyticsワークス

ペースに保存されます。
Microsoft Sentinel 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 Log Analytics ワークスペースを横断的に検索するには、Microsoft Sentinel でハンティングクエリを実行する必要があります。
どの2つの行動をとるべきでしょうか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。
A. リソース式とエイリアス演算子を使用したクエリを作成します。
B. エイリアスステートメントを使用します。
C. 各ワークスペースにMicrosoft Sentinelソリューションを追加します。
D. 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。
E. Microsoft Sentinelワークスペースにセキュリティイベントコネクタを追加します。
正解: **C,D** (コメントを発表する)
複数の Azure サブスクリプションにまたがる複数の Log Analytics ワークスペースがあり、中央の Microsoft Sentinel デプロイメントからワークスペース間のハンティングクエリを実行する場合は、Microsoft の公式 Sentinel ドキュメントに従って、次の 2 つの手順を実行する必要があります。
* 各ワークスペースに Microsoft Sentinel ソリューションを追加します。クエリを実行する Log Analytics ワークスペースはすべて、Microsoft Sentinel が有効になっているか、接続されている必要があります。この手順を実行すると、ワークスペースは Sentinel の分析、ハンティング、および調査機能に参加できるようになります。各ワークスペースで Sentinel が有効になっていない場合、ハンティングクエリはデータへのアクセス許可やアクセス権限を持ちません。
複数のワークスペースにわたってクエリを実行するには、各ワークスペースでMicrosoft Sentinelが有効になっている必要があります。
* workspace() 式と共用体演算子を使用する - Microsoft Sentinel のハンティング クエリは、workspace() 関数で明示的にワークスペースを参照し、共用体演算子で組み合わせることで、複数のワークスペースにまたがって実行できます。例:
* union workspace('ProjectA-Workspace').SecurityEvent、
* workspace('ProjectB-Workspace').SecurityEvent、
* workspace('ProjectC-Workspace').SecurityEvent
* | イベントID == 4625
workspace()関数はリモートワークスペースを識別し、union関数は結果を結合して単一のクエリ出力にします。
他の選択肢は誤りです。
* AとB :エイリアスとリソース式は、ワークスペース内の複数リソースクエリに使用され、ワークスペース間クエリには使用されません。
* E: セキュリティイベントコネクタを追加しても、Windowsログの取り込みにのみ適用され、ワークスペースをまたいだ脅威ハンティングは有効になりません。

質問: **52**
Workbook1とWebapp1のクエリを実装する必要があります。ソリューションはMicrosoft Sentinelの要件を満たす必要があります。クエリはどのように構成すればよいですか？回答するには、回答領域で適切なオプションを選択してください。注：正解ごとに1ポイントが加算されます。



正解:

Explanation:

質問: **53**

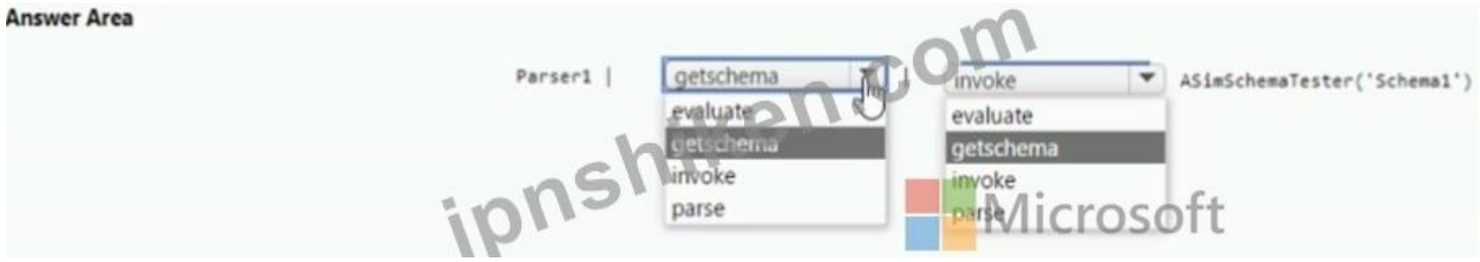
Microsoft Sentinelワークスペースをお持ちです

Parser1という名前のカスタムAdvanced Security Information Model (ASIM)パーサーを開発し、Schema1という名前のスキーマを生成させます。

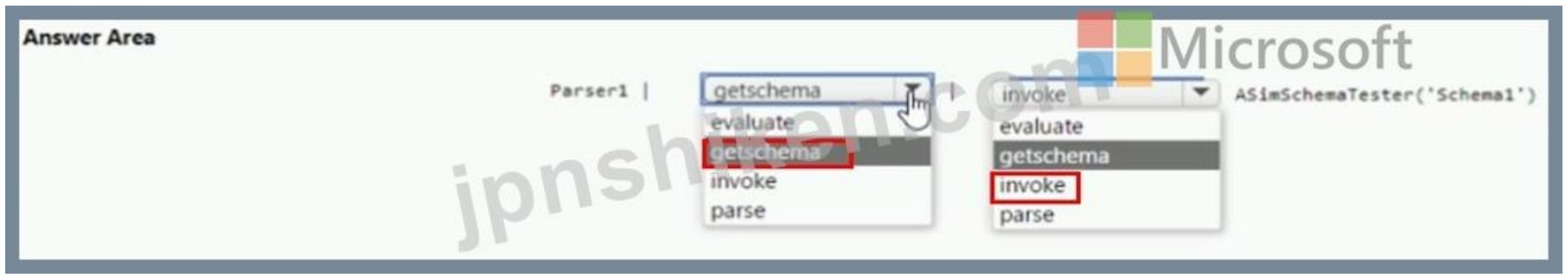
Schema1を検証する必要があります。

このコマンドをどのように完了すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。



正解:



質問: **54**

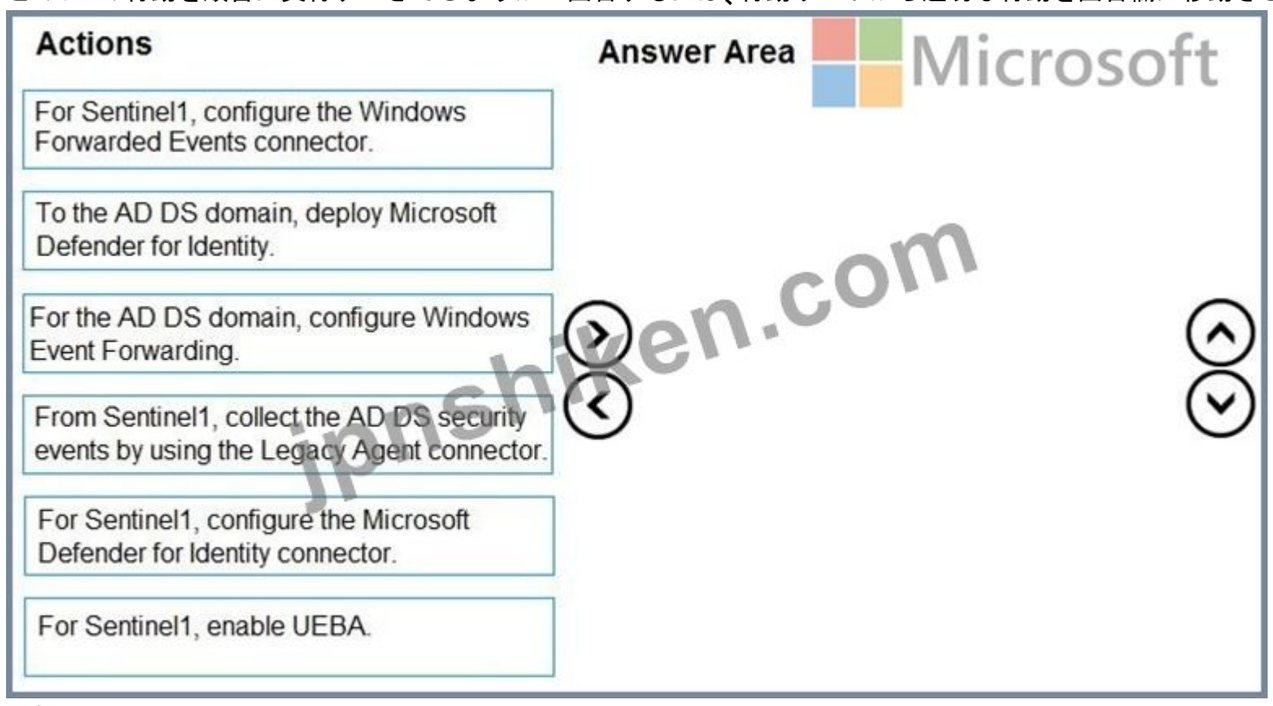
ドラッグアンドドロップ問題

お客様のネットワークには、Azure ADテナントと同期するオンプレミスのActive Directoryドメインサービス（AD DS）ドメインが含まれています。

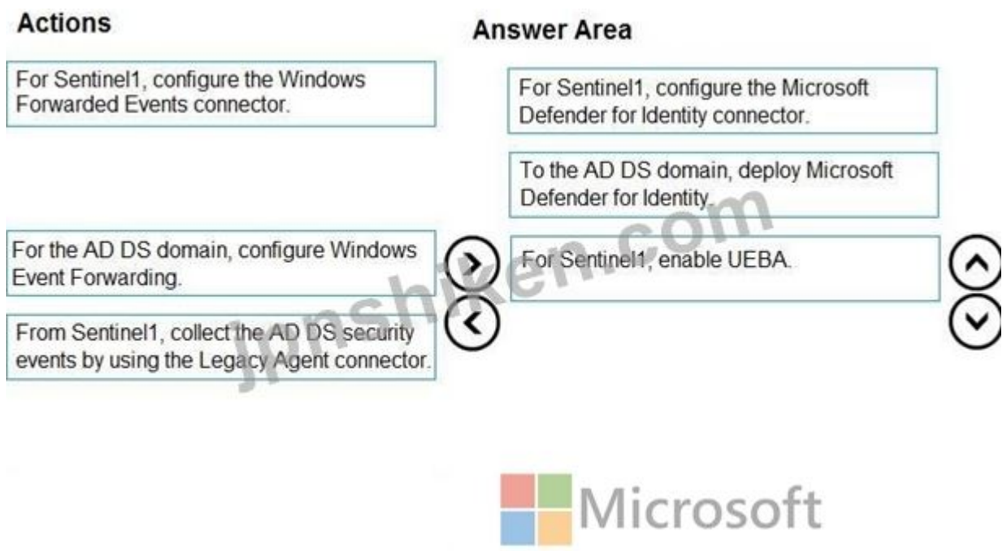
Sentinel1という名前のMicrosoft Sentinelワークスペースがあります。

Sentinel1 でユーザーおよびエンティティ行動分析 (UEBA) を有効にし、AD DS ドメインからセキュリティ イベントを収集する必要があります。

どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



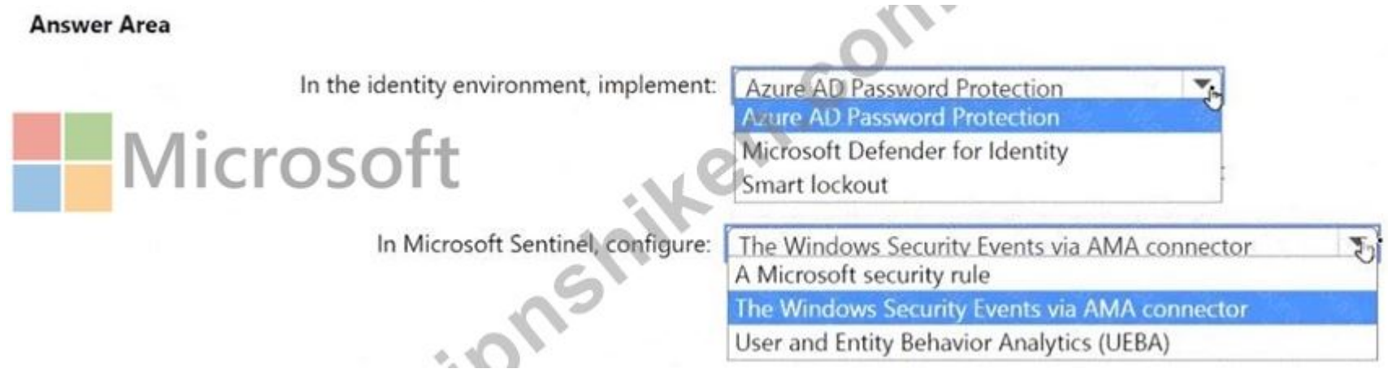
正解:



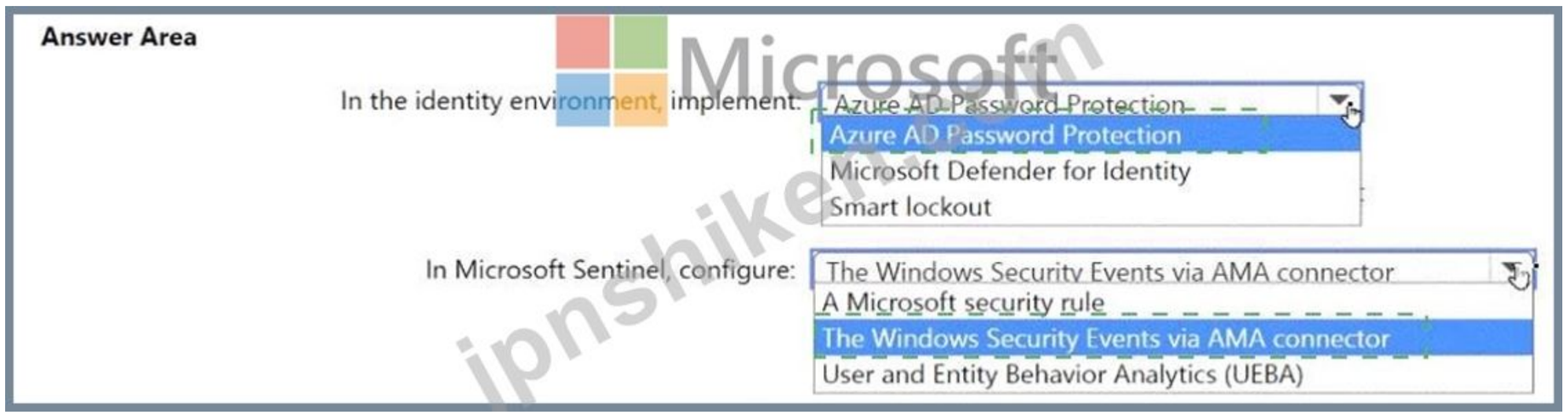
Explanation:
Sentinel1の場合、Microsoft Defender for IDコネクタを構成します。
これにより、Microsoft Defender for Identityを使用して、オンプレミスのActive Directoryからユーザーエンティティを同期できるようになります。
AD DSドメインにMicrosoft Defender for Identityを展開します。
UEBAがオンプレミスのAD DSドメインからセキュリティイベントを収集できるようにするには、Active Directoryドメインコントローラーにmdiセンサーをインストールする必要があります。
Sentinel1の場合、UEBAを有効にしてください。
トグルスイッチをオンに切り替えて、UEBAを有効にするデータソースを選択する必要があります。

質問: **55**
注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。
このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。
Azure Security Center 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信します。
セキュリティセンターで、アラートを解決するための推奨事項を確認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、『アクションを実行する」を選択してから、 『今後の攻撃を防止する」セクションを展開します。
これは目標を達成していると言えるでしょうか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
説明
必要なのは、既存のアラートを解決することであり、将来のアラートを防止することではありません。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: **56**
パスワードのリセットを監視する必要があります。ソリューションは、Microsoft Sentinelの要件を満たしている必要があります。

どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

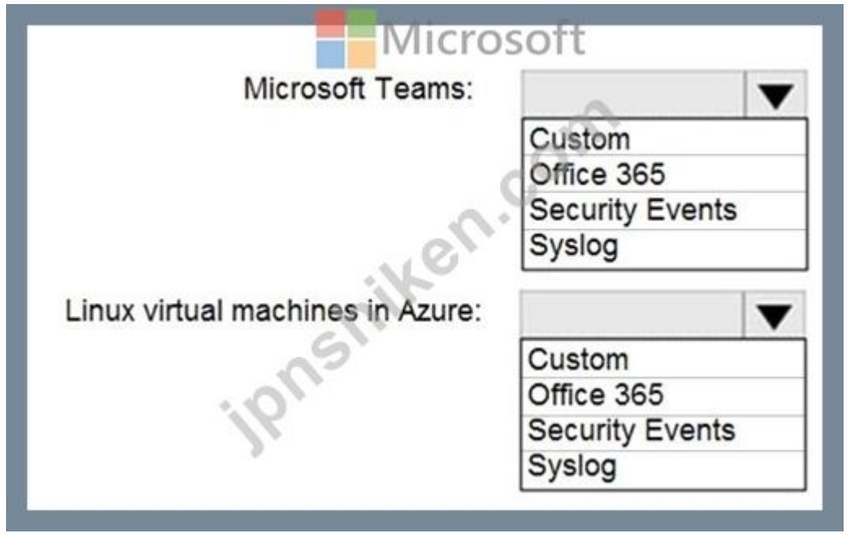


正解:

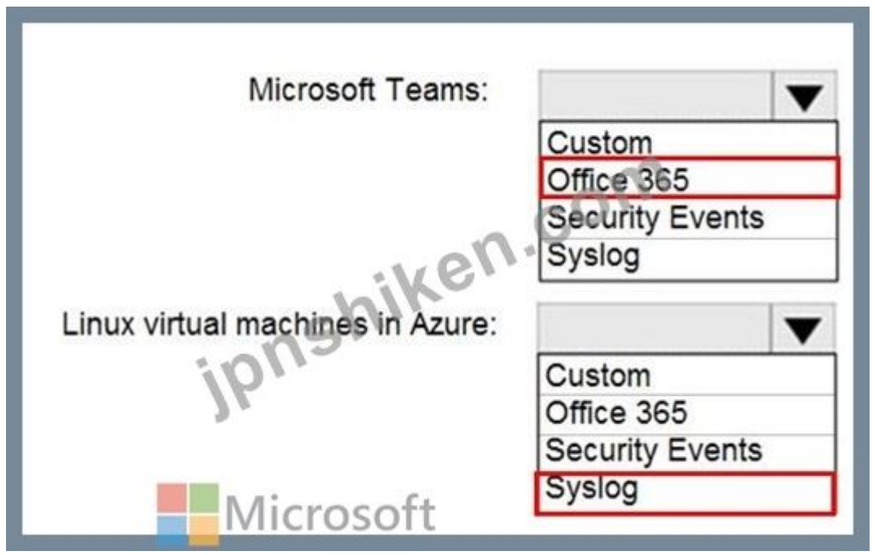


Explanation:

質問: **57**
Azure Sentinelをデプロイします。
Azure Sentinelにコネクタを実装して、Azure上のMicrosoft TeamsとLinux仮想マシンを監視する必要があります。このソリューションは、管理作業を最小限に抑える必要があります。
各ワークロードには、どのデータコネクタタイプを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



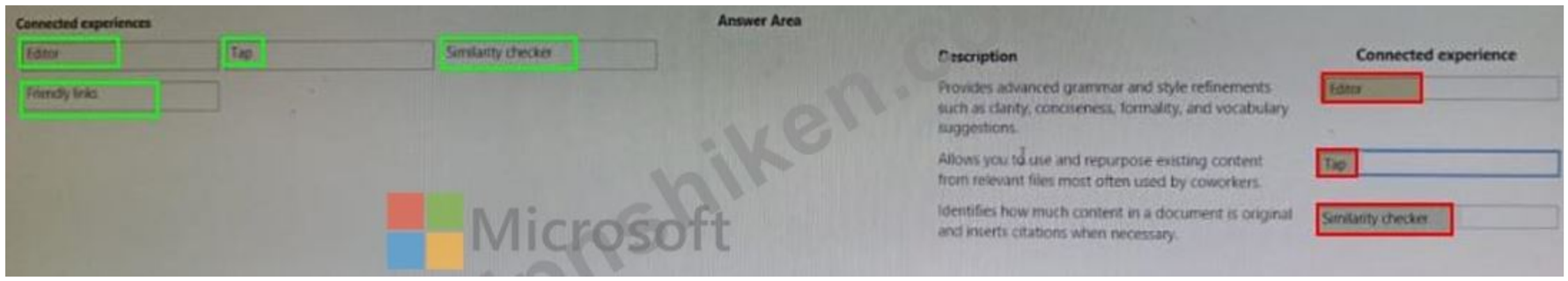
参照：
https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

質問: **58**
Microsoft Sentinelワークスペースを含むAzureサブスクリプションをお持ちです。
Microsoft Sentinelのアラートに応答して自動的に実行されるプレイブックを作成する必要があります。
最初に何を作るべきでしょうか？
A. Azure Functionsのトリガー
B. Microsoft Sentinel でのハンティングクエリ
C. Azureロジックアプリ
D. Microsoft Sentinelの自動化ルール

正解: (正解を表示します)

質問: **59**
ある企業がMicrosoft 365アプリを使用して分析を行いたいと考えている。
企業が活用できる連携体験について説明する必要があります。
どの関連体験を説明すればよいでしょうか？回答するには、適切な関連体験を正しい説明にドラッグしてください。各関連体験は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割をドラッグするか、スクロールする必要がある場合があります。
注：正解ごとに1ポイントが加算されます。

正解:

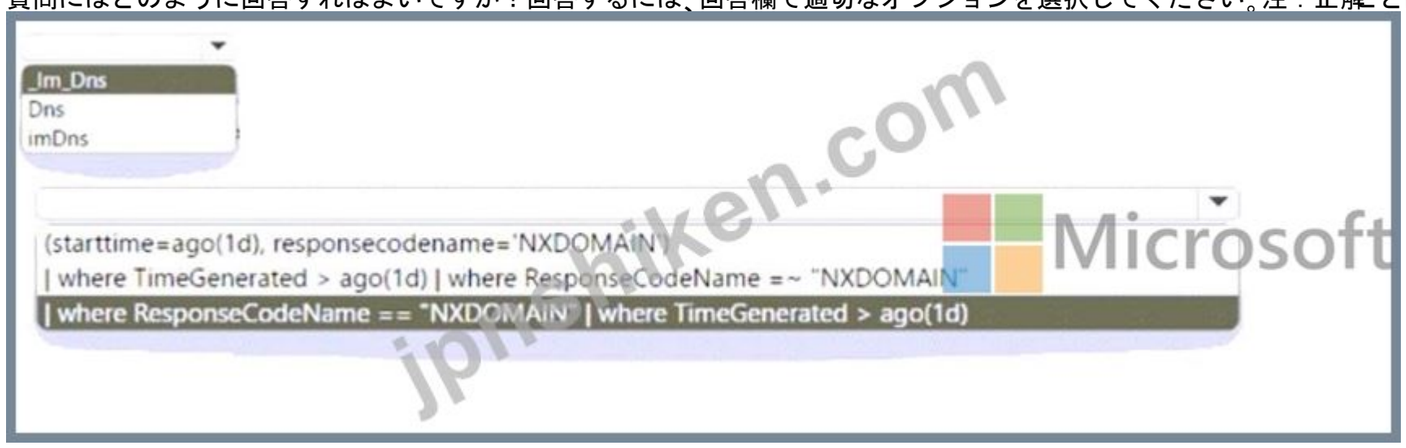


質問: **60**
Microsoft Sentinelの要件を満たすために、ハンティングクエリを実行できることを確認する必要があります。どのようなタイプのワークスペースを作成すればよいでしょうか？
A. AzureDalabricks
B. LogAnalytics
C. Azure Synapse AnarytKS
D. Azure Machine Learning
正解: **D** (コメントを発表する)

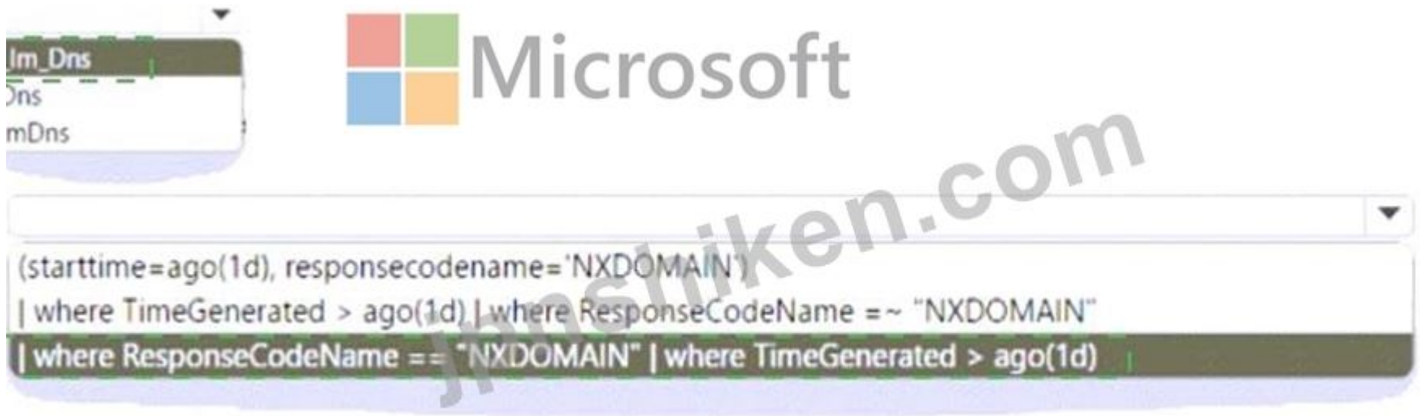
質問: **61**
お客様は、Microsoft Defender for Cloud Appsを使用し、クラウド検出が有効になっているMicrosoft 365サブスクリプションをお持ちです。
クラウド検出データを拡充する必要があります。ソリューションは、クラウド検出トラフィックログ内のユーザー名が、対応するMicrosoft Entra IDユーザーアカウントのユーザープリンシパル名（UPN）に関連付けられていることを保証する必要があります。
まず最初に何をすべきでしょうか？
A. 条件付きアクセス アプリケーション制御から、ユーザー監視を設定します。
B. Microsoft 365 アプリ コネクタを作成します。
C. Microsoft 365 Defenderへの自動リダイレクトを有効にします。

