Microsoft.SC-200J.v2026-08-17.q236

試験コード：	SC-200J
試験名称：	Microsoft Security Operations Analyst (SC-200日本語版)
認証ベンダー：	Microsoft
無料問題の数：	236
バージョン：	v2026-08-17
ページの閲覧量：	102
問題集の閲覧量：	2413

https://www.jpnshiken.com/shiken/Microsoft.SC-200J.v2026-08-17.q236.html

質問: **1**
Azure Sentinel を構成しています。
不審なIPアドレスからのサインインが検出された場合は、Microsoft Teamsのチャネルにメッセージを送信する必要があります。
Azure Sentinelで実行すべき2つの操作はどれですか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。
A. プレイブックを追加します。
B. インシデントにプレイブックを関連付けます。
C. エンティティの動作分析を有効にします。
D. ワークブックを作成します。
E. 融合ルールを有効にします。

正解: **A,B (コメントを発表する)**
Playbooks are collections of procedures that can be run from Azure Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.
Playbooks in Azure Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps.
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

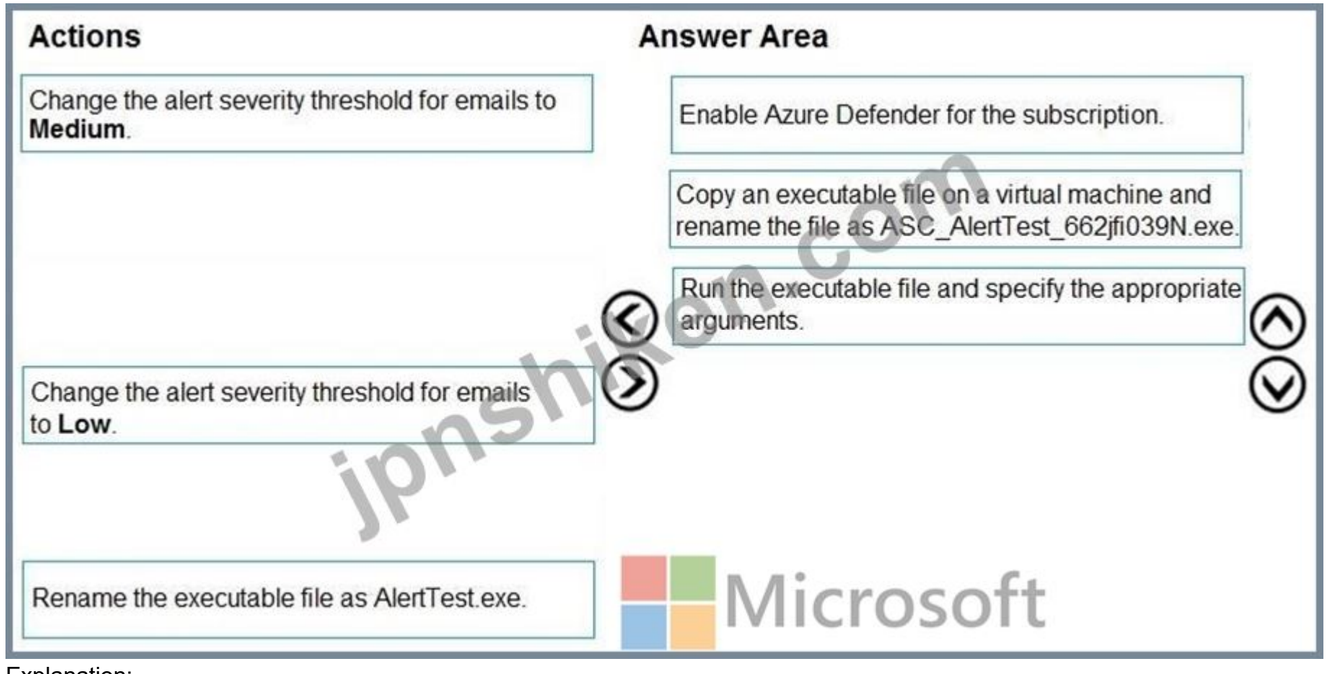
質問: **2**
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションをお持ちです。
セキュリティインシデントを解決するのにかかる平均時間を計算するカスタムワークブックを作成する必要があります。このソリューションは、管理作業を最小限に抑えるものでなければなりません。
Microsoft Sentinelに組み込まれているワークブックテンプレートのうち、どれを選択すべきでしょうか？
A. セキュリティ運用効率
B. 事件概要
C. ワークスペース使用状況レポート
D. 調査分析
正解: **(正解を表示します)**
Microsoft Sentinel, Manage your SOC better with incident metrics
Security operations efficiency workbook
To complement the SecurityIncidents table, we've provided you with an out-of-the-box security operations efficiency workbook template that you can use to monitor your SOC operations. The workbook contains the following metrics:
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/manage-soc-with-incident-metrics

質問: **3**
Microsoft Defender for Cloud を使用する 2 つの Azure サブスクリプションがあります。
特定の Defender for Cloud セキュリティ アラートがルート管理グループ レベルで抑制されていることを確認する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
Azure ポータルでは何をすべきでしょうか?
A. Azure Policy 割り当てを作成します。
B. Defender for Cloud のワークロード保護設定を変更します。
C. Azure Monitor でアラート ルールを作成します。
D. Defender for Cloud のアラート設定を変更します。
正解: **(**正解を表示します**)**
To suppress alerts at the management group level, use Azure Policy.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule

質問: **4**
Microsoft Defender for Cloud の強化されたセキュリティ機能が有効になっている 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Defender for Cloudからアラートデータをエクスポート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？
A. ユーザーアクセス管理者
B. オーナー
C. 寄稿者
D. 読者
正解: **(**正解を表示します**)**
Because Security admin isn't in the answers.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-portal#availability

質問: **5**
ドラッグアンドドロップ問題
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。
どの3つの行動を順番に実行すべきですか？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:

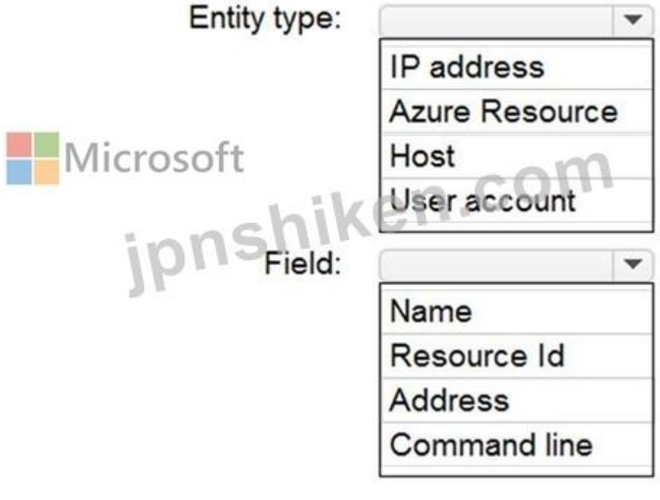
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

質問: **6**
お客様は、以下のリソースを含む Microsoft 365 サブスクリプションをお持ちです。
- Microsoft 365 E5 ライセンスが割り当てられているユーザー 100 人
- Microsoft Entraテナントに参加しているWindows 11デバイス100台
ユーザーは、Web版Outlookを使用してMicrosoft Exchange Onlineのメールボックスにアクセスします。
ユーザーアカウントが侵害された場合に、Outlook on the web のセッショントークンを失効させる必要があります。どのような設定を行うべきでしょうか？
A. Microsoft Entra ID Protection
B. Microsoft Entra のセキュリティのデフォルト設定
C. Microsoft Entra Verified ID
D. Microsoft Entra の条件付きアクセス ポリシー
正解: **(**正解を表示します**)**

質問: **7**
Windows 10システムがデバイス一覧に表示されません。何が原因でしょうか？
A. システムに最新のKBがインストールされていません
B. 過去30日間、システムにはアラートがありません。
C. システム名が変更されました。
D. 上記以外
正解: **(**正解を表示します**)**
Options A, C, D are incorrect. Neither renaming any device nor KB's has any impact on the Device inventory list.
Option B is correct. We can modify the "time setting" to find the system.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/asset-inventory

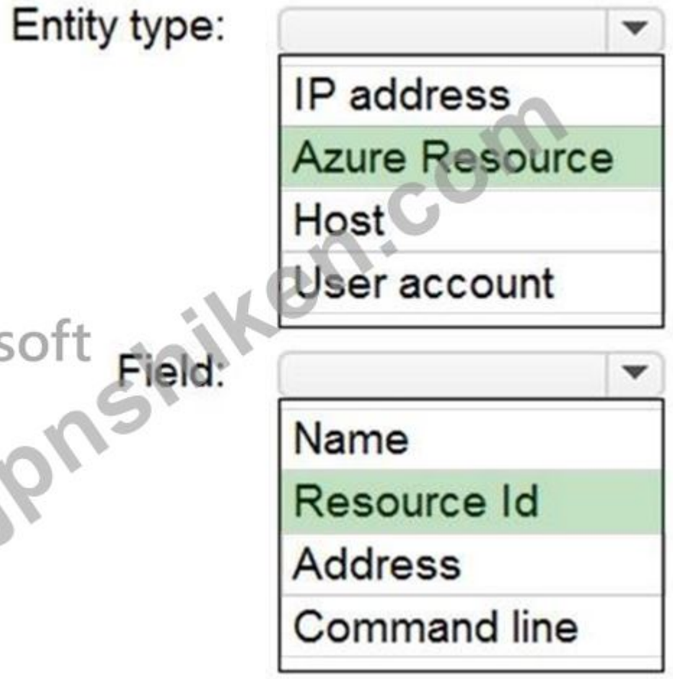
質問: **8**
ホットスポットに関する質問
アプリケーション開発中に複数のAzure Functionsアプリからアクセスされるストレージアカウントをお持ちです。
ストレージアカウントに関するAzure Defenderのアラートを非表示にする必要があります。
抑制ルールでは、どのエンティティタイプとフィールドを使用すべきですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:

Answer Area



Explanation:
Entity Type = Azure Resource (Azure Storage is a Resource)
Field = Resource ID (All Azure resources have an ID)
https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

質問: **9**
事例研究4 - Litware Inc.
概要
アダタム ･コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境
オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。
ライセンス状況
Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。

クラウド環境

クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境

オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件

計画されている変更

Adatum社は以下の変更を実施する予定です。

- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。

Microsoft Defender for Cloud の要件

Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。

グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。

- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。

Microsoft Sentinelの要件

Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。

- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。

- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。
可能な限り、ASIMに組み込まれているパーサーを使用してください。
ビジネス要件
Adatumは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則に従うこと。
可能な限り管理業務を最小限に抑える。
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. Microsoft Antimalware拡張機能
B. Windows 用 Azure Automanage マシン構成拡張機能
C. Azureリソースロック
D. Azureリソースタグ
正解: **(**正解を表示します**)**
Server2 should be excluded from agentless scanning - therefore a tag is needed.

質問: **10**
あなたは、脅威脆弱性管理によって報告された脆弱性を修正するために、エンドポイントチームと連携する責任を負っています。CVE IDを一覧表示することで、システムに存在する脆弱性のインベントリを管理するレポートはどれですか？
A. 弱点
B. ソフトウェアインベントリ
C. イベントタイムライン
D. 事件
正解: **A (**コメントを発表する**)**
Option A is correct. This report is enumerated by the CVE ID.
Option B is incorrect. The software inventory page contains a list of software installed in your organization.
Option C is incorrect. The event timeline is a risk feed that lets you understand how risk is introduced in the organization.
Option D is incorrect. The incident report doesn't contain any weaknesses or vulnerabilities.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/tvm-weaknesses?view=o365-worldwide

質問: **11**
あなたは、User1とUser2という名前の2人のユーザーを含むMicrosoft 365 E5サブスクリプションを所有しており、セキュリティ対策としてMicrosoft Copilotを使用しています。
ユーザー1は、Copilot for Securityポータルからセッションを開始し、以下のプロンプトを作成します。
- プロンプト1 :Entraプラグインへのアクセスを提供します
- プロンプト2 :Intuneプラグインへのアクセスを提供します
- Prompt3: Entraプラグインへのアクセスを提供します
ユーザー1はユーザー2とセッションを共有します。

ユーザー2はMicrosoft Intuneへのアクセス権を持っていません。
ユーザー2は、共有セッション中にどのプロンプトの結果を表示できますか？
A. プロンプト3のみ
B. プロンプト1のみ
C. プロンプト1、プロンプト2、プロンプト3
D. プロンプト1とプロンプト2のみ
E. プロンプト1とプロンプト3のみ
正解: **E** (コメントを発表する)

質問: **12**
機密ファイルの外部共有に対応してアラートを生成し、修復アクションをトリガーするように、Microsoft Defender for Cloud Apps を構成する必要があります。
Microsoft 365 Defender ポータルで実行すべき操作はどれですか？(2つ選択してください。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. 設定から 「クラウド アプリ」を選択し、「Microsoft Information Protection」を選択してから、「このテナントからの Microsoft Information Protection の機密ラベルとコンテンツ検査警告のファイルのみをスキャンする」を選択します。
B. クラウドアプリから 「ファイル」を選択し、ファイルの種類を 「ドキュメント」でフィルタリングします。
C. 設定から、クラウド アプリを選択し、Microsoft Information Protection を選択し、ファイルを選択して、ファイル監視を有効にします。
D. クラウド アプリからファイルを選択し、アプリを Office 365 にフィルタリングします。
E. クラウドアプリから 「ファイル」を選択し、検索から 「新しいポリシー」を選択します。
F. 設定から 「クラウド アプリ」を選択し、「Microsoft Information Protection」を選択してから、「Microsoft Information Protection の機密ラベルとコンテンツ検査警告について新しいファイルを自動的にスキャンする」を選択します。
正解: (正解を表示します)
To configure Microsoft Defender for Cloud Apps to generate alerts and trigger remediation actions for the external sharing of confidential files, perform the following two actions in the Microsoft 365 Defender portal:
1. From Cloud apps, select Files, and then select New policy from search.
This action allows you to create a file policy that detects when confidential files are shared externally. By setting specific filters and conditions, you can configure the policy to generate alerts and apply remediation actions, such as removing external sharing permissions or applying sensitivity labels, when such sharing is detected.
2. From Settings, select Cloud App, select Microsoft Information Protection, and then select Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings.
Enabling this option ensures that Defender for Cloud Apps automatically scans new files for sensitivity labels and content inspection warnings. This scanning is crucial for identifying confidential files and applying appropriate policies to protect them from unauthorized external sharing.
By implementing these two actions, Defender for Cloud Apps will be configured to detect and respond to the external sharing of confidential files effectively.

質問: **13**
事例研究2 - Litware Inc.
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たアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。
Azure Sentinelの要件とビジネス要件を満たすには、admin1にロールベースアクセス制御(RBAC)ロールを割り当てる必要があります。
どの役割を割り当てるべきですか？
A. 自動化オペレーター
B. 自動化ランブックオペレーター
C. Azure Sentinel 貢献者
D. Logic Appコントリビューター
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#microsoft-sentinel-automation-contributor

質問: **14**
1,000 台の Windows 10 デバイスを含む Microsoft 365 サブスクリプションがあります。デバイスには Microsoft Office 365 がインストールされています。
次のデバイスの脅威を軽減する必要があります。
信頼できない Web サイトからスクリプトをダウンロードする Microsoft Excel マクロ
Microsoft Outlook で実行可能な添付ファイルを開くユーザー
Outlook のルールとフォームの悪用
何を使えばいいのでしょうか？
A. Microsoft Defender ウイルス対策
B. Microsoft Defender for Endpoint の攻撃対象領域削減ルール
C. Windows Defender ファイアウォール
D. Azure Defender の適応型アプリケーション制御
正解: **(**正解を表示します**)**
Attack Surface Reduction rules.
Block all Office applications from creating child processes
Block executable content from email client and webmail
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide

質問: **15**
ホットスポットに関する質問
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。
Microsoft Defender for Cloud が特定の警告を受信したときにロジック アプリ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 (ARM) テンプレートを使用する必要があります。
テンプレートはどのように記入すればよいですか？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

```
"actions": [
  {
    "actionType": "LogicApp",
    "logicAppResourceId": "[resourceId('                    /workflows', parameters('logicAppName'))]",
    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
...
}
```

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

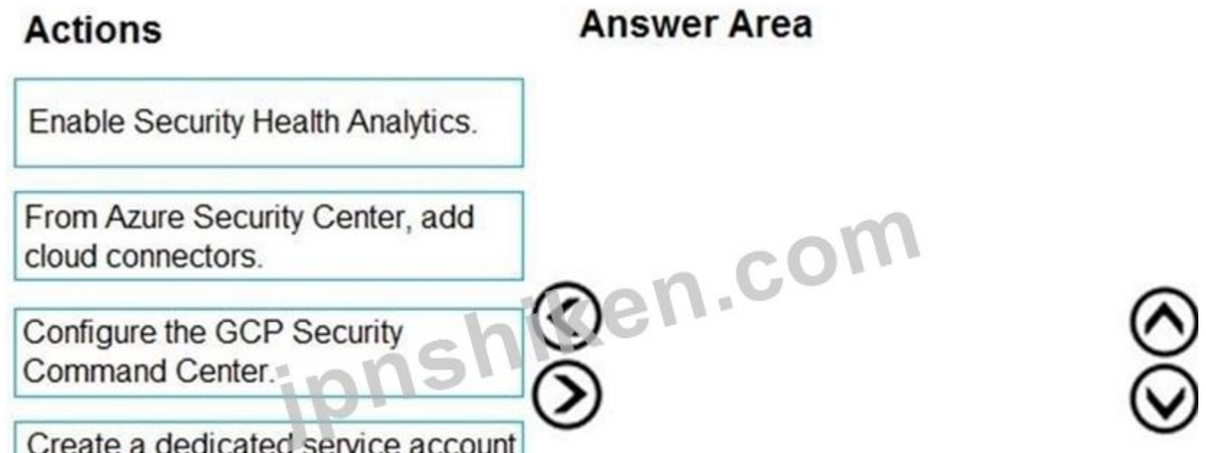
正解:

Answer Area

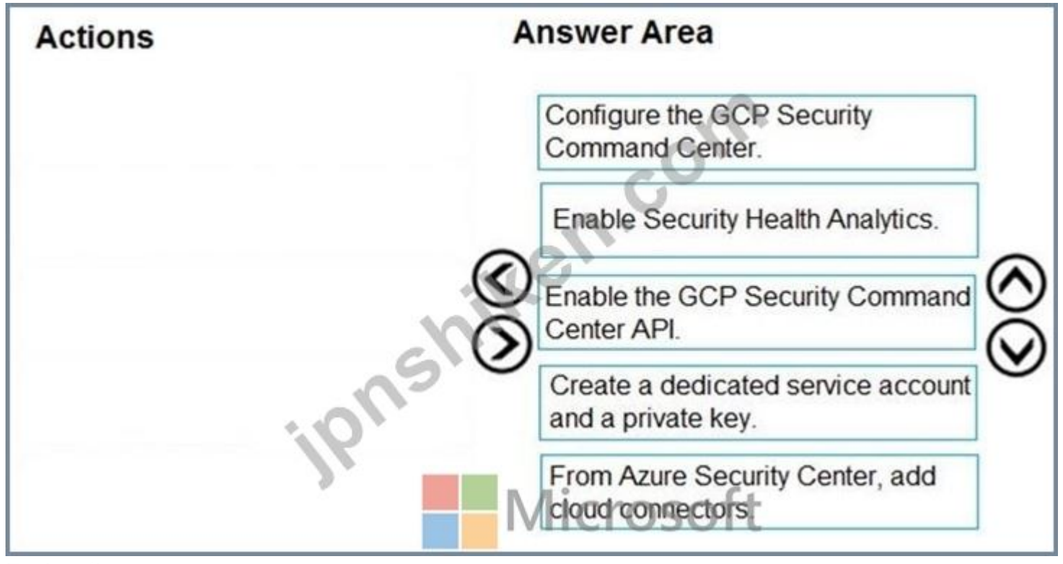
```
"actions": [
  {
    "actionType": "LogicApp",
    "logicAppResourceId": "[resourceId('                                    /workflows', parameters('logicAppName'))]",
    "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'), parameters('logicAppResourceGroupName'),
...
}
```

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

質問: **16**
ドラッグアンドドロップ問題
AzureとGoogle Cloudにリソースがあります。
Google Cloud Platform (GCP) のデータを Azure Defender に取り込む必要があります。
どのような順序で操作を実行すればよいですか？回答するには、操作リストからすべての操作を回答欄に移動し、正しい順序に並べ替えてください。



正解:



Explanation:

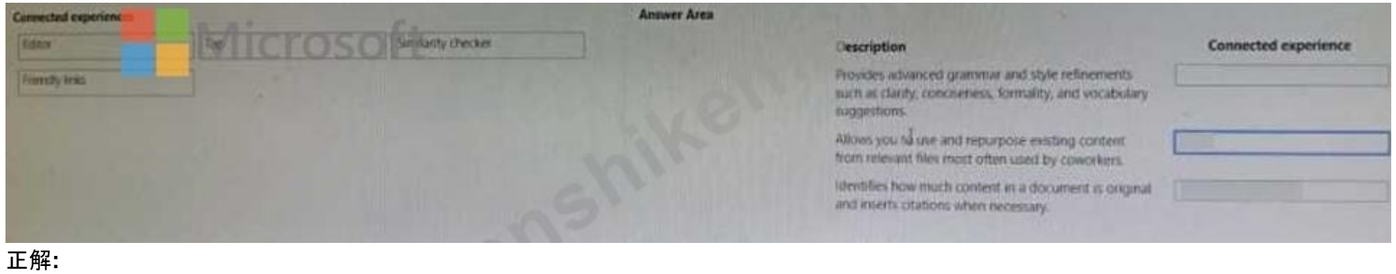
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=classic-connector

質問: **17**
カスタム Kusto クエリを含む workspace1 という名前の Microsoft Sentinel ワークスペースがあります。
ビジュアルを作成する Python ベースの Jupyter ノートブックを作成する必要があります。ビジュアルにはクエリの結果が表示され、ダッシュボードに固定されます。ソリューションでは、開発労力を最小限に抑える必要があります。
ビジュアルを作成するには何を使用する必要がありますか?
A. プロット
B. TensorFlow
C. msticpy
D. matplotlib
正解: **(**正解を表示します**)**
msticpy is a library for InfoSec investigation and hunting in Jupyter Notebooks. It includes functionality to: query log data from multiple sources. enrich the data with Threat Intelligence, geolocations and Azure resource data. extract Indicators of Activity (IoA) from logs and unpack encoded data.
MSTICPy reduces the amount of code that customers need to write for Microsoft Sentinel, and provides:
- Data query capabilities, against Microsoft Sentinel tables, Microsoft Defender for Endpoint, Splunk, and other data sources.
- Threat intelligence lookups with TI providers, such as VirusTotal and AlienVault OTX.
Enrichment functions like geolocation of IP addresses, Indicator of Compromise (IoC) extraction, and WhoIs lookups.
- Visualization tools using event timelines, process trees, and geo mapping. Advanced analyses, such as time series decomposition, anomaly detection, and clustering.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started
https://msticpy.readthedocs.io/en/latest/

質問: **18**
詳細なファイル分析によって、どのような情報が共有されるのでしょうか？
A. レジストリの変更
B. コード変更履歴
C. コマンド履歴
D. プロセス履歴
正解: **(**正解を表示します**)**
Command history, process and code change history are not reported. Only Registry modifications are reported.
Deep file analysis results contain the file's activities, behaviors, and artifacts like dropped files, registry changes and IP communication.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-file- alerts?view=o365-worldwide

質問: **19**
ドラッグアンドドロップ問題
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: **20**
事例研究2 - Litware Inc.
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。

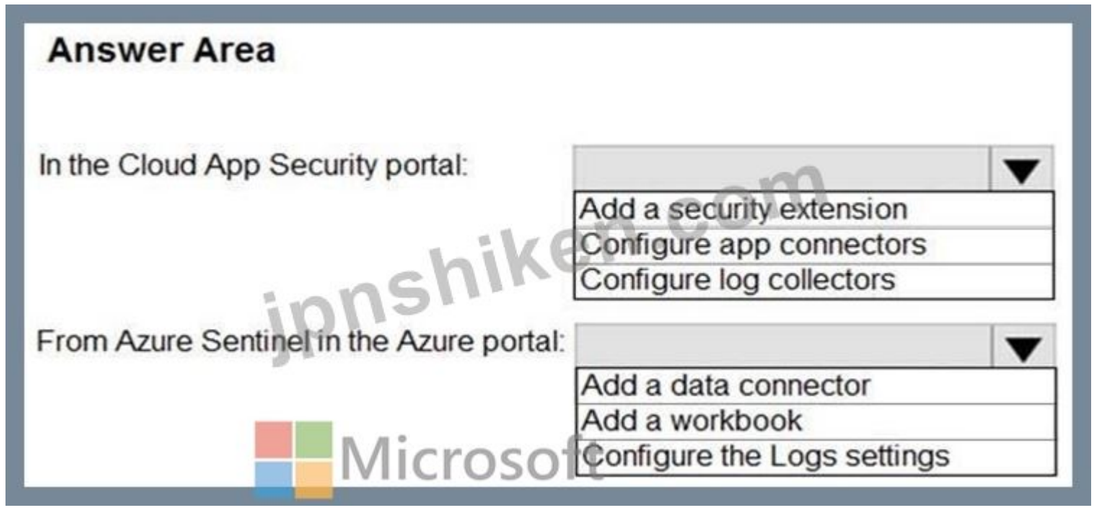
Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

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。

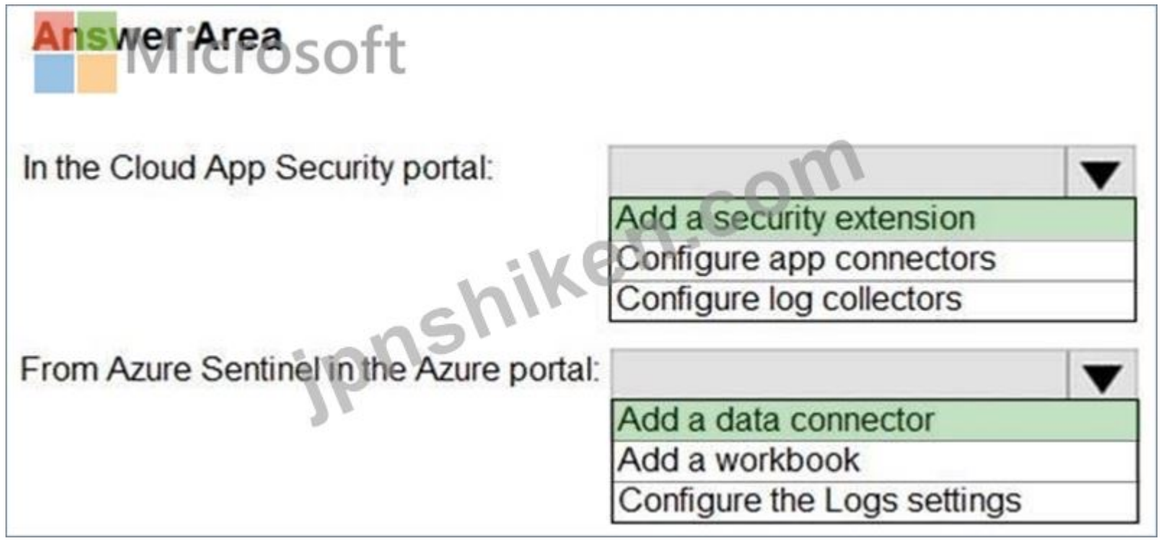
オンプレミス環境
オンプレミスネットワークには、次の表に示すコンピュータが含まれています。

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たアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。
ホットスポットに関する質問
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:



Explanation:

To connect Defender for Cloud Apps (MCAS) to Microsoft Sentinel:

1. From Defender for Cloud Apps --> Security extensions --> Add SIEM agents tab --> then click "Add SIEM agent" and select Microsoft Sentinel
2. From Sentinel --> Data connectors --> Select "Microsoft Defender for Cloud Apps" --> and make sure it is connected.

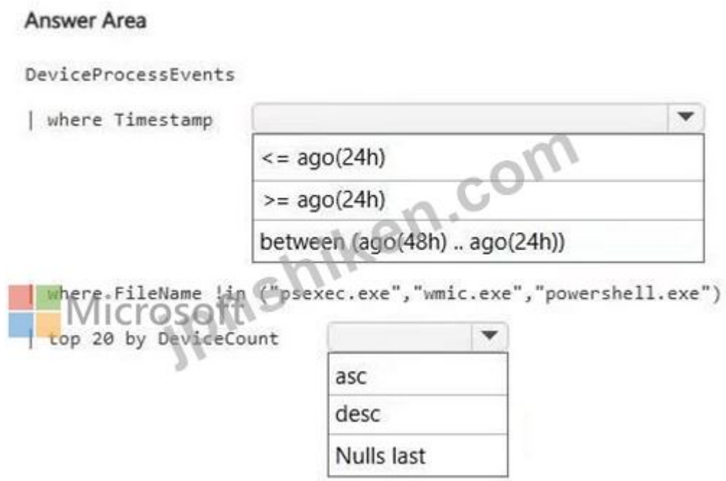
Reference:

https://docs.microsoft.com/en-us/defender-cloud-apps/siem-sentinel

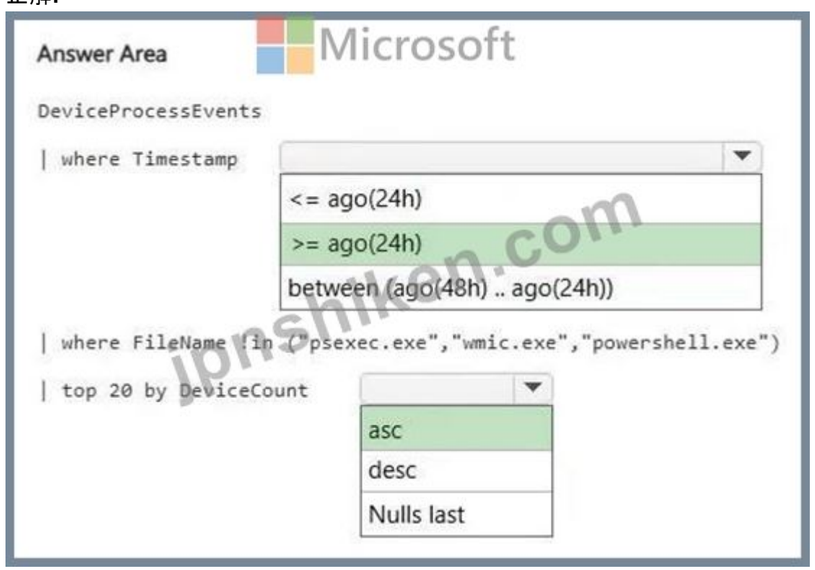
https://docs.microsoft.com/en-us/azure/sentinel/data-connectors-reference#microsoft-defender-for-cloud-apps

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/microsoft-cloud-app-security-mcas-activity-log-in-azure-sentinel/ba-p/1849806

質問: **21**
ホットスポットに関する質問
Microsoft Sentinelワークスペースがあり、そこからエンドポイントのプロセスイベントがLog Analyticsワークスペースに取り込まれます。
Windows デバイス上で、疑わしい、めったに見られないプロセスを特定するハンティングクエリ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 24 時間で観測されたプロセス名のうち、最も出現頻度の低い 20 件を返します
時間。
承認済みの管理ツールの一覧を除外します。
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。



正解:



質問: **22**
ドラッグアンドドロップ問題
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 Entra ID監査ログ用のワークブックを作成し、カスタマイズ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:

Actions

- From Workbooks, select Microsoft Entra ID Audit logs and then select **Save**.
- Enable Workspace manager.
- From Workbooks, select Microsoft Entra ID Audit logs and then select **View Template**.