D. Azure アプリ コネクタを作成します。
正解: **(**正解を表示します**)**
Microsoft Defender for Cloud Apps (MCAS) では、クラウド検出機能がトラフィックログを収集し、シャドウITの使用状況やクラウドアプリのアクティビティを特定します。この検出データを充実させ、トラフィックログ内のユーザー名を実際の Microsoft Entra ID (Azure AD) ユーザーにマッピングするために、Defender for Cloud Apps はユーザー名をユーザーのユーザープリンシパル名 (UPN) と関連付ける必要があります。
Microsoft Defender for Cloud Appsのドキュメントによると、この関連付けは、Microsoft 365アプリコネクタを介してMicrosoft 365（旧Office 365）に接続すると自動的に行われます。
このコネクタはMCASをMicrosoft 365と統合し、以下のことを可能にします。
* 検出ログから取得したユーザー名をUPNに一致するように正規化する。
* Microsoft 365 アプリ全体で、より詳細な ID 情報とアクティビティを提供します。
* アプリケーション間の調査、アラートの相関関係、および条件付きアクセス管理を有効にする。
その他の選択肢について説明します。
* 条件付きアクセス アプリケーション制御 - クラウド ディスカバリの強化ではなく、リアルタイムのセッション制御に使用されます。
* Microsoft 365 Defenderへの自動リダイレクトを有効にする - ポータル統合に使用され、データエンリッチメントには使用されません。
* Azure アプリ コネクタ - サードパーティ製アプリケーションまたは Azure ホスト型アプリケーションを接続するために使用され、UPN の拡張には使用されません。
したがって、Cloud Discovery データを UPN マッピングで強化するには、Microsoft 365 アプリ コネクタを作成する必要があります。

質問: **62**
Microsoft Sentinelワークスペースの名前はWorkspacesです。
Workspace1 を c に設定します。
DNSイベントを収集し、DNSスキーマ用の高度セキュリティ情報モデル（ASIM）統合パーサーを展開します。
ASIM DNSスキーマに対してクエリを実行し、過去24時間以内に応答コードが「NXDOMAIN」で、送信元IPアドレスごとに15分間隔で集計されたすべてのDNSイベントを一覧表示する必要があります。このソリューションは、クエリのパフォーマンスを最大限に高める必要があります。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。注：正解ごとに1ポイントが加算されます。



正解:



説明

質問: **63**

お客様はAzure Defenderを使用するAzureサブスクリプションをお持ちです。

Azure Security Centerのワークフロー自動化機能を使用して、Azure Defenderの脅威アラートに対応する予定です。

脅威の修復を自動的に実行するAzureポリシーを作成する必要があります。

解答には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。

Set available effects to:

Append
DeployIfNotExists
EnforceRegoPolicy

To perform remediation use:

An Azure Automation runbook that has a webhook
An Azure Logic Apps app that has the trigger set to When an Azure Security Center Alert is created or triggered
An Azure Logic Apps app that has the trigger set to When a response to an Azure Security Center alert is triggered

正解:

説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明は自動的に生成されます

参照：

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

質問**: 64**

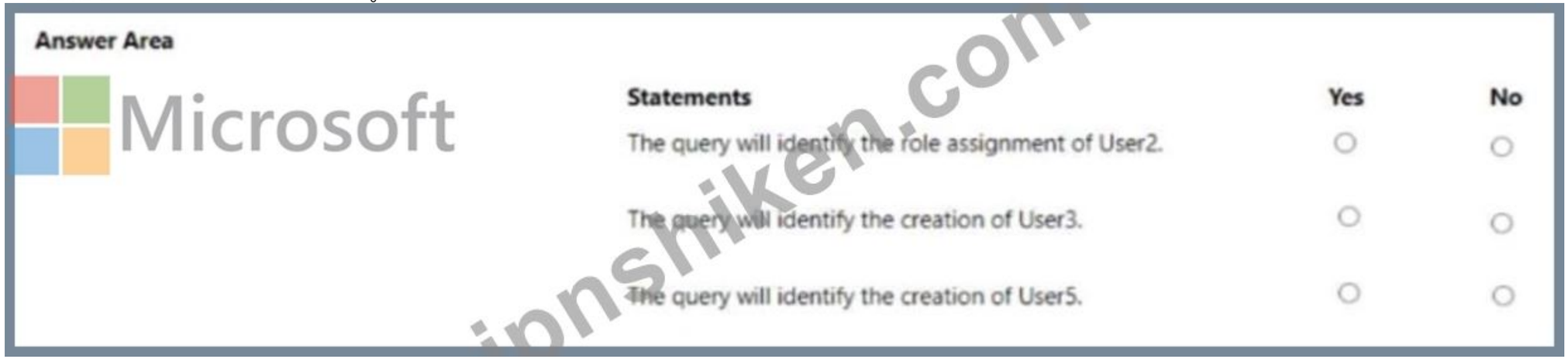
Microsoft 365 E5 サブスクリプションには、User! と User2 という名前の 2 人のユーザーが含まれています。次の図に示すようなハンティングクエリがあります。

ユーザーは以下の陰イオンを実行します。

* User1がUser2にグローバル管理者ロールを割り当てます。
* User1はUser3という名前の新しいユーザーを作成し、そのユーザーにMicrosoft Teamsのライセンスを割り当てます。
* User2 は User4 という名前の新しいユーザーを作成し、そのユーザーにセキュリティ閲覧者の役割を割り当てます。
* User2はUser5という名前の新しいユーザーを作成し、そのユーザーにセキュリティオペレーターの役割を割り当てます。

以下の各記述について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。



正解:

Answer Area

Statements	Yes	No
The query will identify the role assignment of User2.	○	○
The query will identify the creation of User3.	○	○
The query will identify the creation of User5.	○	○

質問: **65**
お客様は、Microsoft Defender XDRを使用するMicrosoft 365サブスクリプションをご利用されています。
以下のステートメントを含むクエリがあります。

```
union DeviceEvents, DeviceProcessEvents
| where ingestion_time() > ago(1d)
...
```

クエリを使用するカスタム検出ルールを設定する必要があります。このソリューションは、クエリに一致するイベントの通知にかかる時間を最小限に抑える必要があります。
ルールにはどの頻度を選択すべきでしょうか？
A. 毎時間
B. 12時間ごと
C. 連続（NRT）
D. 3時間ごと
正解: **C** (コメントを発表する)

質問: **66**
Azure サブスクリプションには、Workspace1 という名前の Microsoft Sentinel ワークスペースと User1 という名前のユーザーが含まれています。
User1がWorkspace1を使用してインシデントを調査できるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1にはどの役割を割り当てるべきですか？
A. Microsoft Sentinel Automation 貢献者
B. マイクロソフト センチネル レスポンダー
C. マイクロソフトセンチネル貢献者
D. Microsoft Sentinel Reader
正解: (正解を表示します)

質問: **67**
Sub1 という名前の Azure サブスクリプションと、AzDO1 という名前の Azure DevOps 組織があります。AzDO1 は Defender for Cloud を使用しており、Pipeline1 という名前の YAML パイプラインを含むプロジェクトが含まれています。
Pipeline1は、発見されたオープンソースソフトウェアの脆弱性の詳細をDefender for Cloudに出力します。
Pipeline1 を構成して、シークレット スキャンの結果を Defender for Cloud に出力する必要があります。Pipeline1 には何を追加すればよいですか？回答するには、回答領域で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

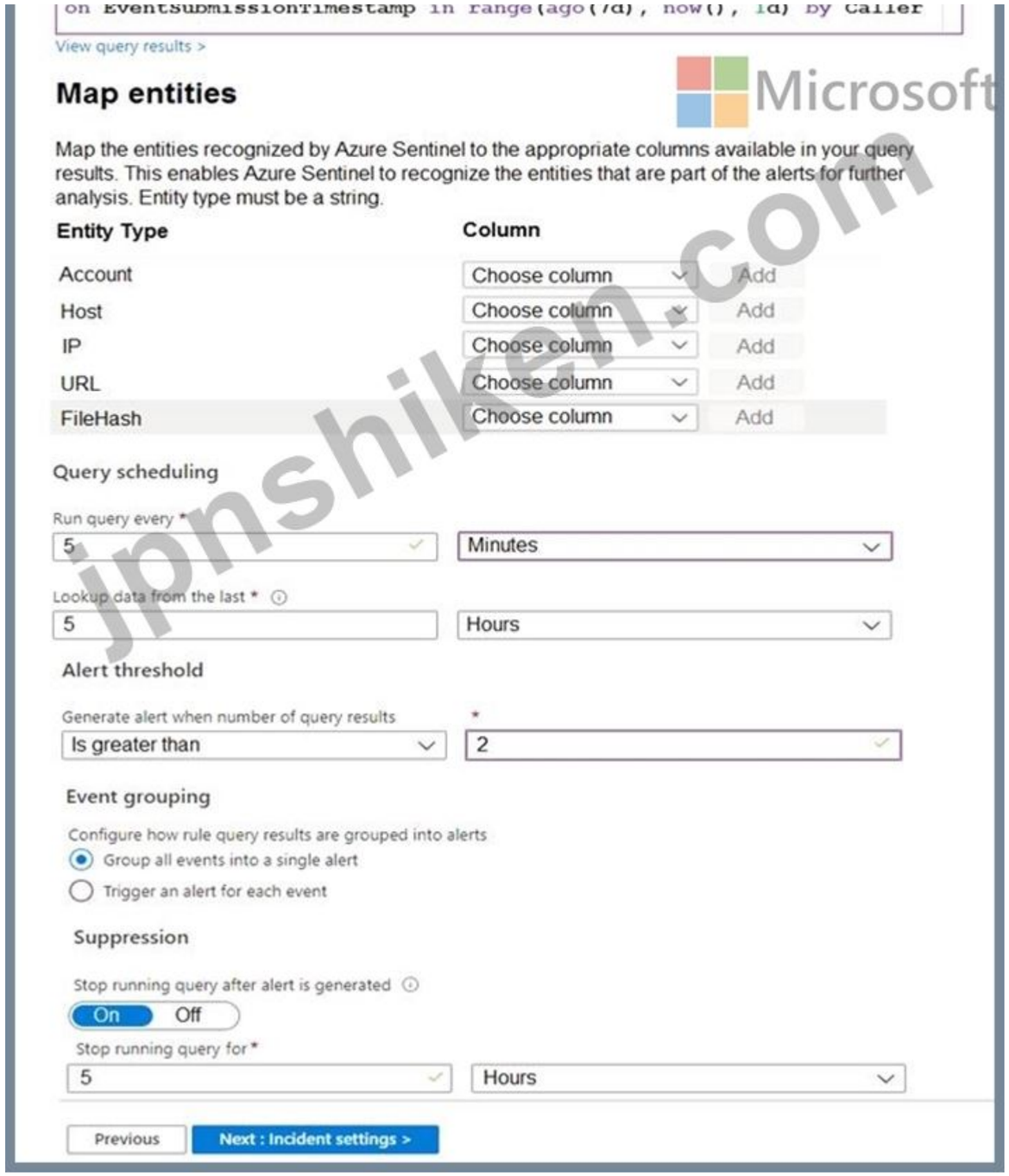
正解:

Explanation:

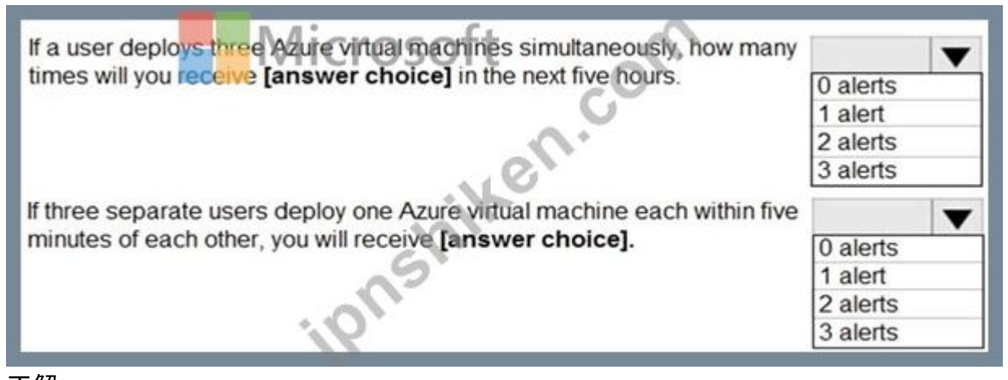
質問: **68**

Azure Sentinel は、Azure の異常なアクティビティを監視するために使用されます。

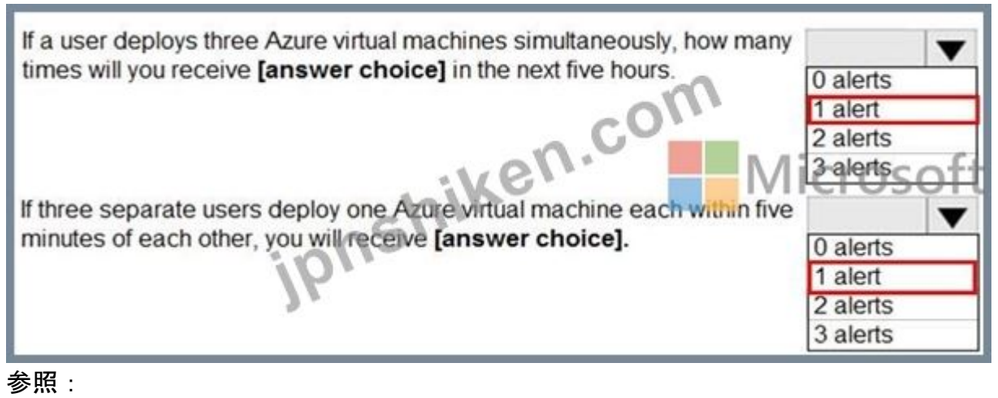
次の図に示すように、脅威を検出するためのカスタム分析ルールを作成します。



ルール定義の一部として、インシデント設定を定義する必要はありません。
図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



参照：

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

質問: **69**

以下のKQLクエリを含むカスタム検出ルールがあります。

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

以下の各項目について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

正解:

Explanation:

質問: **70**

workspace1という名前のMicrosoft Sentinelワークスペースと、VM1という名前のAzure仮想マシンがあります。

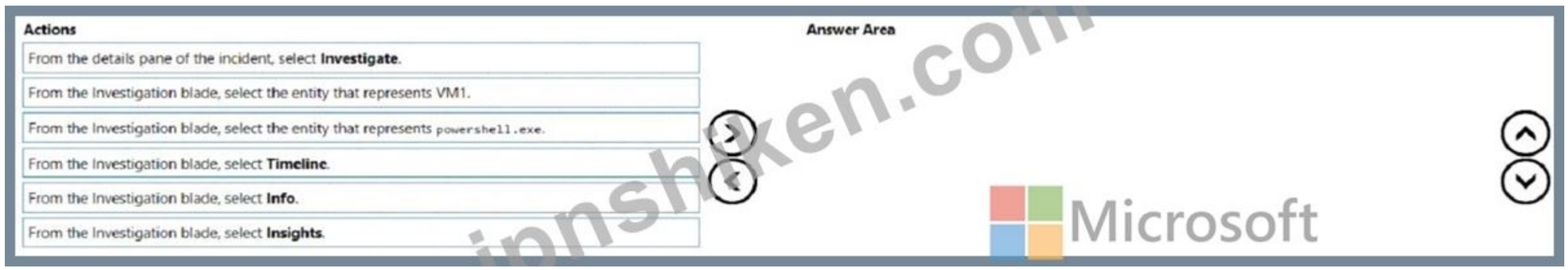
VM1上でPowerShellの不審な使用に関するアラートを受信しました。

インシデントを調査し、アラートをトリガーしたイベントを特定し、アラート発生後にVM1上で以下の操作が行われたかどうかを確認する必要があります。

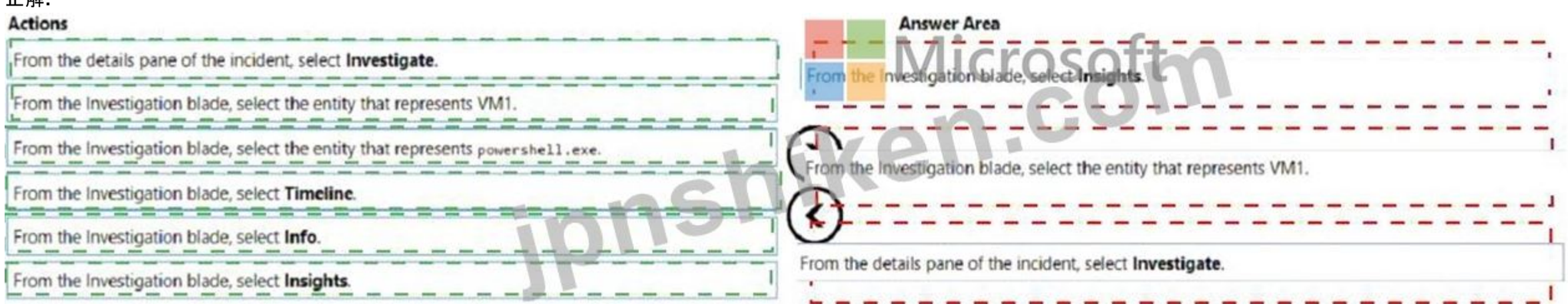
地域グループのメンバーシップの変更

イベントログの削除

Azure ポータルで、どの 3 つの操作を順番に実行する必要がありますか？回答するには、操作の一覧から適切な操作を回答欄に移動して、正しい順序に並べ替えてください。



正解:



説明

ステップ1：調査ブレードから ｢インサイト｣を選択します。

調査インサイトワークブックは、Azure Sentinelインシデントまたは個々のIPアドレス、アカウント、ホスト、URLエンティティの調査を支援するために設計されています。

ステップ2：調査ブレードから、VM1を表すエンティティを選択します。

調査分析ワークブックは、インシデント分析とエンティティ分析という2つの主要なセクションに分かれています。

インシデント分析

インシデントインサイトは、アナリストに進行中のSentinelインシデントの概要を提供し、アラートやエンティティ情報などの関連メタデータへの迅速なアクセスを可能にします。

エンティティに関する洞察

エンティティインサイトを使用すると、アナリストはインシデントまたは手動入力からエンティティデータを取得し、そのエンティティに関する関連情報を探索できます。このワークブックでは現在、以下のエンティティタイプのビューが提供されています。

IPアドレス

アカウント

ホスト

URL

ステップ3 :インシデントの詳細ペインから ｢調査｣を選択します。

単一のインシデントを選択し、 ｢詳細を表示｣または ｢調査｣をクリックしてください。

参照：

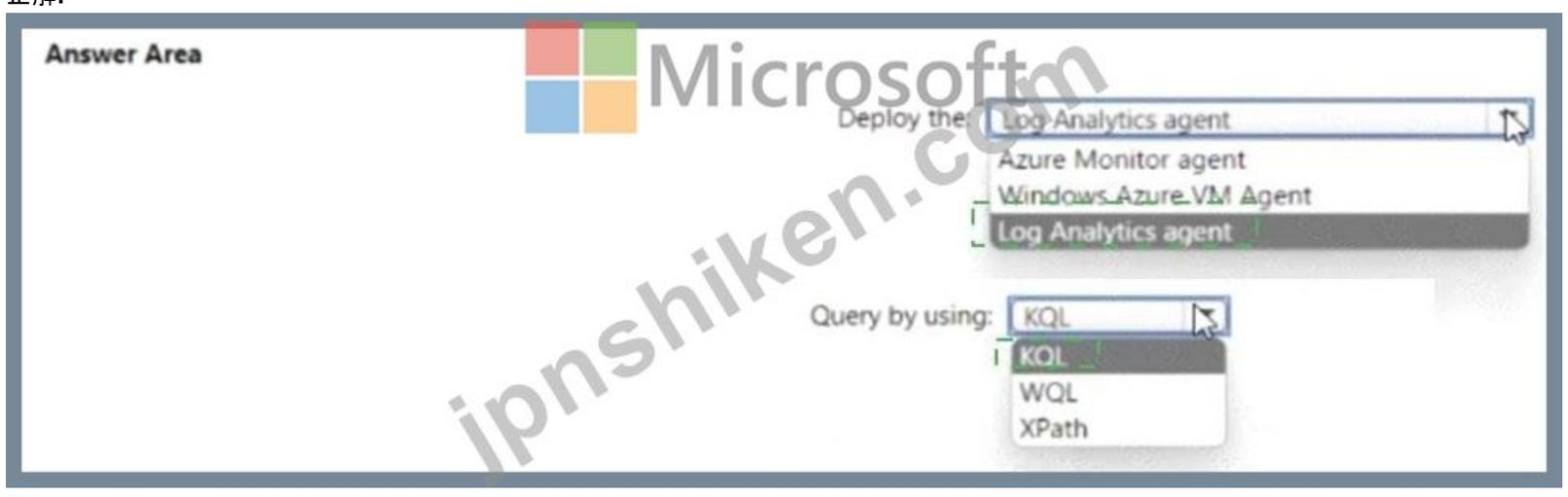
https://github.com/Azure/Azure-Sentinel/wiki/Investigation-Insights---Overview

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

質問: **71**

Windows セキュリティ イベント ログを収集するには、Microsoft Sentinel の要件を満たす必要があります。どうすればよいですか？回答するには、回答領域で適切なオプションを選択してください。注: 正解ごとに 1 ポイントが加算されます。

正解:

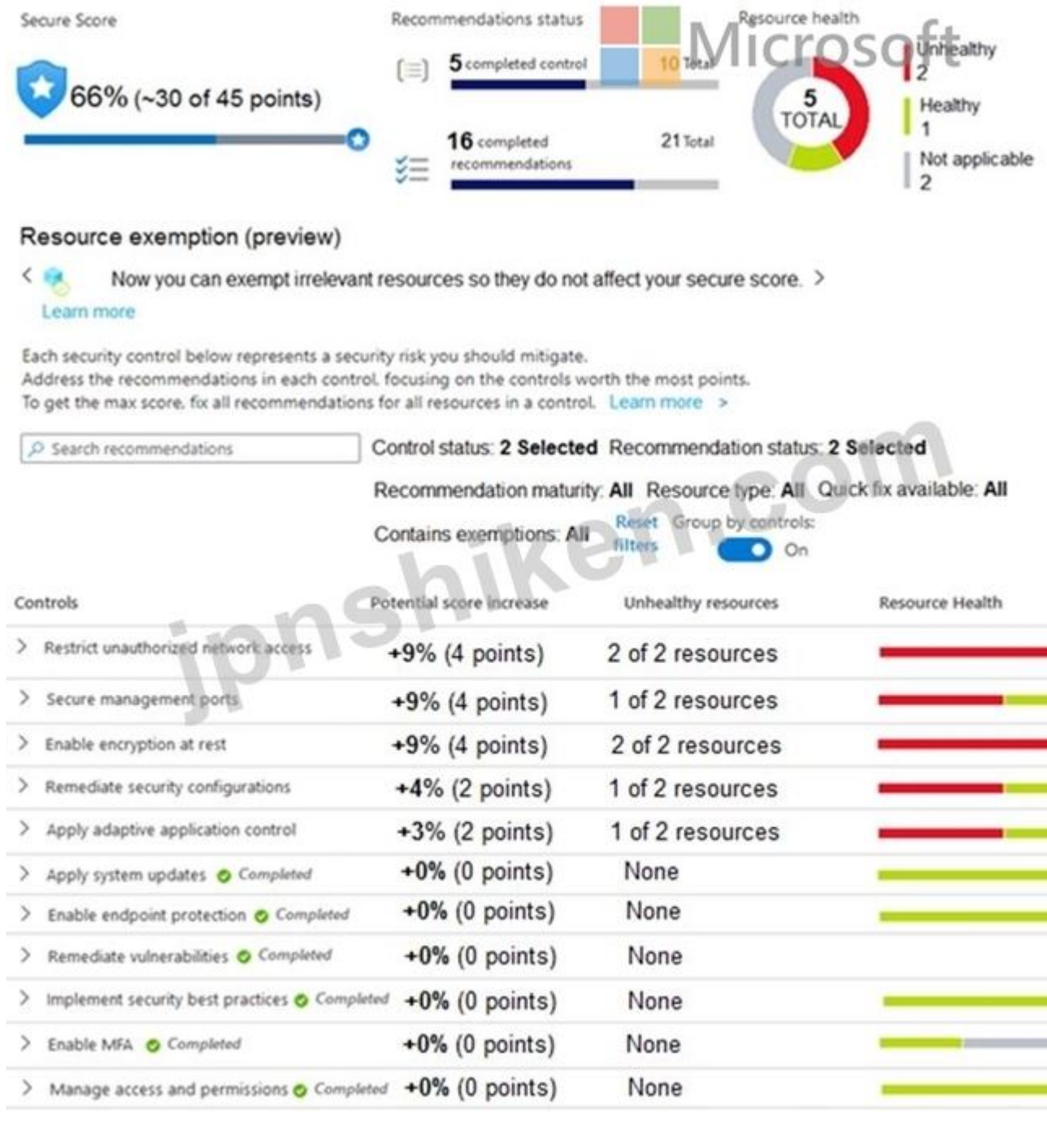


Explanation:

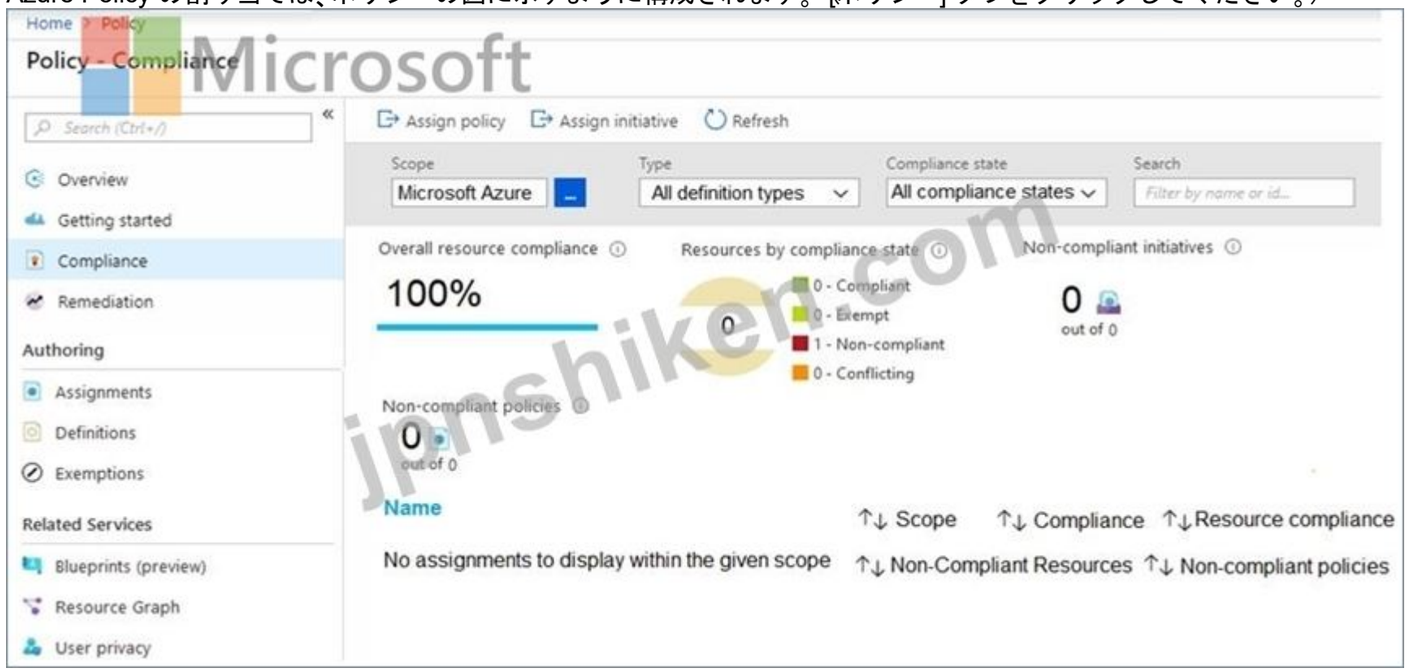
質問: **72**
貴社はAzure Sentinelを使用して、1万台以上のIoTデバイスからのアラートを管理しています。

同社のセキュリティマネージャーによると、インシデントの発生件数が多いため、セキュリティ上の脅威を追跡することがますます困難になっているという。
脅威の調査を簡素化し、機械学習を用いて脅威を推測するための、カスタムビジュアライゼーションを提供するソリューションを提案する必要があります。
推薦状には何を含めるべきでしょうか？
A. ブックマーク
B. ライブ配信
C. 組み込みクエリ
D. ノート
正解: **(**正解を表示します**)**

質問: **73**
あなたは、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体制を管理します。
Azure Security Center のセキュリティスコアは、Security Center の図に表示されます。$Security Center タブをクリックしてください。）



Azure Policy の割り当ては、ポリシーの図に示すように構成されます。[ポリシー] タブをクリックしてください。）



以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

正解:

Explanation:

参照：

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-acc

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/15

質問: **74**

貴社は、Microsoft DefenderをID管理に使用しているオンプレミスネットワークを運用しています。

同社のMicrosoft Secure Scoreには、安全性の低いKerberos委任に関連するセキュリティ評価が含まれています。

セキュリティリスクを是正する必要があります。

あなたはどうすべきでしょうか？

A. 公開対象としてリストされているコンピュータに、ローカル管理者パスワードソリューション（LAPS）拡張機能をインストールします。

B. 公開エンティティとしてリストされているコンピュータオブジェクトのプロパティを変更します。

C. 公開エンティティとしてリストされているコンピュータ上のレガシープロトコルを無効にします。

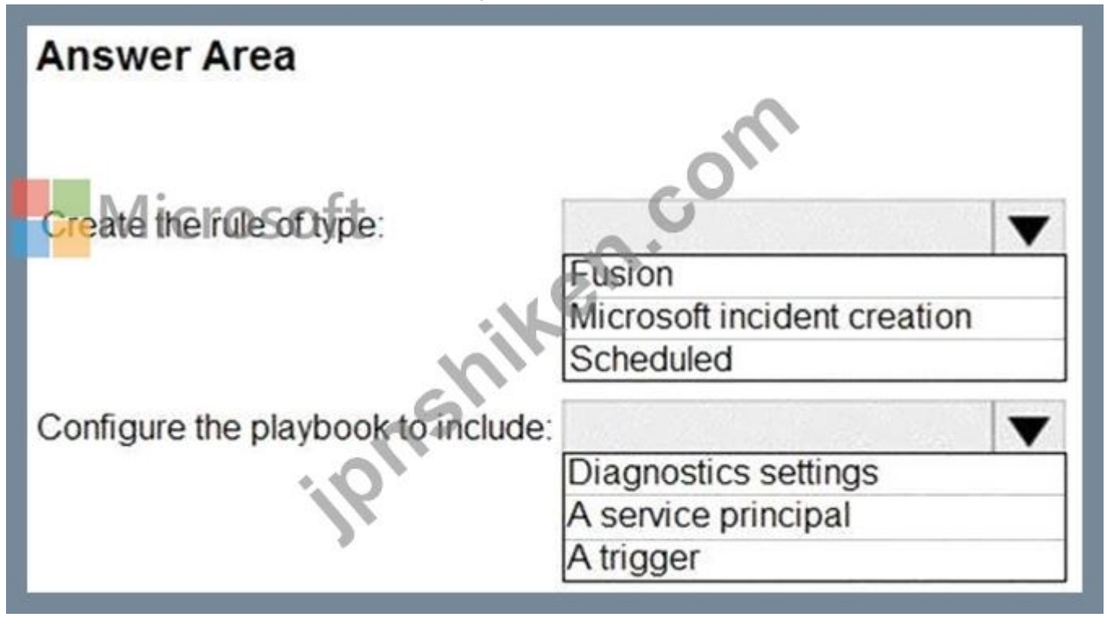
D. 公開エンティティとしてリストされているコンピュータで LDAP 署名を強制します。

正解: **(**正解を表示します**)**

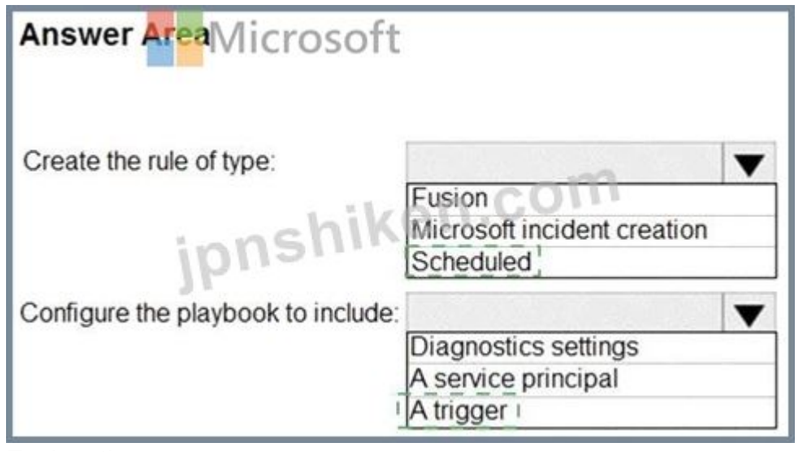
安全でない Kerberos 委任に関連するセキュリティ リスクを軽減するには、公開エンティティとしてリストされているコンピューター オブジェクトのプロパティを変更する必要があります。具体的には、Kerberos 委任設定を 「任意のサービスへの委任をこのコンピューターに許可する」または 「指定されたサービスへの委任のみをこのコンピューターに許可する」のいずれかに設定する必要があります。

これにより、コンピューターが Kerberos 委任を使用してネットワーク上の他のコンピューターにアクセスできないようになります。参照: https://docs.microsoft.com/en-us/windows/security/identity-protection/microsoft-defender-for-identity/configure-kerberos-delegation

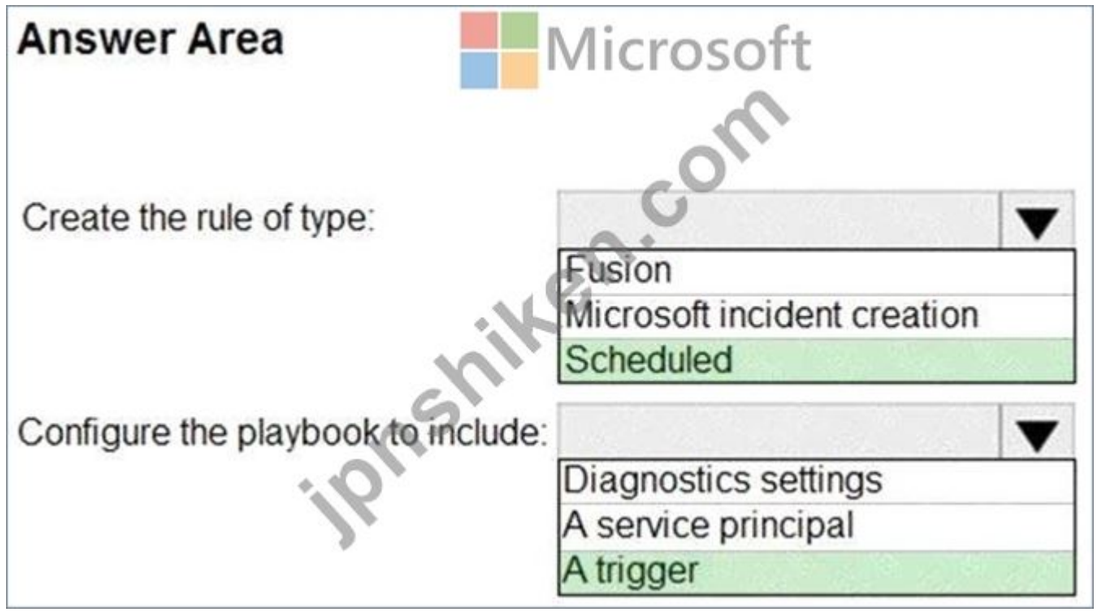
質問: **75**
Azure Sentinelの要件を満たすには、分析ルールを作成する必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。



正解:



Explanation:



質問: 76

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。

このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。

Azure Security Center 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信します。

セキュリティセンターで、アラートを解決するための推奨事項を確認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、「アクションを実行する」を選択してから、「今後の攻撃を防止する」セクションを展開します。

これは目標を達成していると言えるでしょうか？

A. はい

B. いいえ

正解**: (**正解を表示します**)**

セクション: [なし]

Explanation:

必要なのは、既存のアラートを解決することであり、将来のアラートを防止することではありません。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

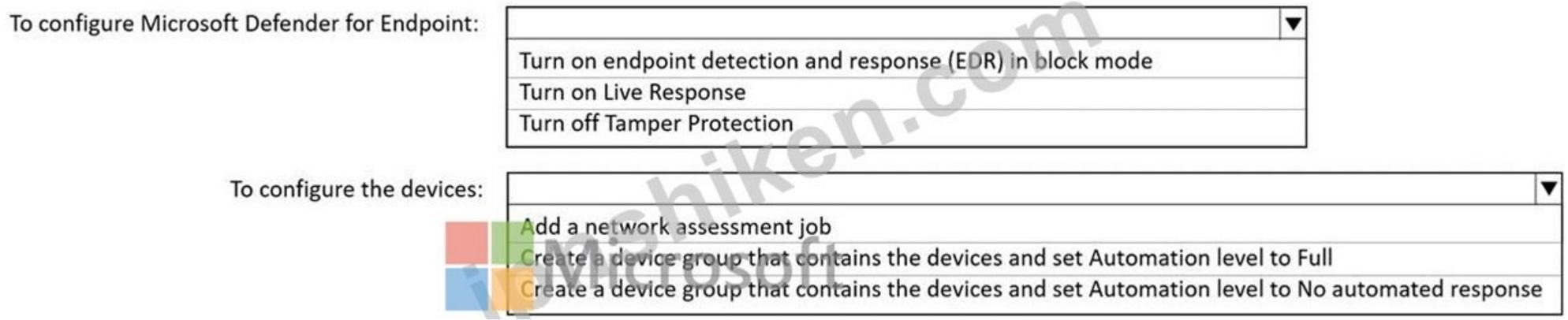
質問: **77**

お客様は、Microsoft Defender for Endpointに登録された200台のWindows 10デバイスを含むMicrosoft 365 E5サブスクリプションをご利用中です。

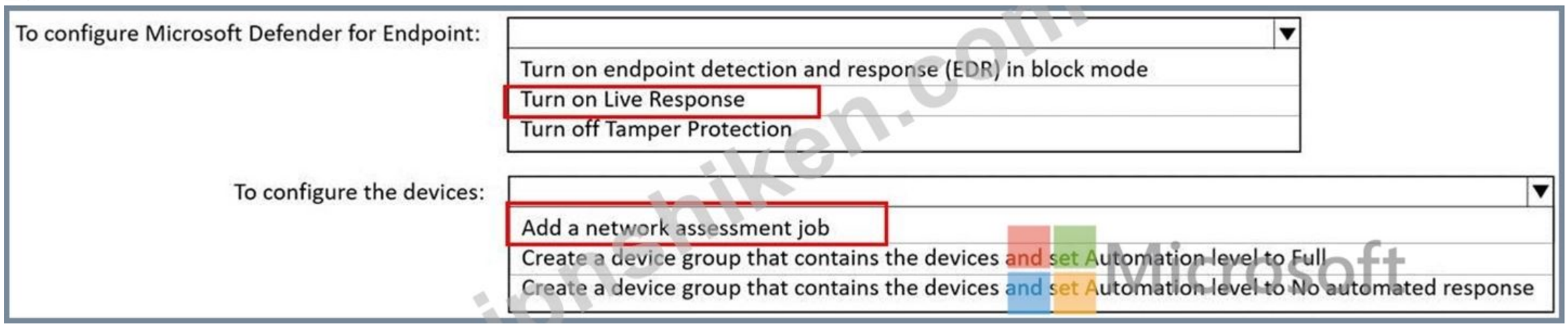
ユーザーがMicrosoft 365 Defenderポータルから直接リモートシェル接続を使用してデバイスにアクセスできることを確認する必要があります。このソリューションは、最小権限の原則に従う必要があります。

Microsoft 365 Defender ポータルで何をすべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。



正解:



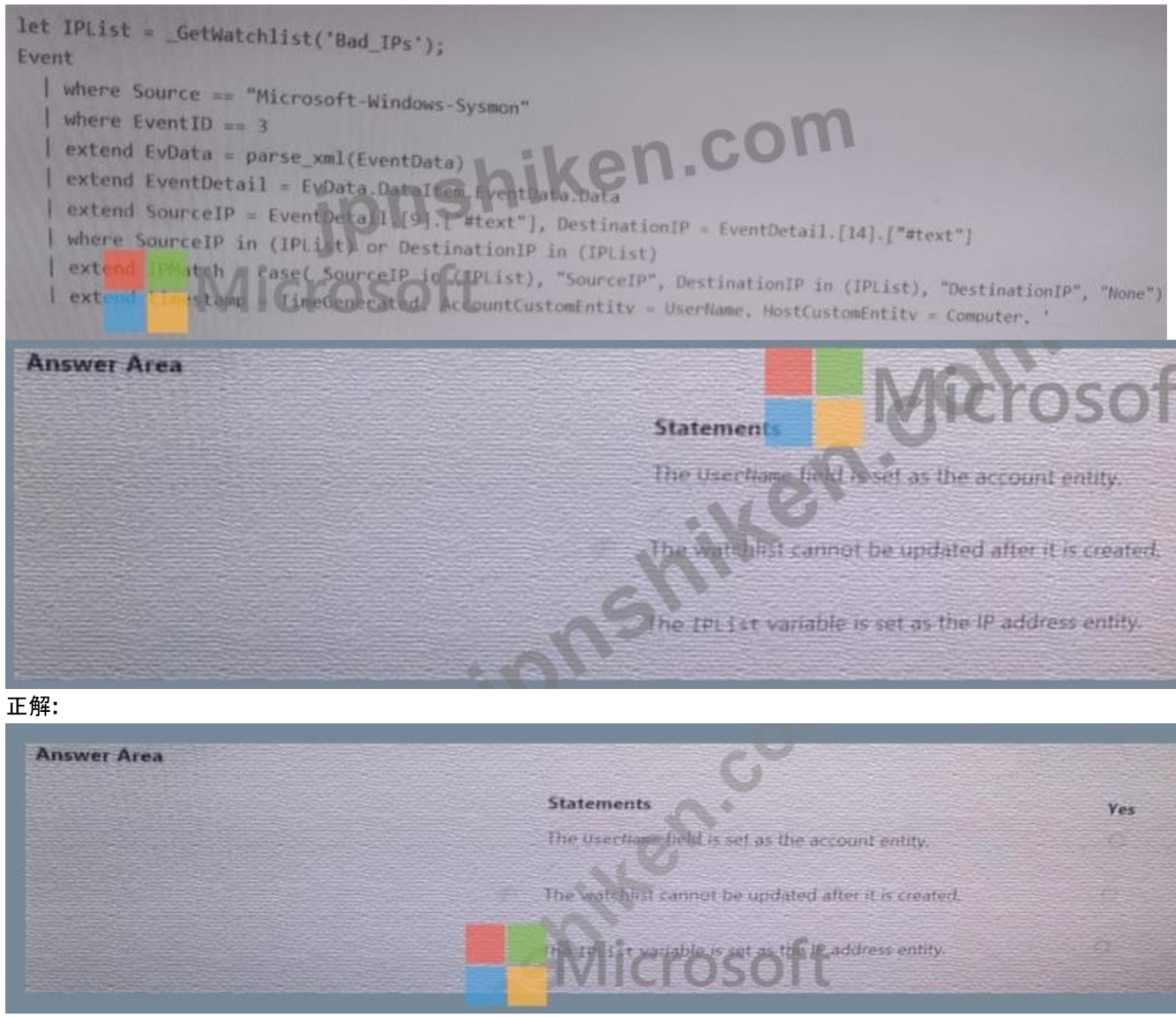
参照：

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldwide

質問: **78**

以下のSQLクエリがあります。



正解:

Explanation:

質問: **79**

お客様は、Userl という名前のクエストユーザーと workspacel という名前の Microsoft Sentinel ワークスペースを含む Azure サブスクリプションをお持ちです。
User1がworkspace1でMicrosoft Sentinelのインシデントをトリアージできるようにする必要があります。このソリューションは、最小権限の原則に基づいている必要があります。
User1にはどの役割を割り当てるべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

正解:

Answer Area

質問: 80

注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。
このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。
お客様は、Microsoft Defender XDR を使用する Azure サブスクリプションをご利用されています。
Microsoft Defender ポータルから監査検索を実行し、結果を File1.csv という名前のファイルとしてエクスポートします。このファイルには 10,000 行のデータが含まれます。
Microsoft Excelを使用して、File1.csvからAuditData列を解析するために、データの取得と変換操作を実行します。しかし、これらの操作では、特定のJSONプロパティに対応する列が生成されません。
監査検索結果において、Excelが特定のJSONプロパティに対応する列を生成するようにする必要があります。
解決策 :Defenderで監査検索の検索条件を変更して返されるレコード数を減らし、結果をエクスポートします。Excelで、新しいエクスポート機能を使用して データの取得と変換」操作を実行します。
これは要件を満たしていますか？

A. はい
B. いいえ

正解: **A** (コメントを発表する)

質問: **81**

Microsoft Sentinelワークスペースをお持ちです。

Microsoft Defenderコネクタによって生成されたインシデントを一時的に抑制するには、Fusion Analyticsルールを構成する必要があります。このソリューションは、以下の要件を満たす必要があります。

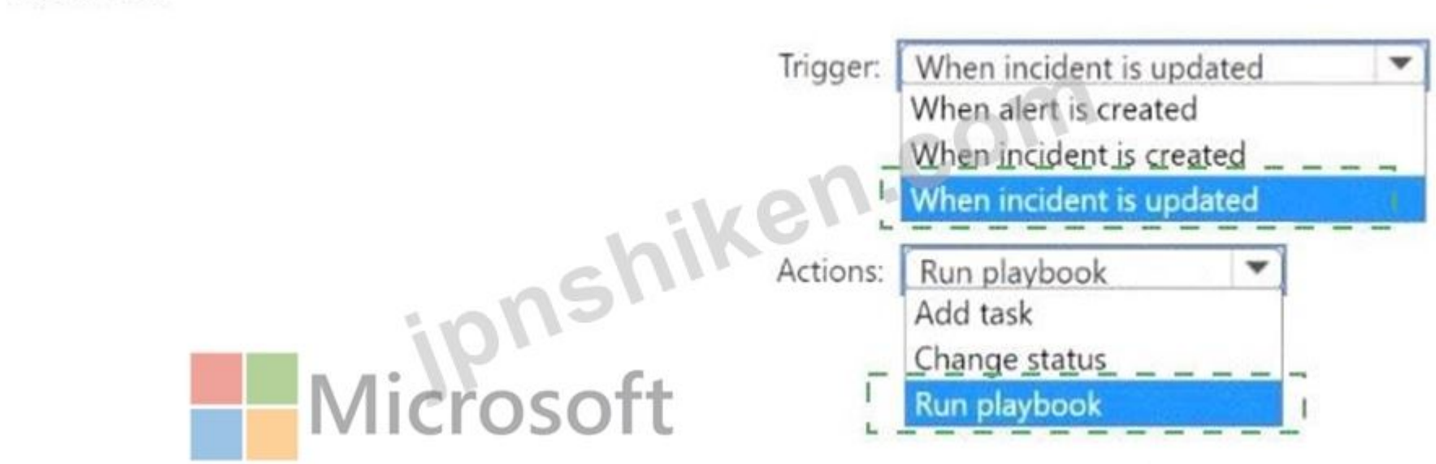
多段階攻撃の検出能力への影響を最小限に抑える。

管理業務の手間を最小限に抑える。

ルールはどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

正解:

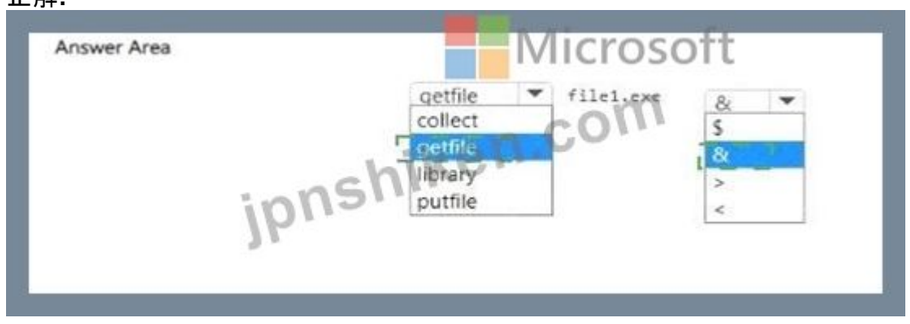


Explanation:

質問: **82**
Azure Sentinel のデータを視覚化し、サードパーティのデータソースを使用してデータを拡充することで、侵害の兆候 (IoC) を特定する必要があります。
何を使うべきでしょうか？
A. Azure Sentinel のノートブック
B. Microsoft Cloud App Security
C. Azure Monitor
D. Azure Sentinel でのクエリの探索
正解: **(正解を表示します)**
セクション: [なし]
説明／参考資料：
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

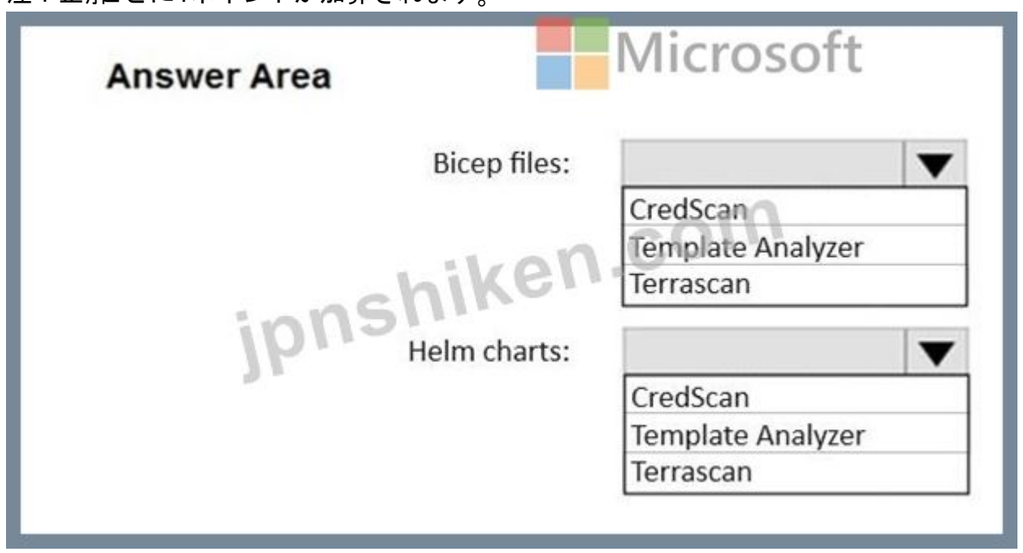
質問: **83**
お客様は、Microsoft Defender for Endpoint Plan 2 を使用する Microsoft 365 サブスクリプションをご利用で、その中に Device! という名前の Windows デバイスが含まれています。
デバイス1でライブレスポンスセッションを開始しました。
ライブレスポンスライブラリからFile!.exeという名前の250MBのファイルをDevice1にダウンロードするコマンドを実行する必要があります。このソリューションでは、Filel.exeがバックグラウンドプロセスとしてダウンロードされるようにする必要があります。
ライブ応答コマンドはどのように完了すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