Order

1. From Content hub, install the Microsoft Entra ID solution.
2. Configure a Data connector.
3. From Workbooks, select Microsoft Entra ID Audit logs and then select **View saved workbook**.

質問: **23**

事例研究1 - Contoso Ltd

概要

Contoso Ltd.という会社は、北米各地に本社と5つの支店を構えています。本社はシアトルにあり、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

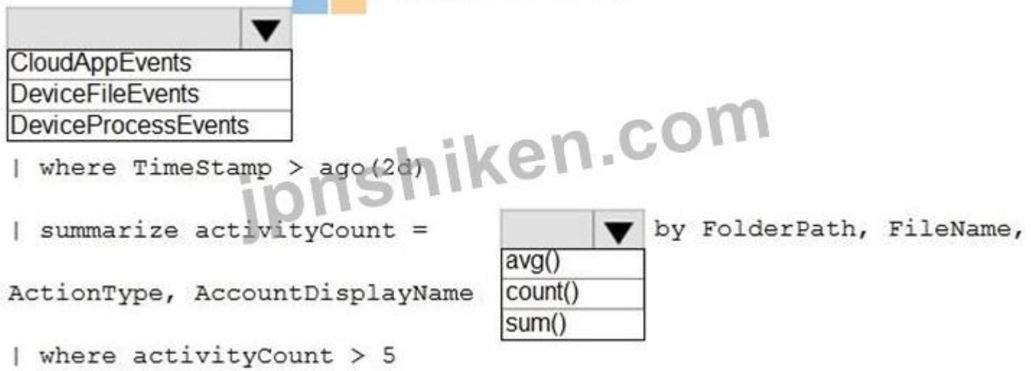
Contosoのセキュリティチームは、大量のサイバーセキュリティアラートを受信している。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威で、どれがそうでないかを判断するのに多くの時間を費やしている。

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る。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複数発生している。

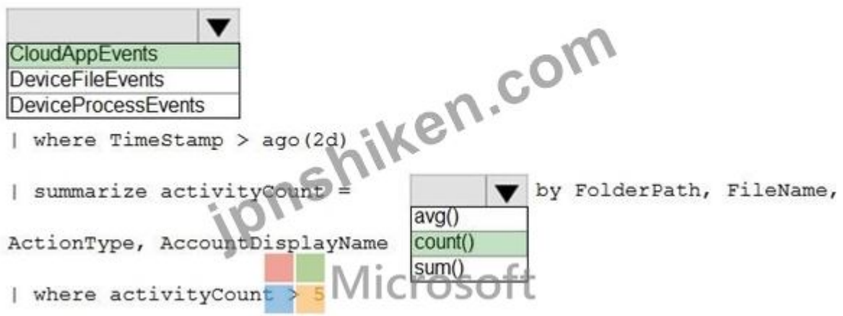
Contosoの経営陣は、セキュリティ侵害が発生した疑いがあると見ています。経営陣は、Microsoft Cloud App Securityで保護されているアプリケーションにおいて、過去48時間以内にデータアクセス、ダウンロード、削除などの操作が5回以上行われたファイルを特定していただくようお願いしています。
要件
計画されている変更
Contosoは、両社のセキュリティ業務を統合し、すべてのセキュリティ業務を一元的に管理する計画だ。
技術要件
Contoso社は、以下の技術要件を特定しました。
* Azure仮想マシンがブルートフォース攻撃を受けている場合にアラートを受信します。
* Azure 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
ホットスポットに関する質問
経営陣の問題を調査するには、高度なハンティングクエリを作成する必要があります。
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



正解:

Answer Area

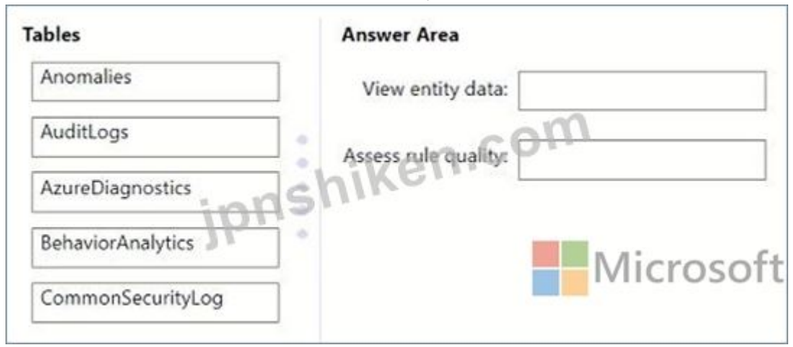


Explanation:
Box 1: CloudAppEvents
The AppFileEvents table, which contains file activities from these applications, will stop getting populated with new data in early 2021. Activities involving these applications, including file activities, will be recorded in the new CloudAppEvents table.
Box 2: Count
https://techcommunity.microsoft.com/t5/microsoft-365-defender/hunt-across-cloud-app-activities-with-microsoft-365-defender/ba-p/1893857

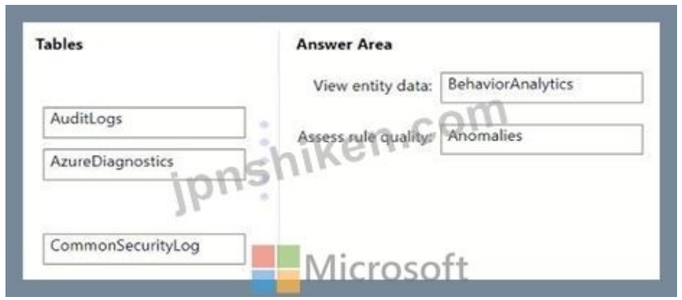
質問**: 24**
Microsoft 365 Defenderは、Microsoft 365サービス全体にわたるセキュリティインシデントとアラートを管理および調査するための、目的に特化したユーザーインターフェースを提供します。
あなたは、Microsoft 365 Defenderソリューション(Defender for Endpoint、Defender for Identity、Defender for Office 365、およびCloud App Securityを含む)を構成しているXYZ社に勤務するSOCアナリストです。
インシデントの影響全体を把握し、根本原因分析(RCA)を実施するには、すべてのソリューションにわたる関連アラートを単一のインシデントとして監視する必要があります。Microsoft セキュリティ センター ポータルでは、インシデントとその対応策が統合的に表示されます。
特定のインシデントを調査する際、インシデントページにはどのタブが表示されますか？
A. 機械
B. 郵便ポスト
C. ネットワーク
D. 事件
正解**: (**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-incidents?view=o365-worldwide

質問**: 25**
ドラッグアンドドロップ問題
SW1という名前のMicrosoft Sentinelワークスペースがあります。
SW1では、ユーザーおよびエンティティ行動分析(UEBA)を有効にします。
以下のタスクを実行するには、KQLを使用する必要があります。
- 各エンティティタイプに対応するフィールドを持つエンティティデータを表示します。
ルールがどれだけ効果的に機能しているかを分析することで、ルールの質を評価する。
各タスクでKQLのどのテーブルを使用すべきでしょうか？回答するには、適切なテーブルを正しいタスクにドラッグしてください。各テーブルは、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:



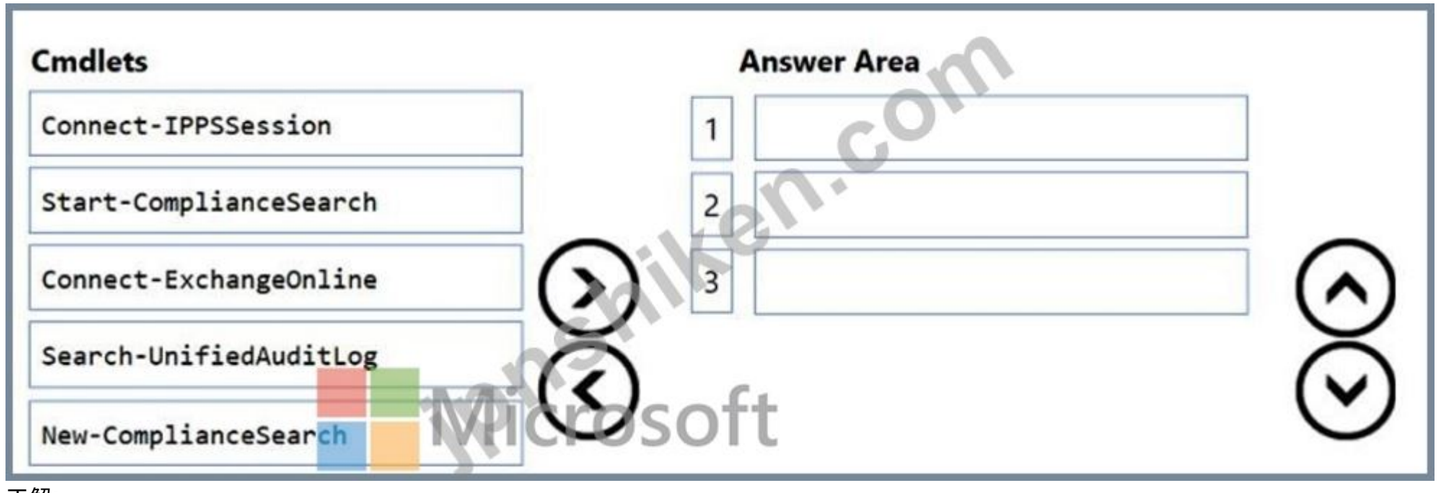
質問: **26**

ドラッグアンドドロップ問題

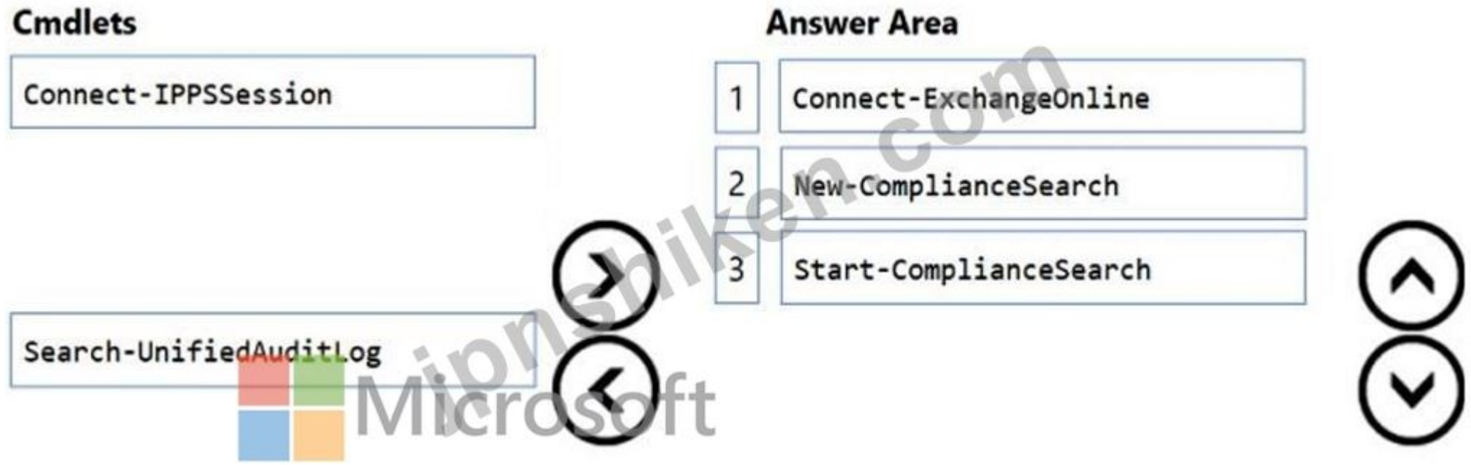
お客様は、Microsoft Exchange Onlineを使用するMicrosoft 365 E5サブスクリプションをお持ちです。

フィッシングメールを識別する必要があります。

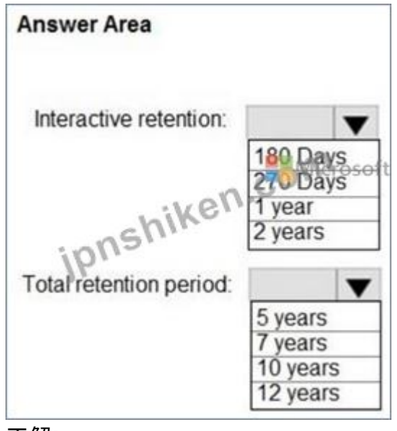
どの 3 つのコマンドレットを順番に実行する必要がありますか？回答するには、コマンドレットの一覧から適切なコマンドレットを回答欄に移動し、正しい順序に並べ替えてください。



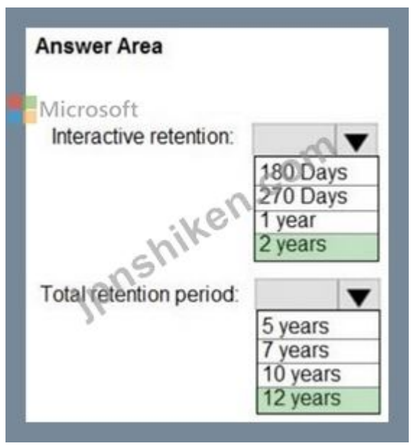
正解:



質問: **27**
ホットスポットに関する質問
Table1という名前のテーブルを含むMicrosoft Sentinelワークスペースがあります。Table1には分析プランが構成されています。
Table1の保持期間を設定する必要があります。ソリューションは、Table1に保存されているデータの保持期間を最大限に確保する必要があります。
データ保持設定はどのように構成すればよいですか？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: **28**
事例研究3 - Litware Inc.
概要
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。
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、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。
Microsoft 365環境
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を実装し、ログコレクターを有効にします。
Azure環境
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.

Amazon Web Services (AWS) 環境
FabrikamはAccount1という名前のAmazon Web Services(AWS)アカウントを持っています。Account1には
カスタム版Windows Server 2022を実行するAmazon Elastic Compute Cloud(EC2)インスタンス100台。
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。
最新の課題
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」に関する警告を大量に発生させます。
Defender for Identityは、DCSync攻撃の疑いに関するアラートを大量に発生させますが、その多くは誤検知です。
要件
計画されている変更
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
ビジネス要件
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。
Microsoft Defender for Cloud Apps の要件
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。
Microsoft Defender for ID の要件
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。
Microsoft Defender for Cloud の要件
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する。

- 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。
Microsoft Sentinelの要件
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の平均解決時間を特定します。
- 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、Pool1に対して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。
App1には、Microsoft Sentinelの要件を満たす必要があります。
App1にはどのような設定が必要ですか？
A. トリガー
B. コネクタ
C. 認証
D. API接続
正解: **C** (コメントを発表する)
Microsoft Sentinel requires permissions to run incident-trigger playbooks(Logic Apps). To run a playbook based on the incident trigger, whether manually or from an automation rule, Microsoft Sentinel uses a service account specifically authorized to do so.
https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks#incident-creation-automated-response

質問: **29**
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。
お客様はAmazon Web Services(AWS)のサブスクリプションをご利用中です。このサブスクリプションには、Windows Serverを実行する複数の仮想マシンが含まれています。
仮想マシン上でMicrosoft Defender for Serversを有効に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. Defender for Cloud から、エージェントレス スキャンを有効にします。
B. 仮想マシンを Microsoft Defender for Endpoint にオンボーディングします。
C. Defender for Cloud から AWS コネクタを設定します。
D. 各仮想マシンに Azure 仮想マシン エージェント (VM エージェント) をインストールします。
E. Defender for Cloud から、自動プロビジョニングを設定します。

正解: (正解を表示します)
For a Defender for Servers deployment, you set up a connector, turn off plans you don't need, configure auto-provisioning settings, authenticate to AWS/GCP, and deploy the settings.
Auto-provisioning includes the agents used by Defender for Cloud and the Azure Connected Machine agent for onboarding to Azure with Azure Arc.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for- servers?source=recommendations

質問: **30**
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. マイクロソフト センチネル レスポンダー
B. マイクロソフトセンチネル貢献者
C. Microsoft Sentinel Automation 貢献者
D. Microsoft Sentinel Reader
正解: **A** (コメントを発表する)
The Microsoft Sentinel Responder role is specifically designed for users who need to investigate and respond to incidents in Microsoft Sentinel. This role provides the necessary permissions to investigate incidents and alerts, while adhering to the principle of least privilege, as it does not grant permissions beyond what is needed for incident response.

質問: **31**
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
組み込みの統合型ASIMパーサーから、ソース固有の組み込み型Advanced Security Information Model(ASIM)パーサーを除外する必要があります。
Workspace1には何を作成すべきですか？
A. ウォッチリスト
B. 解析規則
C. 狩猟に関する質問
D. ワークブック
正解: (正解を表示します)
To support excluding built-in source-specific parsers, ASIM uses a watchlist.
https://learn.microsoft.com/en-us/azure/sentinel/normalization-manage-parsers#set-up-your-workspace

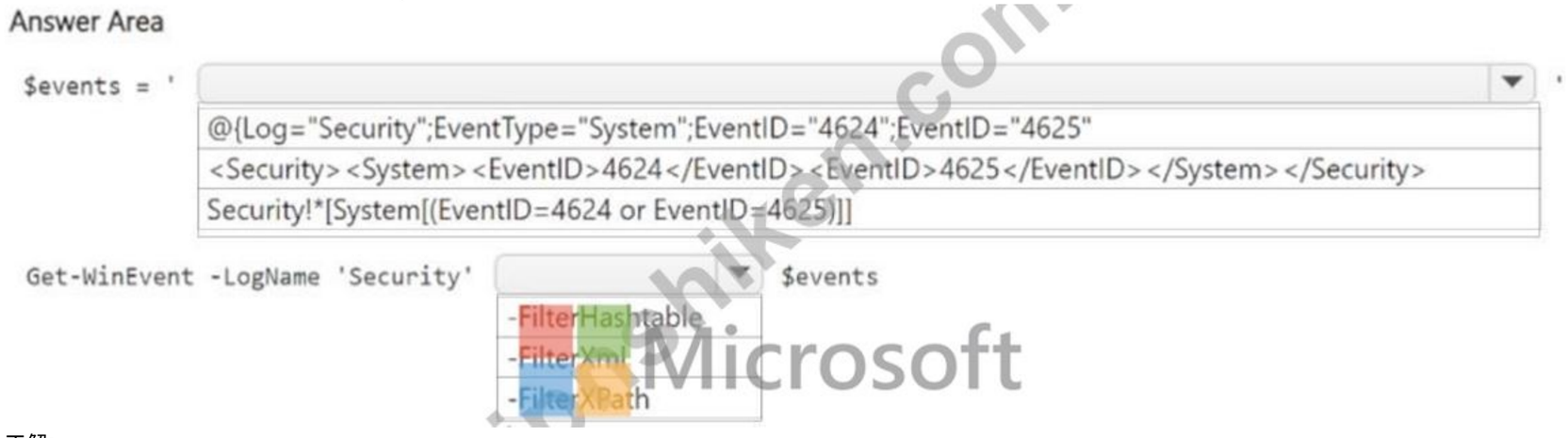
質問: **32**
お客様の環境には、Microsoft Defender for Endpoint にオンボーディングされたオンプレミスの Windows 11 Pro デバイスが 1,000 台あります。
お客様は、Microsoft Defender XDRを使用するMicrosoft 365サブスクリプションをご利用されています。
攻撃者がデバイス上で以下の操作を実行したことを確認しました。
レジストリベースのウイルス対策除外のファイルシステムパスを変更しました
ファイルシステムパスに悪意のあるファイルをダウンロードしました

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。
レジストリの変更を元に戻す必要があります。
どのコマンドを実行すればよいですか？
A. 修復する
B. 登録
C. スキャン
D. 分析
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/defender-endpoint/live-response

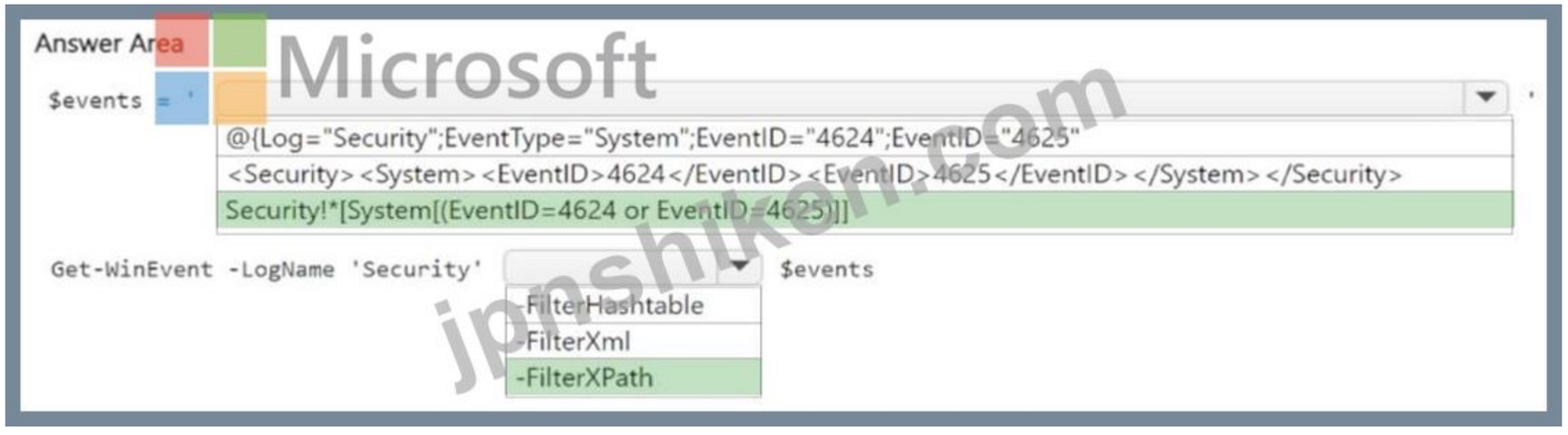
質問: **33**
事例研究1 - Contoso Ltd
概要
Contoso Ltd.という会社は、北米各地に本社と5つの支店を構えています。本社はシアトルにあり、支店はトロント、マイアミ、ヒューストン、ロサンゼルス、バンクーバーにあります。
コントソ社は、ニューヨークとサンフランシスコにオフィスを構えるファブリカム社という子会社を所有している。
既存の環境
エンドユーザー環境
Contosoの全ユーザーはWindows 10デバイスを使用しています。各ユーザーはMicrosoft 365のライセンスを取得しています。さらに、Contosoの営業チームのメンバーにはiOSデバイスが配布されています。
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アラートを受信している。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威で、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る。
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る。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複数発生している。
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
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
D. セキュリティ
正解: **(**正解を表示します**)**
Sales need iOS EndPoint Protection from DfE.
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-ios

質問: **34**
ホットスポットに関する質問
お客様の環境には、Windows Serverを実行するオンプレミスサーバーがあります。
SW1という名前のMicrosoft Sentinelワークスペースがあります。SW1は、Azure Monitor Agentデータコネクタを使用して、サーバーからWindowsセキュリティログエントリを収集するように構成されています。
収集対象イベントの範囲をイベント4624と4625のみに限定する予定です。
コネクタに適用されているフィルタの構文を検証するには、PowerShellスクリプトを使用する必要があります。
スクリプトをどのように完成させればよいでしょうか？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:



質問: **35**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Azure セキュリティ センターを使用します。
セキュリティ センターでセキュリティ警告を受け取ります。
Security Center でアラートを解決するには、推奨事項を表示する必要があります。
解決策: [セキュリティ アラート] からアラートを選択し、[アクションの実行] を選択して、[今後の攻撃の防止] セクションを展開します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **(正解を表示します)**
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the
'Mitigate the threat' option.
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding- alerts

質問: **36**
あなたの会社では Azure Security Center と Azure Defender を使用しています。
会社のセキュリティ運用チームは、セキュリティ アラートの電子メール通知を受け取っていないと通知しました。
電子メール通知を有効にするには、セキュリティ センターで何を構成する必要がありますか?
A. セキュリティ ソリューション
B. セキュリティ ポリシー
C. 価格と設定
D. セキュリティ警告
E. Azure ディフェンダー
正解: **(正解を表示します)**

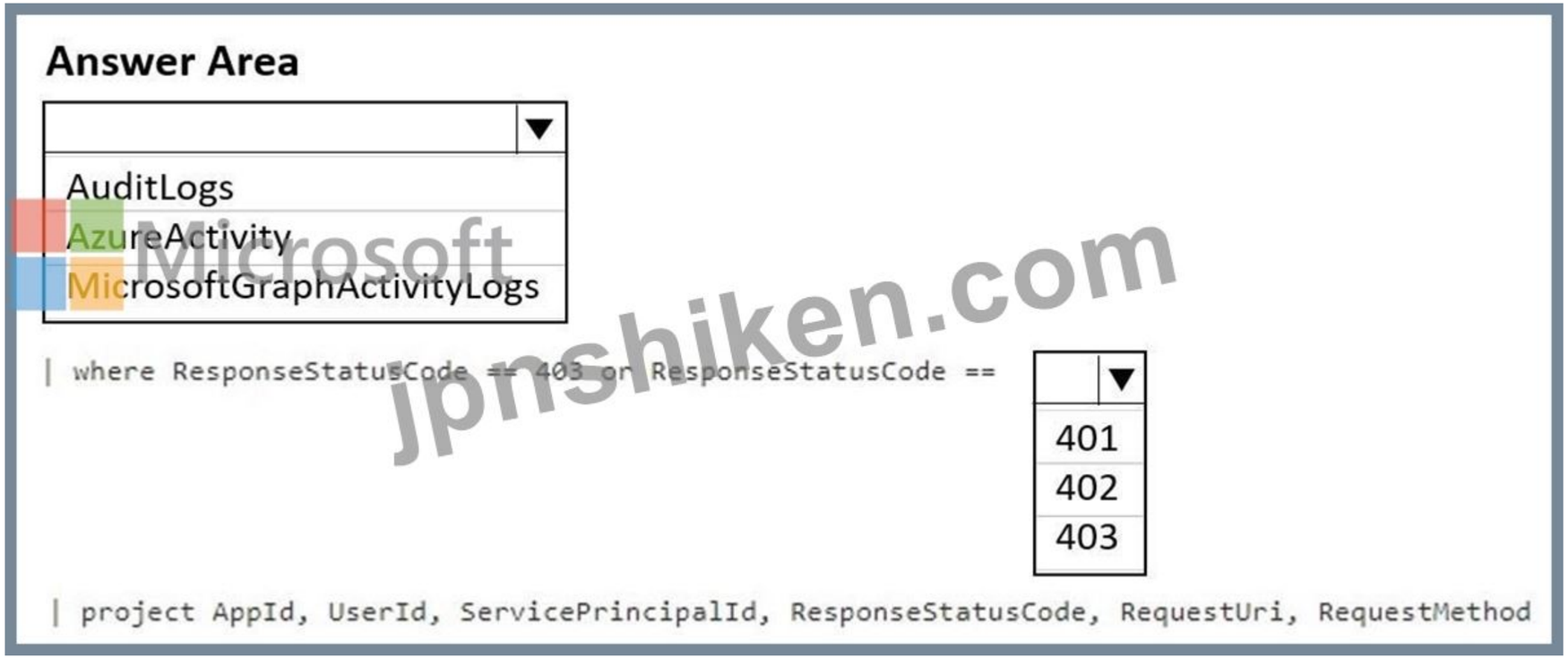
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact- details

質問: **37**
Microsoft Sentinelワークスペースをお持ちです。
あなたは、以下の組織が関与する事件を調査しています。
- Host1という名前のホスト
- User1という名前のユーザーアカウント
- IPアドレスは175.45.176.99です。
脅威インテリジェンスリストを更新して、これらのエンティティを含める必要があります。
インシデントページには、どのエンティティを追加できますか？
A. 175.45.176.99 および Host1 のみ
B. ホスト1のみ
C. 175.45.176.99、ホスト1、およびユーザー1
D. 175.45.176.99のみ
E. ユーザー1のみ
F. ホスト1とユーザー1のみ
正解: **(**正解を表示します**)**

質問: **38**
あなたの会社では、プロジェクトごとのデータが別の Azure サブスクリプションに保存されています。すべてのサブスクリプションは、同じ Azure Active Directory (Azure AD) テナントを使用します。
すべてのプロジェクトは、Windows Server を実行する複数の Azure 仮想マシンで構成されます。仮想マシンの Windows イベントは、各マシンのそれぞれのサブスクリプションの Log Analytics ワークスペースに保存されます。
Azure 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 ワークスペースを検索するには、Azure 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 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. セキュリティ イベント コネクタを Azure Sentinel ワークスペースに追加します。
B. ワークスペース式とユニオン演算子を使用するクエリを作成します。
C. エイリアス ステートメントを使用します。
D. リソース式とエイリアス演算子を使用するクエリを作成します。
E. Azure Sentinel ソリューションを各ワークスペースに追加します。
正解: **(**正解を表示します**)**
Every sentinel deployment must have a workspace - and the union command is used to join multiple workspaces together.
https://docs.microsoft.com/en-us/learn/modules/create-manage-azure-sentinel-workspaces/2-plan-for-azure-sentinel-workspace