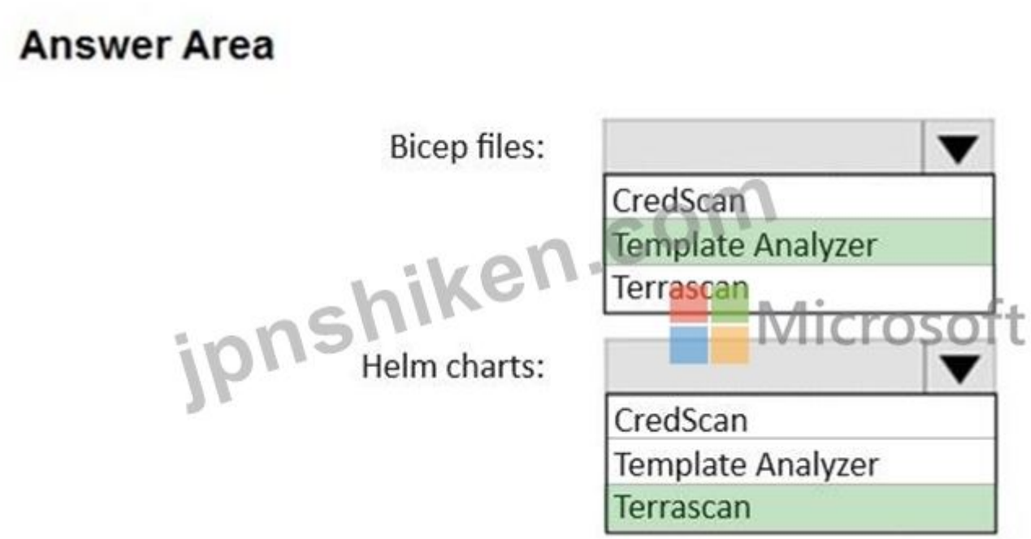


Explanation:

質問: **84**
ホットスポットに関する質問
Azure DevOps 組織があり、その中に Repo1 という名前の Azure Repos リポジトリがあり、Microsoft Defender for DevOps にオンボーディングされています。
インフラストラクチャ・アズ・コード（IaC）ファイルを作成し、Repo1に保存します。IaCファイルは、BicepファイルとHelmチャートの形式で作成されます。
IaCファイル内の設定ミスを特定するには、Defender for DevOpsを設定する必要があります。
ファイルの種類ごとに、どのスキャンツールを使用すべきでしょうか？回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:



質問: **85**
Microsoft Sentinelの要件を満たすには、どのルール設定を構成すればよいですか？
A. セットルールロジックから、抑制をオフにします。

B. 分析ルールの詳細から、戦術を設定します。
C. セットルールロジックからエンティティをマッピングします。
D. 分析ルールの詳細から、重要度を設定します。
正解: **(**正解を表示します**)**
Microsoft Sentinel では、エンティティ マッピングは、検出されたイベントとアラートが調査グラフ、インシデント、およびハンティング エクスペリエンスに正しく反映されることを保証する重要な構成です。ケース スタディの Sentinel 要件は次のとおりです。
「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することで、調査グラフをナビゲートしながらインシデントハンティングを行う際に、そのIPアドレスを参照できるようになります。」この要件を満たすには、分析ルールを 「ルールロジックの設定」セクションで、IPアドレス、ユーザー、ホスト名、URLなどのエンティティをマッピングするように構成する必要があります。このマッピングにより、インシデントとその関連アラートをこれらのエンティティと視覚的に関連付けることができ、アナリストはSentinelの調査グラフ内でピボットして調査を行うことができます。
Microsoft Sentinelのドキュメントによると：
「分析ルールにおけるエンティティマッピングは、アラートやインシデントをアカウント、IPアドレス、ホストなどの特定のエンティティと関連付けるのに役立ち、より詳細な調査と迅速なトリアージを可能にします。」したがって、エンティティマッピングをセットルールロジックの下で直接構成することで、インシデントにコンテキスト情報（特定のIPアドレスなど）が付加され、機能要件と調査要件の両方を満たすことができます。
質問 2 の最終回答: C. セットルールロジックからエンティティをマッピングします。
トピック1、Litware社
事例研究
これはケーススタディです。ケーススタディには個別の時間制限はありません。各ケースを完了するために、試験時間を自由に使うことができます。ただし、この試験には追加のケーススタディやセクションが含まれる場合があります。与えられた時間内に試験に含まれるすべての問題を完了できるよう、時間配分をしっかり行う必要があります。
ケーススタディに含まれる質問に答えるには、ケーススタディに記載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図表やその他の資料が含まれている場合があります。各質問は、このケーススタディ内の他の質問とは独立しています。
このケーススタディの最後に、確認画面が表示されます。この画面では、解答を確認し、次のセクションに進む前に修正することができます。新しいセクションを開始すると、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てください。質問に答える前に、左側のペインにあるボタンを使ってケーススタディの内容を確認してください。これらのボタンをクリックすると、ビジネス要件、既存環境、問題記述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、そこに表示される情報は以降のタブに表示される情報と同一です。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ってください。
概要
Litware Inc.は再生可能エネルギー企業です。
Litwareはボストンとシアトルにオフィスを構えています。また、米国各地にリモートユーザーがいます。リモートユーザーは、クラウドサービスを含むLitwareのリソースにアクセスするために、いずれかのオフィスとVPN接続を確立します。
既存の環境
アイデンティティ環境
このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントと同期します。
Microsoft 365環境
Litwareは、litware.comのAzure ADテナントにリンクされたMicrosoft 365 E5サブスクリプションを保有しています。Windows 10を実行しているすべてのコンピューターにMicrosoft Defender for Endpointが展開されています。Microsoft Cloud App Securityに組み込まれている異常検出ポリシーはすべて有効になっています。
Azure環境
Litwareは、litware.com Azure ADテナントにリンクされたAzureサブスクリプションを保有しています。このサブスクリプションには、以下の表に示すように、米国東部Azureリージョン内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

Litwareの各オフィスはインターネットに直接接続されており、Azureサブスクリプション内の仮想ネットワークへのサイト間VPN接続も確立されています。

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

現在の問題点

クラウドアプリセキュリティは、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。

計画されている変更

Litwareは以下の変更を実施する予定です。

* Azure サブスクリプションに Azure Sentinel を作成および構成します。
* Azure ADのテストユーザーアカウントを使用して、Azure Sentinelの機能を検証します。

ビジネス要件

Litwareは、以下のビジネス要件を特定しました。

可能な限り、最小権限の原則を適用しなければならない。
* 他のすべての要件を満たしている限り、コストは最小限に抑えなければならない。
* Log Analyticsによって収集されるログは、ユーザーアクティビティの完全な監査証跡を提供する必要があります。
* すべてのドメインコントローラーは、Microsoft Defender for Identityを使用して保護する必要があります。

Azure の情報保護要件

セキュリティラベルが付与され、Windows 10 コンピューターに保存されているすべてのファイルは、Azure Information Protection - データ検出ダッシュボードからアクセスできる必要があります。

Microsoft Defender for Endpoint の要件

Windows 10 コンピューターでは、Microsoft Defender for Endpoint を使用して、Cloud App Security によって承認されていないすべてのアプリをブロックする必要があります。

Microsoft Cloud Appのセキュリティ要件

クラウドアプリセキュリティは、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かどうかを識別する必要があります。

Azure Defender の要件

すべてのサーバーは、同じログ分析ワークスペースにログを送信する必要があります。

Azure Sentinel の要件

Litwareは、以下のAzure Sentinelの要件を満たす必要があります。

* Azure SentinelとCloud App Securityを統合する。
* admin1 という名前のユーザーが Azure Sentinel プレイブックを構成できることを確認してください。
* カスタムクエリに基づいて Azure Sentinel 分析ルールを作成します。このルールは、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、調査グラフをナビゲートする際にIPアドレスを参照できるようにします。
* Azure ADテストユーザーアカウントによる Microsoft Office 365への受信アクセスが検出された場合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るアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。

質問: **86**

以下のKQLクエリを含むカスタム検出ルールがあります。

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

以下の各項目について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	○

正解:

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	○

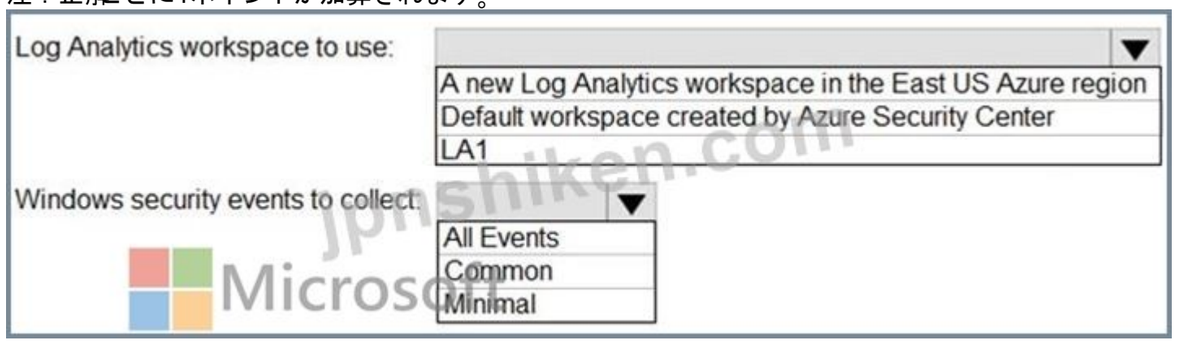
Explanation:

質問: **87**

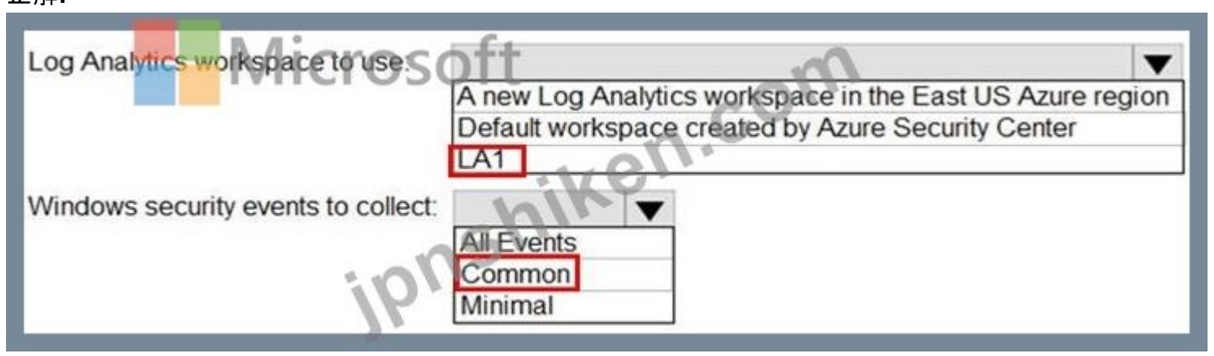
Azure Defenderの要件とビジネス要件を満たすためには、Azure Defenderを実装する必要があります。

解答には何を含めるべきでしょうか？回答するには、回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。



正解:



質問: **88**

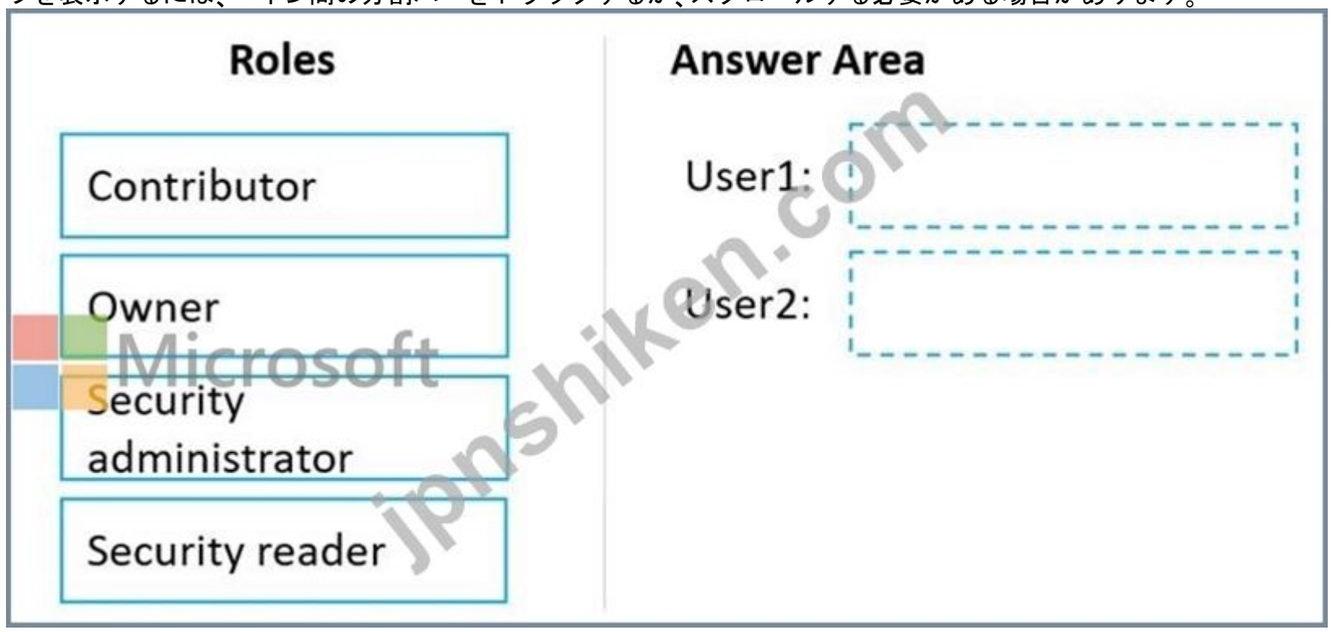
Azure Active Directory (Azure AD) テナントにリンクされた Azure サブスクリプションがあります。このテナントには、User1 と User2 という名前の 2 人のユーザーがいます。

Azure Defender をデプロイする予定です。

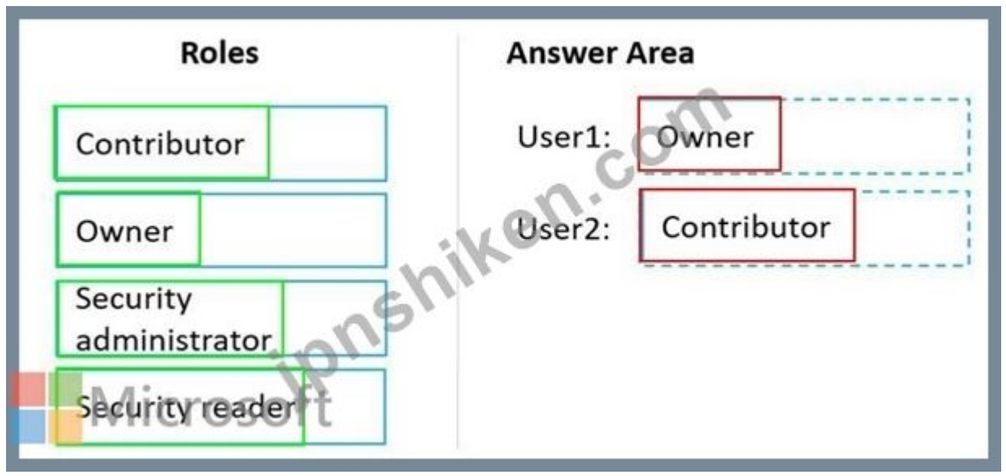
以下の表に示すように、User1とUser2がサブスクリプションレベルでタスクを実行できるようにする必要があります。

User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

解決策は、最小権限の原則に基づかなければならない。
各ユーザーにどの役割を割り当てるべきでしょうか？回答するには、適切な役割を正しいユーザーにドラッグしてください。各役割は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の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。



正解:



参照：
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

質問: **89**
あなたはAzureサブスクリプションをお持ちです。
以下の要件を満たすためには、権限を委任する必要があります。
* Microsoft Defender for Cloud の高度な機能を有効化および無効化します。
* リソースにセキュリティに関する推奨事項を適用する。
解決策は、最小権限の原則に基づかなければならない。
各要件に対して、どの Microsoft Defender for Cloud ロールを使用すべきでしょうか？回答するには、適切なロールを該当する要件にドラッグしてください。各ロールは、1 回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の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：正解ごとに1ポイントが加算されます。

正解:

Explanation:

質問: 90

Azure Sentinel の要件を満たすテスト ルールを作成する必要があります。ルールを作成する際に、どのような手順を踏むべきですか？

A. セットルールロジックから、抑制をオフにします。

B. アナリティクスルールの詳細から、戦術を設定します。

C. セットルールロジックからエンティティをマッピングします。

D. アナリティクスルールの詳細から、重要度を設定します。

正解: **(**正解を表示します**)**

参照：

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

トピック1、Litware社

概要

これはケーススタディです。ケーススタディには個別の時間制限はありません。各ケースを完了するために、試験時間を自由に使うことができます。ただし、この試験には追加のケーススタディやセクションが含まれる場合があります。与えられた時間内に試験に含まれるすべての問題を完了できるよう、時間配分をしっかり行う必要があります。

ケーススタディに含まれる質問に答えるには、ケーススタディに記載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図表やその他の資料が含まれている場合があります。各質問は、このケーススタディ内の他の質問とは独立しています。

このケーススタディの最後に、確認画面が表示されます。この画面では、解答を確認し、次のセクションに進む前に修正することができます。新しいセクションを開始すると、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てください。質問に答える前に、左側のペインにあるボタンを使ってケーススタディの内容を確認してください。これらのボタンをクリックすると、ビジネス要件、既存環境、問題記述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、そこに表示される情報は以降のタブに表示される情報と同一で

す。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ってください。
概要
Litware Inc.は再生可能エネルギー企業です。
Litwareはボストンとシアトルにオフィスを構えています。また、米国各地にリモートユーザーがいます。リモートユーザーは、クラウドサービスを含むLitwareのリソースにアクセスするために、いずれかのオフィスとVPN接続を確立します。
既存の環境
アイデンティティ環境
このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントと同期します。
Microsoft 365環境
Litwareは、litware.comのAzure ADテナントにリンクされたMicrosoft 365 E5サブスクリプションを保有しています。Windows 10を実行しているすべてのコンピューターにMicrosoft Defender for Endpointが展開されています。Microsoft Cloud App Securityに組み込まれている異常検出ポリシーはすべて有効になっています。
Azure環境
Litwareは、litware.com Azure ADテナントにリンクされたAzureサブスクリプションを保有しています。このサブスクリプションには、以下の表に示すように、米国東部Azureリージョン内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

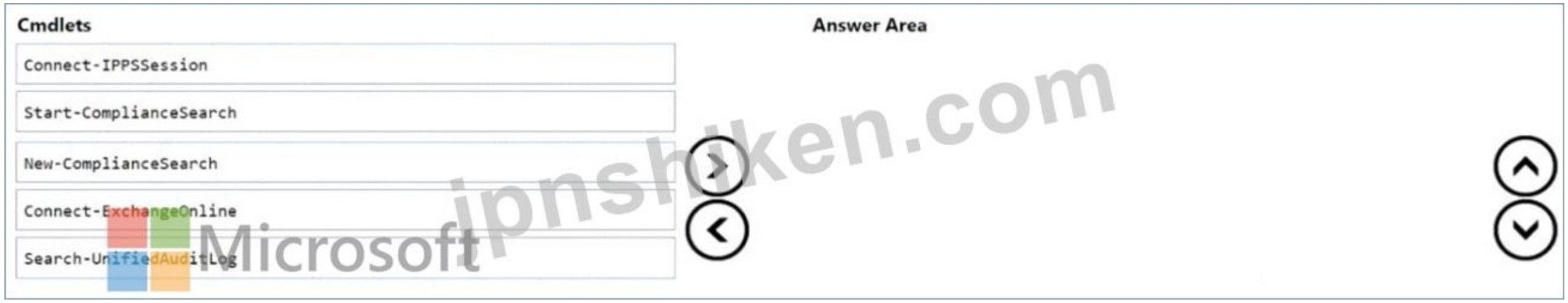
ネットワーク環境
Litwareの各オフィスはインターネットに直接接続されており、Azureサブスクリプション内の仮想ネットワークへのサイト間VPN接続も確立されています。
オンプレミス環境
オンプレミスネットワークには、次の表に示すコンピュータが含まれています。

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

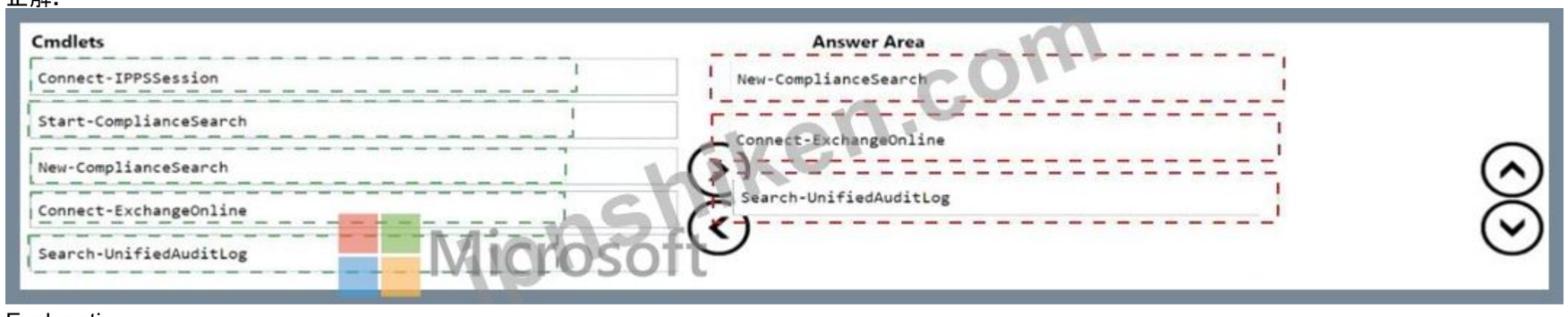
現在の問題点
クラウドアプリセキュリティは、ユーザーが両方のオフィスに同時に接続すると、誤検知アラートを頻繁に生成します。
計画されている変更
Litwareは以下の変更を実施する予定です。
Azure サブスクリプションに Azure Sentinel を作成および構成します。
Azure ADのテストユーザーアカウントを使用して、Azure Sentinelの機能を検証します。
ビジネス要件
Litwareは、以下のビジネス要件を特定しました。
Azure の情報保護要件
セキュリティラベルが付与され、Windows 10 コンピューターに保存されているすべてのファイルは、Azure Information Protection - データ検出ダッシュボードからアクセスできる必要があります。
Microsoft Defender for Endpoint の要件
Windows 10 コンピューターでは、Microsoft Defender for Endpoint を使用して、Cloud App Security によって承認されていないすべてのアプリをブロックする必要があります。
Microsoft Cloud Appのセキュリティ要件
クラウドアプリセキュリティは、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かどうかを識別する必要があります。
Azure Defender の要件

すべてのサーバーは、同じログ分析ワークスペースにログを送信する必要があります。
Azure Sentinel の要件
Litwareは、以下のAzure Sentinelの要件を満たす必要があります。
Azure SentinelとCloud App Securityを統合する。
admin1という名前のユーザーがAzure Sentinelプレイブックを構成できることを確認してください。
カスタムクエリに基づいてAzure Sentinel分析ルールを作成します。このルールは、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することで、調査グラフをナビゲートする際にIPアドレスを参照できるようになります。
Azure ADテストユーザーアカウントによるMicrosoft Office 365への受信アクセスが検出された場合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るアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。

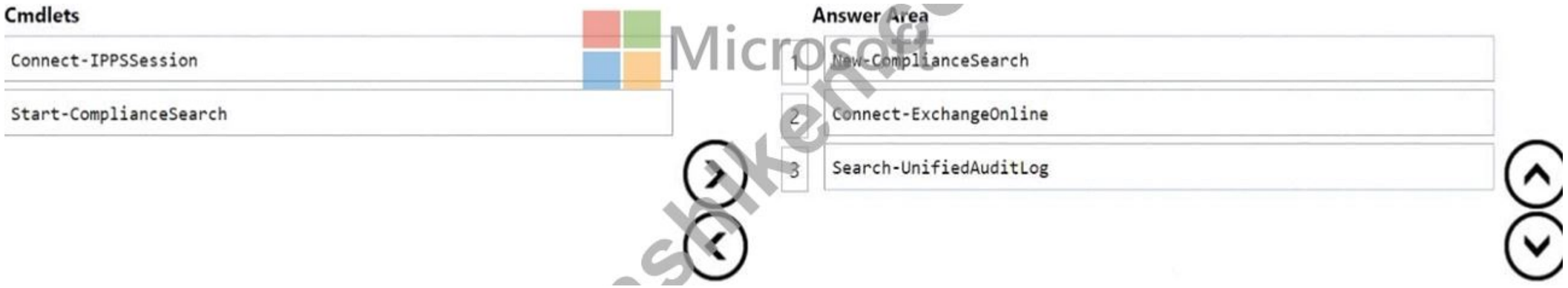
質問: **91**
お客様は、Microsoft Exchange Onlineを使用するMicrosoft 365 E5サブスクリプションをお持ちです。
フィッシングメールを識別する必要があります。
どの 3 つのコマンドレットを順番に実行する必要がありますか？回答するには、コマンドレットの一覧から適切なコマンドレットを回答欄に移動し、正しい順序に並べ替えてください。