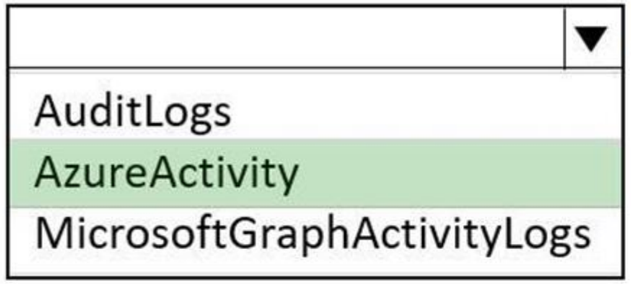
質問: **39**
ホットスポットに関する質問
Workspace1 という名前の Log Analytics ワークスペースを含む Azure サブスクリプションをお持ちです。
Azureアクティビティログと Microsoft Entra IDログをWorkspace1に転送するように構成します。
認証不足が原因で失敗したすべてのリクエストを特定するには、Workspace1 に対してクエリを実行する必要があります。
KQLクエリはどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。



正解:

Answer Area




```
| where ResponseStatusCode == 403 or ResponseStatusCode ==
```


```
| project AppId, UserId, ServicePrincipalId, ResponseStatusCode, RequestUri, RequestMethod
```

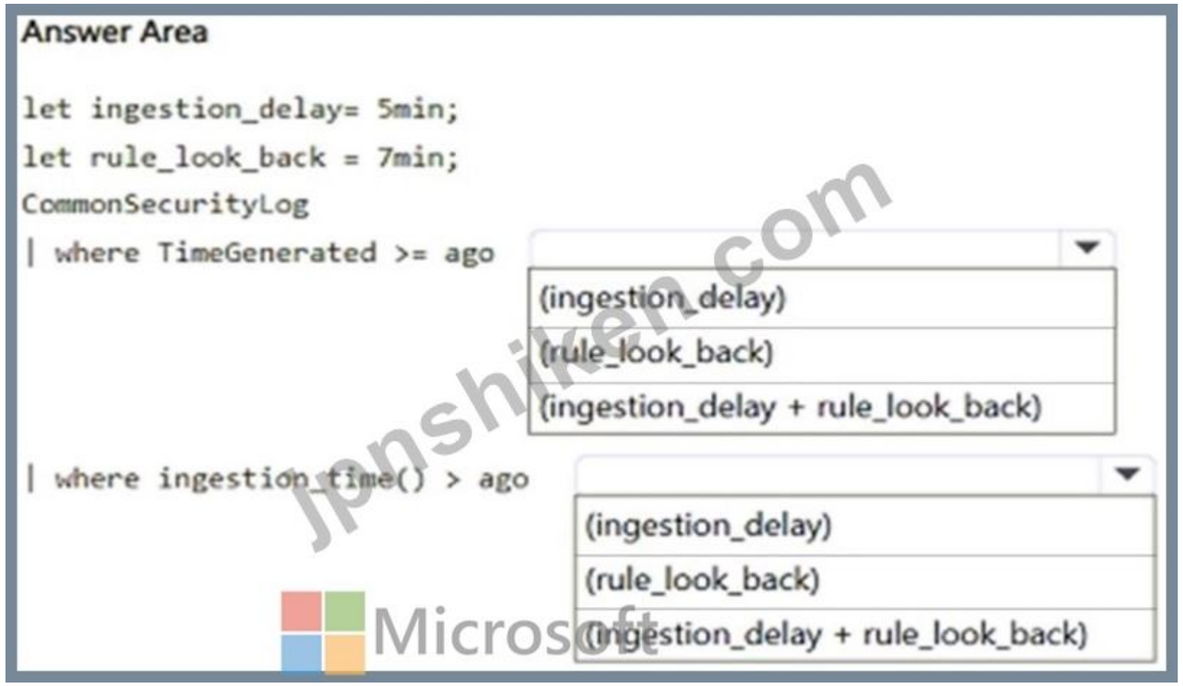
Explanation:
https://learn.microsoft.com/en-us/troubleshoot/developer/webapps/iis/www-administration-management/http-status-code

質問: **40**
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
あなたは事件を調査しています。
実施されたインシデント対応タスクを確認する必要があります。
インシデントページでは何が利用できますか？
A. タスクのみ
B. タスクとアクティビティログのみ
C. タスクとアラートのタイムラインのみ
D. タスク、アクティビティログ、アラートタイムライン
正解: **D (**コメントを発表する**)**
https://learn.microsoft.com/en-us/azure/sentinel/investigate-incidents

質問: **41**
お客様は、Device1 という名前のデバイスを含む Microsoft 365 E5 サブスクリプションを所有しています。
Microsoft Defender ポータルから、Device1 に対してアラートがトリガーされたことがわかります。
デバイスインベントリページから、Device1を分離します。

デバイス1にインストールされているプログラムの一覧を収集する必要があります。
あなたはどうすべきでしょうか？
A. 自動調査を開始し、アクションセンターで結果を確認します。
B. DeviceProcessEvents テーブルに対して高度なハンティングクエリを実行します。
C. DeviceTvmSoftwareInventory テーブルに対して高度なハンティングクエリを実行します。
D. ライブレスポンスセッションを開始し、プロセスコマンドを実行します。
正解: **(正解を表示します)**

質問: **42**
ホットスポットに関する質問
Workspace1 という名前の Microsoft Sentinel ワークスペースがあり、その中に CommonSecurityLog という名前のテーブルが含まれています。
ログはCommonSecurityLogに取り込まれます。CommonSecurityLogのログ取り込み時間は平均5分です。
7分間の遡及期間を持ち、CommonSecurityLogテーブルのデータを使用する分析ルー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。
同じイベントが二度処理されるのを防ぐ。
ログ取り込みの遅延によるイベントの見落としを最小限に抑える。
ルールを定義するKQLクエリ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:

Answer Area

```
let ingestion_delay= 5min;
let rule_look_back = 7min;
CommonSecurityLog
| where TimeGenerated >= ago
| where ingestion_time() > ago
```

(ingestion_delay)
(rule_look_back)
(ingestion_delay + rule_look_back)

(ingestion_delay)
(rule_look_back)
(ingestion_delay + rule_look_back)

質問: **43**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
アマゾン ウェブ サービス (AWS) 上に Linux 仮想マシンがあります。
Azure Defender をデプロイし、自動プロビジョニングを有効にします。
Azure Defender を使用して仮想マシンを監視する必要があります。
解決策: Log Analytics エージェントを仮想マシンに手動でインストールします。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**
A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.
Install Log Analytics manually or when you enable auto provisioning of Log Analytics in

"Autoprovisioning" tag, auto provisioning is already turned on.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-feature

質問: **44**
Microsoft Defender for Cloud を使用し、Windows Server を実行する 100 台の仮想マシンを含む Azure サブスクリプションがあります。
仮想マシンからイベント データを収集するには、Defender for Cloud を構成する必要があります。ソリューションでは、管理の労力とコストを最小限に抑える必要があります。
どの 2 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. Defender for Cloud によって作成されたワークスペースから、データ収集レベルを Common に設定します。
B. Microsoft エンドポイント マネージャー管理センターから、自動登録を有効にします。
C. Azure portal から、Azure Event Grid サブスクリプションを作成します。
D. Defender for Cloud によって作成されたワークスペースから、データ収集レベルを [すべてのイベント] に設定します。
E. Azure portal の Defender for Cloud から、仮想マシンの自動プロビジョニングを有効にします。
正解: **(**正解を表示します**)**
B: From the Microsoft Endpoint Manager admin center, enable automatic enrollment: This will automatically enroll all Windows devices, including the virtual machines in your subscription, in Microsoft Endpoint Manager, which will then allow Defender for Cloud to collect event data from these devices. To enable automatic enrollment, you can follow the steps in the Microsoft documentation.
E: From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines: This will automatically configure the virtual machines to send event data to Defender for Cloud without the need for manual configuration or agent installation. To enable automatic provisioning, you can follow the steps in the Azure Defender documentation.

質問: **45**
サードパーティ製アンチウイルスソフトでは、どのような種類の行動ブロック機能を利用できますか？
A. ブロックモード搭載EDR
B. フィードバックループの遮断
C. クライアントの動作をブロックする
D. 悪意のある動作のブロック
正解: **(**正解を表示します**)**
Option A is correct. EDR with Block mode allows you for blocking even when another AV is in use.
Options B, C, D are incorrect. Feedback-loop and Client behavior blocking are used with Defender AV.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/edr-in-block-mode?view=o365-worldwide

質問: **46**
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
Microsoft Defender for Office 365では自動調査および対応(AIR)が有効になっており、デバイスはMicrosoft Defender for Endpointで完全な自動化機能を使用します。
管理対象デバイス上で、ユーザーがマルウェアに感染した電子メールメッセージを受信したというインシデントが発生しました。
どの操作で、インシデントの手動による修復が必要になりますか？
A. デバイスを含む
B. メールメッセージの完全削除

C. メールメッセージのソフト削除
D. デバイスの隔離
正解: **D** (コメントを発表する)

質問: **47**
Azure Defender を使用する Microsoft 365 サブスクリプションがあります。RG1 という名前のリソース グループに 100 台の仮想マシンがあります。
セキュリティ管理者の役割を SecAdmin1 という名前の新しいユーザーに割り当てます。
SecAdmin1 が Azure Defender を使用して仮想マシンにクイック フィックスを適用できることを確認する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。
どの役割を SecAdmin1 に割り当てるべきですか?
A. サブスクリプションのセキュリティ閲覧者ロール
B. サブスクリプションの共同作成者
C. RG1 の共同作成者の役割
D. RG1 の所有者の役割
正解: **C** (コメントを発表する)
To ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender, while also following the principle of least privilege, you should assign the Contributor role for RG1 to SecAdmin1.
The Contributor role for RG1 will allow SecAdmin1 to perform tasks such as deploying resources and modifying resource properties within RG1, but it will not grant them access to perform administrative tasks at the subscription level. This will allow SecAdmin1 to apply quick fixes to the virtual machines using Azure Defender, while still adhering to the principle of least privilege.

質問: **48**
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、その中に Vault1 という名前の Azure キーコンテナーと Automation1 という名前の Azure Automation アカウントが含まれています。
Automation1がVault1にアクセスできることを確認する必要があります。ソリューション1は以下の要件を満たす必要があります。
- Automation1 が削除された場合、付与された権限が
Vault1は自動的に削除されます。
- Automation1で作成されたランブックがシークレット値を読み取れることを確認します。
Vault1に保管されています。
最小権限の原則に従うこと。
Automation1にはどのような設定が必要ですか？また、Automation1がVault1にアクセスするために使用する組み込みロールはどれですか？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

For Automation1, configure:

- A service account
- A system-assigned managed identity
- A user-assigned managed identity
- An app registration
- An enterprise application

Role:

- Key Vault Crypto Officer
- Key Vault Crypto User
- Key Vault Reader
- Key Vault Secrets Officer
- Key Vault Secrets User

正解:

Answer Area

For Automation1, configure:

- A service account
- A system-assigned managed identity
- A user-assigned managed identity
- An app registration
- An enterprise application

Role:

- Key Vault Crypto Officer
- Key Vault Crypto User
- Key Vault Reader
- Key Vault Secrets Officer
- Key Vault Secrets User

質問: **49**
機密ファイルの外部共有に応じてアラートを生成し、修復アクションをトリガーするには、Microsoft Cloud App Security を構成する必要があります。
Cloud App Security ポータルで実行する必要がある 2 つのアクションはどれですか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. [設定] から、[Information Protection]、[Azure Information Protection] の順に選択し、[このテナントからの Azure Information Protection 分類ラベルとコンテンツ検査警告のファイルのみをスキャンする] を選択します。
B. [ファイルの調査] を選択し、[アプリ] を [Office 365] にフィルターします。
C. [ファイルの調査] を選択し、検索から [新しいポリシー] を選択します。
D. [設定] から、[Information Protection]、[Azure Information Protection] の順に選択し、[新しいファイルの Azure Information Protection 分類ラベルとコンテンツ検査警告を自動的にスキャンする] を選択します。
E. [設定] から、[情報保護]、[ファイル] の順に選択し、ファイル監視を有効にします。
F. [ファイルの調査] を選択し、[ファイル タイプ] を [ドキュメント] にフィルターします。
正解: **(**正解を表示します**)**
In Defender for Cloud Apps, under the settings cog, select the Settings page under the System heading.
Under Microsoft Information Protection, select Automatically scan new files for Microsoft Information Protection sensitivity labels.
https://docs.microsoft.com/en-us/defender-cloud-apps/tutorial-dlp
https://www.microsoft.com/en-us/videoplayer/embed/RE4CMYG?postJsllMsg=true

質問: **50**
次のインシデントを含む Microsoft Sentinel ワークスペースがあります。
Azure Portal 分析ルールに対するブルート フォース攻撃がトリガーされました。
インシデントに対応する地理位置情報を特定する必要があります。
あなたは何をするべきか？
A. [概要] から、[潜在的な悪意のあるイベント] マップを確認します。
B. インシデントから、インシデントに関連付けられた iPCustomEntity エンティティの詳細を確認します。
C. インシデントから、インシデントに関連付けられた AccouncCuscomEntity エンティティの詳細を確認します。
D. 調査から、インシデント エンティティに関する分析情報を確認します。
正解: **(**正解を表示します**)**
The IPCustomEntity entity associated with the incident should provide the IP address that triggered the brute force attack. You can then use a geolocation lookup tool to determine the country or region associated with that IP address.

質問: **51**
Tenant1とTenant2という名前の2つのMicrosoft Entraテナントがあります。各テナントはAzureサブスクリプションにリンクされています。Tenant1にはGroup1という名前のグループがあり、Tenant2にはGroup2という名前のグループがあります。
各テナントに対してMicrosoft Sentinelを実装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。
- グループ1がテナント1のセキュリティインシデントを管理できることを確認し、
単一のワークスペース内にテナント2が存在する。
- Group2がテナント2に関するセキュリティインシデントのみを管理できるようにします。
ゲストアカウントの使用を最小限に抑える。
・管理業務の手間を最小限に抑える。
コストを最小限に抑える。

解決策には何を含めるべきですか？
A. ワンワークスペースと特権ID管理(PIM)
B. 1つのワークスペースと複数のロールベースアクセス制御(RBAC)ロール割り当て
C. 2つのワークスペースとAzure Lighthouse
D. 2つのワークスペースと、きめ細かな委任管理者権限(GDAP)
正解**: (**正解を表示します**)**
To achieve your goal, you must create a central security operations tenant, and use Azure Lighthouse to onboard the two customer Microsoft Entra tenants. Then, deploy individual Microsoft Sentinel workspaces in the customer tenants and grant permissions to your management groups using Azure RBAC, assigning the group for managing both tenants to work with both workspaces and the single-tenant group to only the relevant workspace.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/prepare-multiple-workspaces

質問**: 52**
ホットスポットに関する質問
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。
次の表に示されている不審なメールを特定してください。

Name	From	Subject	Data received	Attachment
Email1	prizes@contoso.com	You have WON a free gold coin	1/1/2024	File1.docx
Email2	hrhr@contoso.com	Update your benefits in the Contoso HR portal	1/1/2024	*None*
Email3	benefits@contoso.com	You have WON a free gold coin	1/1/2024	*None*

Microsoft Purviewでは、次の表に示すようなコンテンツ検索を作成します。

Name	Location	KQL query
Search1	Exchange mailboxes	(c:c)(filetype=docx) (senderauthor=prizes@contoso.com)
Search2	Exchange mailboxes	(c:c)(-subjecttitle=benefits) (from=hrhr@contoso.com)
Search3	Exchange mailboxes	(c:c)(subjecttitle=won) (from=benefits@contoso.com)

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: **53**
あなたはMicrosoft 365テナントをお持ちです。
File1.docxという名前の既知の脅威ファイルが見つかりました。
ユーザーがFile1.docxをダウンロードできない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. Microsoft Defender ポータルからインジケーターを追加します。
B. Microsoft Purview ポータルから、データ損失防止 (DLP) ポリシーを作成します。
C. Microsoft Purview ポータルから、機密ラベルを作成します。
D. Microsoft Defender ポータルから自動調査を設定します。
正解: **A** (コメントを発表する)
Implement Endpoint Indicators
If you have Microsoft Defender for Endpoint, you can create a custom indicator to block the file from being executed on managed devices.
Navigate to: Settings > Endpoints > Indicators > File hashes.
Action: Add the SHA256 hash and set the response action to Block and Remediate. This will stop the file from running and attempt to remove it if found on a device.
Reference:
https://learn.microsoft.com/en-us/defender-endpoint/indicator-file

質問: **54**
お客様は、WS1 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。WS1 には、Azure Activity コネクタと Microsoft Entra ID コネクタが構成されています。
どのアカウントに最も多くの警告が発生しているか、また各警告に関連するインシデント情報を調査する必要があります。ソリューションは管理作業を最小限に抑えるものでなければなりません。
WS1で最初に何をすべきですか？
A. ユーザーおよびエンティティ行動分析(UEBA)を使用して異常を検出します。
B. コンテンツハブから、Cloud Identity Threat Protection Essentialsをインストールします。
C. ユーザーおよびエンティティ行動分析(UEBA)を有効にする。
D. コンテンツハブから、Microsoft Purview インサイダーリスク管理ソリューションをインストールします。
正解: **(**正解を表示します**)**

質問: **55**
ホットスポットに関する質問
ユーザー「User1」と「WS1」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WS1に対してユーザーおよびエンティティ行動分析(UEBA)を有効にできることを確認する必要があります。
解決策は最小権限の原則に従わなければならない。
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

Microsoft Entra role:
- Global Administrator
- Security Administrator
- Security Operator

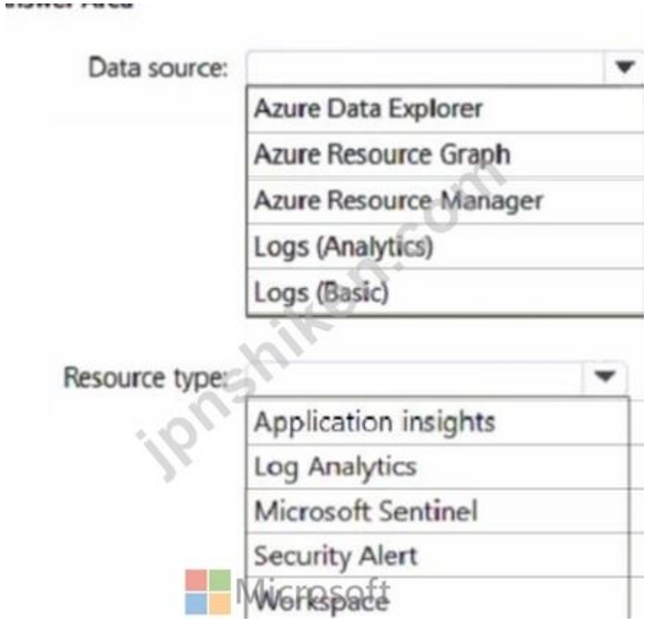
Role for WS1:
- Contributor
- Microsoft Sentinel Contributor
- Microsoft Sentinel Automation Contributor

正解:

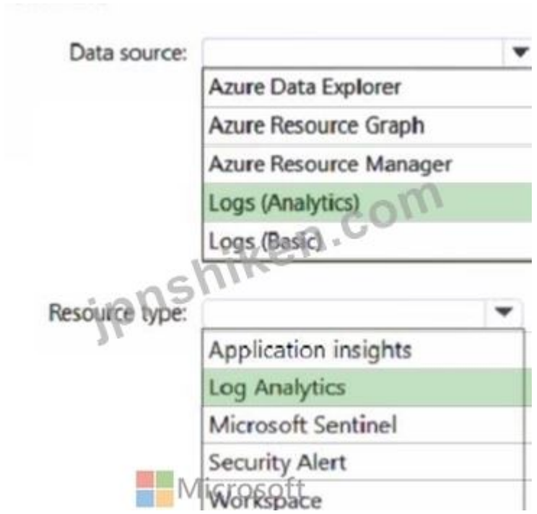
Answer Area

質問: **56**
Workspace1という名前のMicrosoft Sentinelワークスペースと、DNSスキーマに基づいた200個のカスタムAdvanced Security Information Model(ASIM)パーサーがあります。
Workspace1で200個の解析結果を利用できるようにする必要があります。解決策は管理作業を最小限に抑えるものでなければなりません。
まず最初に何をすべきでしょうか？
A. パーサーを Azure Monitor Logs ページにコピーします。
B. DNSテンプレートに基づいてJSONファイルを作成します。
C. DNSテンプレートに基づいてXMLファイルを作成します。
D. DNSテンプレートに基づいてYAMLファイルを作成します。
正解: **D** (コメントを発表する)
https://learn.microsoft.com/en-us/azure/sentinel/normalization-develop-parsers#deploy-parsers

質問: **57**
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。
KQLクエリがあります。このクエリは、SecurityIncidentテーブルに保存されている、過去90日間に発生したMicrosoft Sentinelインシデントを返します。
クエリの視覚化を含むMicrosoft Sentinelワークブックを作成する必要があります。
ワークブックのデータソースとリソースの種類は、それぞれ何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:

Box 1: Logs (Analytics)

Need Logs (Analytics) to access incidents for the last 90 days.

Note: In a Microsoft Sentinel workbook, "Logs (Analytics)" refers to the default, full-featured Log Analytics data source for primary security data, offering complete KQL query capabilities and high-speed access, while "Logs (Basic)" utilizes the Basic Logs plan to query less frequently accessed, high-volume, verbose logs at a lower cost, with limitations on retention (8 days), KQL support, and query costs per scanned GB. Analytics logs are more expensive but retain data longer and support full functionality for security operations, whereas Basic logs are a cost- effective option for specific data types with trade-offs in query complexity and scope.

Box 2: Log Analytics

For a Microsoft Sentinel workbook, the data source "resource type" is Log Analytics, which you select when configuring the data source for your query. You then specify one or more Log Analytics workspaces as the source for the data within that resource type.
Reference:
https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data

質問: **58**
事例研究3 - Litware Inc.
概要
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。
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、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。
Microsoft 365環境
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を実装し、ログコレクターを有効にします。
Azure環境
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.

Amazon Web Services (AWS) 環境
FabrikamはAccount1という名前のAmazon Web Services(AWS)アカウントを持っています。Account1には
カスタム版Windows Server 2022を実行するAmazon Elastic Compute Cloud(EC2)インスタンス100台。
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。
最新の課題

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」に関する警告を大量に発生させます。
Defender for Identityは、DCSync攻撃の疑いに関するアラートを大量に発生させますが、その多くは誤検知です。
要件
計画されている変更
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
ビジネス要件
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。
Microsoft Defender for Cloud Apps の要件
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。
Microsoft Defender for ID の要件
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。
Microsoft Defender for Cloud の要件
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する。
- 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。
Microsoft Sentinelの要件
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の平均解決時間を特定します。
- 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、Pool1に対して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。
Microsoft Sentinelの要件を満たす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べきでしょうか？
A. Azure Synapse Analytics
B. Azure Databricks
C. Azure Machine Learning
D. ログ分析
正解: **C** (コメントを発表する)

質問: **59**
User1 という名前のユーザーを含む Azure サブスクリプションがあります。
User1 には Azure Active Directory Premium Plan 2 ライセンスが割り当てられています
過去 90 日間に User1 の ID が侵害されたかどうかを特定する必要があります。
何を使えばいいのでしょうか？
A. リスク検出レポート
B. 危険なユーザーのレポート
C. ID セキュア スコアの推奨事項
D. 危険なサインイン レポート
正解: (正解を表示します)
The risk detections report contains filterable data for up to the past 90 days (three months).
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity- protection-investigate-risk#risk-detections

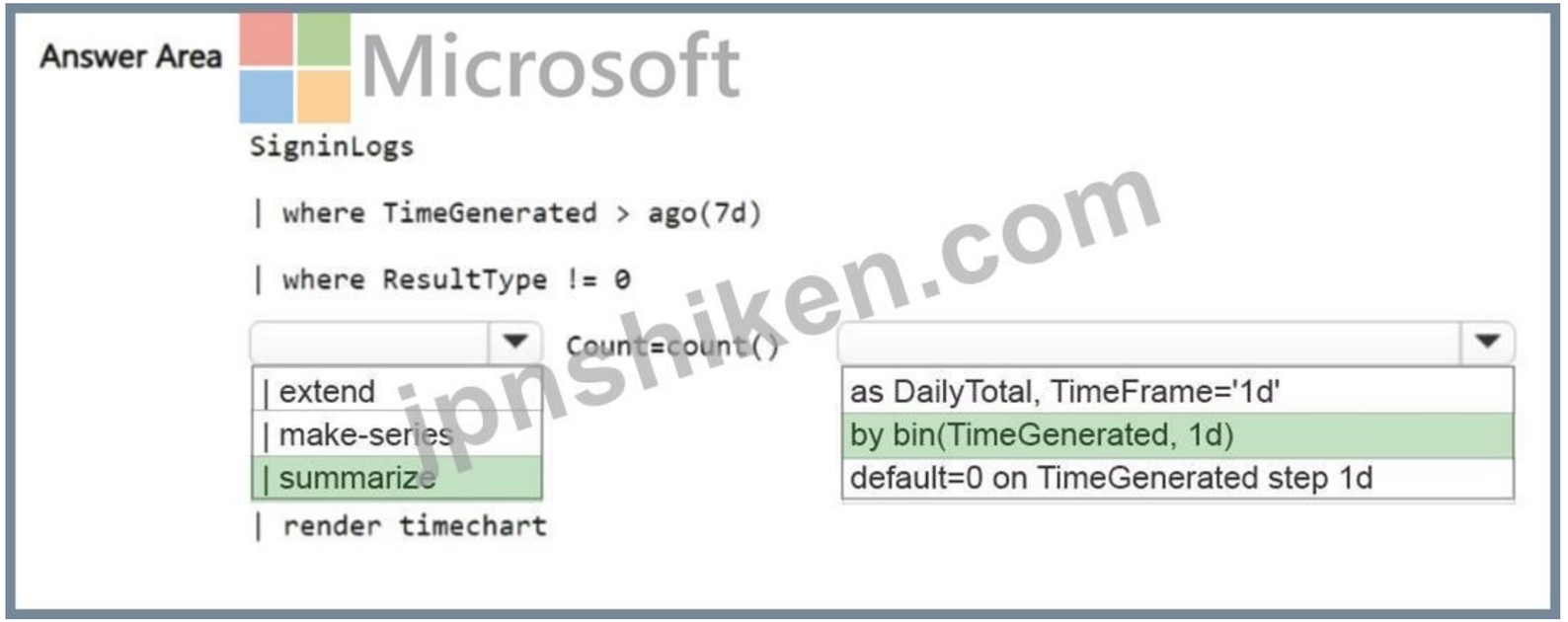
質問: **60**
ホットスポットに関する質問
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
Workspace1 にカスタム ワークブックを作成する必要があります。Workspace1 には、過去 7 日間の Microsoft Entra サインイン失敗回数を示すタイムチャートを表示する必要があります。このチャートには、各日のサインイン失敗回数が含まれるようにしてください。
KQLクエリはどのように入力すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

```
SigninLogs
| where TimeGenerated > ago(7d)
| where ResultType != 0
[ ▼ ]  Count=count()  [ ▼ ]
| render timechart
```

| extend	as DailyTotal, TimeFrame='1d'
| make-series	by bin(TimeGenerated, 1d)
| summarize	default=0 on TimeGenerated step 1d

正解:



質問: **61**

お客様は、Group1とGroup2という名前の2つのグループを含むMicrosoft 365 E5サブスクリプションをご利用で、セキュリティにはMicrosoft Copilotを使用しています。

Copilot for Securityの役割割り当てを以下の要件を満たすように構成する必要があります。

- グループ1のメンバーがプロンプトを実行し、応答できることを確認します。
Microsoft Defender XDR のセキュリティインシデント。
- グループ2のメンバーがプロンプトを実行できることを確認してください。
最小権限の原則に従うこと。
コパイロット貢献者ロールから 全員」を削除します。
次に実行すべき2つの行動はどれですか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。
A. セキュリティオペレーターの役割をグループ1に割り当てます。
B. グループ2に副操縦士オーナーの役割を割り当てます。
C. グループ1の最も投票されたユーザーに副操縦士オーナーの役割を割り当てます
D. セキュリティオペレーターの役割をグループ2に割り当てます。
E. グループ2にコパイロット貢献者ロールを割り当てます。最も投票された
正解: **(**正解を表示します**)**
To follow the principle of least privilege, we must carefully assign roles based on minimum necessary permissions.
Requirement Breakdown:
Group1 needs to run prompts AND respond to Microsoft Defender XDR security incidents.
Solution: Assign the Security Operator role.
The Security Operator role allows responding to Microsoft Defender XDR incidents.
This role provides incident response privileges, but not full administrative rights.
Group2 needs to run prompts ONLY.
Solution: Assign the Copilot Contributor role.
This role allows running prompts without elevated security permissions.