正解:



Explanation:



質問: **92**
注 :この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。
このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。
Azure Security Center 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信します。
セキュリティセンターで、アラートを解決するための推奨事項を確認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、 アクションを実行する」を選択してから、 脅威を軽減する」セクションを展開します。
これは目標を達成していると言えるでしょうか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
説明／参考資料：
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts Azure Sentinel を使用して脅威を軽減する テストレット 1 ケーススタディ これはケーススタディです。ケーススタディには個別の時間制限はありません。各ケースを完了するために、必要なだけ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やセクションが含まれている場合があります。試験に含まれるすべての質問を、与えられた時間内に完了できるように、時間管理を行う必要があります。
ケーススタディに含まれる質問に答えるには、ケーススタディに記載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図表やその他の資料が含まれている場合があります。各質問は、このケーススタディ内の他の質問とは独立しています。
このケーススタディの最後に、確認画面が表示されます。この画面では、解答を確認し、次のセクションに進む前に修正することができます。新しいセクションを開始すると、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てください。質問に答える前に、左側のペインにあるボタンを使ってケーススタディの内容を確認してください。これらのボタンをクリックすると、ビジネス要件、既存環境、問題記述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、そこに表示される情報は以降のタブに表示される情報と同一で

す。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ってください。
概要
Litware Inc.は再生可能エネルギー企業です。
Litwareはボストンとシアトルにオフィスを構えています。また、米国各地にリモートユーザーがいます。リモートユーザーは、クラウドサービスを含むLitwareのリソースにアクセスするために、いずれかのオフィスとVPN接続を確立します。
既存の環境
アイデンティティ環境
このネットワークには、litware.com という名前の Active Directory フォレストが含まれており、それが litware.com という名前の Azure Active Directory (Azure AD) テナントと同期します。
Microsoft 365環境
Litwareは、litware.comのAzure ADテナントにリンクされたMicrosoft 365 E5サブスクリプションを保有しています。Windows 10を実行しているすべてのコンピューターにMicrosoft Defender for Endpointが展開されています。Microsoft Cloud App Securityに組み込まれている異常検出ポリシーはすべて有効になっています。
Azure環境
Litwareは、litware.com Azure ADテナントにリンクされたAzureサブスクリプションを保有しています。このサブスクリプションには、以下の表に示すように、米国東部Azureリージョン内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
Litwareの各オフィスはインターネットに直接接続されており、Azureサブスクリプション内の仮想ネットワークへのサイト間VPN接続も確立されています。
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

現在の問題点
クラウドアプリセキュリティは、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。
計画されている変更
Litwareは以下の変更を実施する予定です。
* Azure サブスクリプションに Azure Sentinel を作成および構成します。
* Azure ADのテストユーザーアカウントを使用して、Azure Sentinelの機能を検証します。
ビジネス要件
Litwareは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則を適用しなければならない。
* 他のすべての要件を満たしている限り、コストは最小限に抑えなければならない。
* Log Analyticsによって収集されるログは、ユーザーアクティビティの完全な監査証跡を提供する必要があります。
* すべてのドメインコントローラーは、Microsoft Defender for Identityを使用して保護する必要があります。
Azure の情報保護要件
セキュリティラベルが付与され、Windows 10 コンピューターに保存されているすべてのファイルは、Azure Information Protection - データ検出ダッシュボードからアクセスできる必要があります。
Microsoft Defender for Endpoint の要件

Windows 10 コンピューターでは、Microsoft Defender for Endpoint を使用して、Cloud App Security によって承認されていないすべてのアプリをブロックする必要があります。
Microsoft Cloud Appのセキュリティ要件
クラウドアプリセキュリティは、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かどうかを識別する必要があります。
Azure Defender の要件
すべてのサーバーは、同じログ分析ワークスペースにログを送信する必要があります。
Azure Sentinel の要件
Litwareは、以下のAzure Sentinelの要件を満たす必要があります。
* Azure SentinelとCloud App Securityを統合する。
* admin1 という名前のユーザーが Azure Sentinel プレイブックを構成できることを確認してください。
* カスタムクエリに基づいて Azure Sentinel 分析ルールを作成します。このルールは、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、調査グラフをナビゲートする際にIPアドレスを参照できるようにします。
* Azure ADテストユーザーアカウントによるMicrosoft Office 365への受信アクセスが検出された場合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るアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。