質問: **62**
ホットスポットに関する質問
貴社にはLinuxが稼働するオンプレミスサーバーが200台あります。
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
あなたは、サーバーから共通イベントフォーマット(CEF)のSyslogイベントを収集し、Azure Monitorのログ取り込みAPIを使用してWorkspace1に取り込むことを計画しています。
APIリクエストを使用して、イベントのデータ収集ルール(DCR)を設定する必要があります。
APIリクエスト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。

Answer Area

```
{
  "dataSources": {
    "syslog": [
      {
        "name": "Stream0",
        "streams": [
          [                                    ▼]
          ],
          [                                    ▼]
            "cron ,
            "daemon"
      ],
        "logLevels": [
          "Error",
          "Critical",
          "Alert",
```

Microsoft-CommonSecurityLog
Microsoft-Syslog
SecurityEvent

facilityNames: [
outputStream: [
type: [

```
            "Emergency"
...
}
```

正解:

Answer Area

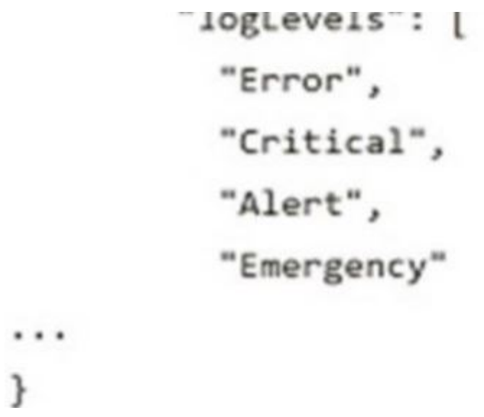
```
{
  "dataSources": {
    "syslog": [
      {
        "name": "Stream0",
        "streams": [
```

Microsoft-CommonSecurityLog
Microsoft-Syslog
SecurityEvent

```
        ],
```

facilityNames: [
outputStream: [
type: [

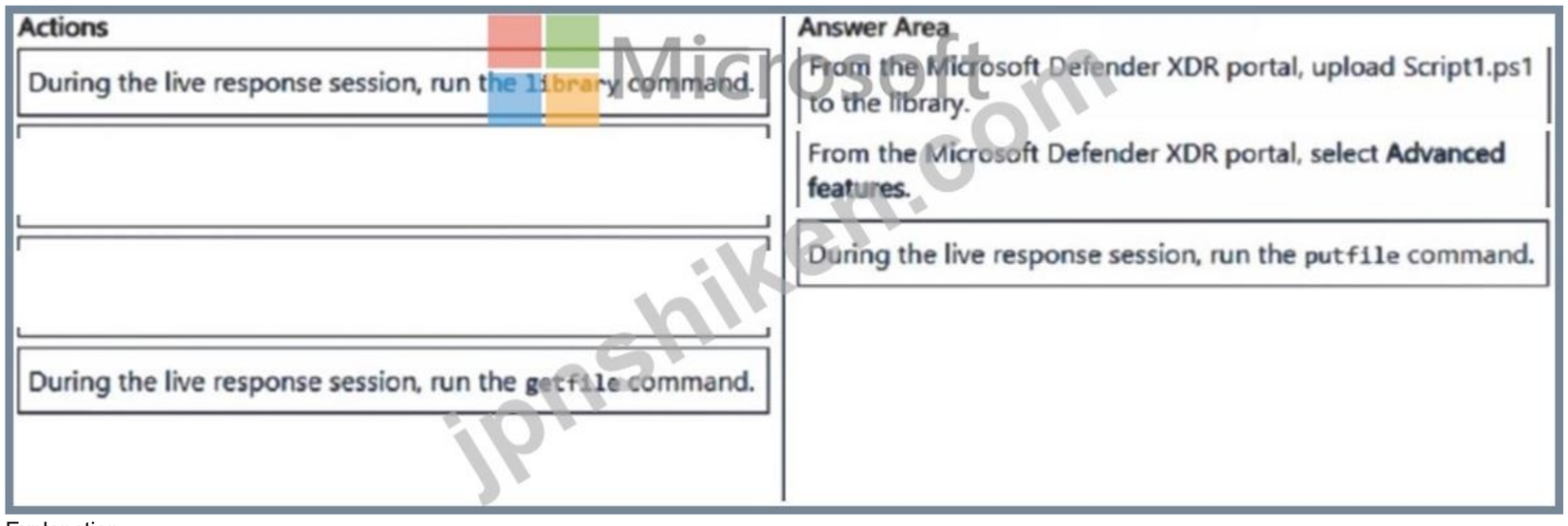
```
          "cron ,
          "daemon"
      ],
```



質問: **63**
お客様は、Microsoft Security Copilot を使用する Azure サブスクリプションをお持ちです。
セキュリティコンピューティングユニットの数を一時的に増やす必要があります。
請求対象となる最短の時間間隔はどれくらいですか？
A. 1秒
B. 1分
C. 1時間
D. 1日
正解: **(**正解を表示します**)**
Billing is calculated on hourly blocks based on provisioned capacity rather than by 60-minute increments and has a minimum of one hour. Any usage consumed within the same hour is billed as a full SCU for provisioned capacity, regardless of start or end times within that hour.
Reference:
https://learn.microsoft.com/en-us/copilot/security/get-started-security-copilot

質問: **64**
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。

正解:



Explanation:

Reference:

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

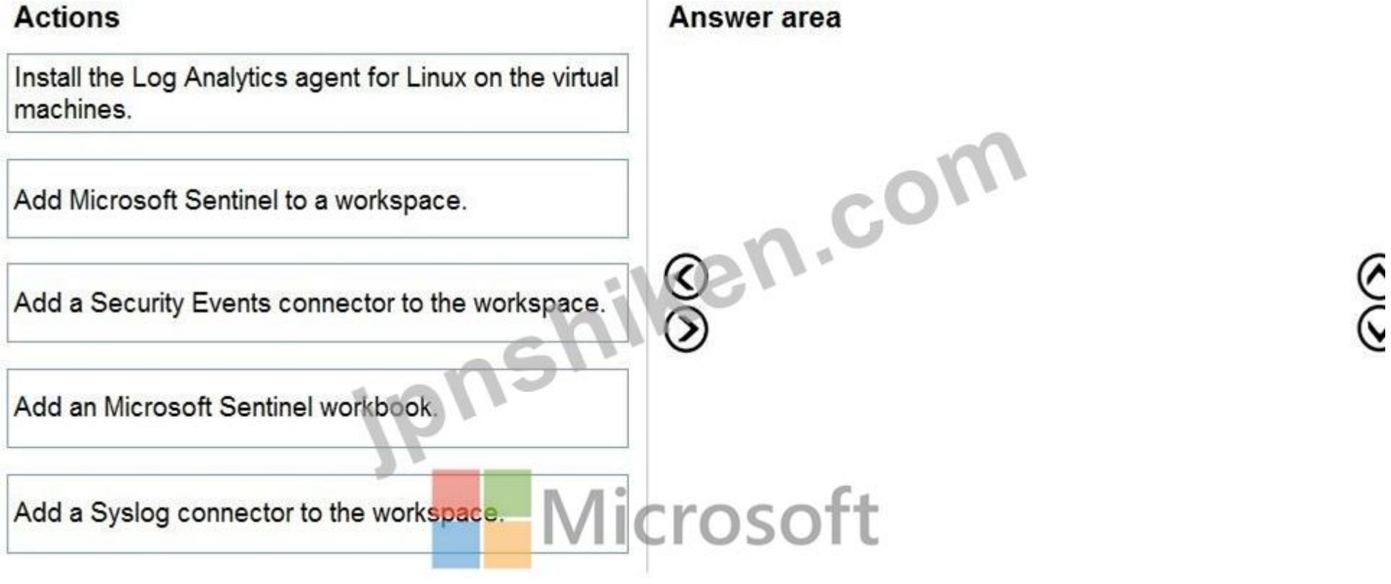
質問: **65**

ドラッグアンドドロップ問題

お客様は、100台のLinux仮想マシンを含むAzureサブスクリプションを所有しています。

仮想マシンからイベントログを収集するように、Microsoft Sentinelを設定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:

Actions

Add a Security Events connector to the workspace.

Add an Microsoft Sentinel workbook.

Answer area

Add Microsoft Sentinel to a workspace.

Add a Syslog connector to the workspace.

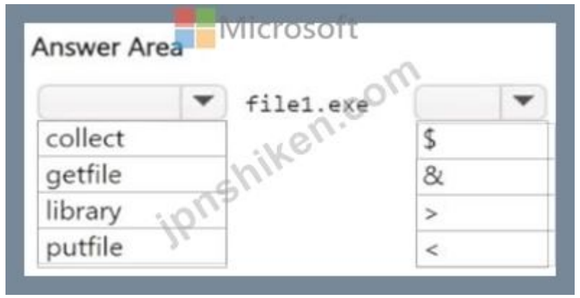
Install the Log Analytics agent for Linux on the virtual machines.

Explanation:
https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

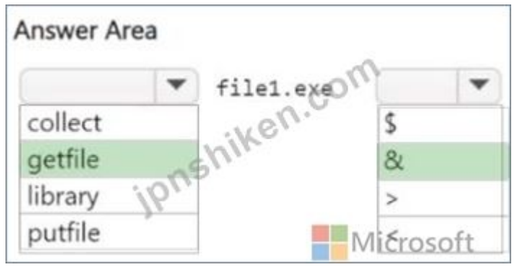
質問: **66**
SW1という名前のMicrosoft Sentinelワークスペースがあります。
SW1では、以下のエンティティに関連するインシデントを調査します。
- ホスト
- IPアドレス
- ユーザーアカウント
- マルウェア名
インシデントのページから直接、侵害指標(IoC)としてラベル付けできるエンティティはどれですか？
A. マルウェア名
B. ホスト
C. ユーザーアカウント
D. IPアドレス
正解: (正解を表示します)

質問: **67**

ホットスポットに関する質問
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、Device1 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File1.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、File1.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。



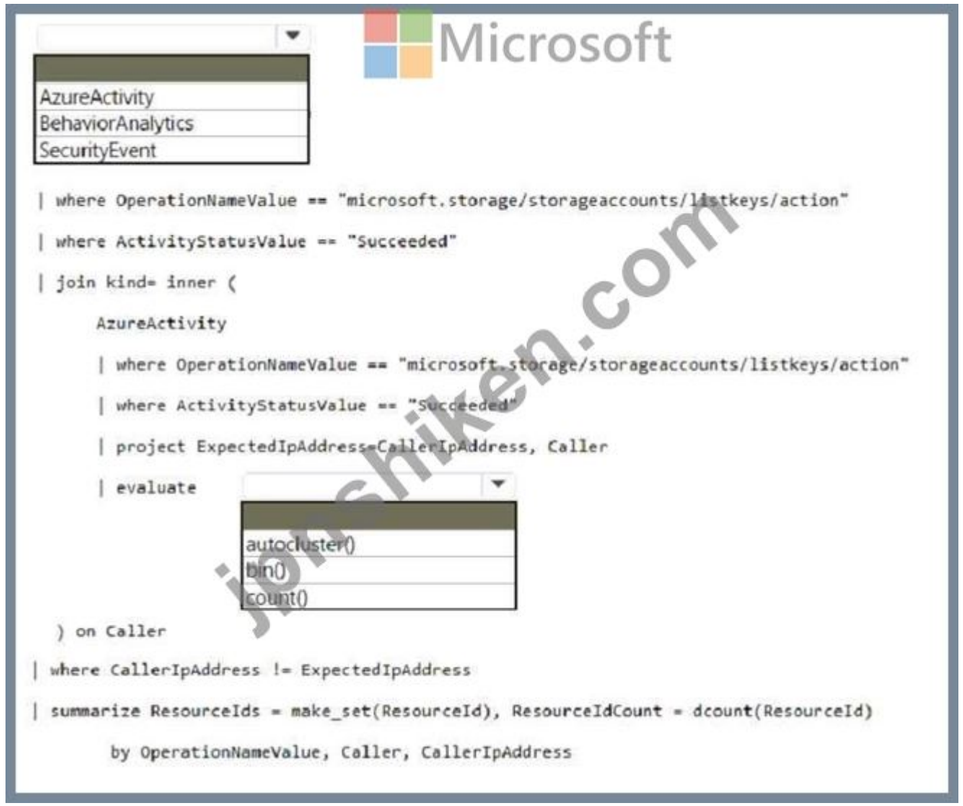
正解:



質問: **68**
Microsoft Defender for Cloud Apps を使用し、Cloud Discovery が有効になっている Microsoft 365 サブスクリプションがあります。
Cloud Discovery データを強化する必要があります
ａ.ソリューションでは、Cloud Discovery 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確認する必要があります。
まず何をすべきでしょうか?
A. Microsoft 365 アプリ コネクタを作成します。
B. Microsoft 365 Defender への自動リダイレクトを有効にします。
C. Azure アプリ コネクタを作成します。
D. 条件付きアクセス アプリ制御から、ユーザー監視を構成します。
正解: **(**正解を表示します**)**

質問: **69**
ホットスポットに関する質問
sws1 という名前の Microsoft Sentinel ワークスペースがあります。
複数の Azure ストレージ アカウントのストレージ キーをリストしているユーザーを特定するためのハンティング クエリを作成する必要があります。このソリューションでは、単一のストレージ アカウントのストレージ キーをリストしているユーザーは除外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:

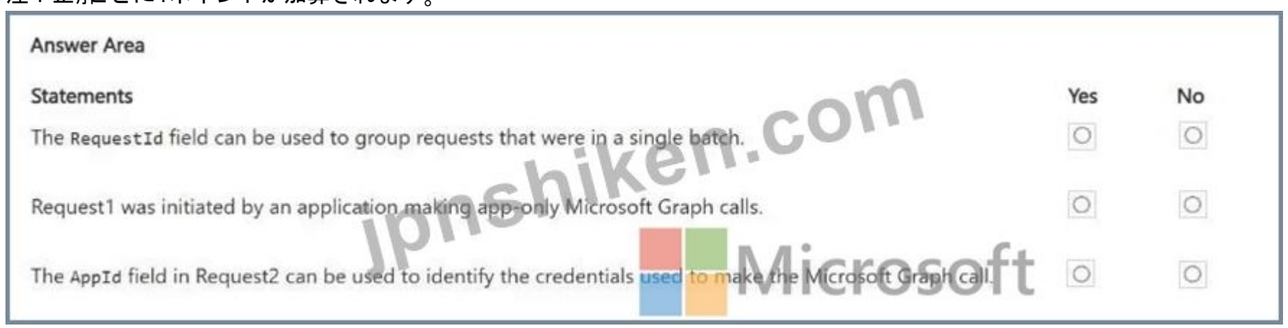

```
| where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
| where ActivityStatusValue == "Succeeded"
| join kind= inner (
      AzureActivity
      | where OperationNameValue == "microsoft.storage/storageaccounts/listkeys/action"
      | where ActivityStatusValue == "Succeeded"
      | project ExpectedIpAddress=CallerIpAddress, Caller
      | evaluate
  ) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId)
    by OperationNameValue, Caller, CallerIpAddress
```

Explanation:
Box 1: AzureActivity
The AzureActivity table includes data from many services, including Microsoft Sentinel. To filter in only data from Microsoft Sentinel, start your query with the following code:
Box 2: autocluster()
Example: description: |
'Listing of storage keys is an interesting operation in Azure which might expose additional secrets and PII to callers as well as granting access to VMs. While there are many benign operations of this type, it would be interesting to see if the account performing this activity or the source IP address from which it is being done is anomalous.
The query below generates known clusters of ip address per caller, notice that users which only had single operations do not appear in this list as we cannot learn from it their normal activity (only based on a single event). The activities for listing storage account keys is correlated with this learned clusters of expected activities and activity which is not expected is returned.' AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action" | where ActivityStatusValue == "Succeeded"
| join kind= inner (
AzureActivity
| where OperationNameValue =~ "microsoft.storage/storageaccounts/listkeys/action" | where ActivityStatusValue == "Succeeded"
| project ExpectedIpAddress=CallerIpAddress, Caller
| evaluate autocluster()
) on Caller
| where CallerIpAddress != ExpectedIpAddress
| summarize StartTime = min(TimeGenerated), EndTime = max(TimeGenerated), ResourceIds = make_set(ResourceId), ResourceIdCount = dcount(ResourceId) by OperationNameValue, Caller, CallerIpAddress
| extend timestamp = StartTime, AccountCustomEntity = Caller, IPCustomEntity = CallerIpAddress Reference: https://github.com/Azure/Azure- Sentinel/blob/master/Hunting

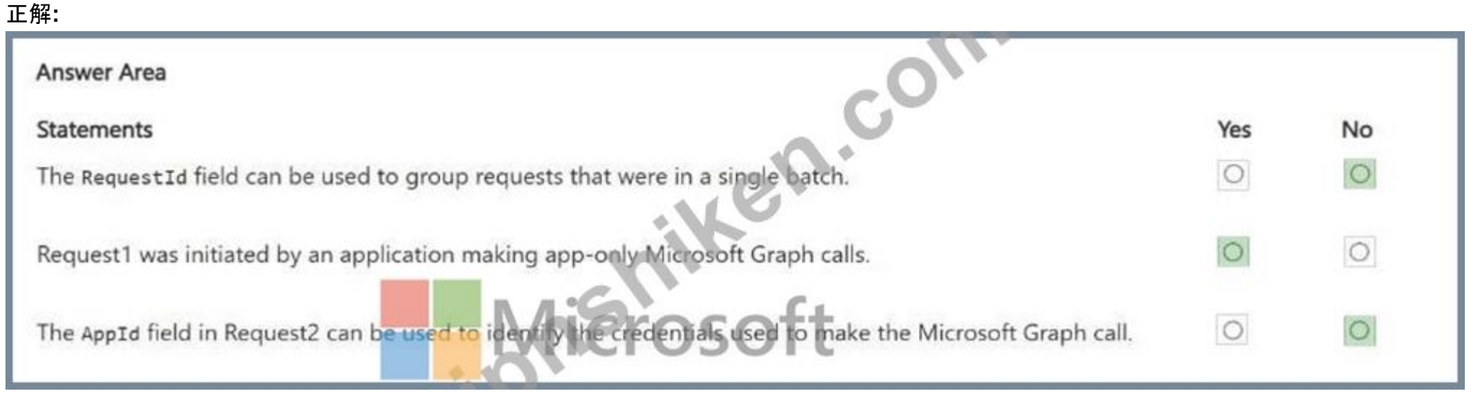
%20Queries/AzureActivity/Anomalous_Listing_Of_Storage_Keys.ya ml

質問: 70
ホットスポットに関する質問
お客様は、Microsoft Entra ID P1ライセンスを持つMicrosoft Entraテナントをご利用中です。
Log AnalyticsワークスペースからMicrosoft Graphのアクティビティログを収集します。
あなたは、Microsoft 365 グループに対する偵察活動の疑いについて調査しています。以下のクエリ結果は、同じ 15 分間に MicrosoftGraphActivityLogs テーブルから取得されたものです。
リクエスト1 :
- AppId: 11111111-1111-1111-1111-111111111111
- サービスプリンシパル ID: aaaaaaaaa-aaaa-aaaa-aaaa-aaaaaaaaaaaa
- ユーザーID: *(空欄)*
- クライアント認証方法: 2
- リクエストメソッド: GET
- RequestUri: https://graph.microsoft.com/v1.0/groups?$top=999
- レスポンスステータスコード: 403
- オペレーションID: op-7001
- リクエストID: req-7001
- 生成日時: 2026-02-09T10:05:12Z
リクエスト2 :
- AppId: 11111111-1111-1111-1111-111111111111
- ServicePrincipalId: aaaaaaaaa-aaaa-aaaa-aaaa-aaaaaaaaaaaa
- ユーザーID: *(空欄)*
- クライアント認証方法: 2
- リクエストメソッド: GET
- RequestUri: https://graph.microsoft.com/v1.0/groups?$top=999
- レスポンスステータスコード: 403
- オペレーションID: op-7002
- リクエストID: req-7002
- 生成日時: 2026-02-09T10:06:01Z
リクエスト3 :
- AppId: 22222222-2222-2222-2222-222222222222
- ServicePrincipalId: bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb
- ユーザー ID: 33333333.3333.3333.3333.33333333333
- クライアント認証方法: 1
- リクエストメソッド: GET
- RequestUri: https://graph.microsoft.com/v1.0/groups/0f00.../members
- レスポンスステータスコード: 200
- オペレーションID: op-8001
- リクエストID: req-8001
- 生成日時: 2026-02-09T10:07:44Z
アプリケーションがグループを列挙しようとしているものの、認証チェックに失敗している可能性があると疑われる。

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:



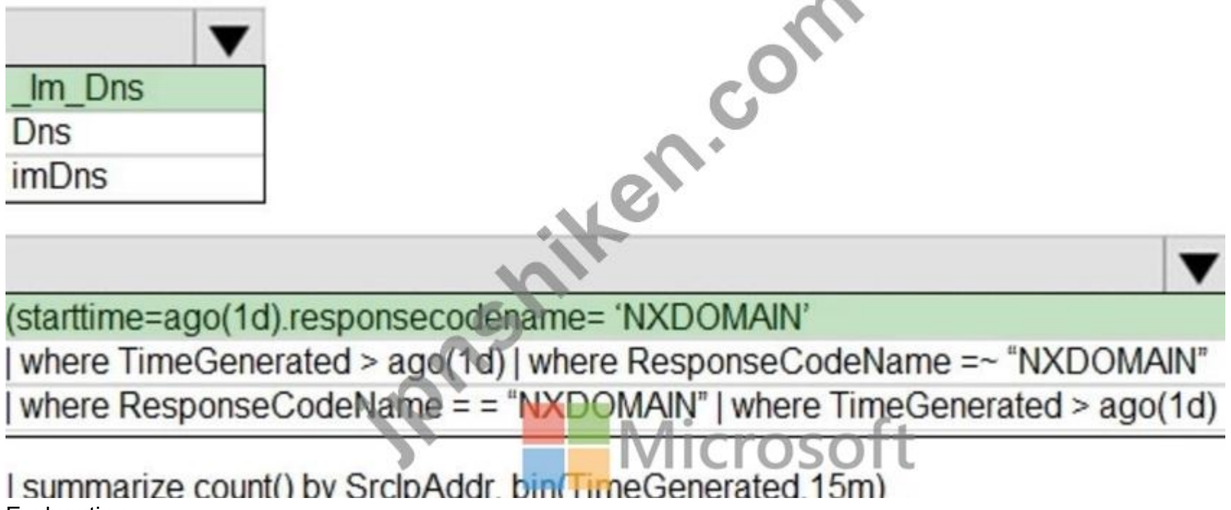
質問: **71**
あなたの会社では Azure Sentinel を使用しています。
新しいセキュリティ アナリストは、Azure Sentinel でインシデントを割り当てたり削除したりできないと報告しています。アナリストのために問題を解決する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。アナリストにはどの役割を割り当てるべきですか?
A. Azure Sentinel レスポンダー
B. ロジック アプリのコントリビューター
C. Azure Sentinel の貢献者
D. Azure Sentinel リーダー
正解: **A** (コメントを発表する)
Roles for working in Azure Sentinel
Azure Sentinel-specific roles
All Azure Sentinel built-in roles grant read access to the data in your Azure Sentinel workspace.
Azure Sentinel Reader can view data, incidents, workbooks, and other Azure Sentinel resources.
Azure Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.) Azure Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Azure Sentinel resources.
Azure Sentinel Automation Contributor allows Azure Sentinel to add playbooks to automation rules. It is not meant for user accounts.
https://docs.microsoft.com/en-us/azure/sentinel/roles

質問: **72**
オンプレミスの Linux サーバーが 5 台あります。
Microsoft Defender for Cloud を使用する Azure サブスクリプションがあります。
Linux サーバーを保護するには、Defender for Cloud を使用する必要があります。
最初にサーバーに何をインストールする必要がありますか?
A. 依存関係エージェント
B. Log Analytics エージェント
C. Azure Connected Machine エージェント
D. ゲスト構成拡張機能
正解: **B (**コメントを発表する**)**
Defender for Cloud depends on the Log Analytics agent.
Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage
https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

質問: **73**
ホットスポットに関する質問
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
Workspace1を構成して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)統合パーサーをデプロイします。
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。
Answer Area

正解:

Answer Area



Explanation:

Every schema that supports filtering parameters supports at least the starttime and endtime parameters and using them is often critical for optimizing performance.

https://learn.microsoft.com/en-us/azure/sentinel/normalization-about-parsers#optimizing-parsing-using-parameters

質問: 74

ホットスポットに関する質問

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,
RecipientEmailAddtess, EntityType, DeviceId, SHA256
```

以下の各記述について、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:
https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions

質問: **75**
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。
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。ソリューションは、収集した情報に基づいて、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ものでなければなりません。
Microsoft 365 Defender ポータルでは何を使用すべきですか？
A. 事件
B. 修復
C. 調査
D. 高度な狩猟
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine- alerts?view=o365-worldwide

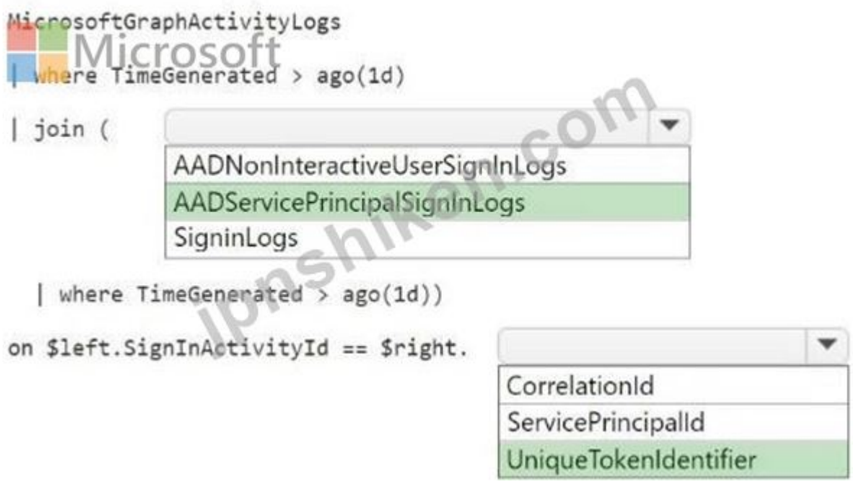
質問: **76**
Azure Activityコネクタを使用してトリガーされるMicrosoft Sentinelプレイブックがあります。
プレイブックを使用する、新しいニアリアルタイム(NRT)分析ルールを作成する必要があります。
ルールにはどのような設定が必要ですか？
A. インシデント自動化設定
B. クエリルール
C. エンティティマッピング
D. アラート自動化設定

正解: (正解を表示します)
To create an NRT rule, you need to follow these steps:
From the Microsoft Sentinel navigation menu, select Analytics.
Select Create from the button bar, then NRT query rule (preview) from the drop-down list.
Follow the instructions of the analytics rule wizard.

質問: 77
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、それが contoso.com という名前の Microsoft Entra テナントにリンクされています。Sub1 には Workspace1 という名前の Log Analytics ワークスペースが含まれています。contoso.com からのすべてのログは Workspace1 にストリーミングされます。
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
Workspace1に対して以下の情報を照会する必要があります。
- contoso.comのMicrosoft GraphサービスへのHTTPリクエスト
- 証明書または秘密情報を使用するサードパーティ製アプリのサインインアクティビティ
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。

正解:

Answer Area



質問: **78**
Microsoft 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. Microsoft Sentinel のノートブック
B. Microsoft Defender for Cloud Apps
C. Azure Monitor
正解: **A** (コメントを発表する)
Notebooks are interactive tools that allow you to run Python code, query data, perform machine learning, and create visualizations. Notebooks can help you hunt for threats, investigate incidents, and perform data analysis using Microsoft Sentinel data and external data sources.

質問: **79**
ホットスポットに関する質問
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。
以下の要件を満たす検出ルールを作成する必要があります。
- 重大なソフトウェア脆弱性を持つデバイスが過去 1 時間以内にアクティブだった場合にトリガーされます
重複する結果の数を制限します
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

```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
[ ▼ ]
```

- | distinct CveId
- | distinct DeviceId
- | project-away CveId
- | project-keep DeviceId

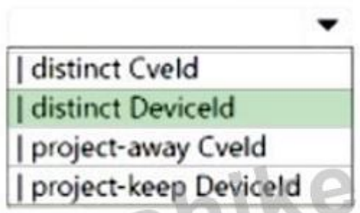
```
| join kind=inner DeviceInfo on DeviceId
| where Timestamp between (now(-1h)..now())
[ ▼ ]
```

- | distinct DeviceId
- | distinct DeviceId, ReportId
- | project Timestamp, DeviceId, ReportId
- | summarize count() by DeviceId, ReportId

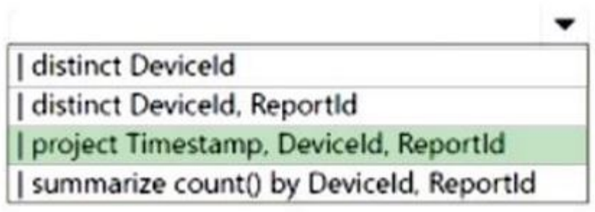
正解:

Answer Area

```
DeviceTvmSoftwareVulnerabilities
| where VulnerabilitySeverityLevel == 'Critical'
```




```
| join kind=inner DeviceInfo on DeviceId
| where Timestamp between (now(-1h)..now())
```



質問: **80**
ドラッグアンドドロップ問題
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
- imProcessCreate
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。
各要件を満たすには、どのパーサーを修正すればよいでしょうか？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回だけ使用することも、複数回使用することも、全く使用しないことも可能です。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:

質問: **81**

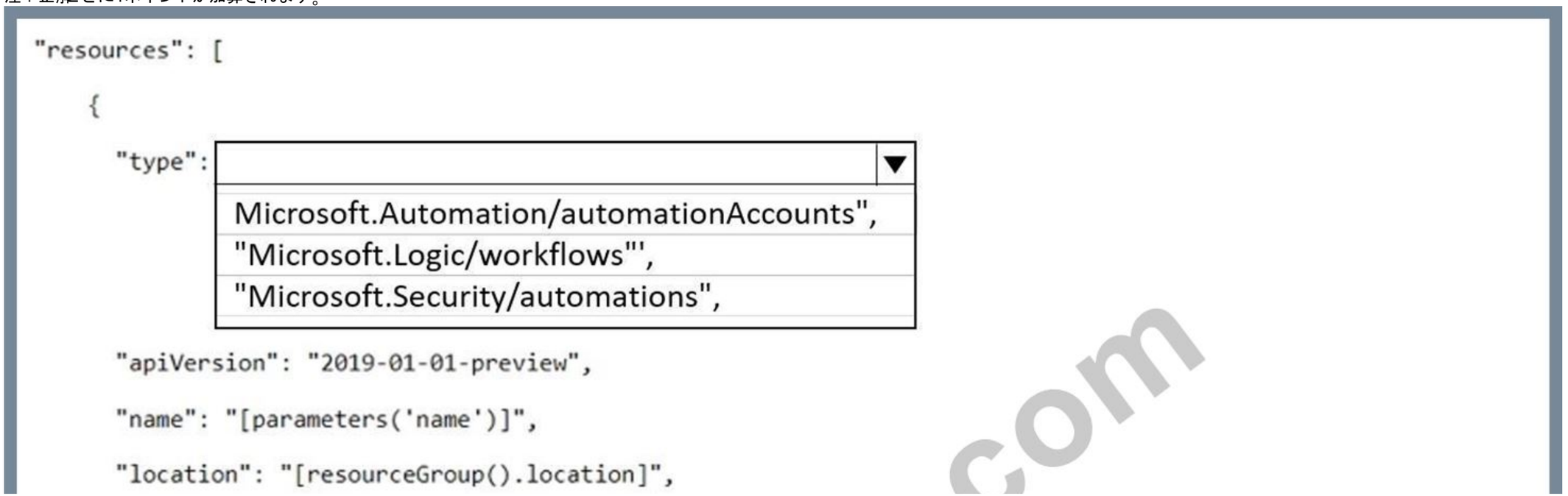
ホットスポットに関する質問

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。