質問: **93**
以下のKQLクエリを含むカスタム検出ルールがあります。

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId, EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId, RecipientEmailAddress, EntityType, DeviceId, SHA256
```

以下の各項目について、該当する場合は「はい」を選択してください。該当しない場合は「いいえ」を選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	○

正解:

質問: **94**

Microsoft Defender for Endpoint Plan 2 を使用する Microsoft 365 サブスクリプションがあり、その中に Device 1 という名前の Windows デバイスが含まれています。Device1 でライブレスポンスセッションを開始し、File1.exe という名前の実行可能ファイルをバックグラウンドで起動します。次の操作を実行する必要があります。

* File1 exe のコマンド ID を特定します。
* InteractwithFile1.exe。

各アクションに対して、どのライブレスポンスコマンドを実行すべきですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

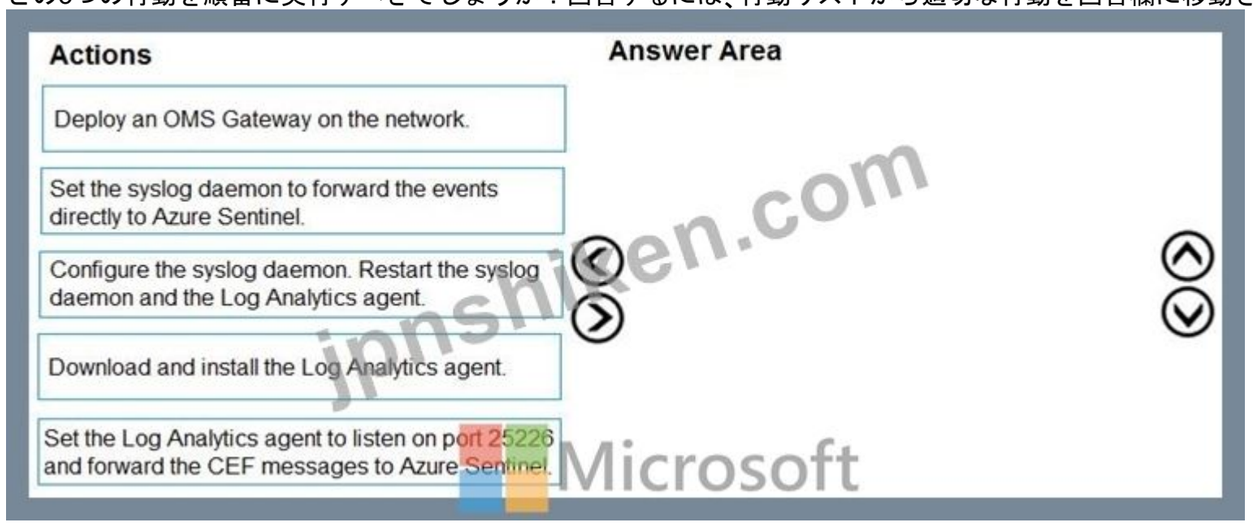
正解:

Explanation:

Microsoft Defender for Endpoint (MDE) Live Response では、セキュリティアナリストはデバイスにリモート接続してフォレンジックコマンドを実行できます。ライブレスポンスセッション中に実行コマ

ンド (例: run File1.exe -background) を使用して実行可能ファイルがバックグラウンドで起動されると、そのコマンドに関連付けられたジョブが作成されます。
バックグラウンドプロセスのコマンドIDを特定するには、jobsコマンドを使用します。jobsコマンドは、ライブレスポンスセッション中に開始された、現在実行中または完了済みのすべてのバックグラウンドジョブを一覧表示します。各ジョブエントリには、ジョブID、実行されたコマンド、現在のステータスなどの詳細が含まれます。これにより、アナリストはFile1.exeとその関連コマンドIDに対応するプロセスを判断できます。
バックグラウンドプロセスが特定されたら、fg（フォアグラウンド）コマンドを使用してFile1.exeと対話できます。fgコマンドは、バックグラウンドジョブをフォアグラウンドに表示するために使用され、入力の送信、出力の監視、ジョブの終了など、ジョブと直接対話できるようになります。
この手順は、Microsoft Defender for Endpoint のドキュメントに準拠しており、以下の内容が規定されています。
* ジョブを使用して、バックグラウンドジョブを表示または管理します。
* 特定のバックグラウンドプロセスとやり取りするには、fg <JobID> を使用します。
したがって、正解は以下のとおりです。
* File1.exeのコマンドIDを特定します: jobs
* File1.exe と対話する: fg

質問: **95**
共通イベントフォーマット（CEF）メッセージをAzure Sentinelに送信する外部ソリューションを接続する予定です。
ログフォワーダーをデプロイする必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



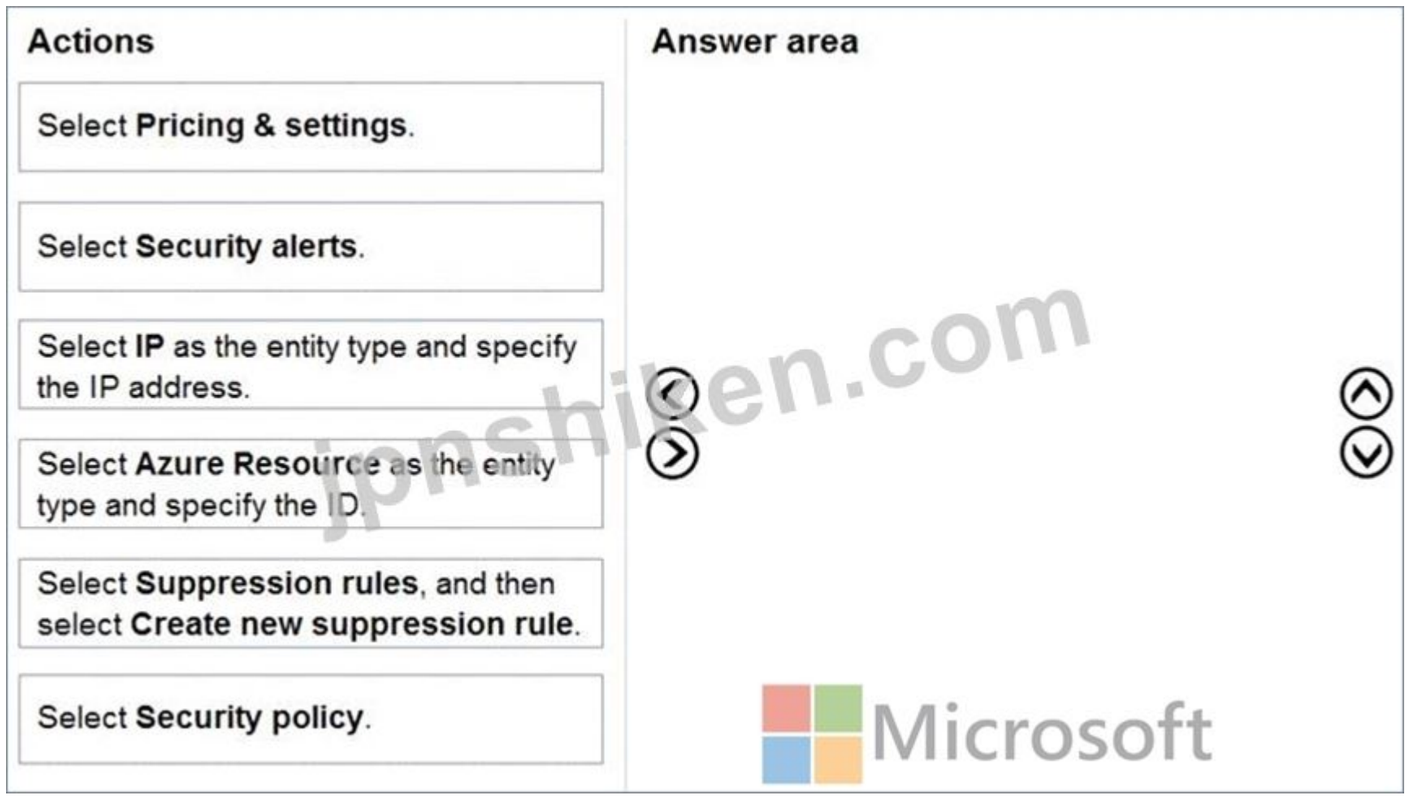
正解:

Answer Area

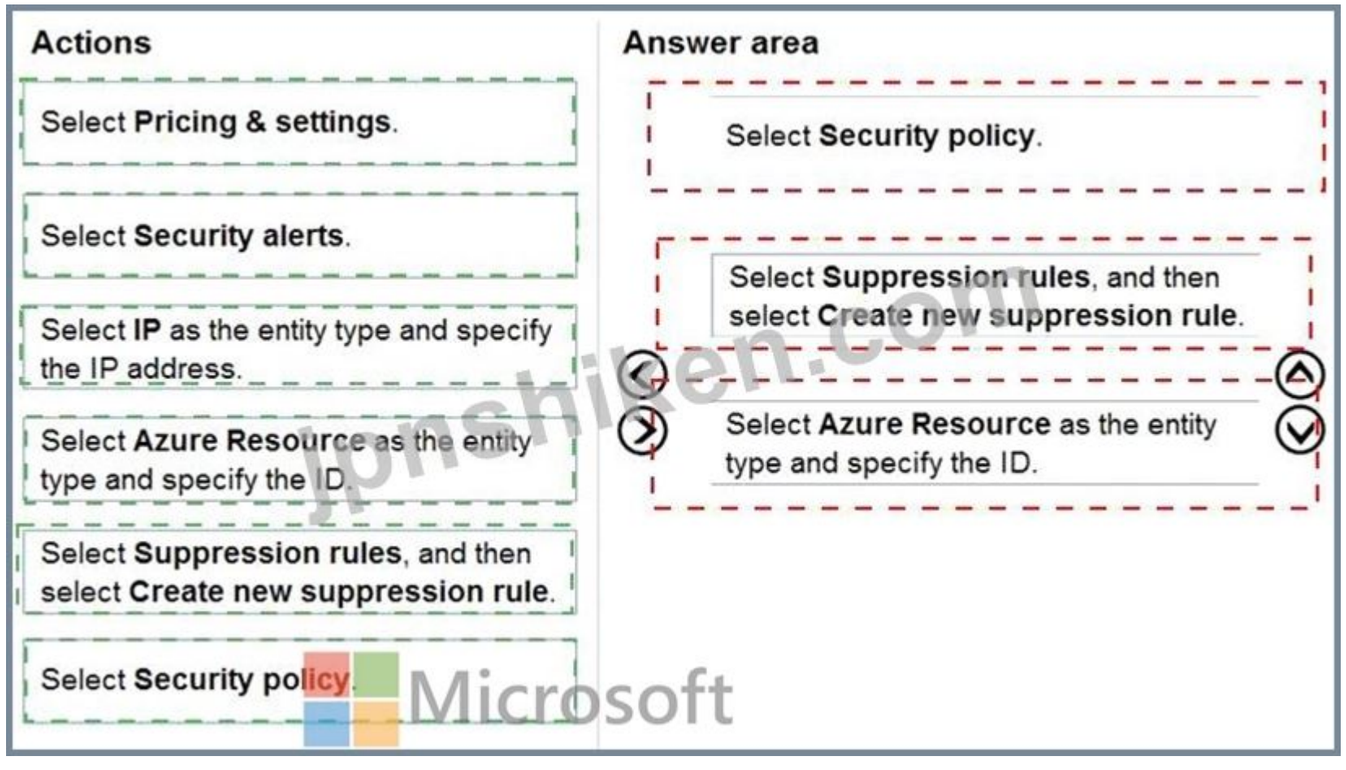
Download and install the Log Analytics agent.
Set the Log Analytics agent to listen on port 25226 and forward the CEF messages to Azure Sentinel.
Configure the syslog deamon. Restart syslog deamon and the Log Analytics agent.

1. Log Analytics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でリッスンし、CEFメッセージをAzure Sentinelに転送するように設定します。
3 - syslogデーモンを設定します。syslogデーモンとLog Analytics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: **96**
Azure Functions アプリがあり、通常の活動に対して毎日数千件のアラートが Azure Security Center に生成されます。
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、どの3つの操作を順番に実行すべきでしょうか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。


Actions
Select Pricing & settings.
Select Security alerts.
Select IP as the entity type and specify the IP address.
Select Azure Resource as the entity type and specify the ID.
Select Suppression rules, and then select Create new suppression rule.
Select Security policy.
Answer area
Microsoft

正解:


Actions
Select Pricing & settings.
Select Security alerts.
Select IP as the entity type and specify the IP address.
Select Azure Resource as the entity type and specify the ID.
Select Suppression rules, and then select Create new suppression rule.
Select Security policy.
Answer area
Select Security policy.
Select Suppression rules, and then select Create new suppression rule.
Select Azure Resource as the entity type and specify the ID.
Microsoft

説明

Select **Security policy**.

Select **Suppression rules**, and then select **Create new suppression rule**.

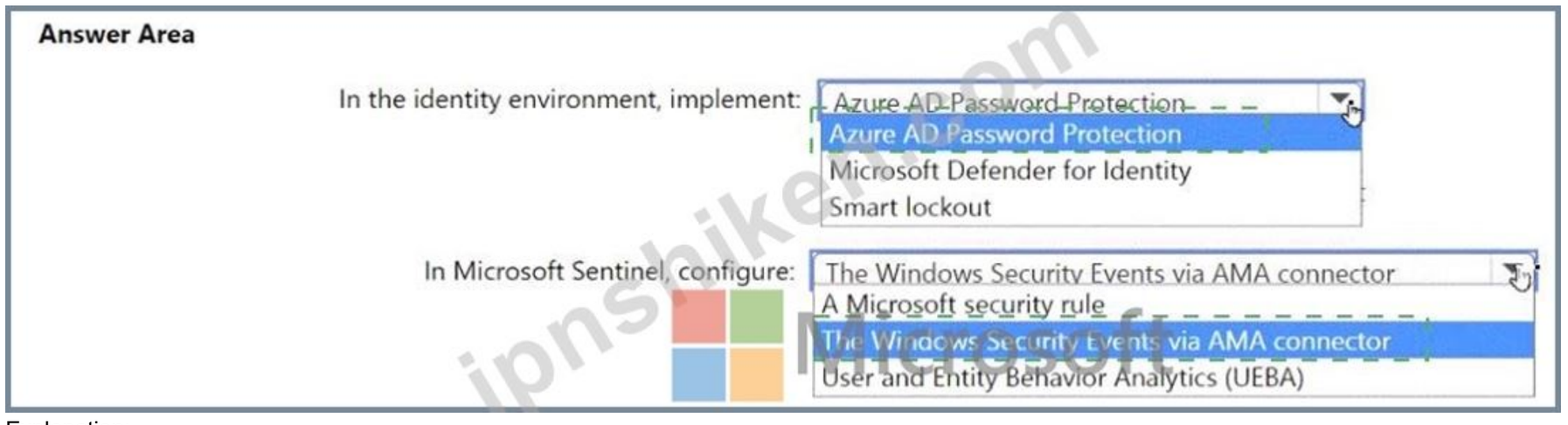
Select **Azure Resource** as the entity type and specify the ID.

参照：
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-

質問: **97**
パスワードのリセットを監視する必要があります。ソリューションは、Microsoft Sentinelの要件を満たしている必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

Answer Area

正解:



Explanation:

Answer Area

In the identity environment, implement: Azure AD Password Protection

In Microsoft Sentinel, configure: The Windows Security Events via AMA connector

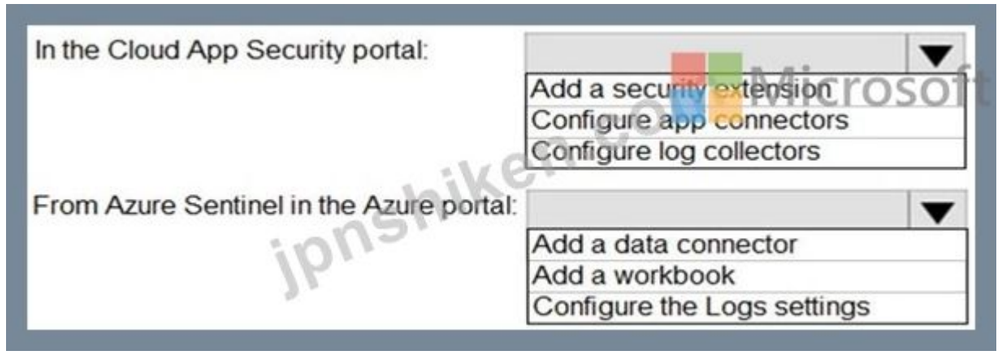
トピック4、その他の質問
ファブリカム社は金融サービス会社です。
同社はニューヨーク、ロンドン、シンガポールに支社を構えている。Fabrikamには世界中にリモートユーザーがおり、これらのユーザーはVPN接続を介して支社にアクセスすることで、クラウドサービスを含む社内リソースにアクセスする。
このネットワークには、fabrikam.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれており、fabrikam.com という名前の Azure AD テナントと同期しています。フォレストを同期するために、Fabrikam はパススルー認証を有効にし、パスワード ハッシュ同期を無効にした Azure AD Connect を使用しています。
fabrikam.comのフォレストには、Group1とGroup2という2つのグローバルグループが含まれています。
Fabrikamの全ユーザーには、Microsoft 365 E5ライセンスとAzure Active Directory Premium Plan 2ライセンスが割り当てられています。Fabrikamは、Microsoft Defender for IdentityとMicrosoft Defender for Cloud Appsを導入し、ログコレクターを有効にしています。
Fabrikamは、以下の表に示すリソースを含むAzureサブスクリプションを保有しています。

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

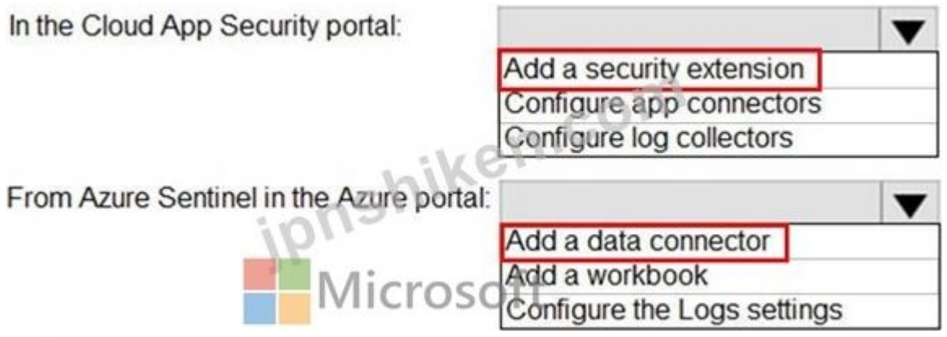
Fabrikamは、Account1という名前のAmazon Web Services（AWS）アカウントを所有しています。Account1には、カスタムWindows Server 2022を実行する100個のAmazon Elastic Compute Cloud（EC2）インスタンスが含まれています。このイメージにはMicrosoft SQL Server 2019が含まれていますが、エージェントはインストールされていません。
ユーザーが VPN 接続を使用すると、Microsoft 365 Defender は、誤検知である「あり得ない旅行」アラートを大量に発生させます。また、Defender for Identity は、誤検知である「疑わしい DCSync 攻撃」アラートを大量に発生させます。
Fabrikamは以下のサービスを導入する予定です。
* Microsoft Defender for Cloud
* マイクロソフトセンチネル
Fabrikamは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則を適用する。
管理業務の手間を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloud Appsの要件として以下の点を挙げています。
* 渡航不可能な場合の警告ポリシーは、各ユーザーの過去の活動に基づいていることを確認してください。
* 誤検知による、あり得ない旅行に関する警告の数を減らす。
誤検知アラートの調査に必要な管理上の労力を最小限に抑える。
Fabrikamは、Microsoft Defender for Cloudに関して以下の要件を特定しました。
* グループ2のメンバーがセキュリティポリシーを変更できることを確認してください。
* Group1のメンバーがAzureサブスクリプションレベルで規制遵守ポリシーのイニシアチブを割り当てられるようにします。

* Azure Arc対応サーバー向けAzure Connected Machineエージェントのデプロイを、Account1の既存および将来のリソースに自動化します。
誤検知アラートの調査に必要な管理作業を最小限に抑える。
Fabrikamは、Microsoft Sentinelに関する以下の要件を特定しました。
* 組み込みの高度セキュリティ情報モデル（ASIM）統合パーサーを使用して、過去7日間のNXDOMAIN DNSリクエストを照会します。
* AWS EC2インスタンスから、ローカルグループメンバーシップの変更を含むWindowsセキュリティイベントログエントリを収集します。
* ユーザーおよびエンティティ行動分析（UEBA）を使用して、Azure ADユーザーの異常なアクティビティを特定します。
* UEBAを使用して、侵害されたAzure ADユーザー認証情報の潜在的な影響を評価します。
* App1がMicrosoft Sentinelの自動化ルールで使用できることを確認してください。
* 過去30日間に発生したインシデントについて、トリアージにかかる平均時間を特定する。
* 過去30日間に発生したインシデントをクローズするまでの平均時間を特定します。
* グループ1のメンバーがプレイブックを作成および実行できることを確認する。
* グループ1のメンバーが分析ルールを管理できることを確認してください。
* Jupyterノートブックを使用して、Pool! でハンティングクエリを実行します。
* グループ2のメンバーがインシデントを管理できることを確認する。
* データクエリのパフォーマンスを最大化する。
収集するデータ量を最小限に抑える。

質問: **98**
Azure Sentinelの要件を満たすように、Azure Sentinelとの統合を構成する必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。



正解:



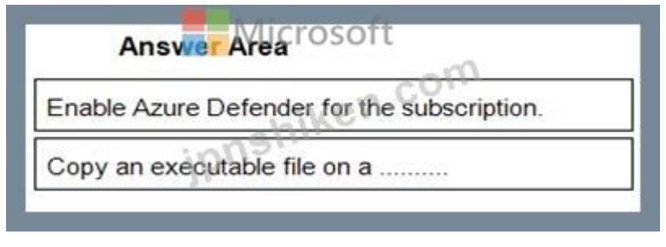
参照：

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

質問: **99**
組織内の他のユーザーがこれまで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した場合に、セキュリティアラートを受け取る必要があります。
どの異常検知ポリシーを使用すべきでしょうか？
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. 活動頻度の低い国からの活動
D. マルウェア検出
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

質問: **100**
新しいAzureサブスクリプションを作成し、Azure Monitor用のログの収集を開始します。
Azure Security Center を構成して、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潜在的な脅威を検出できるようにする必要があります。ソリューションは、この構成を検証する必要があります。
3つの行動を順番に実行する必要があります。回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。

正解:

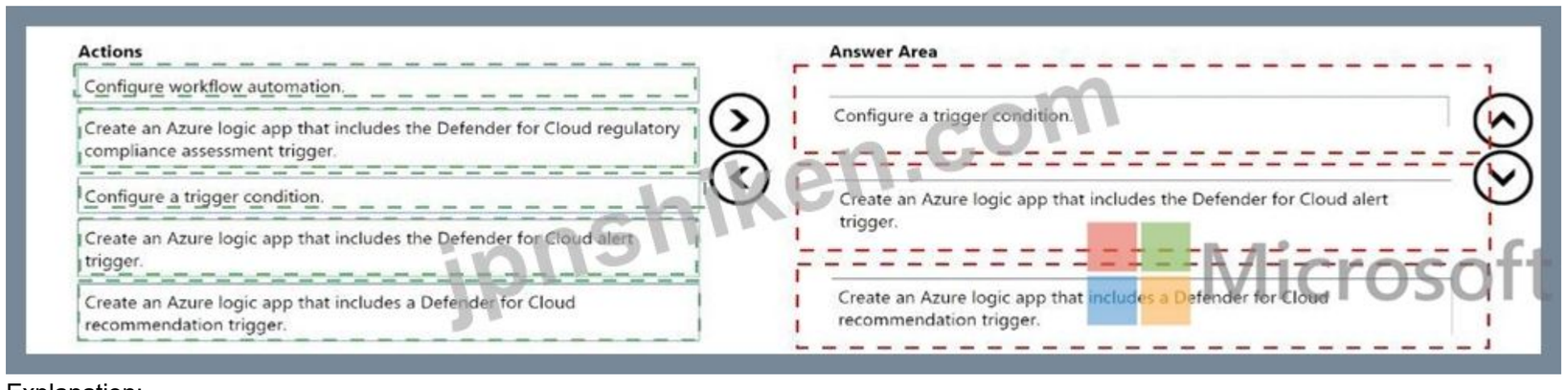


1 - サブスクリプションで Azure Defender を有効にします。
2 - 実行可能ファイルを.....にコピーします。
参照：
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

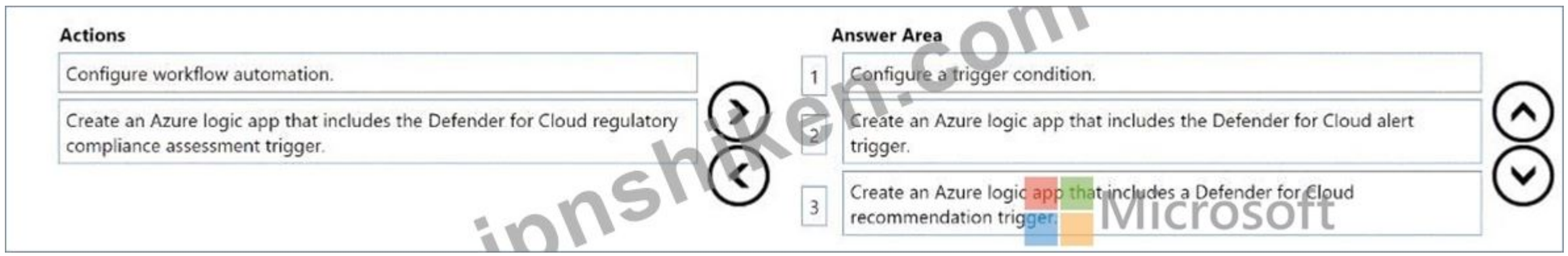
質問: **101**
技術要件を満たすためには、ログイン失敗に関するクエリを完了する必要があります。
WHERE句を完成させるための列名はどこで確認できますか？
A. Azure Security Center のセキュリティ警告
B. Azureのアクティビティログ
C. Log Analyticsワークスペースのクエリウィンドウ
D. Azure Advisor
正解: **C** (コメントを発表する)

質問: **102**
お客様は、Microsoft Defender for Cloudを使用するAzureサブスクリプションをお持ちです。
新しいMicrosoft Secure Scoreアクションが生成された際に、会社のIT部門にMicrosoft Teamsメッセージを送信するワークフローを作成する必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。

正解:



Explanation:

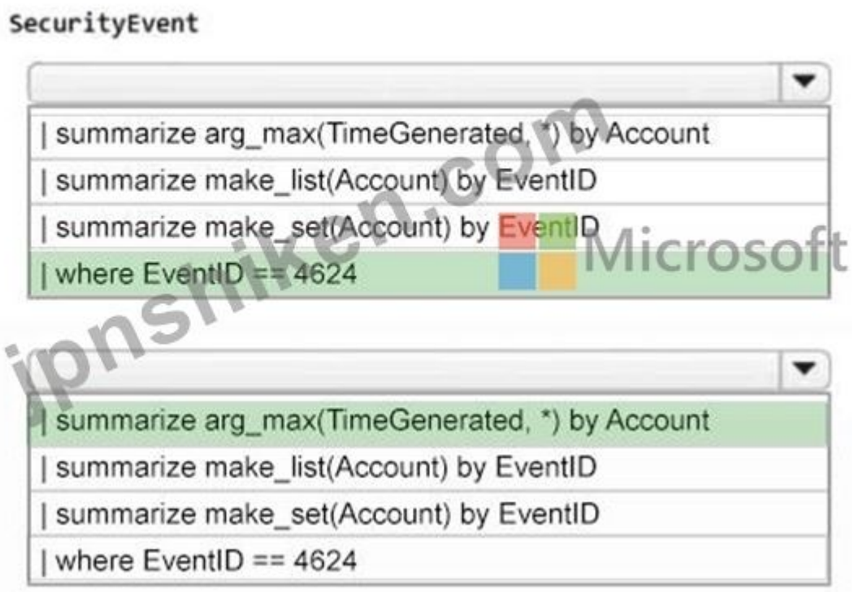


質問: **103**
お客様は、Microsoft Defender for Cloud Appsを使用し、クラウド検出が有効になっているMicrosoft 365サブスクリプションをお持ちです。
クラウド検出データを拡充する必要があります。ソリューションは、クラウド検出トラフィックログ内のユーザー名が、対応するMicrosoft Entra IDユーザーアカウントのユーザープリンシパル名（UPN）に関連付けられていることを保証する必要があります。
まず最初に何をすべきでしょうか？
A. 条件付きアクセス アプリケーション制御から、ユーザー監視を設定します。
B. Azureアプリコネクタを作成します。
C. Microsoft 365 Defenderへの自動リダイレクトを有効にします。
D. Microsoft 365 アプリ コネクタを作成します。
正解: **B** (コメントを発表する)

質問: **104**
ホットスポットに関する質問