```
"properties": {
  "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
  "isEnabled": true,
  "actions": [
    { "actionType": "LogicApp",
      "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
      "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
              'Microsoft.Logic/workflows/ [ ▼ ]
                                                  actions
                                                  contents
                                                  triggers
                    parameters('app1'),'manual'), '2019-05-01').value]"
    }
  ],
```

正解:

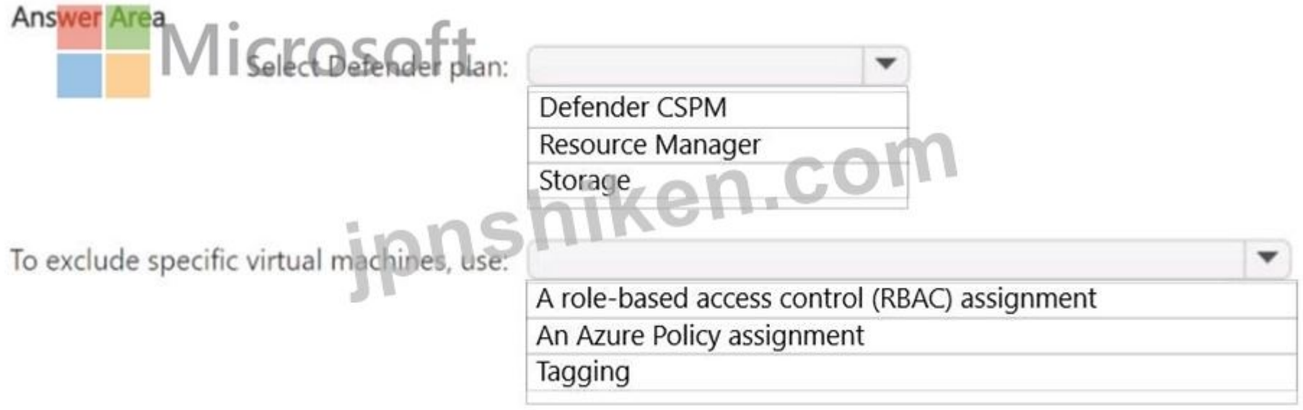
```
"resources": [
  {
    "type": [ ▼ ]
              Microsoft.Automation/automationAccounts",
              "Microsoft.Logic/workflows"',
              "Microsoft.Security/automations",
```

```
Microsoft.Security/automations')

"apiVersion": "2019-01-01-preview",

"name": "[parameters('name')]",

"location": "[resourceGroup().location]",

"properties": {

  "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",

  "isEnabled": true,

  "actions": [

    { "actionType": "LogicApp",

      "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",

      "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),

              'Microsoft.Logic/workflows/                                    ▼

                                                                  actions
                                                                  contents
                                                                  triggers

              parameters('app1'),'manual'), '2019-05-01').value]"

    }

  ],
```

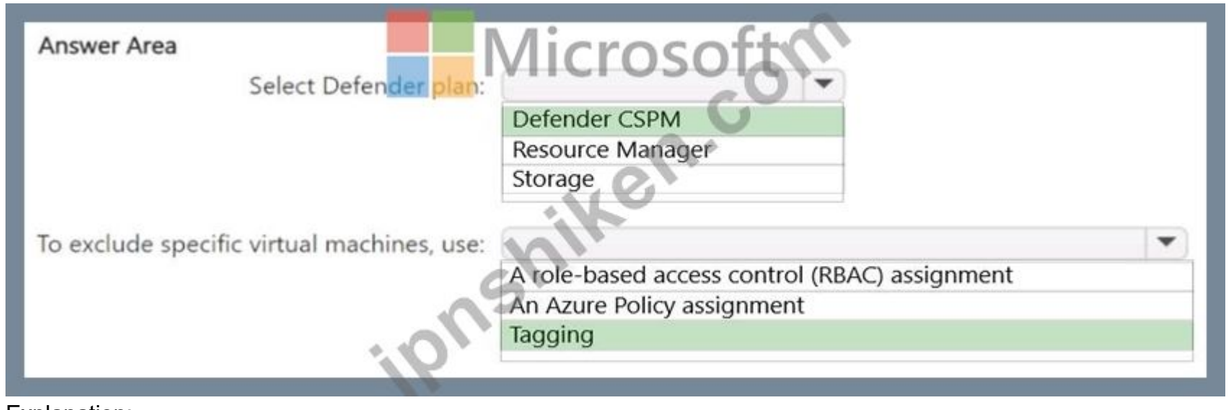
Explanation:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-automation-alert?tabs=CLI

質問: 82

ホットスポットに関する質問
お客様は、50台の仮想マシンを含むAzureサブスクリプションを所有しています。
Microsoft Defender for Cloud を導入する予定です。
40台の仮想マシンに対してエージェントレススキャンを有効にする必要があります。ソリューションは、仮想マシンのディスクスナップショットを作成し、そのスナップショットに対して帯域外分析を実行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:
Defender CSPM:
https://learn.microsoft.com/eN-us/azure/defender-for-cloud/concept-agentless-data-collection Tagging:
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming-and-tagging-decision-guide

質問: **83**
お客様は、User1 という名前のユーザーと、Device1 および Device2 という名前の 2 台の Windows デバイスを含む Microsoft 365 サブスクリプションを所有しています。Device1 と Device2 は、Microsoft Defender for Endpoint に登録されています。
以下の出来事が起こります。
- ユーザー1がデバイス1にサインインします。

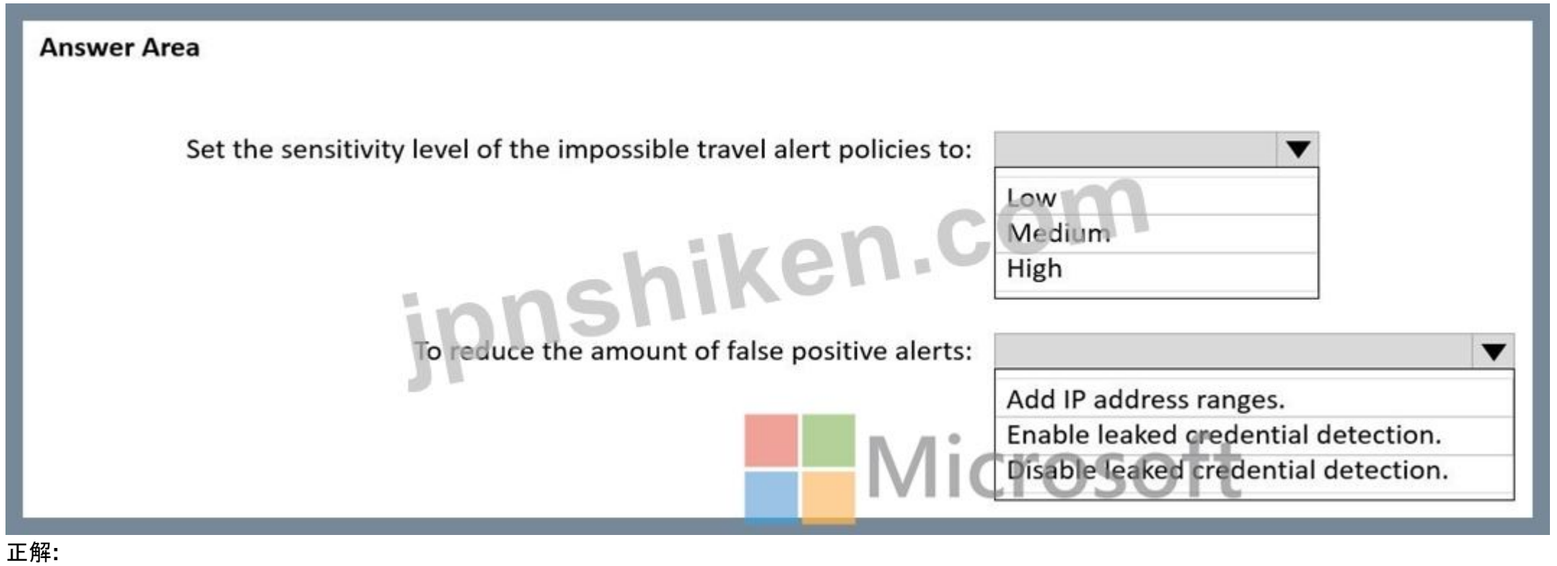
- Microsoft Defender XDR の自動攻撃阻止機能は、
Device1に対する攻撃であり、User1が含まれています。
- ユーザー1がデバイス2への接続を試みます。
User1がDevice2に接続しようとした際、Device2はどのプロトコルをブロックしますか？
A. RDP、RPC、SMB
B. SMBのみ
C. SMBとRPCのみ
D. RDPのみ
E. RDPとRPCのみ
F. RPCのみ
正解: **A (**コメントを発表する**)**

質問: **84**
事例研究3 - Litware Inc.
概要
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。
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、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。
Microsoft 365環境
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を実装し、ログコレクターを有効にします。
Azure環境
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.

Amazon Web Services (AWS) 環境
FabrikamはAccount1という名前のAmazon Web Services(AWS)アカウントを持っています。Account1には
カスタム版Windows Server 2022を実行するAmazon Elastic Compute Cloud(EC2)インスタンス100台。
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。
最新の課題
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」に関する警告を大量に発生させます。
Defender for Identityは、DCSync攻撃の疑いに関するアラートを大量に発生させますが、その多くは誤検知です。
要件
計画されている変更
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
ビジネス要件
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。
Microsoft Defender for Cloud Apps の要件
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。
Microsoft Defender for ID の要件
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。
Microsoft Defender for Cloud の要件
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する。

- 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。
Microsoft Sentinelの要件
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の平均解決時間を特定します。
- 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、Pool1に対して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。
ホットスポットに関する質問
Microsoft Defender for Cloud Apps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:

Answer Area

Set the sensitivity level of the impossible travel alert policies to:

- Low
- Medium
- High

To reduce the amount of false positive alerts:

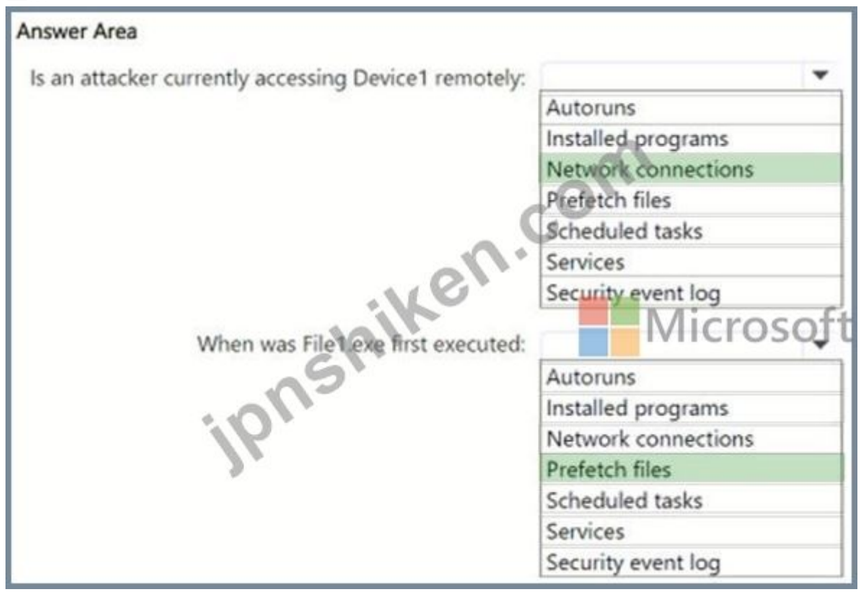
- Add IP address ranges.
- Enable leaked credential detection.
- Disable leaked credential detection.

質問: **85**
ハイブリッド 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があります。
過去 30 日間に Domain Admins グループに加えられたすべての変更を特定する必要があります。
何を使えばいいのでしょうか？
A. Azure Active Directory プロビジョニング分析ワークブック
B. インサイダー リスク管理の概要設定
C. Microsoft Defender for Identity の機密グループの変更レポート
D. Microsoft Defender for Cloud Apps の ID セキュリティ体制評価
正解: **(**正解を表示します**)**
The Modifications of sensitive groups report in Microsoft Defender for Identity would be the best option to use to identify all the changes made to the Domain Admins group during the past 30 days. This report provides information about changes made to sensitive groups, including the Domain Admins group, in the Azure AD environment and helps to identify potential security threats.

質問: **86**
ホットスポットに関する質問
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用で、Device1という名前のWindowsデバイスが含まれています。
デバイス1の悪意のある活動を調査したところ、File1.exeという名前の疑わしいファイルを発見しました。
デバイス1から調査パッケージを受け取ります。
以下の鑑識データポイントを確認する必要があります。
- 現在、攻撃者がリモートでDevice1にアクセスしていますか？

File1.exeはいつ最初に実行されましたか？
各データポイントについて、調査パッケージ内のどのフォルダを確認すればよいですか？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: **87**
ドラッグアンドドロップ問題
以下の表に示すリソースが利用可能です。

Name	Description
SW1	An Azure Sentinel workspace
CEF1	A Linux sever configured to forward Common Event Format (CEF) logs to SW1
Server1	A Linux server configured to send Common Event Format (CEF) logs to CEF1
Server2	A Linux server configured to send Syslog logs to CEF1

SW1では、重複するイベントが発生しないようにする必要があります。
それぞれの操作には何を使用すればよいでしょうか？回答するには、適切なリソースを正しい操作にドラッグしてください。各リソースは、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。

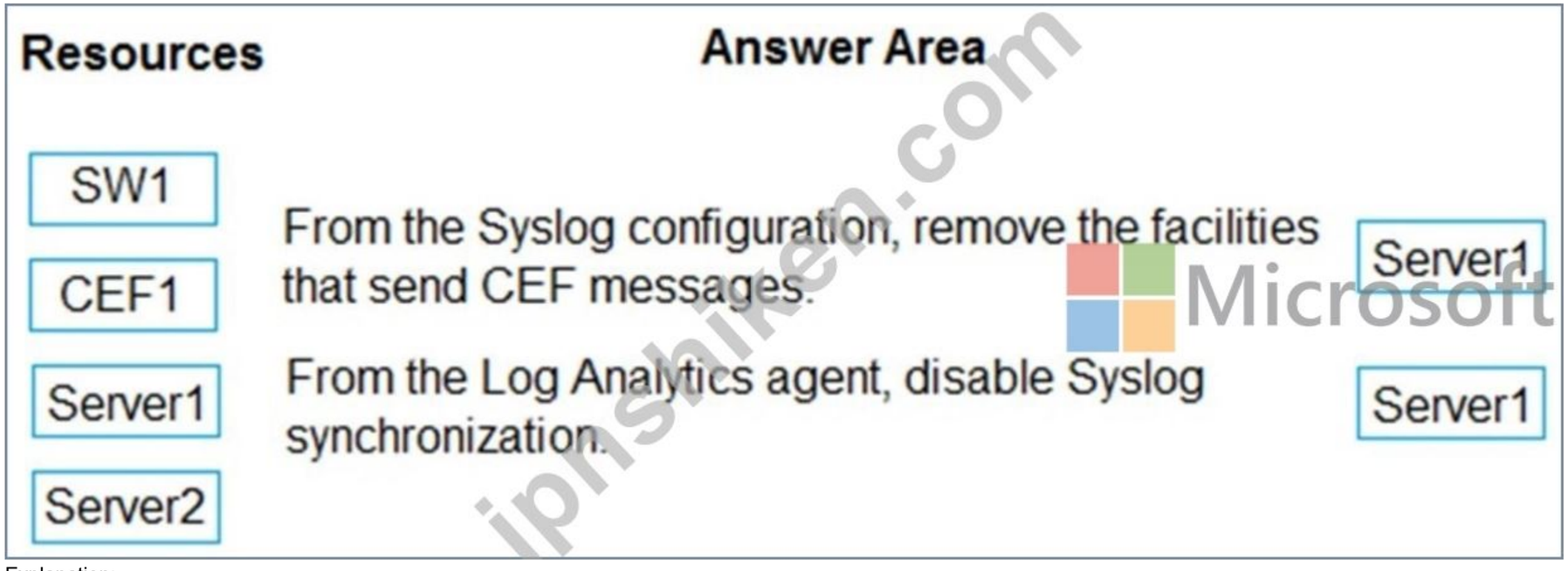
Resources

- SW1
- CEF1
- Server1
- Server2

Answer Area

From the Syslog configuration, remove the facilities that send CEF messages. [ ]

From the Log Analytics agent, disable Syslog synchronization. [ ]



Explanation:
Box 1: Server1
On each source machine that sends logs to the forwarder in CEF format (SERVER1), you must edit the Syslog configuration file to remove the facilities that are being used to send CEF messages. This way, the facilities that are sent in CEF won't also be sent in Syslog.
Box 2: Server1
You must run the following command on those machines (the ones you ran it previously, i.e SERVER1) to disable the synchronization of the agent with the Syslog configuration in Microsoft Sentinel. This ensures that the configuration change you made in the previous step does not get overwritten Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog#run-the-deployment-script

質問**: 88**
事例研究3 - Litware Inc.
概要
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。
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、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。
Microsoft 365環境
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を実装し、ログコレクターを有効にします。
Azure環境
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.

Amazon Web Services (AWS) 環境
FabrikamはAccount1という名前のAmazon Web Services(AWS)アカウントを持っています。Account1には
カスタム版Windows Server 2022を実行するAmazon Elastic Compute Cloud(EC2)インスタンス100台。
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。
最新の課題
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」に関する警告を大量に発生させます。
Defender for Identityは、DCSync攻撃の疑いに関するアラートを大量に発生させますが、その多くは誤検知です。
要件
計画されている変更
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
ビジネス要件
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。
Microsoft Defender for Cloud Apps の要件
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。
Microsoft Defender for ID の要件
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。
Microsoft Defender for Cloud の要件

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する。
- 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。
Microsoft Sentinelの要件
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の平均解決時間を特定します。
- 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、Pool1に対して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。
UEBAを使用するためのMicrosoft Sentinelの要件を満たすには、SecurityEvent Log Analyticsテーブルのデータを関連付ける必要があります。
どのログ分析テーブルを使用すべきですか？
A. SentinelAudit
B. アイデンティティ情報
C. IdentityDirectoryEvents
D. AADRiskyUsers
正解: **(**正解を表示します**)**

質問: **89**
Microsoft Sentinelデータレイクに接続されたMicrosoft Sentinelワークスペースをお持ちです。
Microsoft Visual Studio Code では、脅威を検出する GitHub Copilot エージェントを使用して Jupyter Notebook を実行する予定です。このエージェントは、自然言語クエリを使用して、データレイク内の関連するテーブルを検索し、長期データに対してクエリを実行します。
GitHub CopilotエージェントをMicrosoft Sentinel Model Context Protocol(MCP)コレクションエンドポイントに接続する必要があります。
どのURLを使用すべきですか？
A. https://sentinel.microsoft.com/mcp/triage
B. https://sentinel.microsoft.com/mcp/data-exploration
C. https://sentinel.microsoft.com/mcp/graph
D. https://sentinel.microsoft.com/mcp/security-copilot-agent-creation
正解: **B (**コメントを発表する**)**
To connect your GitHub Copilot agent to the Microsoft Sentinel Model Context Protocol (MCP) collection endpoint for data lake schema searching and log exploration, you must use the following URL:

https://sentinel.microsoft.com/mcp/data-exploration Reference:
https://learn.microsoft.com/en-us/azure/sentinel/datalake/sentinel-mcp-data-exploration-tool

質問: **90**
あなたはMicrosoft 365のサブスクリプションをお持ちです。
以下のKQLクエリがあります。

```
DeviceEvents
| where ActionType == "AntivirusDetection"
```

クエリを使用して、Microsoft Defender XDR のカスタム検出ルールを作成できることを確認する必要があります。
クエリには何を追加すべきですか？
A. | summarize (ReportId)=make_set(ReportId), count() by DeviceId
B. | summarize (Timestamp)=range(Timestamp), count() by DeviceId
C. | summarize (Timestamp, DeviceName)=arg_min(Timestamp, DeviceName), count() by DeviceId
D. | summarize (Timestamp, ReportId)=arg_max(Timestamp, ReportId), count() by DeviceId
正解: **(正解を表示します)**

質問: **91**
お客様は、DB1 という名前のデータベース サーバーを含む Microsoft 365 E5 サブスクリプションをご利用中です。DB1 は Microsoft Defender XDR にオンボーディングされています。
攻撃対象領域マップにDB1が表示されるようにする必要があります。
何を設定すればよいですか？
A. 重要な資産ルール
B. 機密性の高いエンティティタグ
C. 資産ルール
D. ハニートークンエンティティタグ
正解: **A (コメントを発表する)**

質問: **92**
お客様は、Microsoft Entra ID P1ライセンスを持つMicrosoft Entraテナントをご利用中です。
Azure Monitor の診断設定を使用して、Microsoft Graph のアクティビティ ログを Workspace1 という名前の Log Analytics ワークスペースにストリーミングします。
Workspace1 にクエリを実行できます。
社内基幹業務(LOB)アプリケーションが、Microsoft 365 グループを列挙し、認証チェックに失敗している疑いがあります。このアプリケーションは過去 3 日間で大量の Microsoft Graph リクエストを生成し始め、その失敗は HTTP 401 および HTTP として報告されています。
403エラー。
失敗したリクエストに関連付けられているIDを特定する必要があります。ソリューションは、過去3日間に/groupsリソースに対して不正なリクエストを生成した上位のIDを、AppId、ServicePrincipalId、およびUserIdごとにグループ化して返す必要があります。
Workspace1で実行すべきKQLクエリはどれですか？

A.
```
MicrosoftGraphActivityLogs
| where TimeGenerated >= ago(3d)
| where ResponseStatusCode == 200
| where RequestUri contains "/groups"
| summarize UniqueRequests=count_distinct(RequestId) by AppId
| sort by UniqueRequests desc
| limit 20
```

B.
```
MicrosoftGraphActivityLogs
| where TimeGenerated >= ago(30d)
| where ResponseStatusCode == 401 or ResponseStatusCode == 403
| where RequestUri contains "/users"
| summarize UniqueRequests=count_distinct(RequestId) by AppId, ServicePrincipalId, UserId
| sort by UniqueRequests desc
| limit 20
```

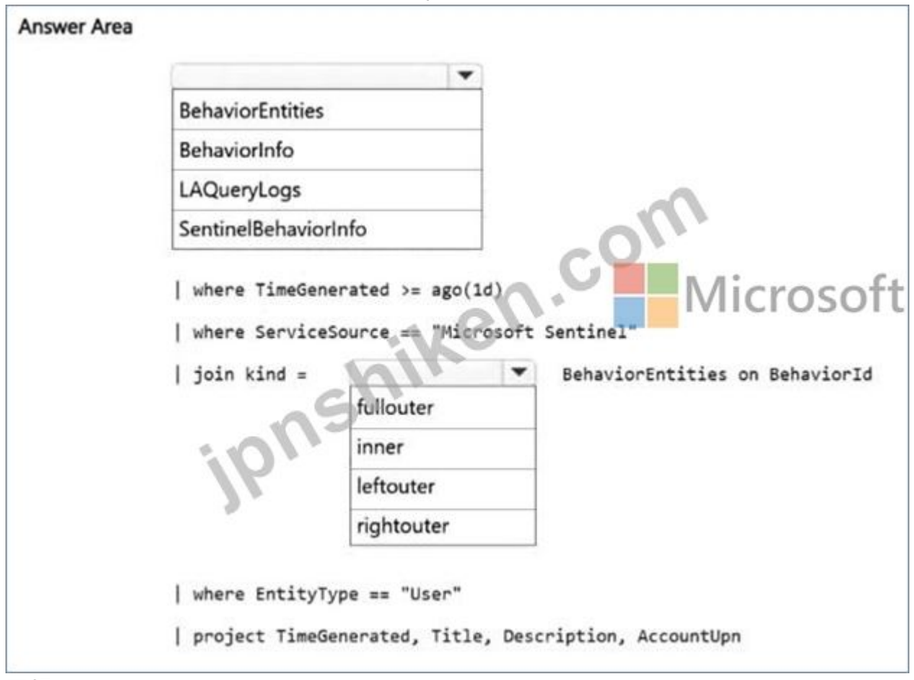
C.
```
MicrosoftGraphActivityLogs
| where TimeGenerated >= ago(3d)
| where ResponseStatusCode == 401 or ResponseStatusCode == 403
| where RequestUri contains "/groups"
| summarize UniqueRequests=count_distinct(RequestId) by AppId, ServicePrincipalId, UserId
| sort by UniqueRequests desc
| limit 20
```

D.
```
SigninLogs
| where TimeGenerated >= ago(3d)
| where Status.errorCode == 401 or Status.errorCode == 403
| summarize UniqueRequests=count_distinct(CorrelationId) by AppId, UserId
| sort by UniqueRequests desc
| limit 20
```

正解: (正解を表示します)

Run the following KQL query in your Log Analytics workspace using the Azure Monitor Log Analytics to filter for the /groups endpoint and identify the unauthorized identities:kustoMicrosoftGraphActivityLogs
| where TimeGenerated >= ago(3d)
| where ResponseStatusCode in (401, 403)
| where RequestUri contains "/groups"
| summarize RequestCount = count() by AppId, ServicePrincipalId, UserId
| order by RequestCount desc
Reference:
https://learn.microsoft.com/en-us/graph/microsoft-graph-activity-logs-overview

質問: **93**
ホットスポットに関する質問
Microsoft Defenderポータルに接続されたWorkspace1という名前のMicrosoft Sentinelワークスペースがあります。
あなたは以下の操作を実行します。
- Log Analyticsワークスペースの診断設定を構成して収集します
Workspace1 内の LAQueryLogs という名前のテーブルに監査データをクエリします。
- ユーザーおよびエンティティ行動分析(UEBA)行動レイヤーを有効にする
また、動作記録が生成され、Workspace1 の SentinelBehaviorInfo テーブルと SentinelBehaviorEntities テーブルに保存されていることを確認します。
以下の要件を満たす高度なハンティングクエリを作成する必要があります。
- Microsoft Sentinelによって生成されたUEBA動作を返します
過去24時間以内
- 各動作に関連付けられたユーザープリンシパル名(UPN)が含まれます
- UPNが関連付けられていない場合でも、動作行を返します
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。



正解:

Answer Area

Explanation:

Box 1: BehaviorInfo

The query projects Title and Description, which are columns specific to the behavior alert data stored in the BehaviorInfo table. The BehaviorEntities table only handles the mapping of entities to those behaviors.

Box 2: leftouter

The third requirement states that the query must return the behavior row even when there is no UPN associated. A Left Outer Join (kind = leftouter) ensures all rows from the left table (BehaviorInfo) are kept, even if there is no matching entity row on the right side (BehaviorEntities).

Reference:

https://medium.com/@esilvalabh/kql-script-to-identify-mfa-compromised-in-azure-cloud-adf6b1bc8308

質問**: 94**

ホットスポットに関する質問

あなたは、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Team1という名前のMicrosoft Teamsチームが含まれています。

あなたは、Teamsチャットのメッセージや共有ファイルを介した内部認証情報の漏洩の疑いについて調査しています。

Team1のプライベートチャンネルと共有チャンネルからコンテンツを返すコンテンツ検索を作成する必要があります。

各チャンネルの種類ごとに、コンテンツ検索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

Private channel:

- The mailbox of Team1
- The Microsoft SharePoint Online site of Team1
- The Microsoft Exchange Online mailbox of each Team1 member

Shared channel:

- The mailbox of Team1
- The Microsoft SharePoint Online site of Team1
- The Microsoft OneDrive location of each Team1 owner

正解:

Answer Area

Private channel:

- The mailbox of Team1
- The Microsoft SharePoint Online site of Team1
- The Microsoft Exchange Online mailbox of each Team1 member

Shared channel:

- The mailbox of Team1
- The Microsoft SharePoint Online site of Team1
- The Microsoft OneDrive location of each Team1 owner

Explanation:

Box 1: The Microsoft Exchange Online mailboxes of each Team1 member

Private Channels

Channel Messages:

Newer Content: Target the dedicated private channel mailbox linked to the parent Microsoft 365 Group.

*-> Historical Content: Target the individual Exchange Online mailboxes of all members belonging to that private channel.

Shared Files: Target the distinct SharePoint site collection automatically generated specifically for that individual private channel Box 2: The Microsoft SharePint Online site of Team1 Shared Channels Channel Messages: Target the primary Exchange Online mailbox of the parent team (the host Microsoft 365 Group mailbox). Individual system mailboxes for shared channels cannot be targeted independently.

Shared Files: Target the distinct SharePoint site collection automatically provisioned for that specific shared channel.

Reference:
https://learn.microsoft.com/en-us/purview/edisc-search-teams

質問: **95**
異常な Azure Active Directory (Azure AD) サインイン アクティビティを追跡し、アクティビティを日ごとに集計したタイム チャートとして表示するカスタム Azure Sentinel クエリを作成する予定です。
タイム チャートを表示するために使用されるクエリを作成する必要があります。クエリには何を含めるべきでしょうか?
A. 拡張します
B. ビン
C. Makeset
D. ワークスペース
正解: **(**正解を表示します**)**
Grouping results can also be based on a time column, or another continuous value. Simply summarizing by TimeGenerated, though, would create groups for every single millisecond over the time range, because these are unique values.
To create groups that are based on continuous values, it's best to break the range into manageable units by using bin.

質問: **96**
ホットスポットに関する質問
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
以下の要件を満たすKQLのハンティングクエリを作成する必要があります。
- 電子メールを受信したデバイスを特定します
過去 12 時間以内に File1.pdf という名前の添付ファイルを開き、
添付ファイル。
クエリの実行に必要なリソースを最小限に抑えます。
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:

Explanation:
Box 1: innerunique
The innerunique join flavor removes duplicate keys from the left side. This behavior ensures that the output contains a row for every combination of unique left and right keys.
By default, the innerunique join flavor is used if the kind parameter isn't specified. This default implementation is useful in log/trace analysis scenarios, where you aim to correlate two events based on a shared correlation ID. It allows you to retrieve all instances of the phenomenon while disregarding duplicate trace records that contribute to the correlation.
Box 2: FileOriginUrl
The DeviceFileEvents table in the advanced hunting schema contains information about file creation, modification, and other file system events.
Reference:
https://learn.microsoft.com/en-us/kusto/query/join-innerunique
https://learn.microsoft.com/en-us/kusto/query/join-operator
https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-devicefileevents-table

質問: **97**
あなたは、Microsoft Defender for Endpointを導入しているXYZ社のSOCアナリストです。疑わしいPowerShellコマンドラインに関連するアラートを含むインシデントを担当することになりました。まず、インシデントの内容を確認し、関連するすべてのアラート、デバイス、および証拠を収集します。
アラートページを開いてアラートを評価し、デバイスに対してさらに分析を実行することを選択します。デバイスページを開き、カスタムの.ps1スクリプトを使用してより多くのフォレンジック情報を収集するために、デバイスへのリモートアクセスが必要であると判断します。
調査パッケージにはどのような種類の情報が含まれますか？
A. ファイルのプリフェッチ
B. ネットワーク取引
C. コマンド履歴
D. プロセス履歴
正解: **(正解を表示します)**
Network transactions, Process and Command History are not collected. Only Prefetch files are collected.
An investigation package contains the following folders when you collect it from a device as part of the investigation process. These can help us identify the present state of devices and methods used by attackers.
Autoruns, installed programs, Network Connections, Prefetch files, Prefetch folder, Processes, Scheduled tasks, Security event log, Services, Windows Server Message Block (SMB) sessions, System Information, Temp Directories, Users and Groups, WdSupportLogs, CollectionSummaryReport.xls Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide
質問: **98**
ホットスポットに関する質問

お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
お客様のネットワークには、Microsoft Entra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。
デバイスおよびAD DSドメインコントローラーに記録された、直近100件のサインイン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

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [ join kind=full outer | join kind=inner | union ] (
    [ IdentityInfo | IdentityLogonEvents | IdentityQueryEvents ]
  | extend Table = 'table2'
  | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

正解:

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [ join kind=full outer | join kind=inner | union ] (
    [ IdentityInfo | IdentityLogonEvents | IdentityQueryEvents ]
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```


Explanation:

Box 1: union

Use union to add the DeviceLogonEvent and the IdentityLogonEvents.

Box 2: IdentityLogonEvents

Example:

// Notice we no longer have the extra columns from a join. This might be useful if you want to track

// logon activity with devices (the DeviceLogonEvents table) and Active Directory \ Azure Active Directory

// (the IdentityLogonEvents table) in one query.

DeviceLogonEvents

| extend Table = 'DeviceLogonEvents'

| take 100

| union (
IdentityLogonEvents
| extend Table = 'IdentityLogonEvents'
| take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
Reference:
https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Webcasts/TrackingTheAdversary/Episode%202%20-%20Joins.txt

質問: **99**
Workspace1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。
Content Hub から、Microsoft Sentinel 用の Microsoft Entra ソリューションを展開し、コネクタを構成します。
サブスクリプションに対する管理者権限を持つユーザーが行った操作を分析する必要があります。
どのワークブックを使うべきですか？
A. Azureアクティビティ
B. Microsoft Entra監査ログ
C. Microsoft Entra サインインログ
D. アイデンティティとアクセス
正解: **(**正解を表示します**)**
The Azure Monitor Activity Log is a platform log that provides insight into subscription-level events.
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-insights

質問: **100**
お客様は、Microsoft Defender for Cloudが有効になっているAzureサブスクリプションをご利用中です。
Windows 10が動作し、Log Analyticsエージェントがインストールされている仮想マシンがあります。
仮想マシンに対する攻撃をシミュレートし、アラートを生成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. Log Analyticsトラブルシューティングツールを実行します。
B. ファイルをコピーして実行し、ファイル名を ASC_AlertTest_662jfi039N.exe に変更します。
C. Microsoft Monitoring Agent の設定を変更します。
D. MMASetup実行ファイルを実行し、-foo引数を指定します。
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation

質問: **101**
事例研究4 - Litware Inc.
概要
アダタム ･コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境

オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。

ライセンス状況

Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。

クラウド環境

クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境

オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件

計画されている変更

Adatum社は以下の変更を実施する予定です。

- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。

Microsoft Defender for Cloud の要件

Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。

グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。

- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。

Microsoft Sentinelの要件

Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。

- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。

- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。

可能な限り、ASIMに組み込まれているパーサーを使用してください。

ビジネス要件

Adatumは、以下のビジネス要件を特定しました。

可能な限り、最小権限の原則に従うこと。

可能な限り管理業務を最小限に抑える。

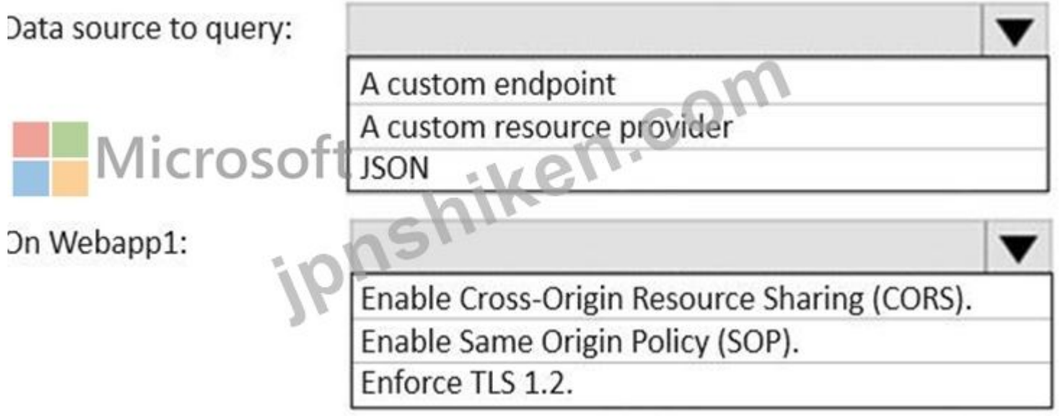
ホットスポットに関する質問

Workbook1とWebapp1に対して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の要件を満たしている必要があります。

クエリ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。

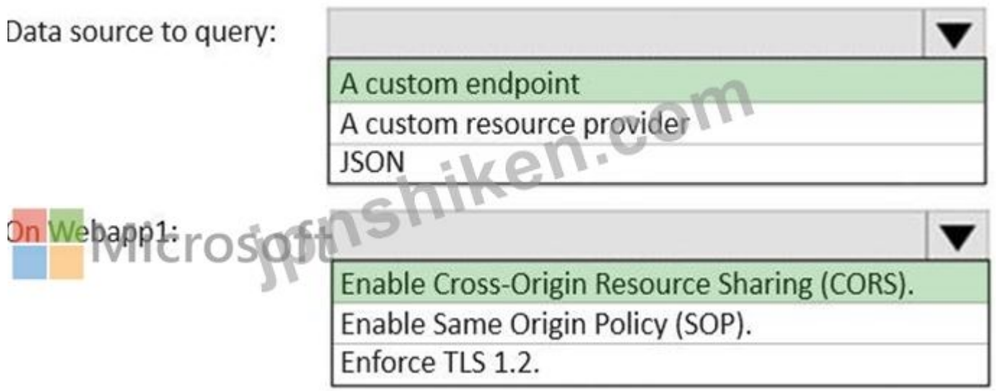
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:

Answer Area

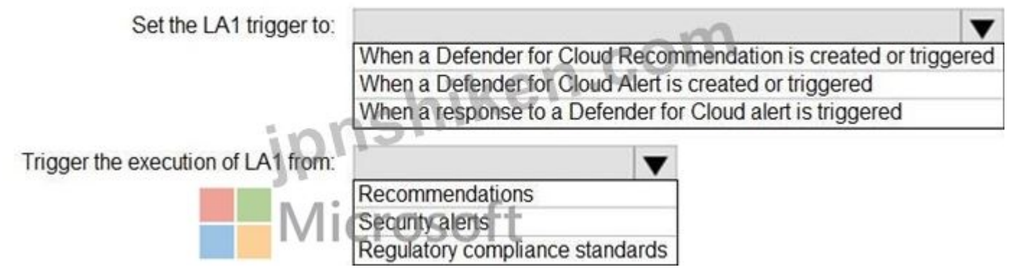


Explanation:
https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-data-sources#custom-endpoint

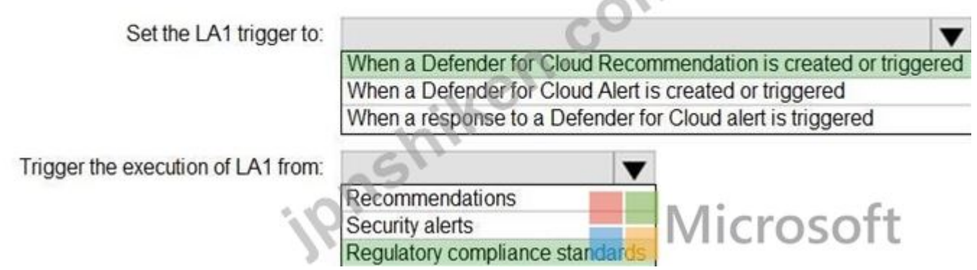
質問**: 102**
Azure サブスクリプションを作成します。
サブスクリプションに対して Azure Defender を有効にします。
オンプレミスのコンピューターを保護するには、Azure Defender を使用する必要があります。
オンプレミスのコンピューターでは何をすべきでしょうか?
A. Log Analytics エージェントをインストールします。
B. 依存関係エージェントをインストールします。
C. Hybrid Runbook Worker ロールを構成します。
D. Connected Machine エージェントをインストールします。
正解**: A (**コメントを発表する**)**
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

質問**: 103**
ホットスポットに関する質問
お客様のAzureサブスクリプションでは、サポートされているすべてのリソースタイプに対してMicrosoft Defender for Cloudが有効になっています。
LA1という名前のAzureロジックアプリを作成します。
あなたは、LA1を使用してDefender for Cloudで検出されたセキュリティリスクを自動的に修復することを計画しています。
Defender for CloudでLA1をテスト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。
Answer Area



正解:
Answer Area



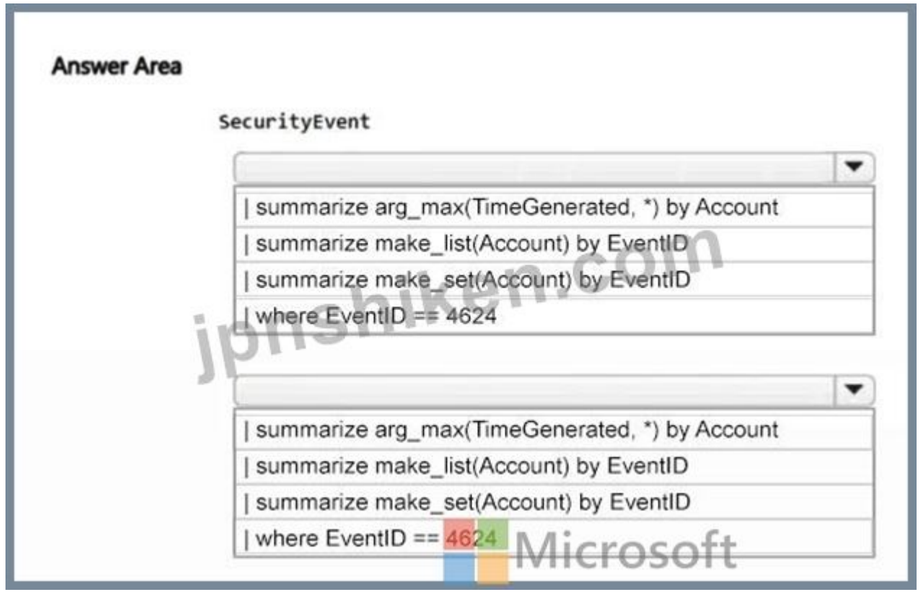
質問: 104
Microsoft Defender for Endpointに登録され、改ざん防止機能が有効になっている、Device1という名前のWindows 11デバイスがあります。
あなたはデバイス1における潜在的な脅威を調査しています。
デバイス1のトラブルシューティングモードを有効にします。
デバイス1の改ざん防止機能を一時的に無効にする必要があります。
Device1で実行すべきPowerShellコマンドはどれですか？
A. Set-MpPreference
B. mpcmdrun.exe
C. Get-MpComputerStatus
D. MDELiveAnalyzer.ps1
正解: C (コメントを発表する)
Once troubleshooting mode has been enabled for the device from the Microsoft Defender Portal, you must run the following PowerShell command as an administrator to temporarily disable Tamper Protection:
Set-MpComputerStatus -DisableTamperProtection $trueBy default, troubleshooting mode is limited to 4 hours per device. Once the troubleshooting period expires, Tamper Protection will automatically revert to its previously configured (enabled) state and any changes made will be rolled back.
Reference:
https://learn.microsoft.com/en-us/defender-endpoint/enable-troubleshooting-mode
質問: 105

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
アマゾン ウェブ サービス (AWS) 上に Linux 仮想マシンがあります。
Azure Defender をデプロイし、自動プロビジョニングを有効にします。
Azure Defender を使用して仮想マシンを監視する必要があります。
解決策: Azure Arc を有効にし、仮想マシンを Azure Arc にオンボードします。
これは目標を達成していますか?
A. はい
B. いいえ
正解**: (**正解を表示します**)**
A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.
Install Log Analytics manually or when you enable auto provisioning of Log Analytics in
"Autoprovisioning" tag, auto provisioning is already turned on.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc
https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-feature

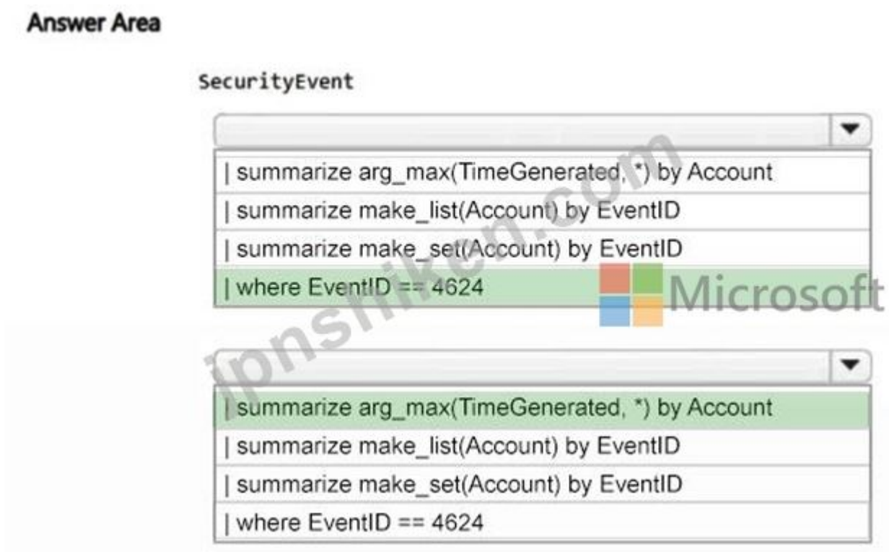
質問**: 106**
お客様は、Microsoft Defender for Cloudを使用するAzureサブスクリプションをお持ちです。
セキュリティアラートビューをフィルタリングして、以下のアラートを表示する必要があります。
- 不審なユーザーがキー保管庫にアクセスしました
- 通常とは異なる場所からログインする
- 不可能な旅行アクティビティ
どの重症度を適用すべきですか？
A. 情報提供
B. 中
C. 高
正解**: (**正解を表示します**)**
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview#how-are-alerts-classified

質問**: 107**
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:



質問: **108**

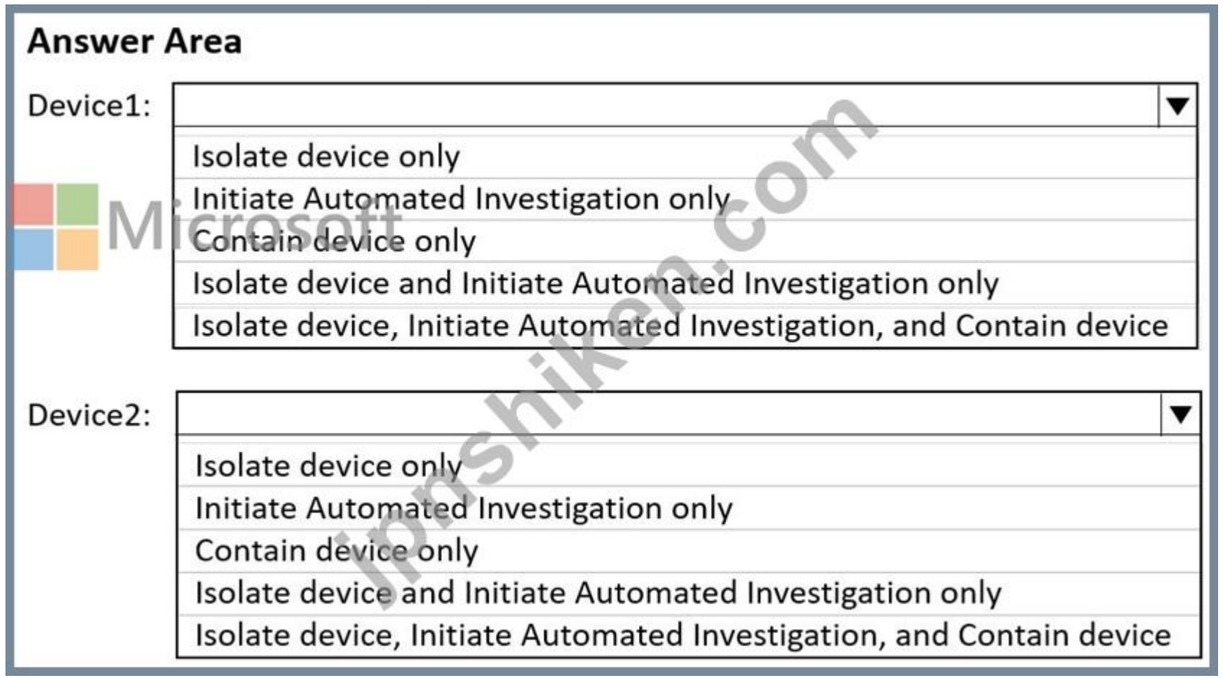
ホットスポットに関する質問

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

あなたは、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:

Answer Area

Device1:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Device2:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

質問: **109**
お客様のオンプレミスネットワークには、contoso.com と fabrikam.com という名前の 2 つの Active Directory ドメインサービス (AD DS) ドメインが含まれています。contoso.com には Group1 という名前のグループが含まれています。
Fabrikam.comには、Group2という名前のグループが存在します。
Microsoft SentinelワークスペースWS1には、Rule1という名前のスケジュール済みクエリルールが含まれています。Rule1は、異常なAD DSセキュリティイベントに応じてアラートを生成します。各アラートはインシデントを作成します。
以下の要件を満たすインシデントトリアージソリューションを導入する必要があります。
- contoso.com からのセキュリティインシデントはグループ1に割り当てる必要があります。
- fabrikam.com からのセキュリティインシデントはグループ2に割り当てる必要があります。
- 管理業務の負担を最小限に抑える必要がある。
解決策には何を含めるべきですか？
A. ルール1に割り当てられた自動化ルール1つ
B. インシデントの発生によってトリガーされるプレイブック
C. ルール1に割り当てられた2つの自動化ルール
D. アラートの作成によってトリガーされるプレイブック
正解: **(**正解を表示します**)**
質問: **110**
ホットスポットに関する質問

お客様のAzureサブスクリプションには、以下の表に示すユーザーが含まれています。

Name	Role	Scope
User1	Contributor	Subscription
User2	Contributor	Subscription
User3	Security Reader	Resource group

このサブスクリプションには、次の表に示すように、Azure Firewall のインスタンスが含まれています。

Name	Log configuration	Destination
AFW1	Unstructured logs	Log Analytics
AFW2	Structured intrusion detection and prevention system (IDPS) logs	Azure Event Hubs
AFW3	Structured intrusion detection and prevention system (IDPS) logs	Log Analytics

お客様は、Microsoft Copilot for Security を使用する Microsoft 365 E5 サブスクリプションをお持ちです。Copilot for Security の役割割り当ては、次の表に示すとおりです。

User	Role
User1	Copilot Owner
User2	Copilot Contributor
User3	Copilot Owner

各ユーザーは、Copilot for Securityのセッションを実行します。

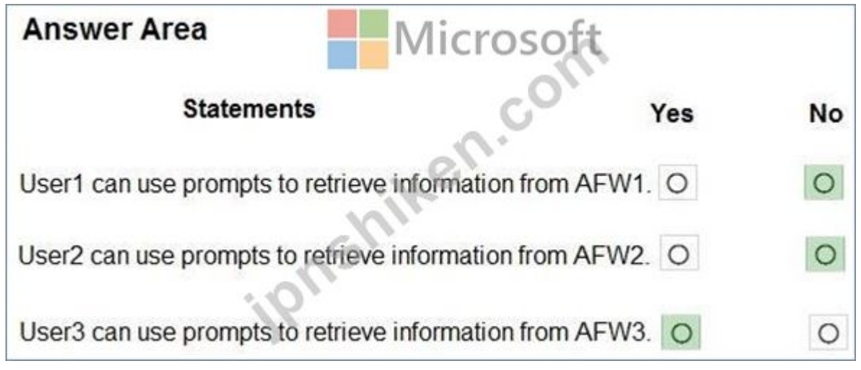
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can use prompts to retrieve information from AFW1.	○	○
User2 can use prompts to retrieve information from AFW2.	○	○
User3 can use prompts to retrieve information from AFW3.	○	○

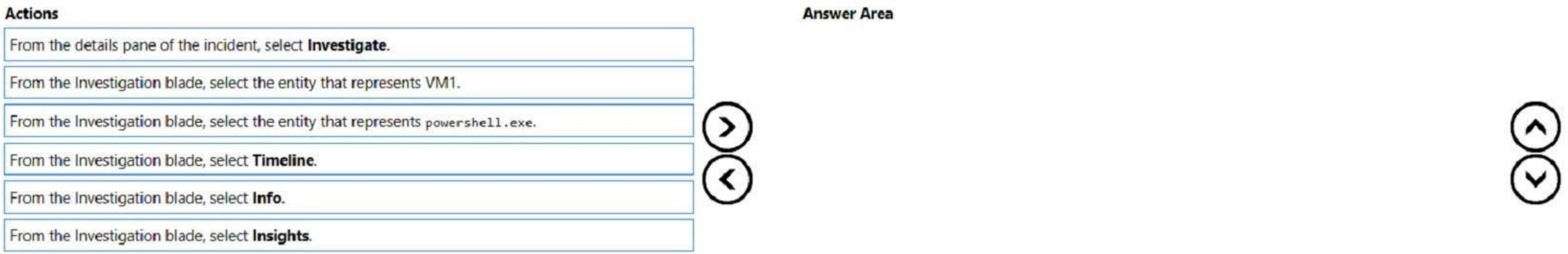
正解:



質問: **111**
事例研究1 - Contoso Ltd
概要
Contoso Ltd.という会社は、北米各地に本社と5つの支店を構えています。本社はシアトルにあり、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アラートを受信している。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威で、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る。
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る。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複数発生している。
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
技術要件を満たすためには、現在発生している攻撃に対処する必要があります。
解決策には何を含めるべきですか？
A. Azure Automation ランブック
B. Azure Logic Apps
C. Azure Functions
D. Azure Sentinel のライブ配信
正解**: (**正解を表示します**)**
Playbooks in Azure Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise. This means that playbooks can take advantage of all the power and customizability of Logic Apps' built-in templates.
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

質問**: 112**
ドラッグアンドドロップ問題
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**:**

Explanation:

Step 1: From the details pane of the incident, select Investigate.

Choose a single incident and click View full details or Investigate.

Step 2: From the Investigation blade, select the entity that represents VM1.

The Investigation Insights workbook is broken up into 2 main sections, Incident Insights and Entity Insights.

Incident Insights

The Incident Insights gives the analyst a view of ongoing Sentinel Incidents and allows for quick access to their associated metadata including alerts and entity information.

Entity Insights

The Entity Insights allows the analyst to take entity data either from an incident or through manual entry and explore related information about that entity. This workbook presently provides view of the following entity types:

* IP Address
* Account
* Host
* URL

Step 3: From the Investigation blade, select Insights

The Investigation Insights Workbook is designed to assist in investigations of Azure Sentinel Incidents or individual IP/Account/Host/URL entities.

Reference:

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

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

質問**: 113**

Microsoft SharePoint Online を使用する Microsoft 365 E5 サブスクリプションを持っています。

サブスクリプションからユーザーを削除します。

削除されたユーザーが、アカウントが削除される前の月に SharePoint Online サイトから多数のドキュメントをダウンロードした場合は、通知する必要があります。

何を使えばいいのでしょうか？

A. Microsoft Defender for Cloud Apps のファイル ポリシー

B. アクセスレビューポリシー

C. Microsoft Defender for Office 365 のアラート ポリシー

D. インサイダー リスク ポリシー

正解**: (**正解を表示します**)**

When users leave your organization, there are specific risk indicators typically associated with data theft by departing users. This policy template uses exfiltration indicators for risk scoring and focuses on detection and alerts in this risk area.

Reference:

https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management- policies?view=o365-worldwide#data-theft-by-departing-users

質問: **114**
事例研究1 - Contoso Ltd
概要
Contoso Ltd.という会社は、北米各地に本社と5つの支店を構えています。本社はシアトルにあり、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アラートを受信している。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威で、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る。
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る。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複数発生している。
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
Microsoft Defender for Office 365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. マーケティング
C. セキュリティ

D. 売上

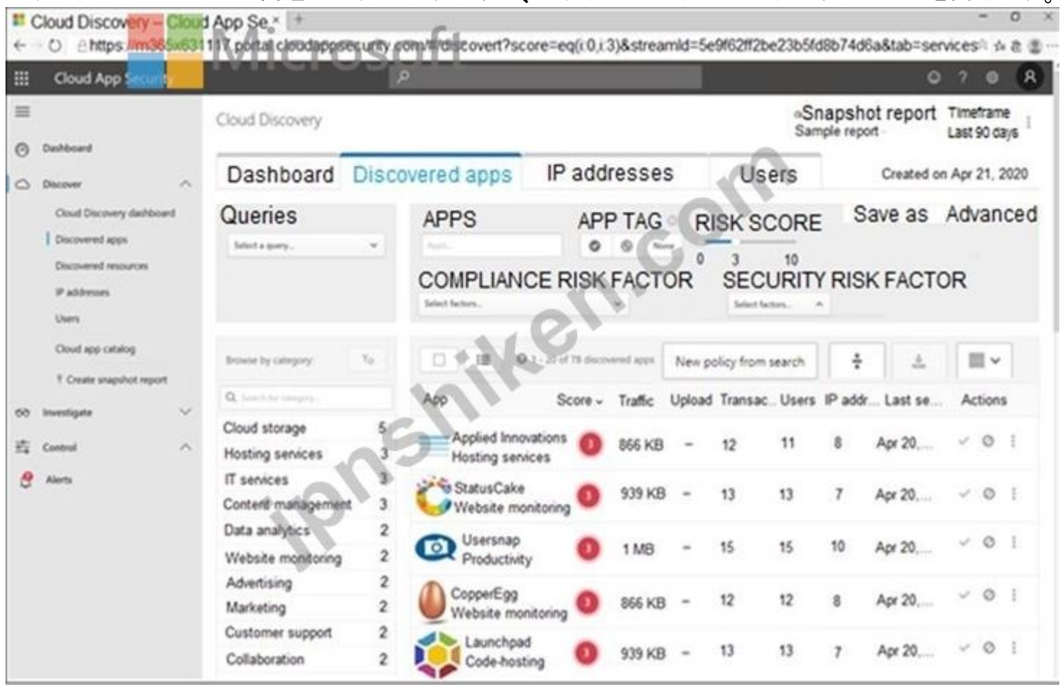
正解: **(**正解を表示します**)**

If the marketing team at Contoso has experienced incidents in which vendors uploaded files that contain malware to SharePoint Online sites, Microsoft Defender for Office 365 could potentially be useful for helping to protect against these types of threats.