Microsoft SentinelワークスペースでKQLクエリを作成する必要があります。このクエリは、EventID値が4624の最後のレコードを持つアカウントのSecurityEventレコードを返す必要があります。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

Answer Area



質問: 105

あなたはMicrosoft Teamsを使用するMicrosoft 365 E5サブスクリプションをお持ちです。

Microsoft Purviewコンプライアンスポータルを使用して、特定のユーザーのTeamsチャットのコンテンツ検索を実行する必要があります。このソリューションは、検索範囲を最小限に抑える必要があります。

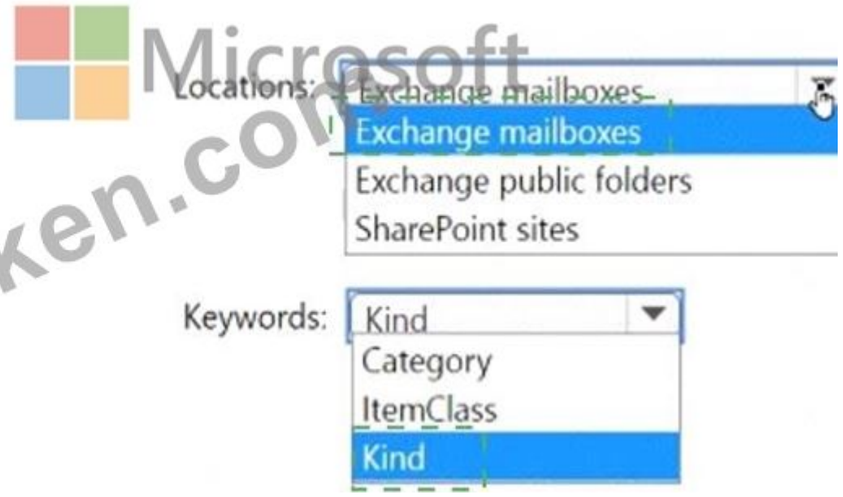
コンテンツ検索はどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

正解:

Answer Area

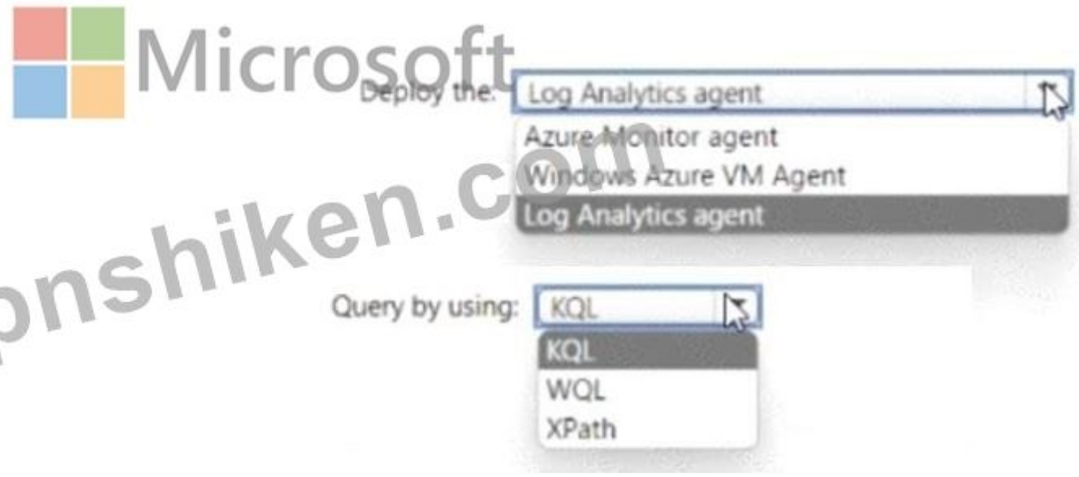


Explanation:

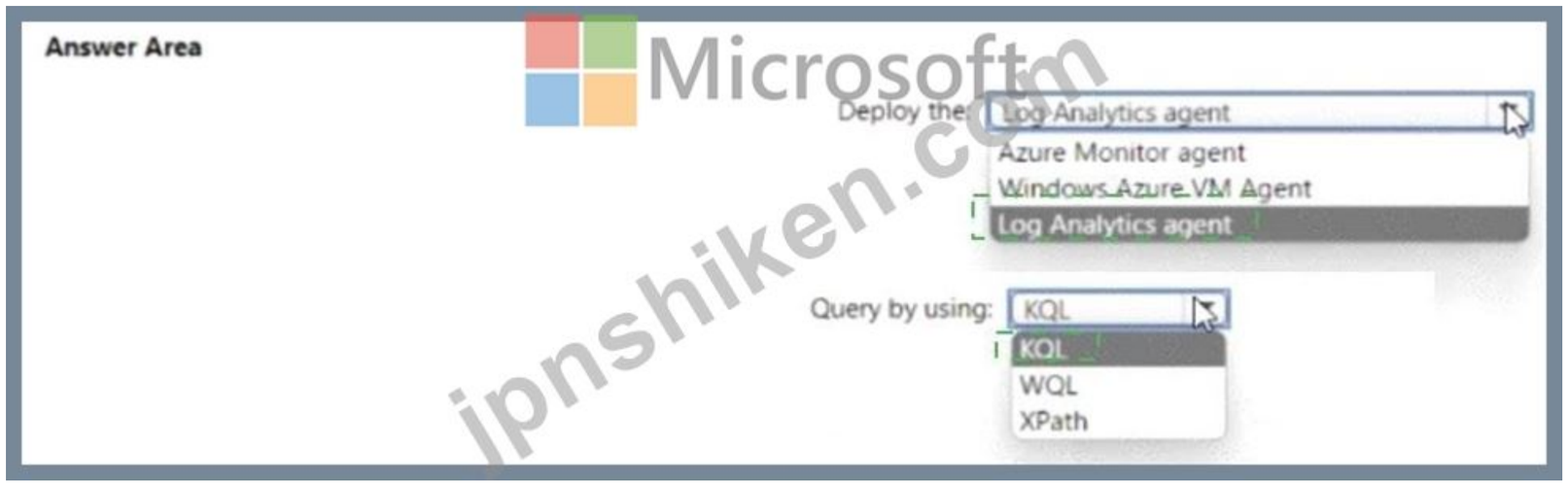
質問: 106

Windows セキュリティ イベント ログを収集するには、Microsoft Sentinel の要件を満たす必要があります。どうすればよいですか？回答するには、回答領域で適切なオプションを選択してください。注: 正解ごとに 1 ポイントが加算されます。

Answer Area

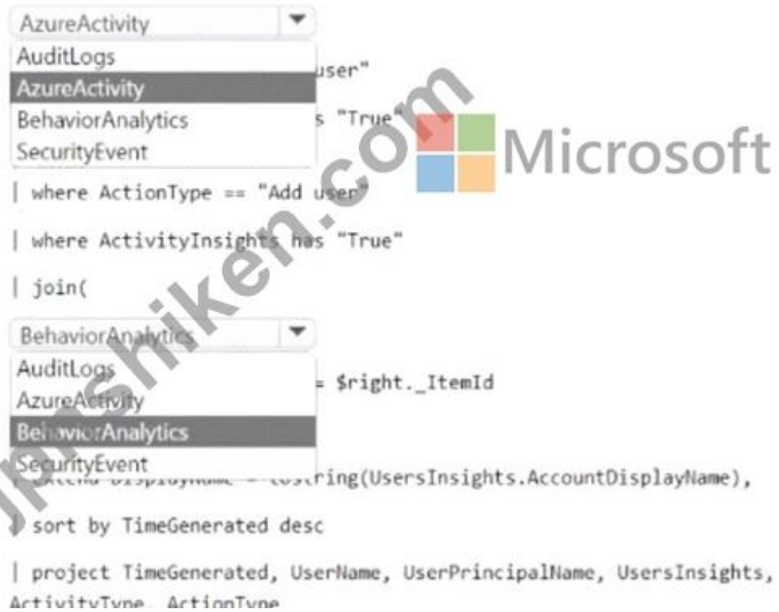


正解:



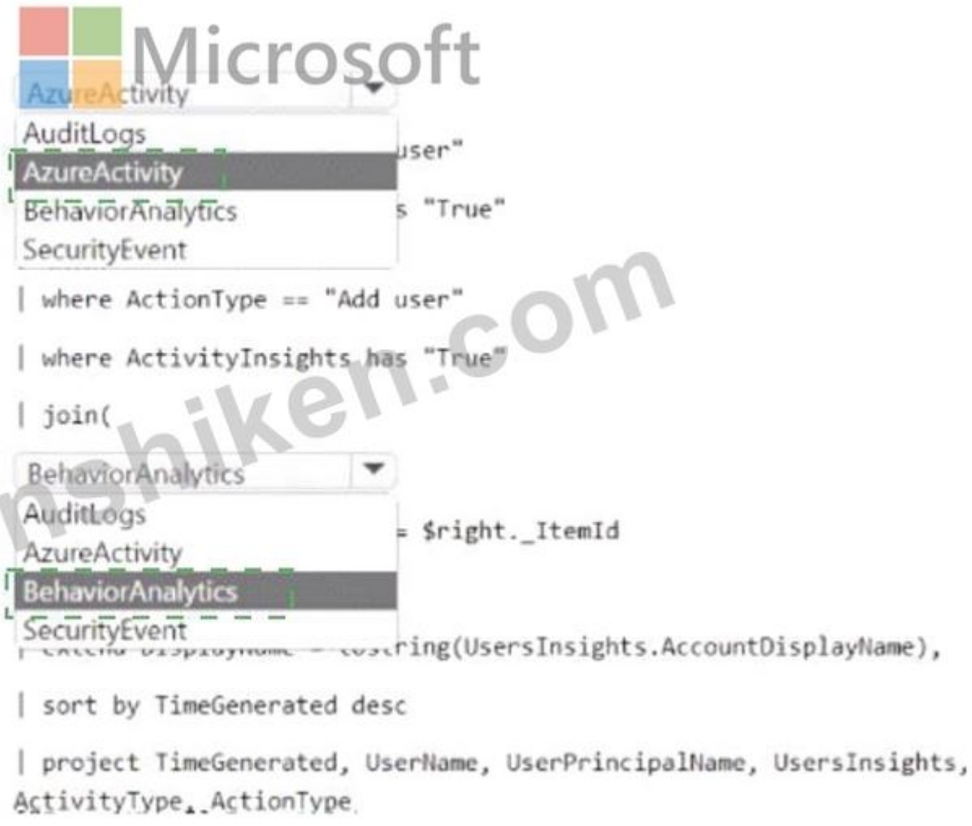
Explanation:

質問: **107**
sws1 という名前の Microsoft Sentinel ワークスペースがあります。
ユーザーが異常に多数のAzure ADユーザーアカウントを作成したことを検出するクエリを作成する必要があります。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。



正解:

Answer Area



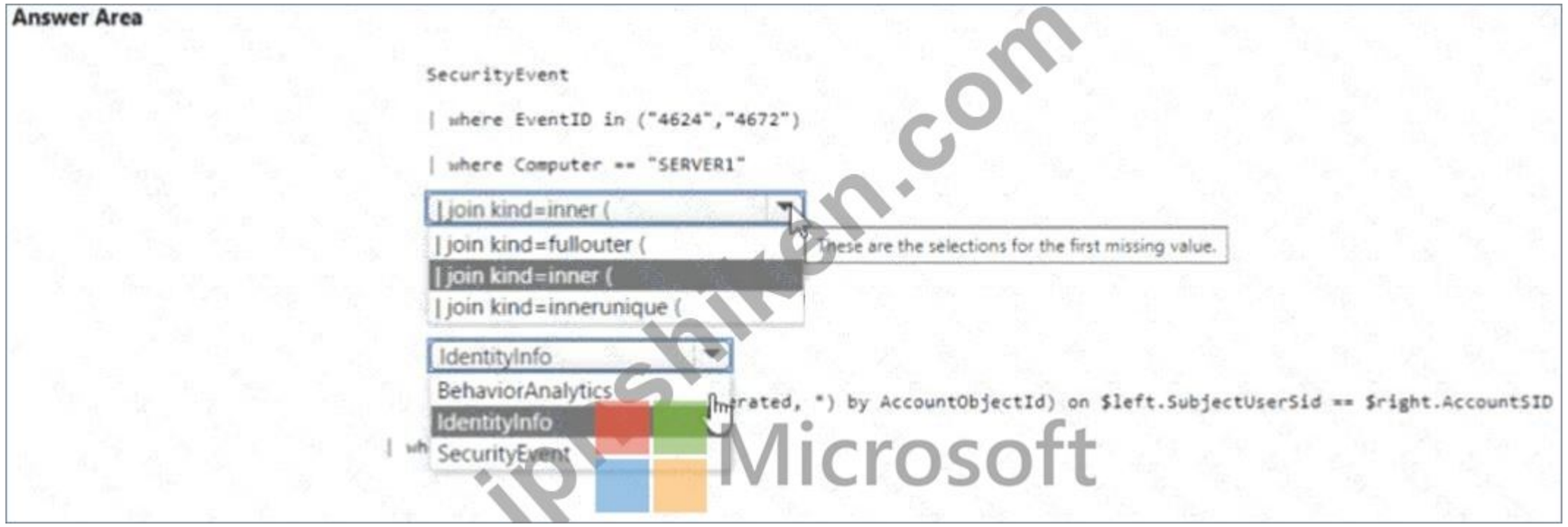
説明

Answer Area

質問: **108**
画像ファイルを利用した潜在的な攻撃に関するセキュリティ速報を受け取ります。
攻撃を防ぐには、Microsoft Defender for Endpointで侵害指標（IoC）を作成する必要があります。
どのタイプのインジケーターを使用すべきですか？
A. アクションが設定されている URL/ドメインインジケーター
B. アクションが設定されている URL/ドメインインジケーター
C. Action が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 警告とブロック」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: **109**
ユーザーおよびエンティティ行動分析（UEBA）が有効になっているMicrosoft Sentinelワークスペースをお持ちです。
Server1という名前のサーバー上で実行された、セキュリティ上重要なユーザー操作に関連するすべてのログエントリを特定する必要があります。解決策は以下の要件を満たす必要があります。
* IT部門のメンバーではないユーザーによる、セキュリティ上重要な操作のみを含めてください。
偽陽性の数を最小限に抑える。
質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。注：
正解ごとに1ポイント獲得できます。

Answer Area



正解:

Explanation:

UEBAが有効になっているMicrosoft Sentinelでは、IDに関するユーザーエンリッチメントデータ（部署 役職など）
アカウント/SID マッピングなどの情報は IdentityInfo テーブルに書き込まれます。Microsoft のガイダンスでは、セキュリティ テレメトリ (SecurityEvent など) を IdentityInfo と結合して、部門などの組織属性で結果をフィルタリングまたは範囲指定することを推奨しています。要件 IT 部門のメンバーではないユーザーによるセキュリティに関係するアクションのみを含める」を満たすには、Windows セキュリティ イベントに IdentityInfo を追加し、部門 !~ "IT " (または同等のもの) でフィルタリングします。
多対一のIDレコードを結合する際にノイズや重複行を最小限に抑えるため、Sentinel KQLのベストプラクティスでは、join kind=innerunique の使用を推奨しています。この結合では、左側の各行に対して右側のテーブルから一致する行が最大1つ返されるため、重複または古いIDレコードから発生する可能性のある誤検出を減らしつつ、一致が必要であること（つまり、内部一致）が保証されます。エンリッチメント後、クエリロジック（たとえば、Server1とセキュリティに敏感なイベントIDのサブセット、またはUEBAから派生したマッピングに制限するなど）を続行して、関連するアクションのみを識別します。
したがって、正しい補完方法は、join kind=innerunique を使用して IdentityInfo に結合し、部門フィルターを適用して誤検出を減らすことです。

質問: **110**
Microsoft Sentinelワークスペースに、Workbook1という名前のカスタムワークブックが含まれています。
SecuntyEvent テーブルに基づいてビジュアルを作成する必要があります。ソリューションは以下の要件を満たす必要があります。
* 過去1週間に取り込まれたセキュリティイベントの数を特定します。
* タイムチャートで日ごとのイベント数を表示する
ワークブック1には何を追加すべきですか？
A. グループ
B. リンクまたはタブ
C. クエリ
D. 指標
正解: **(**正解を表示します**)**

質問: **111**
Microsoft Sentinelを使用するAzureサブスクリプションがあり、その中にUser1という名前のユーザーが存在します。
User1がMicrosoft Entraテナント内のエンティティ動作に対してユーザーおよびエンティティ動作分析（UEBA）を有効にできるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1にはどの役割を割り当てるべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

正解:

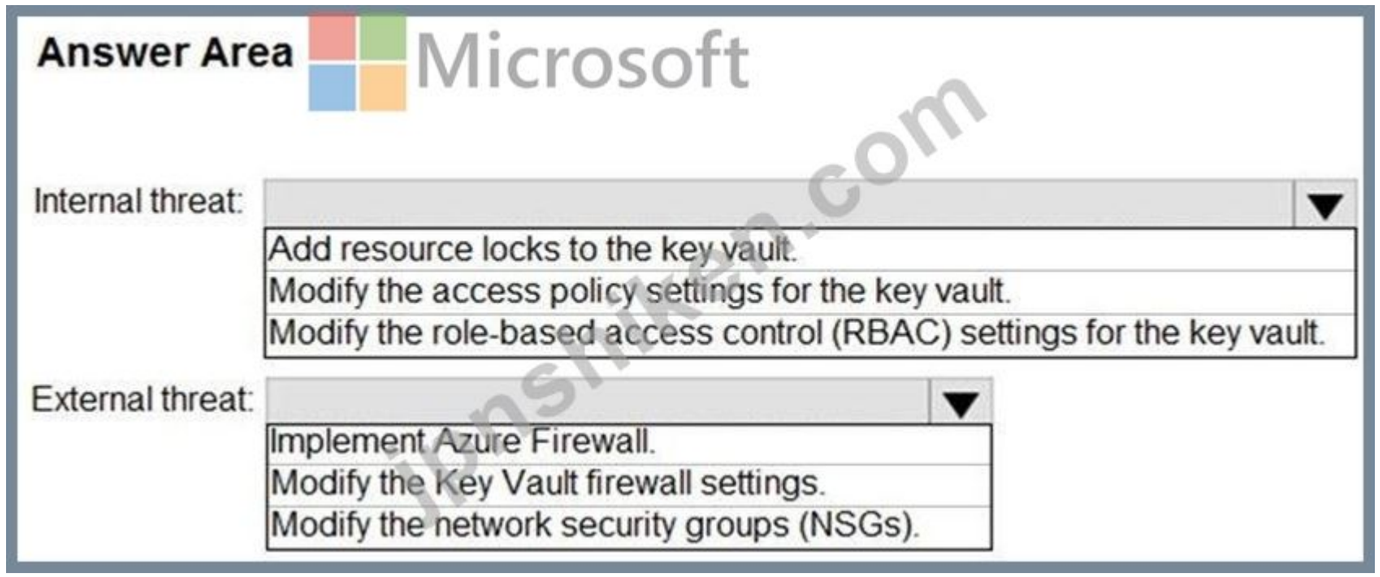
Explanation:

質問: 112

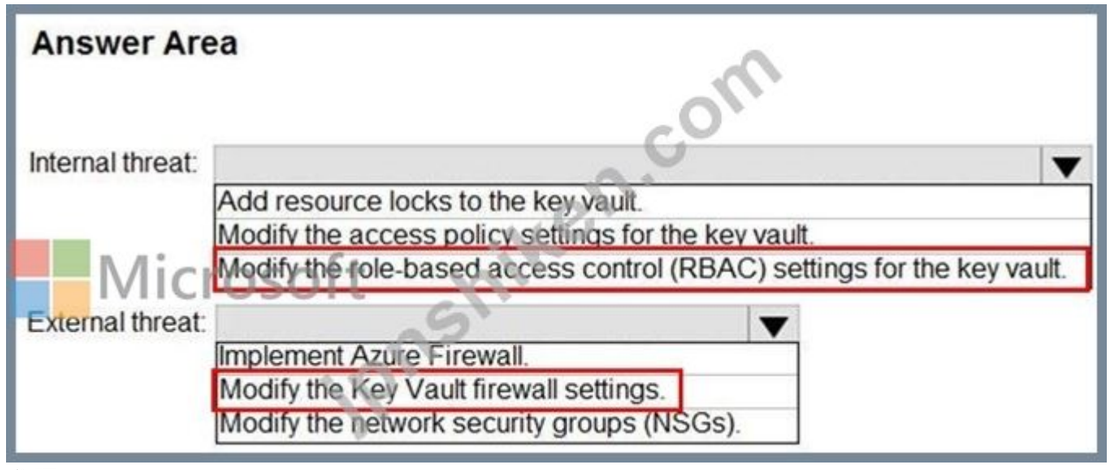
FabrikamIに関するAzure Defenderのアラートに対して、修復措置を推奨する必要があります。

それぞれの脅威に対して、どのような対策を推奨しますか？回答欄で適切な選択肢を選んでください。

注：正解ごとに1ポイントが加算されます。



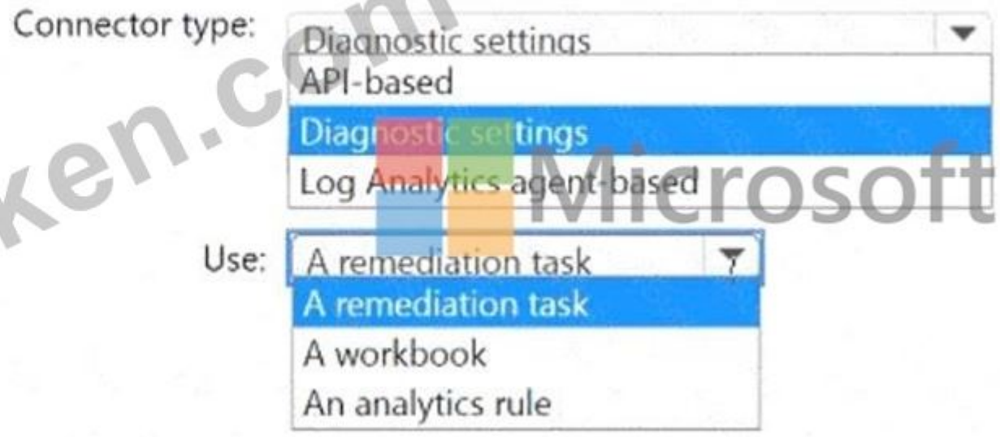
正解:



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

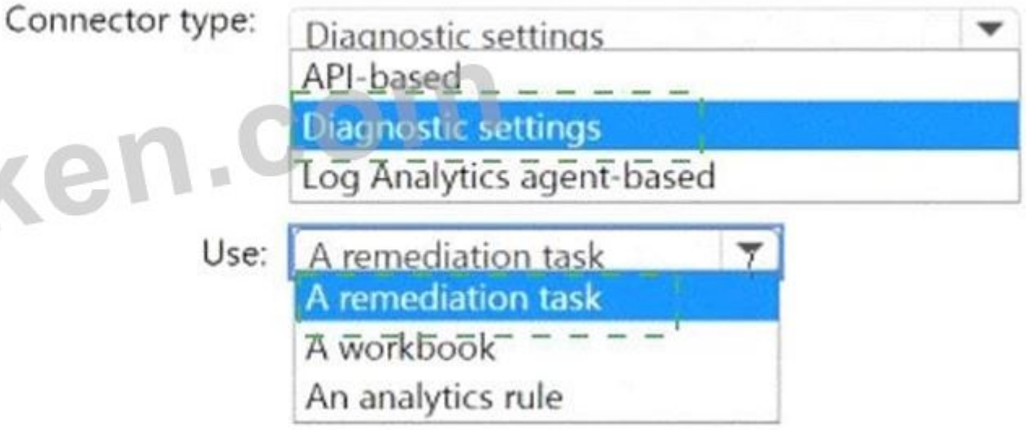
質問: **113**
お客様は4つのAzureサブスクリプションをお持ちです。そのうちの1つのサブスクリプションには、Microsoft Sentinelワークスペースが含まれています。
Azure Policy を使用してサブスクリプションからデータを収集するには、Microsoft Sentinel データコネクタをデプロイする必要があります。このソリューションでは、ポリシーがサブスクリプション内の新規リソースと既存リソースの両方に適用されることを保証する必要があります。
どのタイプのコネクタをプロビジョニングすべきか、また、すべてのリソースが監視されるようにするには何を使用すべきか。回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:

Answer Area

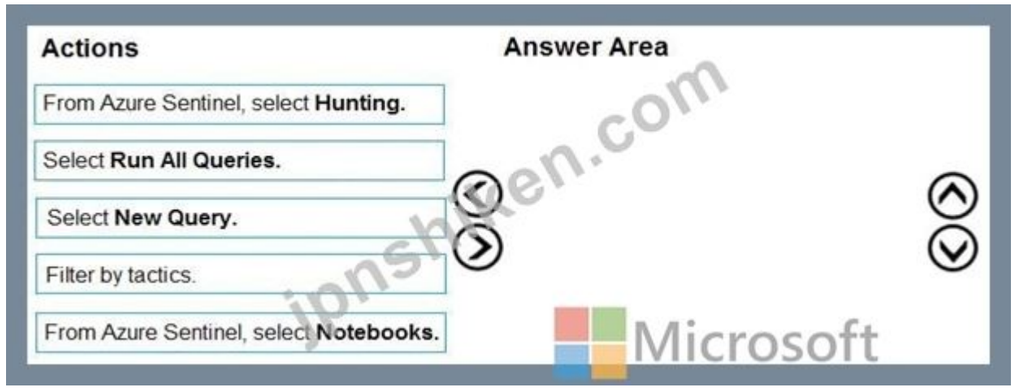


Explanation:

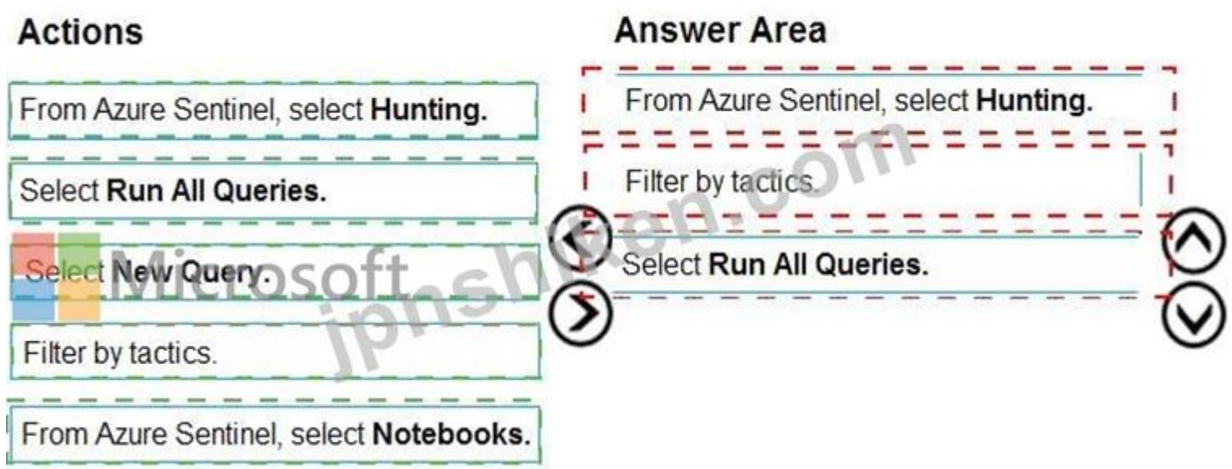
Microsoft Sentinelでは、データコネクタは、AzureおよびAzure以外のさまざまなソースからログとテレメトリを収集し、Log Analyticsワークスペースに取り込むためのメカニズムです。
複数の Azure サブスクリプション (既存のリソースと新規リソースの両方) を Sentinel に自動的に接続することが目的の場合、診断設定に依存するコネクタを備えた Azure Policy を使用するのが適切な方法です。

多くの Azure リソース (Key Vault、ストレージ アカウント、Azure ファイアウォール、アクティビティ ログなど) は、診断設定を介してログを Sentinel に送信します。このコネクタ タイプを使用すると、エージェントや手動構成を必要とせずに、ログを Sentinel ワークスペースに直接エクスポートできます。
Azure Policy を使用すると、これらの診断設定を現在および将来のすべてのリソースに自動的に適用および展開できるため、管理上の負担を最小限に抑えながら継続的なログ取り込みが保証されます。
Azure Policy を適用する際、既存のリソースに診断設定がまだ構成されていない場合があります。これを解決するには、修復タスクを作成します。これにより、Azure Policy は新規リソースだけでなく、既存のリソースにもコンプライアンス設定を適用するようになります。修復タスクがない場合、新しく作成されたリソースのみが自動的に準拠します。
* コネクタタイプ: 診断設定 # サブスクリプション全体にわたるポリシーベースの展開に使用されます。
* 使用法: 修復タスク # は、ポリシーが既存のリソースと新しいリソースの両方に適用され、完全なカバレッジが確保されるようにします。
# 最終回答:
* コネクタタイプ: 診断設定
* 用途: 修復作業

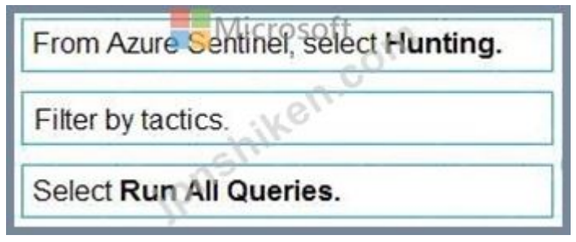
質問: **114**
Azure Sentinelがデプロイされています。
不審な認証情報アクセス活動をすべて照会する必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:

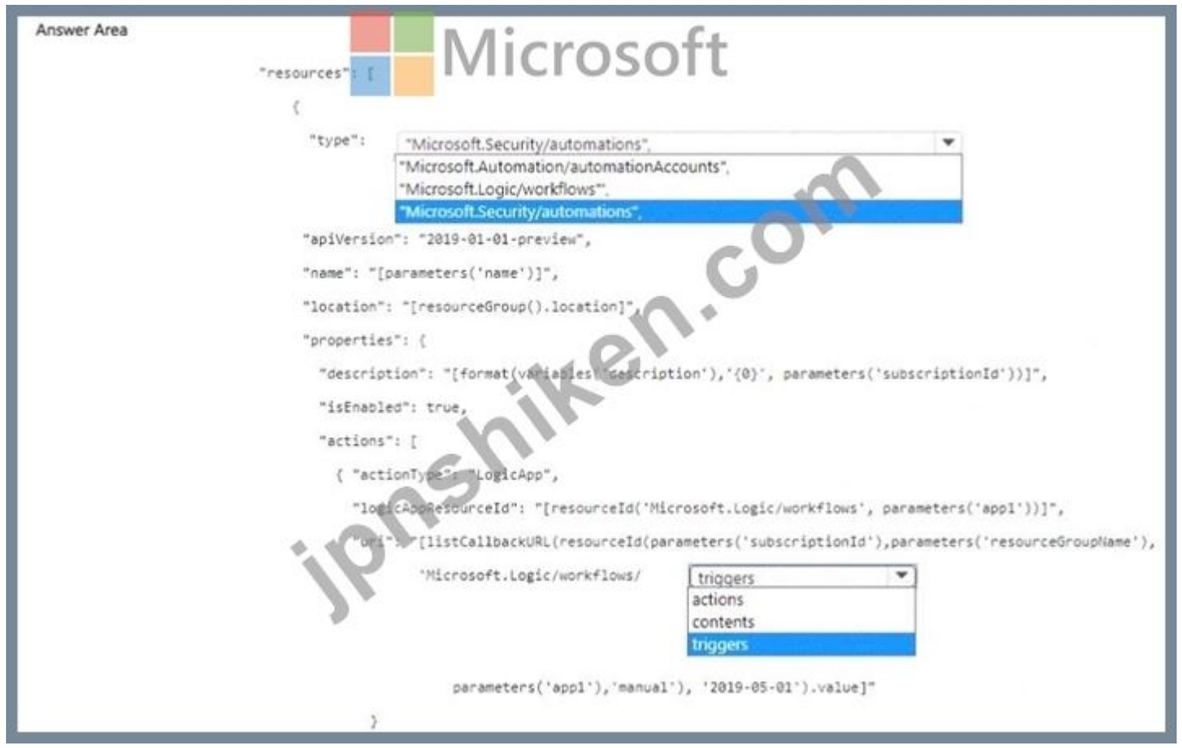


質問: **115**
オンプレミスネットワークをお持ちです。
お客様は、Microsoft Defender for Identityを使用するMicrosoft 365 E5サブスクリプションをご利用中です。
Microsoft Defender ポータルから、User1 というユーザーの Device1 というデバイスで発生したインシデントを調査します。このインシデントには、Defender for Identity の次のアラートが含まれています。
個人情報盗難の疑い（パス・ザ・チケット）（外部 2018）
ユーザーやデバイスに影響を与えることなく、インシデントを封じ込める必要があります。解決策は、管理上の負担を最小限に抑えるものでなければなりません。
あなたはどうすべきでしょうか？
A. ユーザー1のみ無効化します。
B. 隔離装置1のみ。
C. デバイス1に以前サインインしたすべてのアカウントのパスワードをリセットします。
D. ユーザー1を無効化し、デバイス1を隔離します。
E. User1を無効にし、Device1を隔離し、以前Device1にサインインしたすべてのアカウントのパスワードをリセットします。
正解: **(**正解を表示します**)**
Microsoft Defender for Identityのドキュメントによると、「ID窃盗の疑い（Pass-the-Ticket）」などのアラートが表示された場合、侵害されたKerberosチケットが攻撃者によって悪用され、正規のアカウントになりすまされた可能性があることを示しています。このシナリオにおける目標は、影響を受けていないユーザーやシステムへの影響を最小限に抑えつつ、攻撃の拡散を阻止することです。
マイクロソフトは、悪意のある活動の発生源である可能性が高い侵害されたデバイスを、まず隔離または検疫することを推奨しています。デバイス1を検疫することで、他のネットワークシステムとの通信が遮断され、認証情報の盗難や横方向への拡散を防ぐとともに、SOCチームが問題の調査と修復を行うことができます。
この段階で全てのアカウントパスワードをリセットしたり、ユーザーアカウントを無効化したりすると、重大な運用上の混乱が生じる可能性があるため、複数の認証情報が侵害されたという証拠がない限り推奨されません。Defender for Identityの封じ込めに関するガイダンスには、以下の点が明記されています。
「影響を受けたデバイスを隔離し、さらなる認証情報の盗難や移動を防いでください。」
* 「侵害が確認されたアカウントのみパスワードをリセットしてください。」
したがって、最も影響が少なく効率的な封じ込め策は、デバイス1のみを隔離することです。この措置により、他のユーザーやデバイスの正常な動作を維持しながら脅威を効果的に隔離することができ、管理上の負担とユーザーへの影響を最小限に抑えるという要件を満たします。
したがって、検証済みの回答はB.隔離装置1のみです。

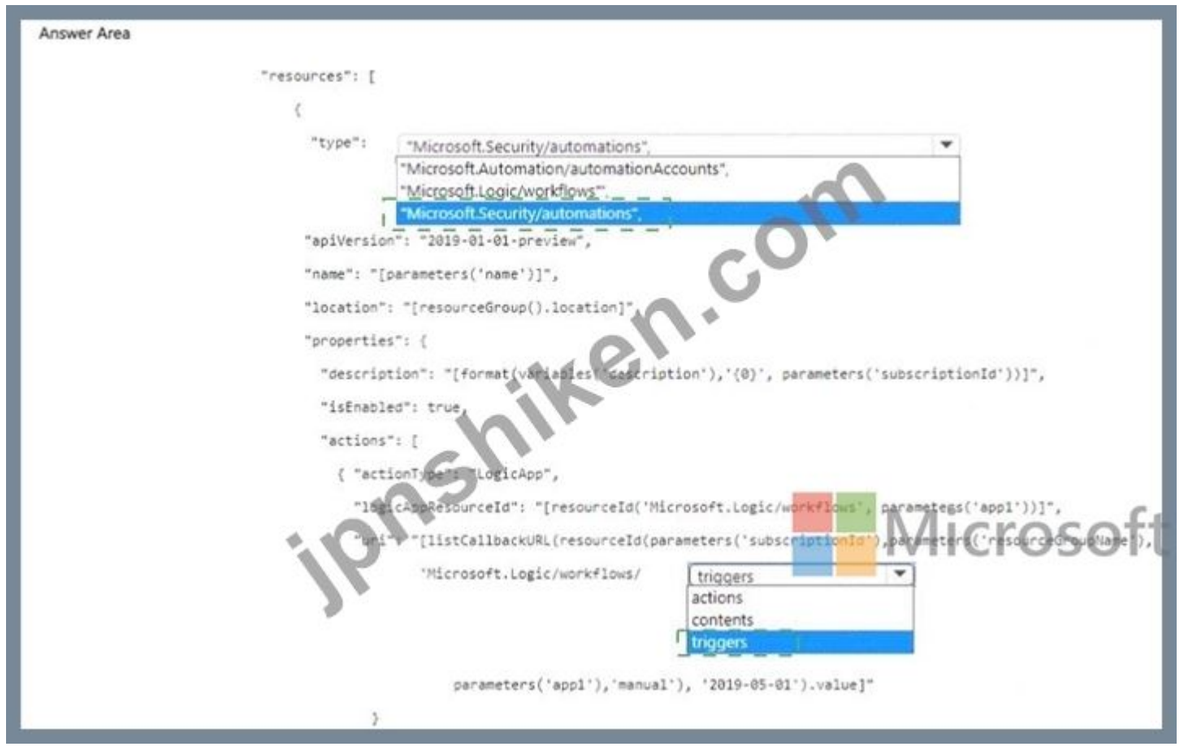
質問: **116**
Azure Sentinel にプレイブックがあります。
プレイブックを実行すると、指定された配信グループにメールが送信されます。
プレイブックを修正して、メールを配布グループではなくリソースの所有者に送信するようにする必要があります。
あなたはどうすべきでしょうか？
A. パラメータを追加してトリガーを変更します。
B. カスタムデータコネクタを追加し、トリガーを変更します。

C. 条件を追加してアクションを変更します。
D. パラメータを追加して動作を変更します。
正解: **(**正解を表示します**)**
セクション: [なし]
説明／参考資料：
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

質問: **117**
Microsoft Defender for Cloudを使用するAzureサブスクリプションがあり、その中にapp1という名前のAzureロジックアプリが含まれています。
特定のDefender for Cloudセキュリティアラートが生成された際に、app1が起動するようにする必要があります。
Azure Resource Manager (ARM) テンプレートをどのように完成させるべきですか？回答するには、回答欄で適切なオプションを選択してください。注：正解ごとに 1 ポイントが加算されます。



正解:



Explanation:

質問: 118

お客様のネットワークには、Azure ADと同期するオンプレミスのActive Directoryドメインサービス（AD DS）ドメインが含まれています。
お客様は、Microsoft Defender 365を使用するMicrosoft 365 E5サブスクリプションをご利用中です。
貴社の財務部門のユーザーによる、すべての対話型認証試行を特定する必要があります。
KQLクエリはどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

正解:

Answer Area

説明

質問: **119**

Microsoft Defender for Cloud の要件とビジネス要件を満たすために、Group1 と Group2 にロールベースのアクセス制御 (RBAQ ロール) を割り当てる必要があります。各グループにはどのロールを割り当てるべきですか? 回答するには、回答領域で適切なオプションを選択してください。注: 正解ごとに 1 ポイントが加算されます。

Answer Area

正解:

質問: **120**

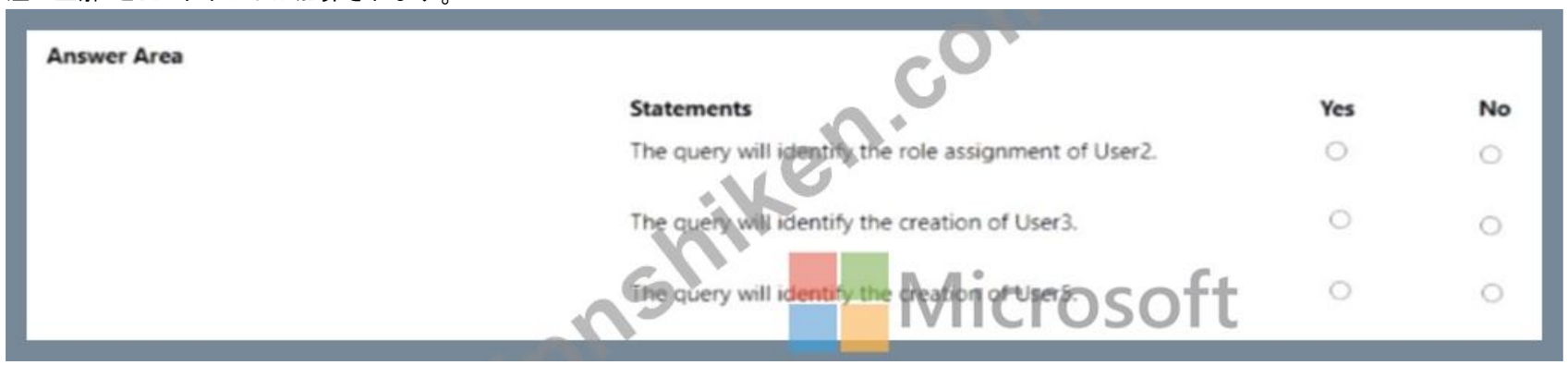
Microsoft 365 E5 サブスクリプションには、User! と User2 という名前の 2 人のユーザーが含まれています。次の図に示すようなハンティングクエリがあります。

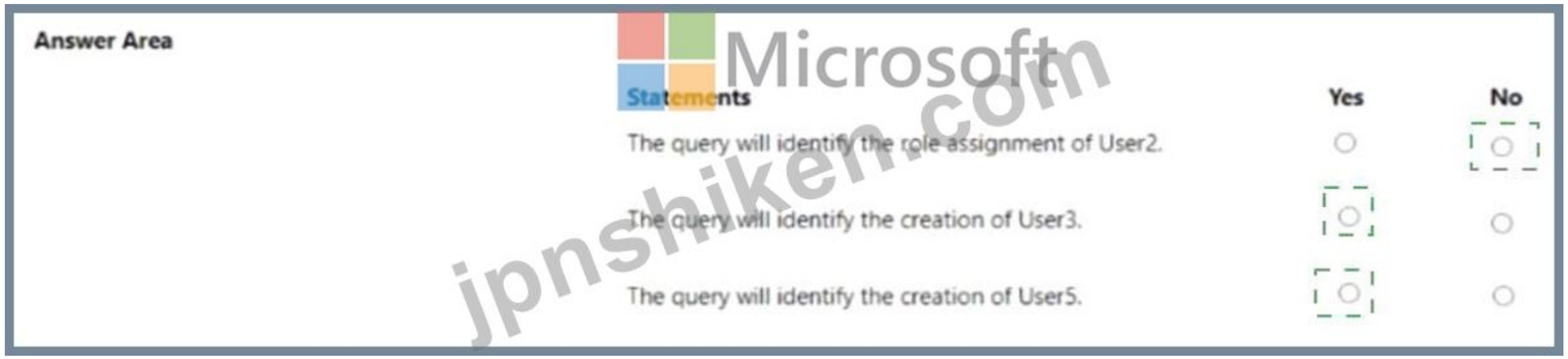
ユーザーは以下の陰イオンを実行します。

* User1がUser2にグローバル管理者ロールを割り当てます。
* User1はUser3という名前の新しいユーザーを作成し、そのユーザーにMicrosoft Teamsのライセンスを割り当てます。
* User2 は User4 という名前の新しいユーザーを作成し、そのユーザーにセキュリティ閲覧者の役割を割り当てます。
* User2はUser5という名前の新しいユーザーを作成し、そのユーザーにセキュリティオペレーターの役割を割り当てます。

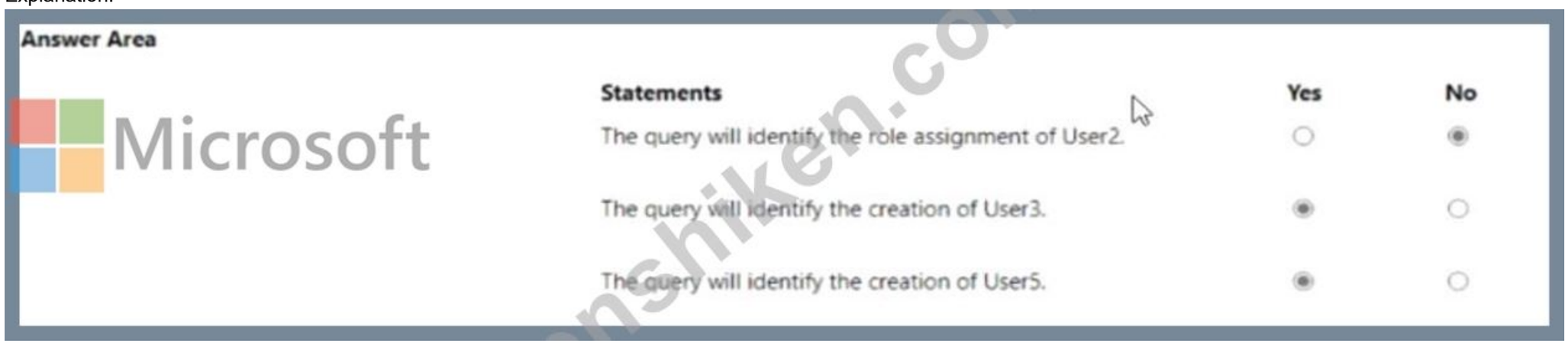
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。





Explanation:



質問: 121

ドラッグ＆ドロップ

あなたはMicrosoft 365 Defenderを使用してインシデントを調査しています。

CFOLaptop、CEOLaptop、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カウントするための高度なハンティングクエリを作成する必要があります。

質問にはどのように回答すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

選択して配置する：

Values