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-for-spo-odb-and-teams?view=o365-worldwide

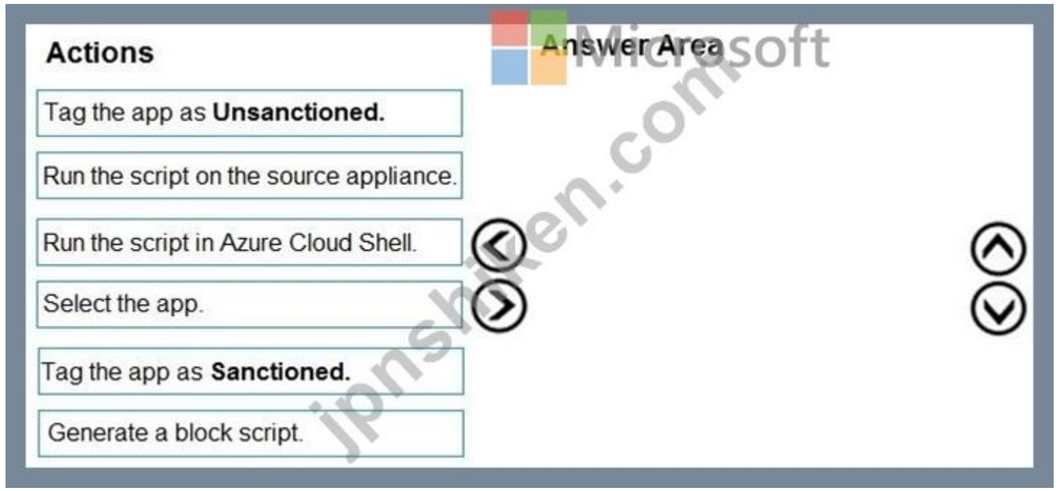
質問: **115**

ドラッグアンドドロップ問題 次の図に示すように、クラウドアプリセキュリティポータルを開きます。

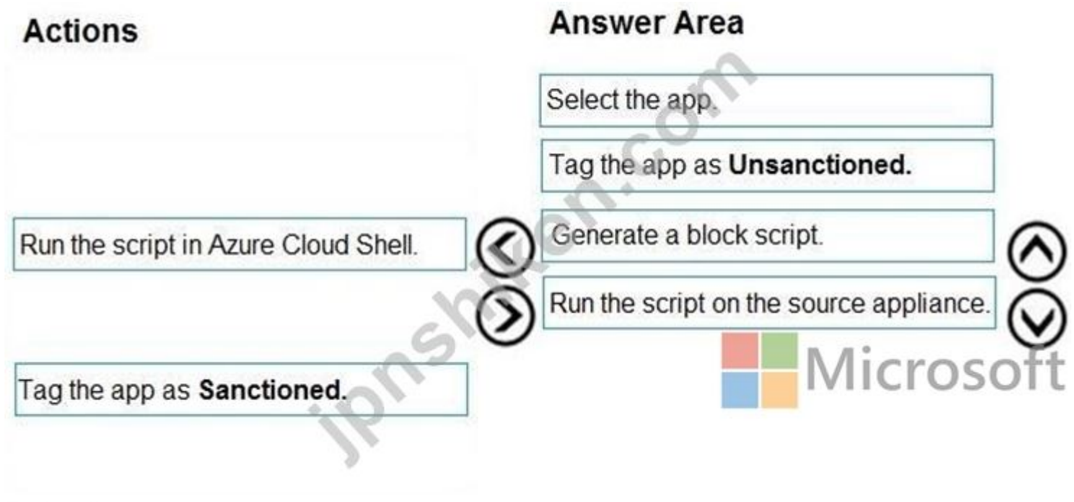


Launchpadアプリのリスクを軽減する必要があります。

どの4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:
https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

質問: **116**
Microsoft 365 Defenderは、Microsoft 365サービス全体にわたるセキュリティインシデントとアラートを管理および調査するための、目的に特化したユーザーインターフェースを提供します。
あなたは、Microsoft 365 Defenderソリューション(Defender for Endpoint、Defender for Identity、Defender for Office 365、およびCloud App Securityを含む)を構成しているXYZ社に勤務するSOCアナリストです。
インシデントの影響全体を把握し、根本原因分析(RCA)を実施するには、関連するアラートをすべてのソリューションにわたって単一のインシデントとして監視する必要があります。Microsoft セキュリティ センター ポータルには、インシデントとその対応策が統合的に表示されます。
次のうち、インシデントに分類されるものはどれですか？
A. テストアラート
B. 真の警戒
C. 厳戒態勢

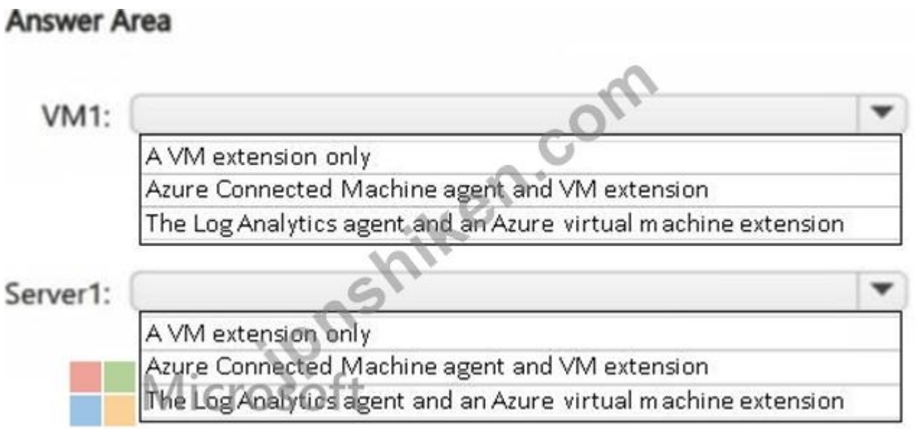
D. 陽性反応
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/investigate-incidents?view=o365-worldwide

質問: **117**
あなたの会社は次のサービスを展開しています。
ID 用の Microsoft Defender
エンドポイント用 Microsoft Defender
Office 365 用 Microsoft Defender
セキュリティ アナリストに Microsoft 365 セキュリティ センターを使用できるようにする必要があります。アナリストは、Microsoft Defender for Endpoint によって生成された保留中のアクションを承認および拒否できる必要があります。ソリューションでは、最小特権の原則を使用する必要があります。
アナリストに割り当てるべき 2 つの役割はどれですか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure Active Directory (Azure AD) のコンプライアンス データ管理者
B. Microsoft Defender for Endpoint のアクティブな修復アクションのロール
C. Azure Active Directory (Azure AD) のセキュリティ管理者ロール
D. Azure Active Directory (Azure AD) のセキュリティ閲覧者ロール
正解: **B,D (**コメントを発表する**)**
Security Reader - can access M365 Security Center.
Active Remediation Actions role in Defender for Endpoint meets need to 'approve and reject' pending actions with respect to Defender For Endpoint.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365- worldwide

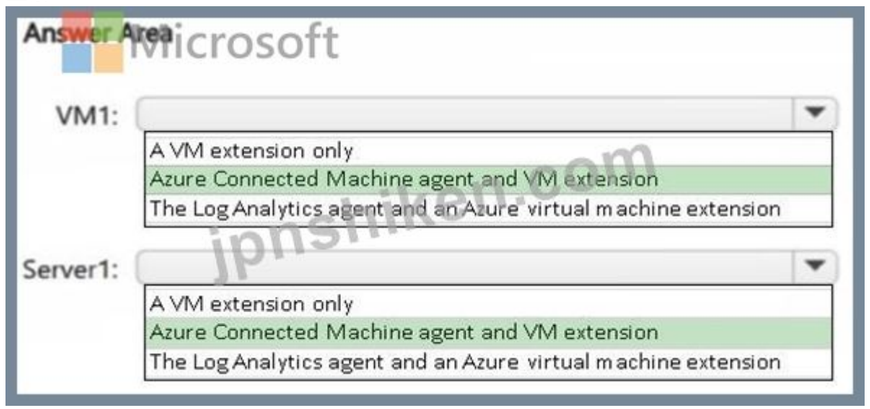
質問: **118**
ホットスポットに関する質問
以下の表に示すリソースが利用可能です。

Name	Type	Description
Server1	On-premises server	Runs Windows Server 2022 Has Microsoft SQL Server 2022 installed
VM1	SQL Server on Azure Virtual Machines	Runs Windows Server 2022 Has Microsoft SQL Server 2022 installed

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。
VM1とServer1を保護するには、Defender for Cloudを使用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。
-高度な脅威対策と脆弱性評価をサポートする。
- 各SQL Server 2022インスタンスをSQL仮想マシンとして登録します。
導入および管理の手間を最小限に抑える。
各サーバーには何をデプロイすべきですか？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:

Box 1: The Azure Connected Machine agent and an Azure virtual machine extension.

Microsoft Defender for Cloud, Enable Microsoft Defender for SQL servers on machines Set up Microsoft Defender for SQL servers on machines The Defender for SQL server on machines plan requires Azure Monitoring Agent (AMA) to prevent attacks and detect misconfigurations.

Note: The Azure Connected Machine agent (Azure Arc agent) connects your non-Azure machine to Azure for management and governance, while the Azure Monitor agent (AMA) collects performance data, logs, and metrics from the machine. The Connected Machine agent is a prerequisite, acting as a bridge to Azure, and it enables you to install the AMA as an extension to send monitoring data to Azure Monitor.

Box 2: The Azure Connected Machine agent and an Azure virtual machine extension.

Reference:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-sql-usage

https://learn.microsoft.com/en-us/sql/sql-server/azure-arc/overview

質問**: 119**

お客様は、Windows 10 デバイス 100 台を含む Microsoft 365 E5 サブスクリプションをお持ちです。

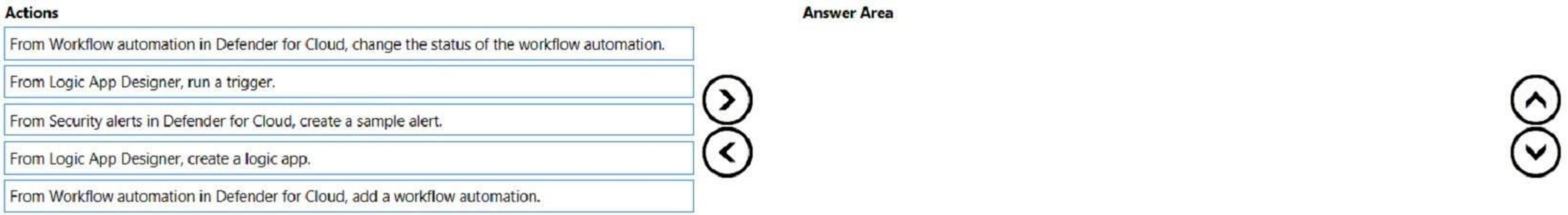
デバイスをMicrosoft Defender 365に登録します。

Microsoft 365 Defender ポータルから、オンボーディング済みのデバイス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。

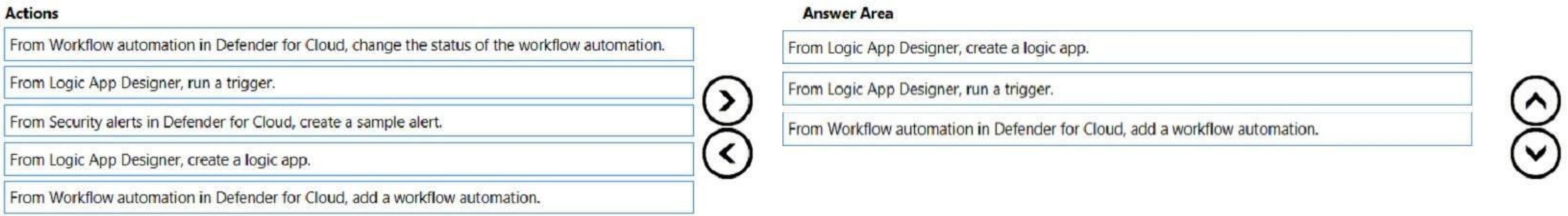
まず最初に何をすべきでしょうか？

A. Microsoft 365 Defender のアクセス許可を変更します。
B. デバイスグループを作成します。
C. Microsoft 365 Defender ポータルのエンドポイント設定の 高度な機能」から、自動調査を有効にします。
D. ロールベースアクセス制御 (RBAC) を設定します。
正解: **D (**コメントを発表する**)**
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

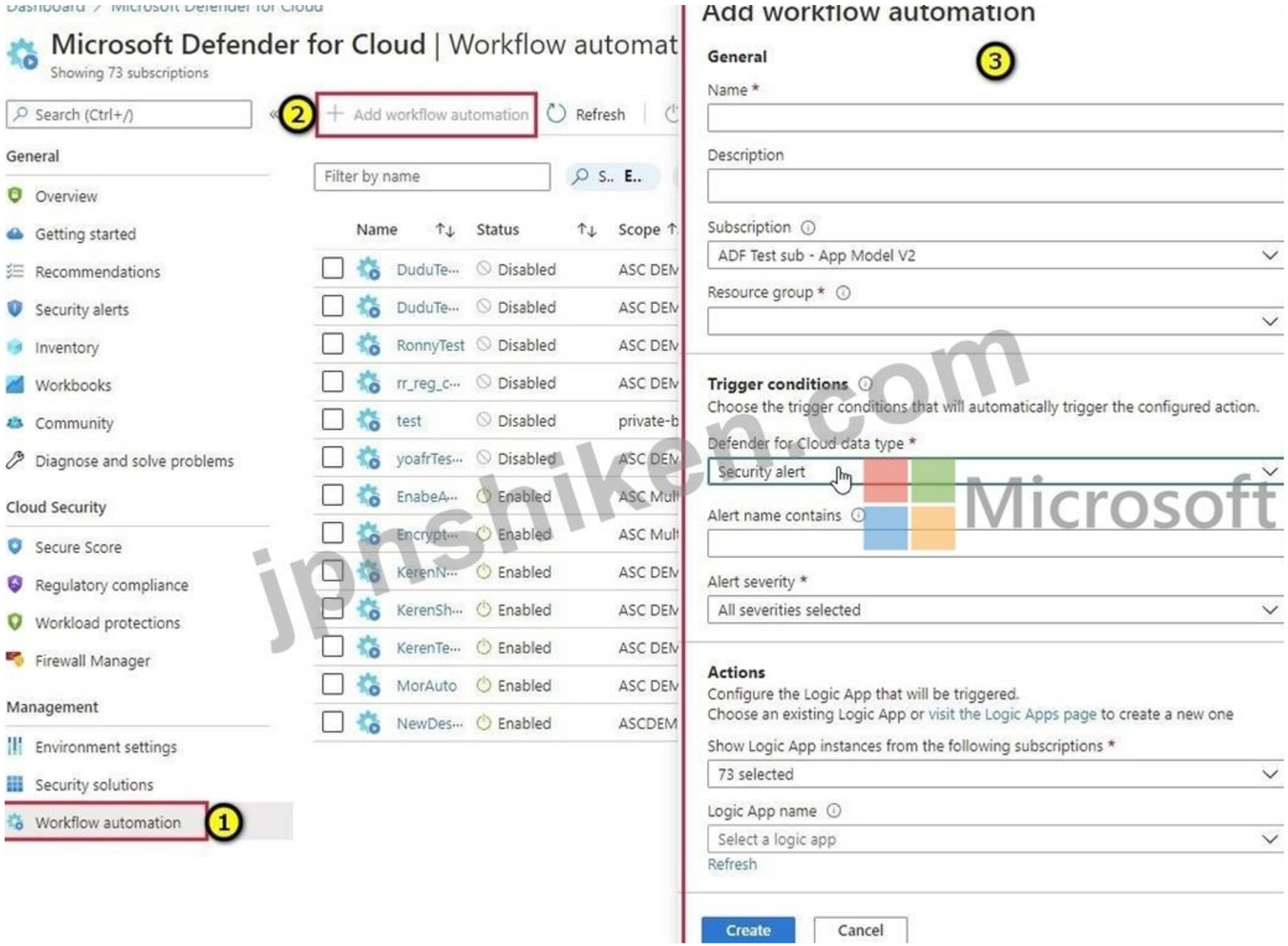
質問: **120**
ドラッグアンドドロップ問題
お客様はAzureサブスクリプションをお持ちです。このサブスクリプションには、Microsoft Defender for Cloudにオンボーディングされた10台の仮想マシンが含まれています。
Defender for Cloudが仮想マシン上でデジタル通貨マイニング行為を検出した際に、メール通知が届くようにする必要があります。このソリューションはテストメールを生成する機能を備えている必要があります。
どの3つの行動を順番に実行すべきでしょうか？回答するには、行動リストから適切な行動を回答欄に移動させ、正しい順序に並べ替えてください。



正解:



Explanation:
Step 1: From Logic App Designer, create a logic app.
Create a logic app and define when it should automatically run
1. From Defender for Cloud's sidebar, select Workflow automation.
2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

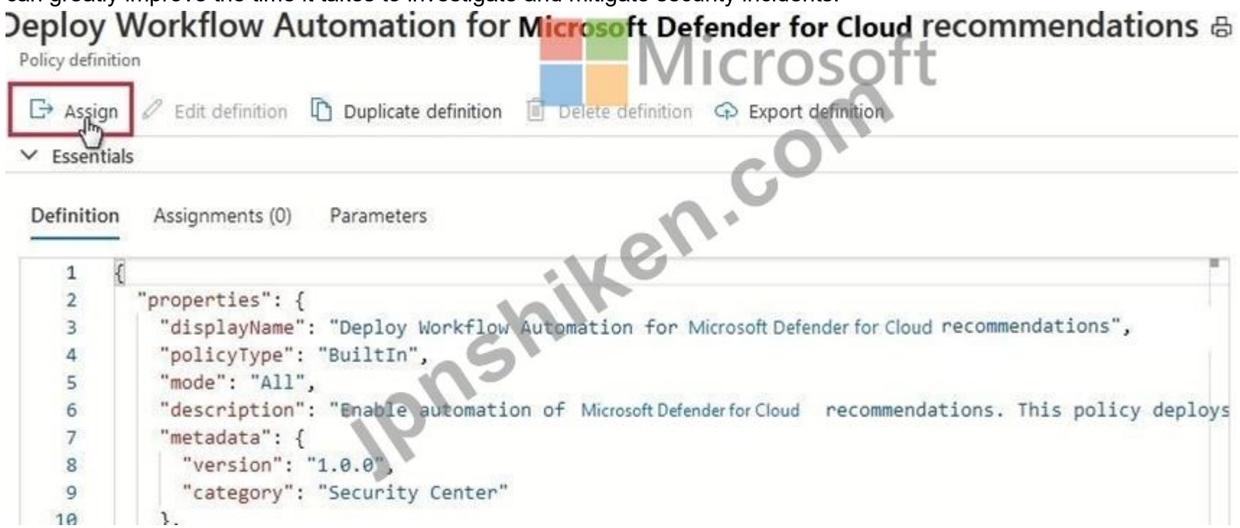
4. Etc.

Step 2: From Logic App Designer, run a trigger.

Manually trigger a Logic App

You can also run Logic Apps manually when viewing any security alert or recommendation.

Step 3: From Workflow automation in Defender for cloud, add a workflow automation. Configure workflow automation at scale using the supplied policies Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.



Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

質問: 121

Microsoft Cloud App Security を構成しています。

貴社は、米国にあるオフィスのIPアドレス範囲に基づいた、独自の脅威検出ポリシーを設定しています。

不可能な旅行や危険なIPアドレスからのログインに関するアラートを多数受信します。

アラートの99%が、自社オフィスからの正当なサインインであると判断します。

既知の場所からの正当なサインインに対するアラートを防止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. 自動データエンリッチメントを設定します。

B. IPアドレスを企業アドレス範囲カテゴリに追加します。

C. 不可能な旅行異常検出ポリシーの感度レベルを上げる。

D. IPアドレスを他のアドレス範囲カテゴリに追加し、タグを追加します。

E. IP アドレスを除外するアクティビティ ポリシーを作成します。

正解: **(正解を表示します)**

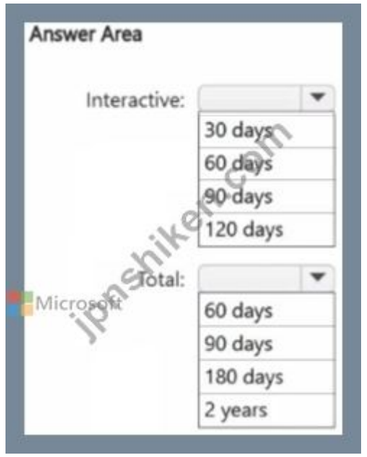
If you override the automatic detection of location for company IP address ranges, you can prevent the impossible travel alerts.

And you need to define your corporate address ranges so that they are not seen as risky.

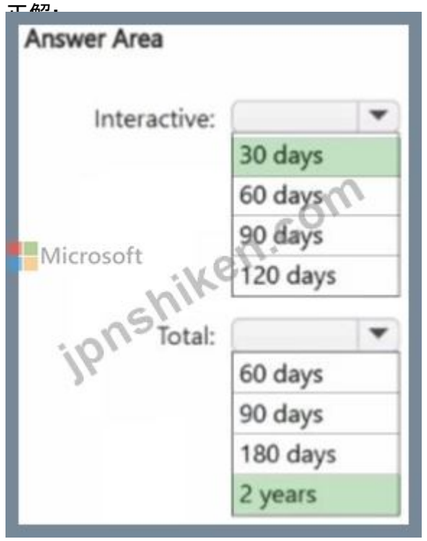
https://docs.microsoft.com/en-us/defender-cloud-apps/media/newipaddress-range.png

https://docs.microsoft.com/en-us/cloud-app-security/ip-tags

質問: **122**
ホットスポットに関する質問
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
Workspace1 の AzureActivity テーブルには、以下の保持期間が設定されています。
- インタラクティブ :180日間
合計 :180日
以下の要件を満たすように、保存期間を変更する必要があります。
テーブルへのデータ保存に伴うコストを最小限に抑える。
テーブルデータが利用可能な期間を最大限に延ばす。
各保持期間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:

Box 1: 30 days
The minimum value for the Interactive (Analytics) retention setting for the AzureActivity table in a Microsoft Sentinel workspace is four days, though the default is 90 days and a value between 30-730 days is the standard range for Analytics Logs.
Note: To minimize costs for the AzureActivity table in Microsoft Sentinel, you should adjust its data retention settings in the Log Analytics workspace. Navigate to Data retention under the Usage and estimated costs section of your workspace and decrease the Interactive retention period for that table to a duration that meets your security and compliance needs, while enabling Total retention (or long-term retention) to keep older data at a much-reduced cost for infrequent investigations.
Box 2: 2 years
3. Set Total Retention:
Ensure Total retention is enabled for the AzureActivity table.
Adjust the total retention period to store older data for longer, less frequent use, at a significantly lower cost than interactive retention. You can set this for up to 12 years, which can be crucial for audit or sporadic investigations.
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure

質問**: 123**
sub1という名前のAzureサブスクリプションを作成します。
sub1では、workspace1という名前のLog Analyticsワークスペースを作成します。
Microsoft Defender for Cloud を有効にし、ワークスペース 1 を使用するように Defender for Cloud を構成します。
workspace1にレポートを送信するAzure仮想マシンから、セキュリティイベントログを収集する必要があります。
あなたはどうすべきでしょうか？
A. Defender for Cloud から、Microsoft Defender for Servers のプラン設定を変更します。
B. サブ1でプロバイダーを登録します。
C. Defender for Cloud からワークフロー自動化を作成します。
D. workspace1 でワークブックを作成します。
正解**: (**正解を表示します**)**
https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan

質問**: 124**
事例研究4 - Litware Inc.
概要
アダタム ･コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境
オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。
ライセンス状況
Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。
クラウド環境
クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境

オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件

計画されている変更

Adatum社は以下の変更を実施する予定です。

- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。

Microsoft Defender for Cloud の要件

Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。

グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。

- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。

Microsoft Sentinelの要件

Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。

- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。

- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。
可能な限り、ASIMに組み込まれているパーサーを使用してください。
ビジネス要件
Adatumは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則に従うこと。
可能な限り管理業務を最小限に抑える。
rulequery1によって生成されたインシデントの処理が、Microsoft Sentinelの要件を満たしていることを確認する必要があります。
最初に何を作るべきでしょうか？
A. インシデント発生をトリガーとするプレイブック
B. アラートトリガー付きのプレイブック
C. エンティティトリガーを含むプレイブック
D. Azure Automationルール
正解: **A** (コメントを発表する)

質問: **125**
Microsoft Defender XDR を使用する Microsoft 365 サブスクリプションをお持ちです。
Microsoft Defender for Endpoint が、よく使用される実行可能ファイルに対してアラートを生成すると、アラート疲れが発生することがわかりました。アラートを調整する必要があります。
アラート チューニング ルールは、アラートに対してどの 2 つのアクションを実行できますか?
それぞれの正解は完全な解決策を提示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. 削除
B. 隠す
C. 解決する
D. merge
E. 割り当てる
正解: (正解を表示します)
Hide : This action allows you to hide alerts generated by the specified executable file, reducing the noise and alert fatigue. These hidden alerts will not appear in the incident queue but will still be logged for historical purposes.
Resolve : This action automatically resolves alerts generated by the specified executable file. The alerts are marked as resolved, indicating that no further action is required. This helps in managing alert fatigue by automatically handling known benign alerts.

質問: **126**
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。
あなたは事件を調査しています。
実行されたインシデントタスクを確認する必要があります。解決策には、ワークブックにインシデントを表示し、各インシデントのタスクを別のグリッドに表示するクエリを含める必要があります。
クエリではどのテーブルを対象とすべきですか？
A. セキュリティインシデント
B. セキュリティイベント
C. SentinelAudit
D. セキュリティアラート

正解: **A** (コメントを発表する)
The SecurityIncident table in Microsoft Sentinel contains information about incidents, including details such as incident ID, severity, status, and tasks.

質問: **127**
Microsoft Sentinelワークスペースには、以下のテーブルが含まれています。

Name	Table plan	Log data state
Table1	Basic	Interactive retention
Table2	Basic	Archive period
Table3	Analytics	Interactive retention
Table4	Analytics	Archive period

検索機能を使ってログデータを調査する必要があります。
どのテーブルを検索できますか？
A. 表3のみ
B. 表1と表3のみ
C. 表3と表4のみ
D. 表1、表3、表4のみ
E. 表1、表2、表3、表4
正解: **D** (コメントを発表する)
* Table1 - Yes, Table2 - No
Basic Plan: Data is interactive for 30 days at a lower cost, optimized for single-table queries (troubleshooting/incidents).
* Table3 - Yes, Table4 - Yes
Analytics Plan: Data is interactive for 4-730 days (default 30-90 days), ideal for real-time analytics, with full KQL support.
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/search-jobs

質問: **128**
あなたはMicrosoft Purviewを使用するMicrosoft 365サブスクリプションをお持ちです。
アカウント侵害の疑いがある状況下で、役員のアカウントがMicrosoft 365 Copilotの操作を実行する。
どのCopilot操作が実行されたかを特定する必要があります。解決策は、管理作業を最小限に抑えるものでなければなりません。
どのMicrosoft Purviewソリューションを使用すべきでしょうか？
A. 監査
B. eディスカバリー
C. データ損失防止(DLP)
D. データセキュリティ調査
正解: (正解を表示します)
To identify which Microsoft 365 Copilot interactions were performed by the compromised executive account with the minimum administrative effort, you should use Audit (Standard) (or simply Audit) within the Microsoft Purview portal.
Reference:
https://learn.microsoft.com/en-us/purview/audit-copilot

質問: **129**

貴社は、1万台以上のIoTデバイスからのアラートを管理するためにMicrosoft Sentinelを使用しています。
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. 組み込みクエリ
B. ライブ配信
C. ワークブック
D. ブックマーク
正解: **(**正解を表示します**)**
Correct:
* notebooks
Jupyter notebooks combine full programmability with a huge collection of libraries for machine learning, visualization, and data analysis. These attributes make Jupyter a compelling tool for security investigation and hunting.
* workbooks (best)
In Microsoft Sentinel, Workbooks are for interactive, visual dashboards (like Power BI) for monitoring and reporting, ideal for SOC analysts to see trends and metrics.
Incorrect:
* built-in queries
* livestream
* bookmarks
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks
https://learn.microsoft.com/en-gb/azure/sentinel/resources

質問: **130**
ドラッグアンドドロップ問題
お客様の環境に影響を与える新たな共通脆弱性識別子(CVE)の脆弱性についてお知らせします。
既知の脆弱性が存在する場合は、Microsoft Defender Security Center を使用して、影響を受けるシステムを担当するチームに修復を依頼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すか？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。

Actions

From Device Inventory, search for the CVE.

Open the Threat Protection report.

From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.

From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Create the remediation request.

Select **Security recommendations**.

Answer Area

正解:

Actions

- From Device Inventory, search for the CVE.
- Open the Threat Protection report.
- From Advanced hunting, search for `CveId` in the `DeviceTvmSoftwareInventoryVulnerabilitites` table.

Answer Area

- From Threat & Vulnerability Management, select **Weaknesses**, and search for the CVE.
- Select **Security recommendations**.
- Create the remediation request.

Explanation:
Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud. We've also renamed Azure Defender plans to Microsoft Defender plans. The answers in this are based on Azure Security Center.
Open Security.microsoft.com --> Enpoints --> Vulnerabilty Management --> Weakness Search/select CVE and click "Go to related security recommendations" Click on Security recommendation task i.e. "update putty to version x.x.x" Click on Request Remediation.
Reference:
https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

質問**: 131**
ホットスポットに関する質問
お客様のAzureサブスクリプションでは、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が有効になっています。
LA1という名前のAzureロジックアプリを作成します。
Azure Security Centerで検出されたセキュリティリスクを自動的に修復するために、LA1を使用する予定です。
セキュリティセンターでLA1をテストする必要があります。
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

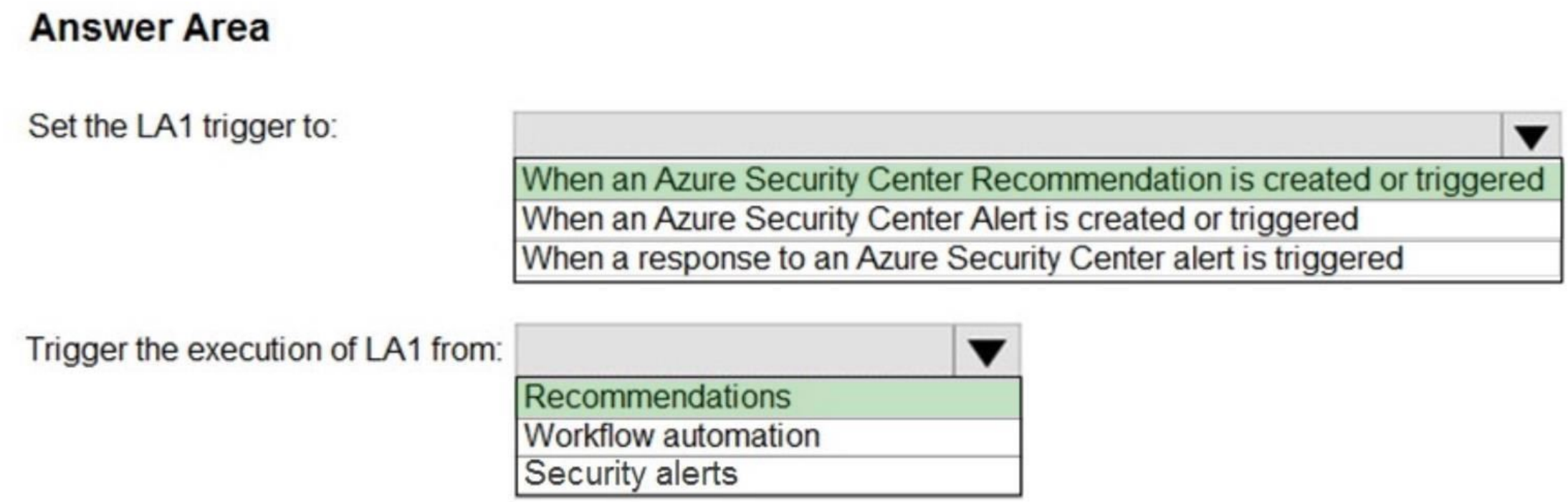
Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Workflow automation
- Security alerts

正解:

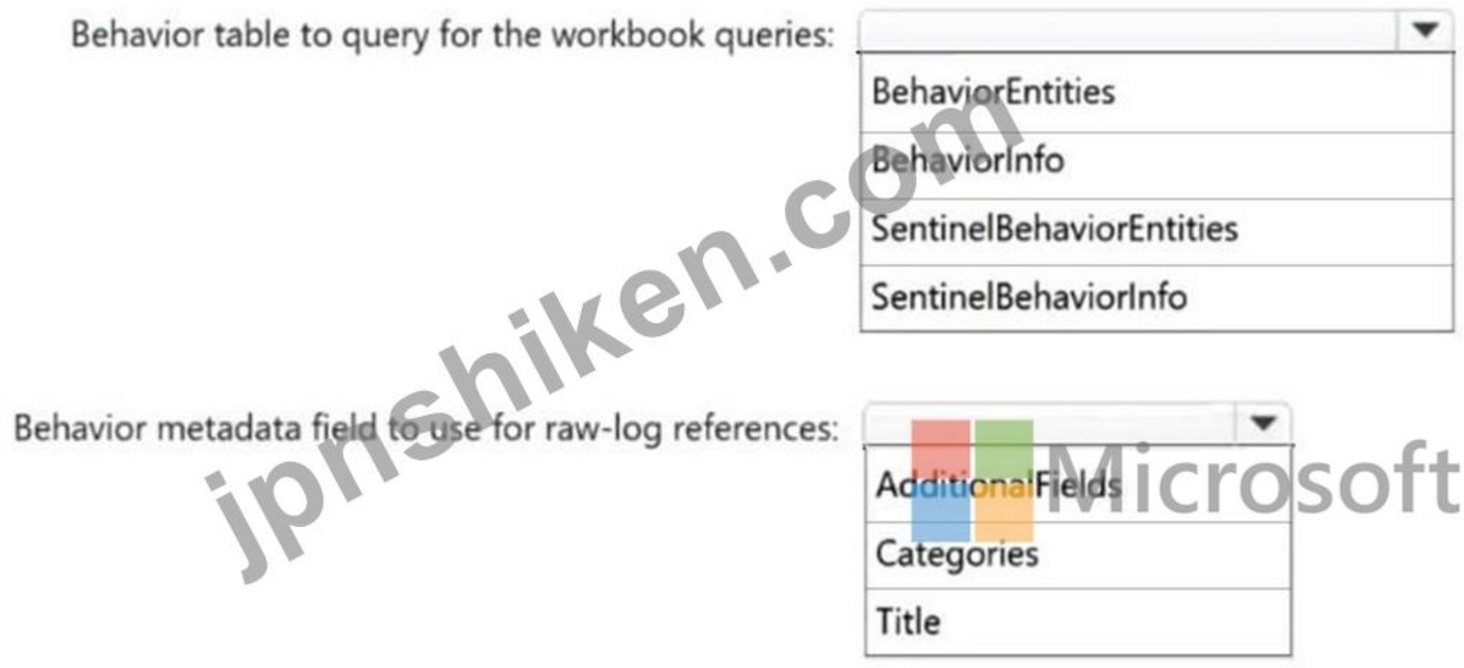


Explanation:
To manually run a Logic App, open an alert or a recommendation and click Trigger Logic App.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#manually-trigger-a-logic-app

質問: 132

ホットスポットに関する質問
Microsoft Defender ポータルに接続され、ユーザーおよびエンティティ動作分析 (UEBA) 動作レイヤーが有効になっている、Workspace1 という名前の Microsoft Sentinel ワークスペースがあります。
あなたはワークブックを作成しています。
以下の要件を満たすために、ワークスペースクエリを標準化する必要があります。
- ワークブックのクエリは、Microsoft Sentinel テーブルを使用する必要があります。
行動記録。
- アナリストはワークブック内の動作からドリルダウンして
証拠メタデータを使用して、貢献する生レコードを
行動記録。
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。

Answer Area



正解:

Answer Area

Behavior table to query for the workbook queries:

- BehaviorEntities
- BehaviorInfo
- SentinelBehaviorEntities
- **SentinelBehaviorInfo**

Behavior metadata field to use for raw-log references:

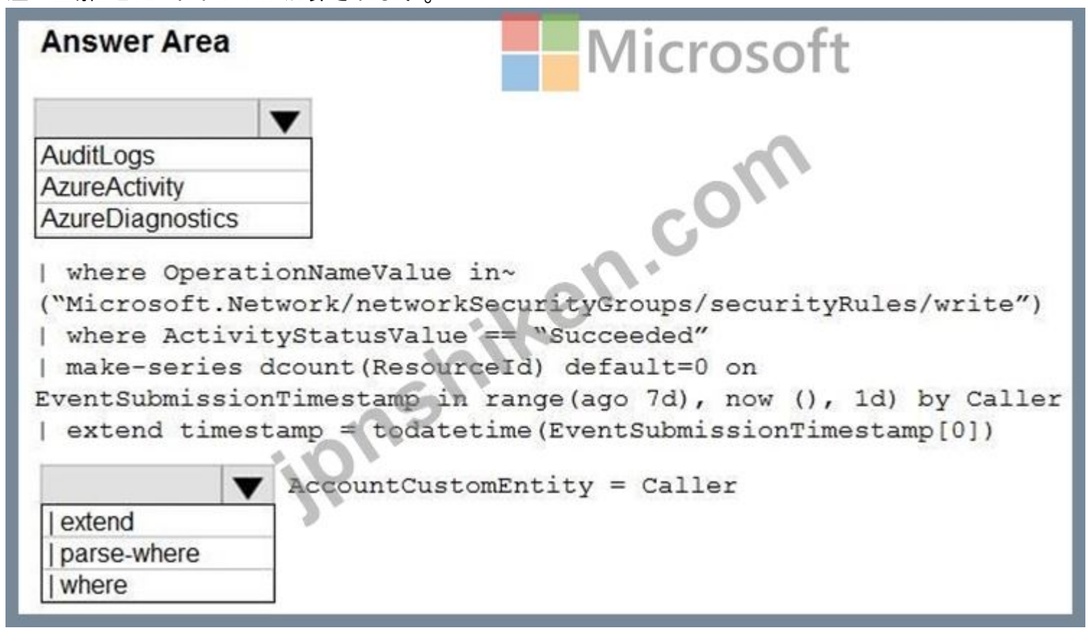
- **AdditionalFields**
- Categories
- Title

Explanation:
Box 1: SentinelBehaviorInfo
You should query the SentinelBehaviorInfo table for the primary behavior records.While Microsoft Sentinel uses tables like BehaviorInfo for its Advanced Hunting layer, Azure Monitor Workbooks require the workspace-native schema. Therefore, queries built into workbooks must rely on the SentinelBehaviorInfo table to fetch core behavioral data such as MITRE ATT&CK mappings, threat indicators, and descriptions.
Box 2: AdditionalFields
Use the AdditionalFields metadata field to reference and drill down to raw logs.In Microsoft Sentinel's UEBA behaviors layer, the AdditionalFields column in the BehaviorInfo table is specifically designed to store references and metadata to the underlying raw telemetry (such as specific record or event IDs). In contrast, Categories is used for MITRE ATT&CK and tactic mappings, and Title is reserved for the behavioral summary description.
Reference:
https://www.modernsecurity.nl/ueba-behaviors-layer-in-microsoft-sentinel/
https://learn.microsoft.com/en-us/azure/sentinel/entity-behaviors-layer

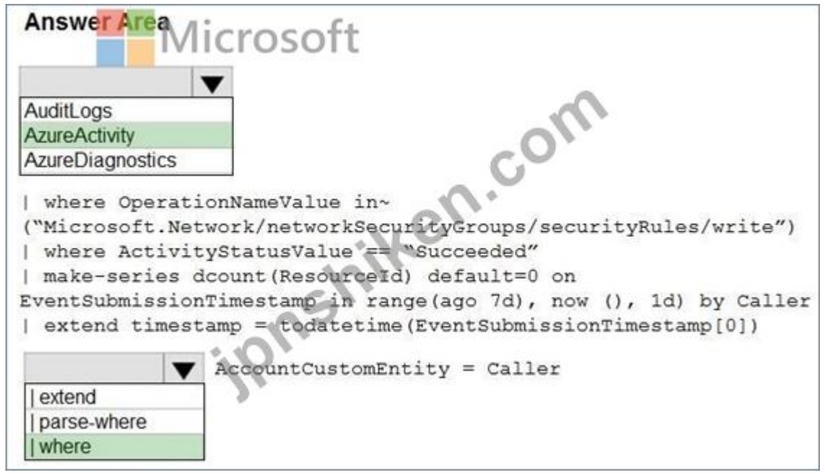
質問: 133
高度な機能設定で、サードパーティ製のウイルス対策ソフトが使用されている場合でもファイルをブロックするには、どの設定をオンにする必要がありますか？
A. EDRをブロックモードでオンにします。
B. 自動調査
C. ファイルを許可またはブロックします
D. 上記のすべて
正解: (正解を表示します)
Option A is correct. EDR with block mode can be used with third-party AV.
Option B is incorrect. The "Allow or block file" feature requires Defender AV.

Option C is incorrect. Automated investigations do not block files.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-antivirus-compatibility?view=o365-worldwide

質問**: 134**
ホットスポットに関する質問
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。
以下の要件を満たす、Kustoクエリ言語(KQL)を使用したハンティングクエリを作成する必要があります。
ネットワークのルールに対する異常な数の変更を特定します
同一のセキュリティ主体によって作成されたセキュリティグループ(NSG)。
- セキュリティプリンシパルをMicrosoftに自動的に関連付けます
監視役となる存在。
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:



質問: 135

事例研究2 - Litware Inc.

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。

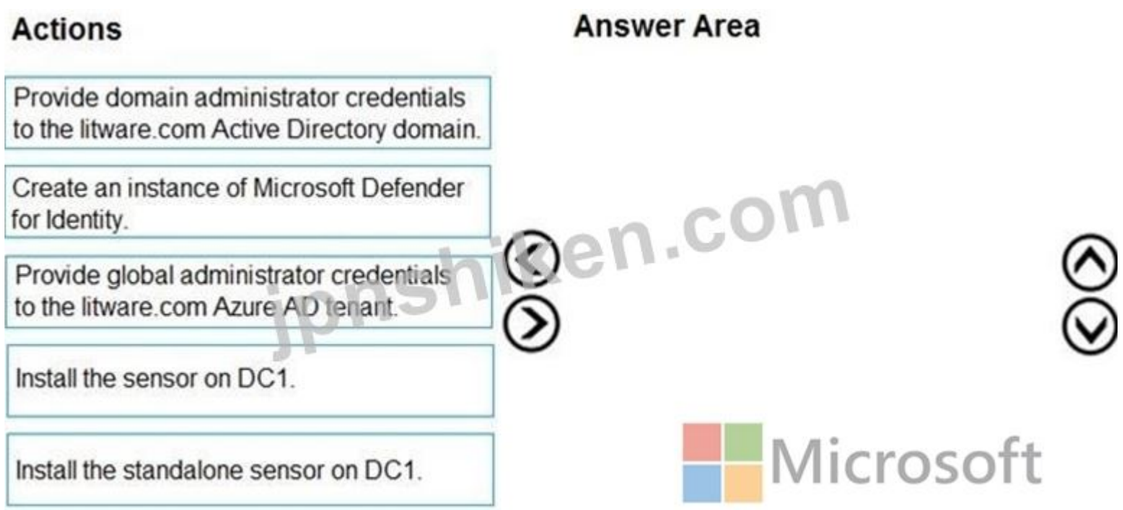
オンプレミス環境

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。

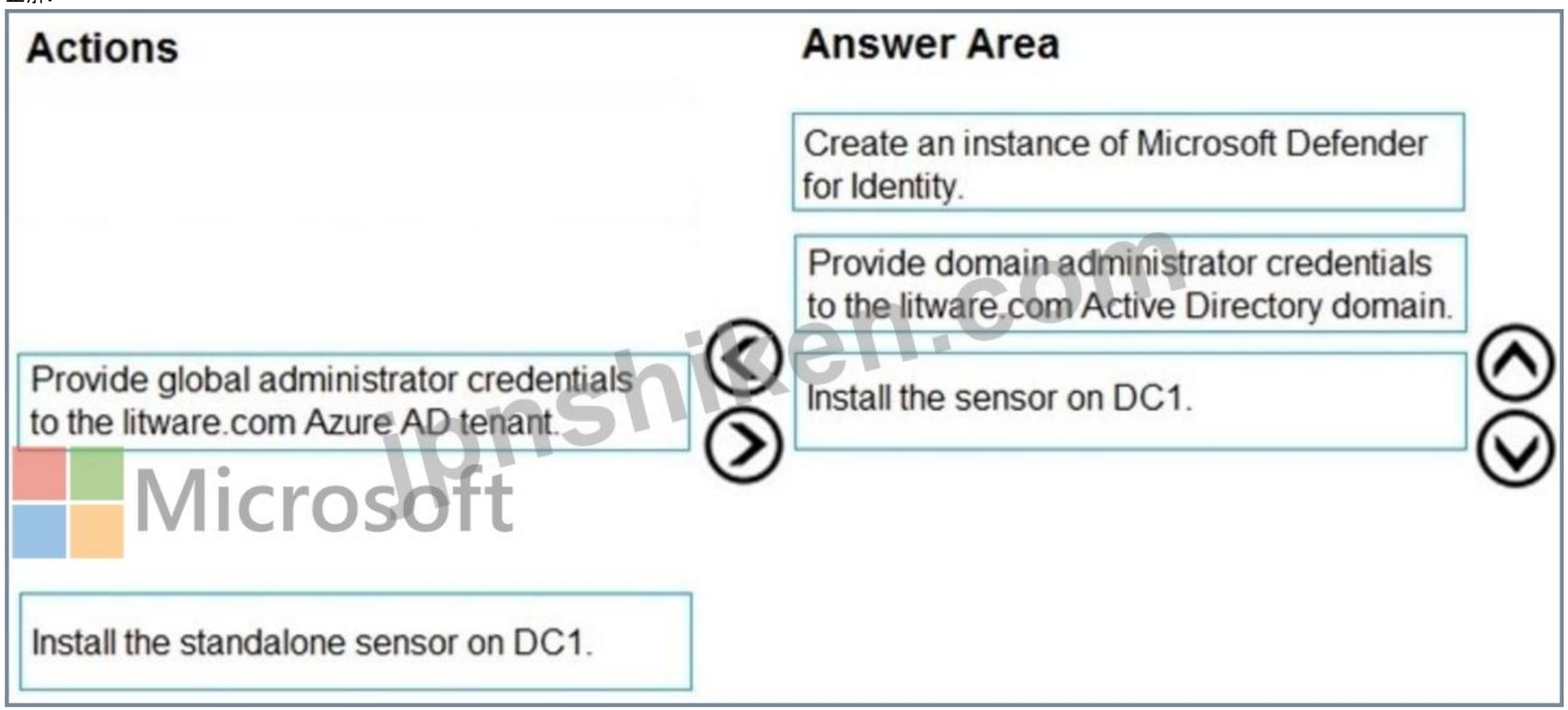
Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

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たアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。
ドラッグアンドドロップ問題
ビジネス要件を満たすようにDC1を設定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:



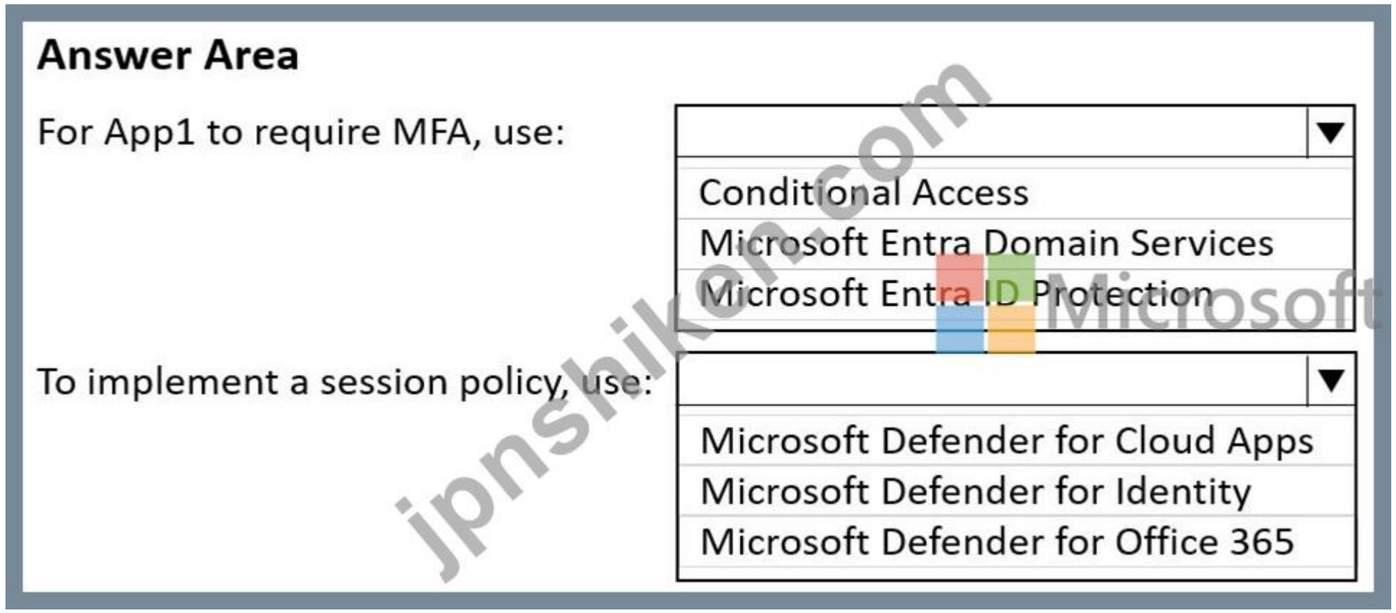
Explanation:

Step 1: Create the instance of Microsoft Defender for Identity.

Step 2: Provide domain administrator credentials to the litware.com Active Directory domain.

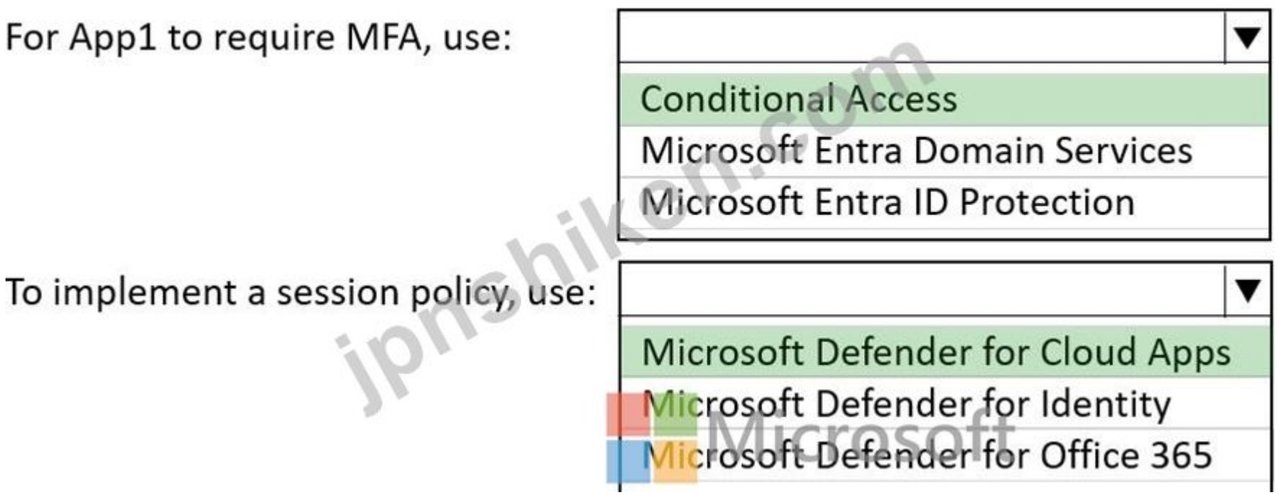
Step 3: Install the sensor on DC1.
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/install-step1
https://docs.microsoft.com/en-us/defender-for-identity/install-step4

質問: **136**
ホットスポットに関する質問
オンプレミスのデータセンターに、App1 という名前のカスタム Web アプリケーションがあります。App1 は Active Directory ドメイン サービス (AD DS) 認証を使用し、Microsoft Entra アプリケーション プロキシを使用してアクセスできます。
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
ユーザーが極秘文書をダウンロードしたというアラートを受け取ります。
ユーザーがApp1を使用して 「極秘」ラベルが付与されたドキュメントのダウンロードを開始する際に、多要素認証(MFA)を必須とすることで、アラートに関連するリスクを軽減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。



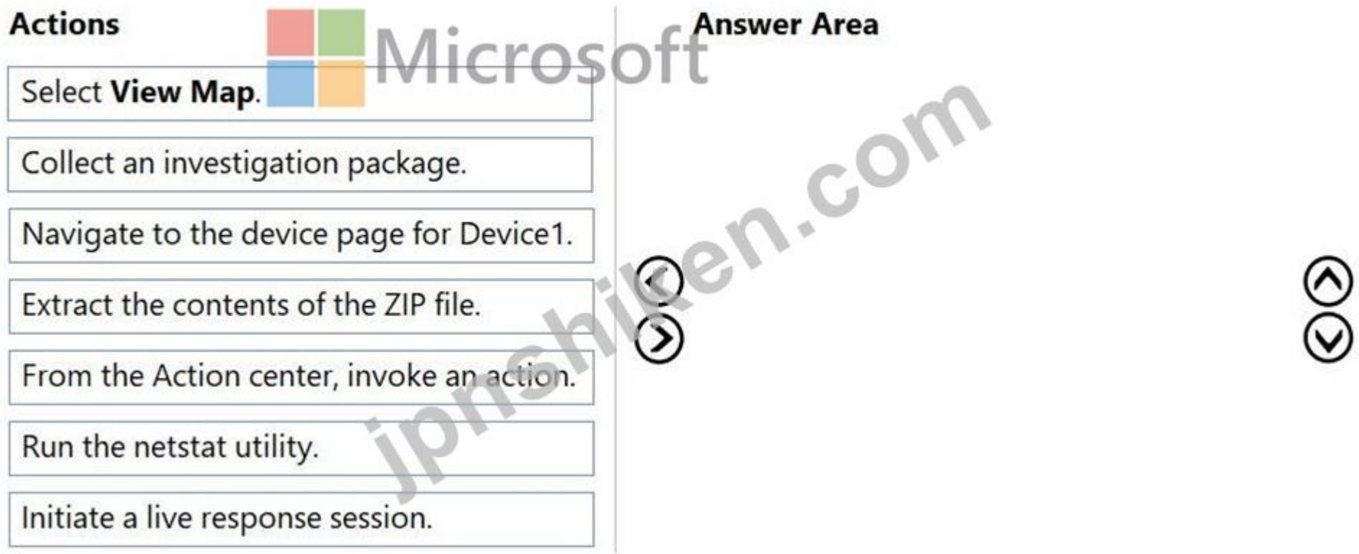
正解:

Answer Area

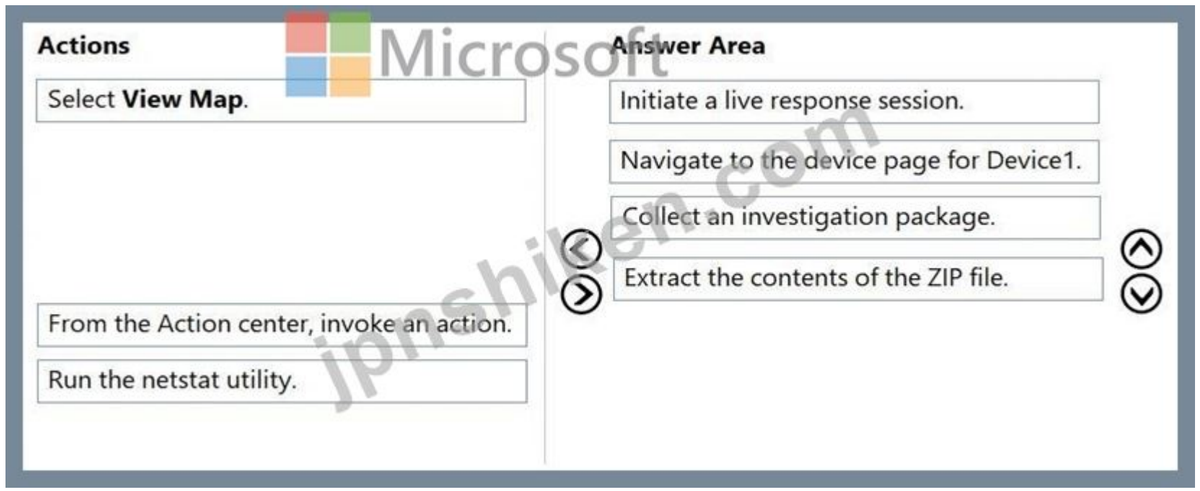


Explanation:
Box 1: Conditional Access
Conditional Access in Microsoft Entra (formerly Azure AD) is the correct mechanism for enforcing multi-factor authentication (MFA) based on specific conditions, such as accessing App1 when sensitive documents are involved.
Conditional Access policies can enforce MFA based on user risk, location, or the sensitivity of the data being accessed.
Box 2: Microsoft Defender for Cloud Apps
Microsoft Defender for Cloud Apps allows you to implement session control policies that monitor and control user sessions in real time. It can enforce policies such as blocking downloads of sensitive documents or enforcing additional authentication measures during specific activities within the session.

質問: **137**
ドラッグアンドドロップ問題
オンプレミス環境に設置された、Device1 という名前の Windows 11 Pro デバイスがあり、このデバイスは Microsoft Defender for Endpoint にオンボーディングされています。
あなたはMicrosoft 365のサブスクリプションをお持ちです。
Device1上で実行されているプロセスと、それらのプロセスが開いているネットワーク接続を特定する必要があります。解決策は、管理作業を最小限に抑えるものでなければなりません。
Microsoft Defender ポータルで、どの 4 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、正しい順序に並べ替えてください。



正解:



質問: **138**

お客様は、Microsoft Defender for Cloudが有効になっているAzureサブスクリプションをご利用中です。

Amazon Web Services (AWS) 上にホストされている、Windows Server 2022 を実行する Server1 という名前の仮想マシンがあります。

Defender for Cloudを使用して、Server1のログを収集し、脆弱性を解決する必要があります。

Server1に最初にインストールすべきものは何ですか？

A. Microsoft Monitoring Agent

B. Azure Monitorエージェント

C. Azure Arcエージェント

D. Azure Pipelines エージェント

正解: **C** (コメントを発表する)
Azure Arc for servers installed on your EC2 instances.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

質問: **139**
ホットスポットに関する質問
お客様は、Microsoft Defender XDR および Microsoft Defender for Endpoint を使用する Microsoft 365 サブスクリプションをご利用中です。このサブスクリプションには、次の表に示すデバイスが含まれています。

Name	Microsoft Defender status	Operating system
Device1	Onboarded	Windows
Device2	Onboarded	Windows
Device3	Onboarded	Windows
Device4	Network discovered	Other

あなたは以下の鑑識データを発見しました。
- Device1の起動時に、ポート5555を介してDevice2との接続が確立されます。
- Device2はポート5555を使用してDevice3に接続します。
- デバイス4はポート5555を使用してデバイス1に接続します。
あなたは以下の操作を実行します。
- Device1でライブレスポンスセッションを開始し、プロセスを実行します。
- Microsoft Defender ポータルのデバイスから Device1 を隔離し、
デバイス2。
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:

質問: **140**
貴社では、Microsoft Office VBAマクロを含む業務アプリケーションを使用しています。
Office VBAマクロから追加のペイロードがダウンロードされ、子プロセスとして実行されることを防ぐための保護機能を有効にする予定です。
影響を受ける可能性のあるOffice VBAマクロを特定する必要があります。
目的を達成するために実行できるコマンドはどれですか？正解はそれぞれ完全な解決策を示しています。
注：正解ごとに1ポイントが加算されます。

A.
```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