```
| project LogonFailures=count()
```

```
| summarize LogonFailures=count()
by DeviceName, LogonType
```

```
| where ActionType == FailureReason
```

```
| where DeviceName in ("CFOLaptop",
"CEOLaptop", "COOLaptop")
```

```
ActionType == "LogonFailed"
```

```
ActionType == FailureReason
```

```
DeviceEvents
```

```
DeviceLogonEvents
```

Answer Area

an

正解:

Values

- `| project LogonFailures=count()`
- `| summarize LogonFailures=count() by DeviceName, LogonType`
- `| where ActionType == FailureReason`
- `| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")`
- `ActionType == "LogonFailed"`
- `ActionType == FailureReason`
- `DeviceEvents`
- `DeviceLogonEvents`

Answer Area

`DeviceLogonEvents`

`| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")` and

`ActionType == FailureReason`

`| summarize LogonFailures=count() by DeviceName, LogonType`

セクション: [なし]

質問: **122**

お客様は、Microsoft Exchange OnlineとMicrosoft Defender for Office 365を使用するMicrosoft 365テナントをお持ちです。

ゼロアワー自動削除（ZAP）によってユーザーのメールボックスからメールメッセージが移動されたかどうかを判断するには、何を使用すればよいですか？

A. Microsoft Defender for Office 365 の脅威保護ステータス レポート

B. Exchangeのメールボックス監査ログ

C. Microsoft Defender for Office 365 の安全な添付ファイルファイルタイプのレポート

D. Exchangeのメールフローレポート

正解: **(**正解を表示します**)**

ZAPがメッセージを移動したかどうかを確認するには、脅威保護ステータスレポートまたは脅威エクスプローラー（およびリアルタイム検出）を使用できます。

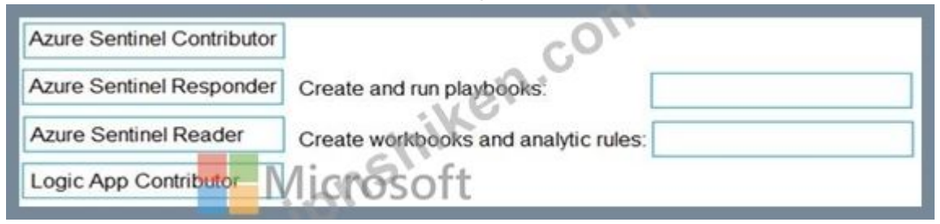
参照：

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

質問: **123**

貴社はAzure Sentinelを導入します。

Azure Sentinelの管理を複数のグループに委任する予定です。
以下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。
解決策は、最小権限の原則に基づかなければならない。
各タスクにはどの役割を割り当てるべきでしょうか？回答するには、適切な役割を正しいタスクにドラッグしてください。各役割は、1回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の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：正解ごとに1ポイントが加算されます。



正解:

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

質問: **124**
Microsoft Defender for Cloud を使用する Azure サブスクリプションがあり、storage1 という名前のストレージ アカウントが含まれています。storage1 内の BLOB に対して異常に多くの削除操作が行われたというアラートを受け取りました。どの BLOB が削除されたかを特定する必要があります。何を調査すべきでしょうか？
A. ストレージ1のアクティビティログ
B. Azure Storage Analyticsのログ
C. アラートの詳細
D. アラートに関連するエンティティ
正解: **(**正解を表示します**)**
削除されたBLOBを特定するには、ストレージアカウントのアクティビティログを確認してください。アクティビティログには、削除操作を含む、ストレージアカウントで行われたすべての操作に関する情報が含まれています。これらのログは、Azureポータルでストレージアカウントに移動し、 監視」セクションの 「アクティビティログ」を選択して、適切な期間でフィルタリングすることでアクセスできます。また、Azure MonitorとLog Analyticsを使用して、アクティビティログデータを照会および分析することもできます。
参考文献：
https://docs.microsoft.com/en-us/azure/storage/common/storage-activity-logs
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-azure-storage

質問: **125**

sws1 という名前の Microsoft Sentinel ワークスペースがあります。

あなたは、sws1でインシデントが発生したときに、オンプレミスのITサービス管理システムにインシデントを登録するAzureロジックアプリを作成する予定です。

ロジック アプリの Microsoft Sentinel コネクタの資格情報を構成する必要があります。ソリューションは、次の要件を満たす必要があります。

管理業務の手間を最小限に抑える。

最小権限の原則を適用する。

認証情報はどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

正解:

Explanation:

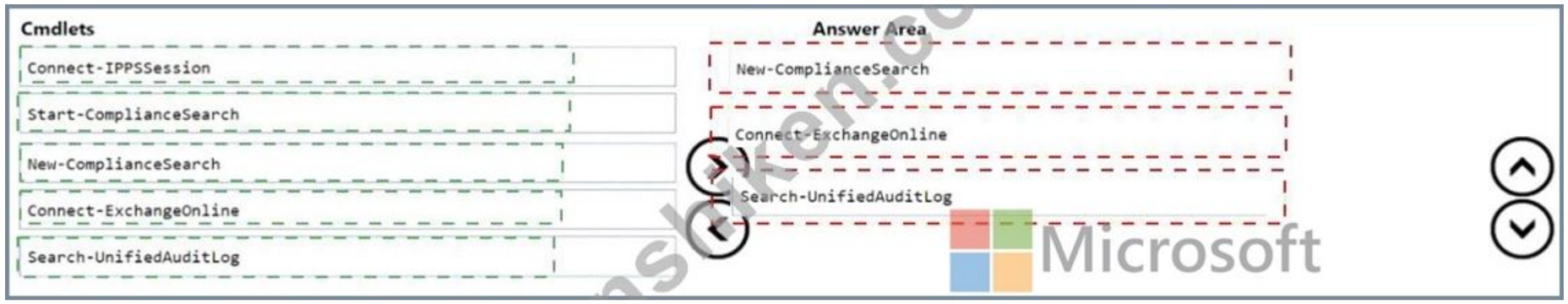
質問: **126**

Microsoft Defender for Endpointの要件を満たすには、CLIENT1上で実行されるクラウドアプリを制限する必要があります。
どの2つの設定を変更すべきでしょうか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。
A. Microsoft Defender Security Center のデバイス管理にあるオンボーディング設定
B. クラウドアプリセキュリティ異常検知ポリシー
C. Microsoft Defender セキュリティ センターの「設定」にある高度な機能
D. クラウドアプリセキュリティのクラウド検出設定
正解: **C,D (**コメントを発表する**)**
Microsoft Defender for Endpoint および Microsoft Defender for Cloud Apps (旧称 Cloud App Security) を使用して Windows 10 エンドポイントで未承認のクラウド アプリをブロックするには、両方の側で製品統合を有効にして構成する必要があります。まず、Microsoft Defender Security Center > 設定 > 高度な機能で、Microsoft Defender for Cloud Apps 統合を有効にします (ネットワーク保護の前提条件が満たされていることを確認してください)。これにより、Defender for Endpoint は未承認アプリのリストを受信し、CLIENT1 のユーザーがブラウザーまたはクライアント経由でこれらのアプリにアクセスしようとしたときに、エンドポイント ベースのブロックを適用できるようになります。
次に、Defender for Cloud Appsの「設定」→「クラウド検出」で、Microsoft Defender for Endpointの統合を設定し、「未承認アプリのブロック」を有効にします。クラウド検出では、アプリが検出、評価され、「未承認」としてタグ付けされます。MDE統合が有効になると、そのタグがエンドポイントにエクスポートされ、テナントのアプリカタログとポリシーに基づいてブロックが適用されます。
オプション A (オンボーディング設定) はデバイスの登録用であり、アプリのブロック動作を制御するものではありません。B (異常検出ポリシー) は動作検出 (不可能な移動、匿名 IP など) を制御するものであり、エンドポイントでのアプリ アクセスの強制とは関係ありません。したがって、「Microsoft Defender for Endpoint を使用して Windows 10 コンピューターで未承認のアプリをブロックする」という要件を満たすために変更する必要がある 2 つの構成は、C. Microsoft Defender セキュリティ センターの高度な機能と、D. Cloud App Security のクラウド検出設定です。
トピック2、コントソ社
事例研究
これはケーススタディです。ケーススタディには個別の時間制限はありません。各ケースを完了するために、試験時間を自由に使うことができます。ただし、この試験には追加のケーススタディやセクションが含まれる場合があります。与えられた時間内に試験に含まれるすべての問題を完了できるよう、時間配分をしっかり行う必要があります。
ケーススタディに含まれる質問に答えるには、ケーススタディに記載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図表やその他の資料が含まれている場合があります。各質問は、このケーススタディ内の他の質問とは独立しています。
このケーススタディの最後に、確認画面が表示されます。この画面では、解答を確認し、次のセクションに進む前に修正することができます。新しいセクションを開始すると、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てください。質問に答える前に、左側のペインにあるボタンを使ってケーススタディの内容を確認してください。これらのボタンをクリックすると、ビジネス要件、既存環境、問題記述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、そこに表示される情報は以降のタブに表示される情報と同一です。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ってください。
概要
Contoso Ltd.という会社は、本社と北米各地に5つの支店を構えている。
本社はシアトルにあります。支店はトロント、マイアミ、ヒューストン、ロサンゼルス、バンクーバーにあります。
コントソ社は、ニューヨークとサンフランシスコにオフィスを構えるファブリカム社という子会社を所有している。
既存の環境
エンドユーザー環境
Contosoの全ユーザーはWindows 10デバイスを使用しています。各ユーザーはMicrosoft 365のライセンスを取得しています。さらに、Contosoの営業チームのメンバーにはiOSデバイスが配布されています。
クラウドおよびハイブリッドインフラストラクチャ
ContosoのすべてのアプリケーションはAzureにデプロイされています。
Microsoft Cloud App Securityを有効にします。

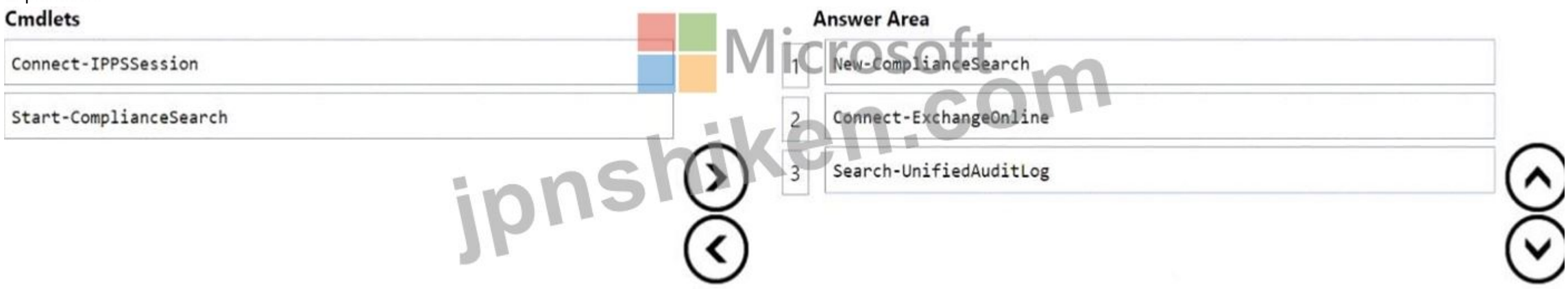
ContosoとFabrikamは、それぞれ異なるAzure Active Directory（Azure AD）テナントを使用しています。Fabrikamは最近Azureサブスクリプションを購入し、サポートされているすべてのリソースタイプに対してAzure Defenderを有効にしました。
現在の問題点
Contosoのセキュリティチームは、大量のサイバーセキュリティ警告を受け取っています。セキュリティチームは、どの警告が正当な脅威で、どれがそうでないかを判断するのに多くの時間を費やしています。
Contosoの営業チームはiOSデバイスのみを使用しています。営業チームのメンバーは、さまざまなサードパーティ製ツールを使用して顧客とファイルをやり取りしています。過去には、営業チームのデバイスがさまざまな攻撃を受けたことがあります。
Contoso社のマーケティングチームは、外部ベンダーとの連携のために複数のMicrosoft SharePoint Onlineサイトを運用しています。しかし、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態が何度か発生しています。
Contosoの経営陣は、セキュリティ侵害が発生した疑いがあると見ています。経営陣は、Microsoft Cloud App Securityで保護されているアプリケーションにおいて、過去48時間以内にデータアクセス、ダウンロード、削除などの操作が5回以上行われたファイルを特定していただくようお願いしています。
要件
計画されている変更
Contosoは、両社のセキュリティ業務を統合し、すべてのセキュリティ業務を一元的に管理する計画だ。
技術要件
Contoso社は、以下の技術要件を特定しました。
* 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 を使用すると、環境に対するアクティブな攻撃を迅速に修復することで、組織のリスクを軽減できます。
* ContosoとFabrikamのAzure ADテナント間でデータを関連付けるAzure Sentinelクエリを実装する。
* 外部からの攻撃や、Fabrikam自身のAzure ADアプリケーションが侵害される可能性が発生した場合に、Azure Defender for Key VaultのアラートをFabrikam向けに修復するための手順を開発する。
* 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。下級セキュリティ管理者が、以下の不完全なクエリを提供します。
行動分析
| ActivityType == "FailedLogOn"
| ただし、_____ == True

質問: **127**
お客様は、Microsoft Exchange Onlineを使用するMicrosoft 365 E5サブスクリプションをお持ちです。
フィッシングメールを識別する必要があります。
どの 3 つのコマンドレットを順番に実行する必要がありますか？回答するには、コマンドレットの一覧から適切なコマンドレットを回答欄に移動し、正しい順序に並べ替えてください。

正解:



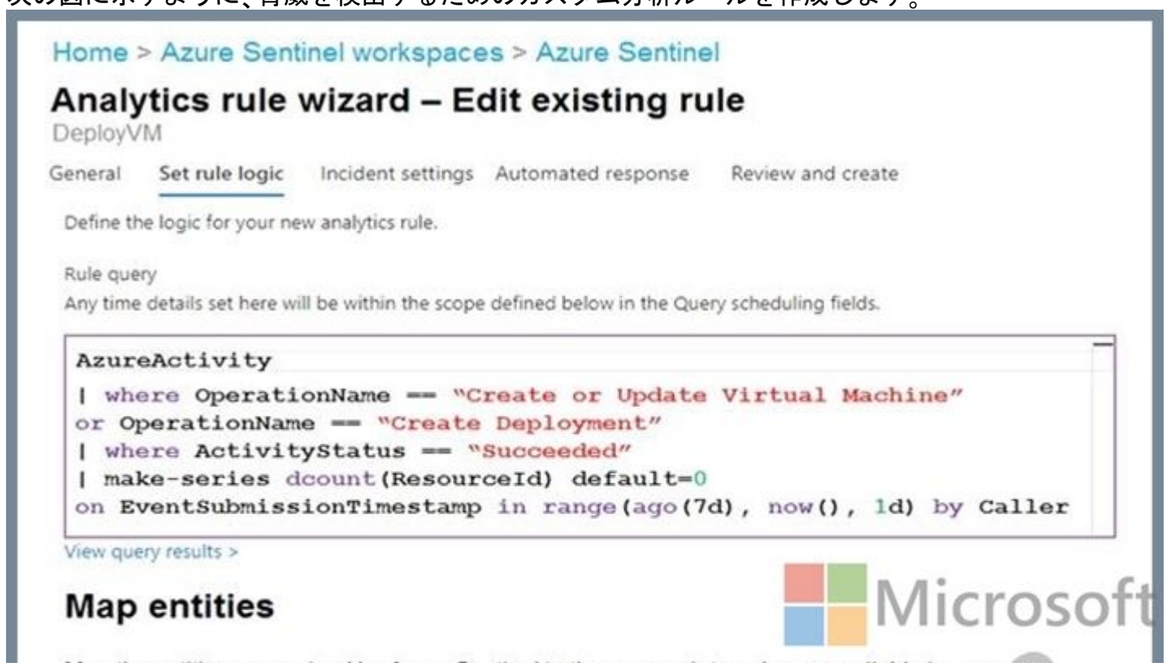
Explanation:

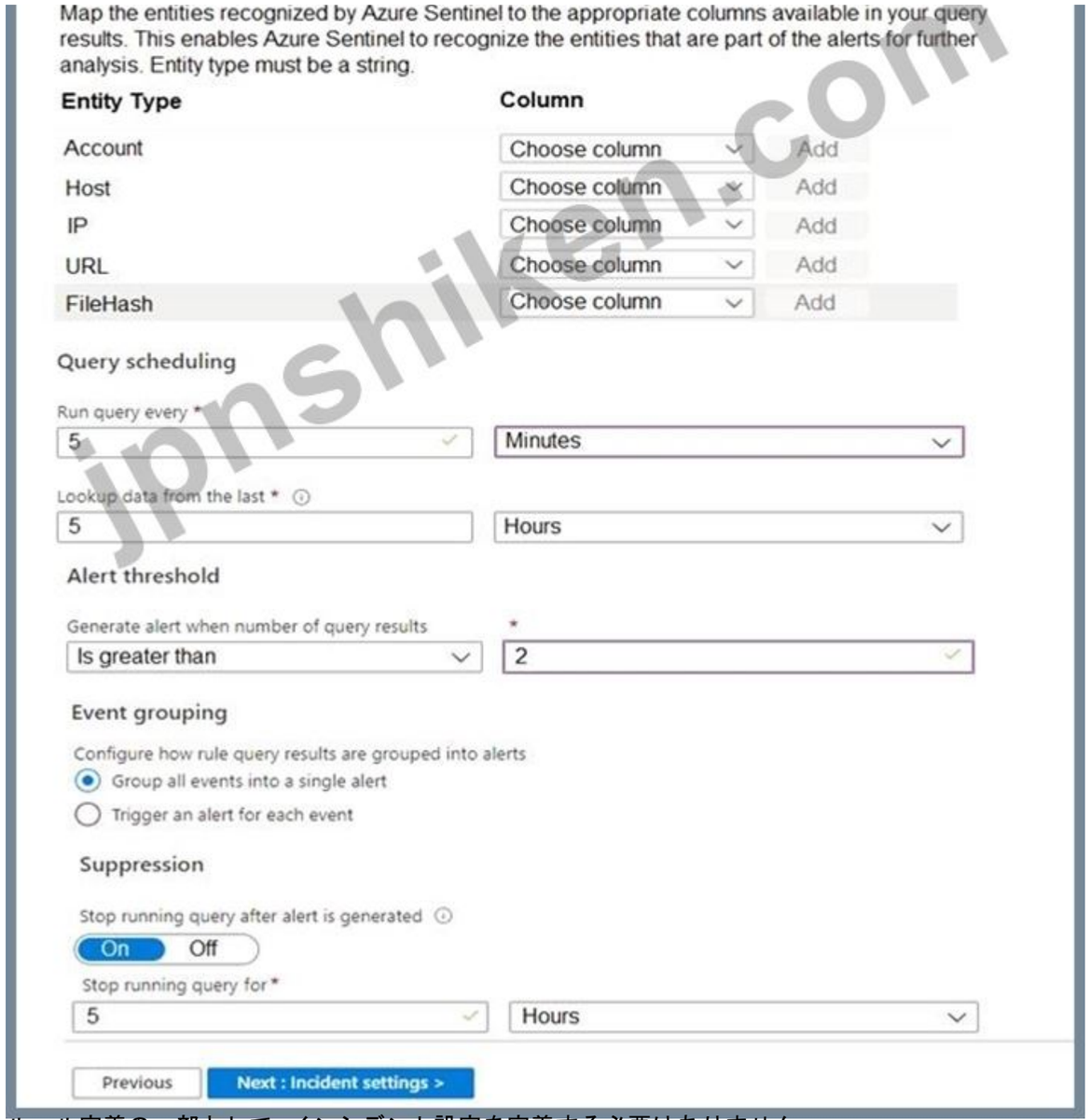


質問: **128**

Azure Sentinel は、Azure の異常なアクティビティを監視するために使用されます。

次の図に示すように、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。

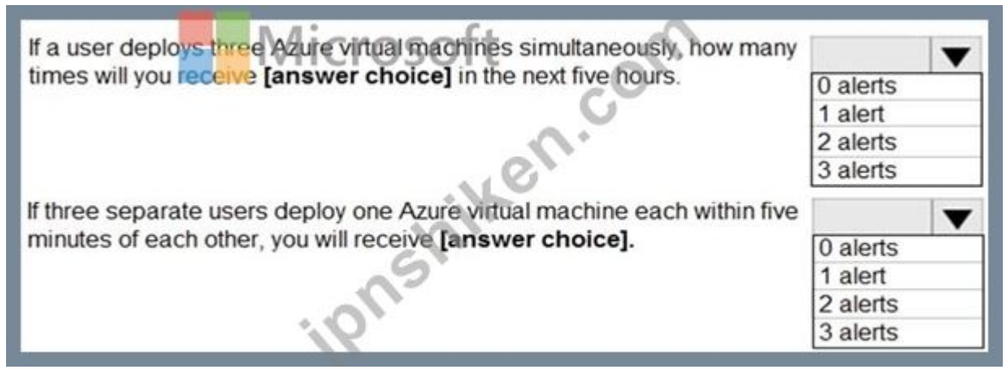




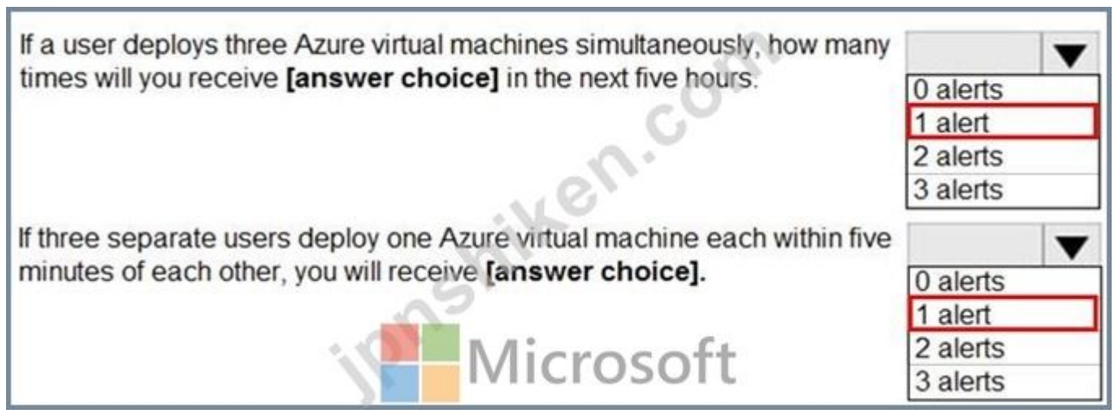
ルール定義の一部として、インシデント設定を定義する必要はありません。

図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。

注：正解ごとに1ポイントが加算されます。



正解:



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