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

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

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

正解: **(正解を表示します)**
Must use Set-MpPreference with Enabled and then Add-MpPreference with Enabled. Audit does not block.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#powershell

質問: **141**
ホットスポットに関する質問
あなたは、User1とUser2という名前の2人のユーザーとMicrosoft Sentinelワークスペースを含むAzureサブスクリプションを持っています。
各ユーザーが以下の操作を実行できることを確認する必要があります。
- ユーザー1：既知の攻撃手法に対するインシデント検出のトリアージ
そして、インシデントのステータスを管理する。
- ユーザー2: 複雑なインシデントを調査し、指標を作成し、ハンティングを行う
ルールとワークブック。
解決策は最小権限の原則に従わなければならない。
各ユーザー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。

Answer Area

User1:

- Microsoft Sentinel Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder
- Owner
- Reader
- Security Reader

User2:

- Microsoft Sentinel Contributor
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder
- Owner
- Reader
- Security Reader

正解:

Answer Area

User1:
- Microsoft Sentinel Contributor
- Microsoft Sentinel Reader
- **Microsoft Sentinel Responder**
- Owner
- Reader
- Security Reader

User2:
- **Microsoft Sentinel Contributor**
- Microsoft Sentinel Reader
- Microsoft Sentinel Responder
- Owner
- Reader
- Security Reader

質問: **142**

ホットスポットに関する質問

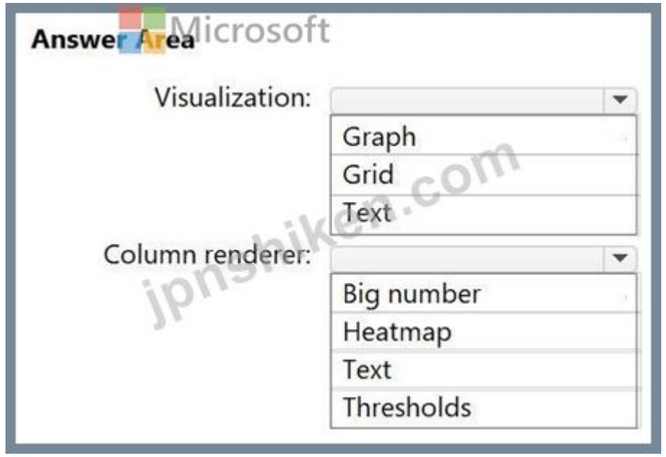
次の KQL クエリを含む Microsoft Sentinel ワークブックがあります。

```
let nonInteractive = AADNonInteractiveUserSignInLogs
| extend Status = parse_json(Status);
union SigninLogs,nonInteractive
| extend ErrorCode = tostring(Status.errorCode)
| extend FailureReason = tostring(Status.failureReason)
| summarize errCount = count() by ErrorCode, FailureReason, Category
```

返された値に基づいてerrCount列の色を変更するビジュアルを作成する必要があります。

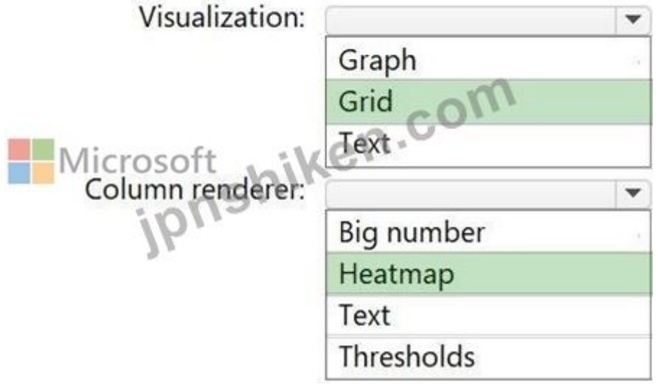
ビジュアルをどのように設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。



正解:

Answer Area



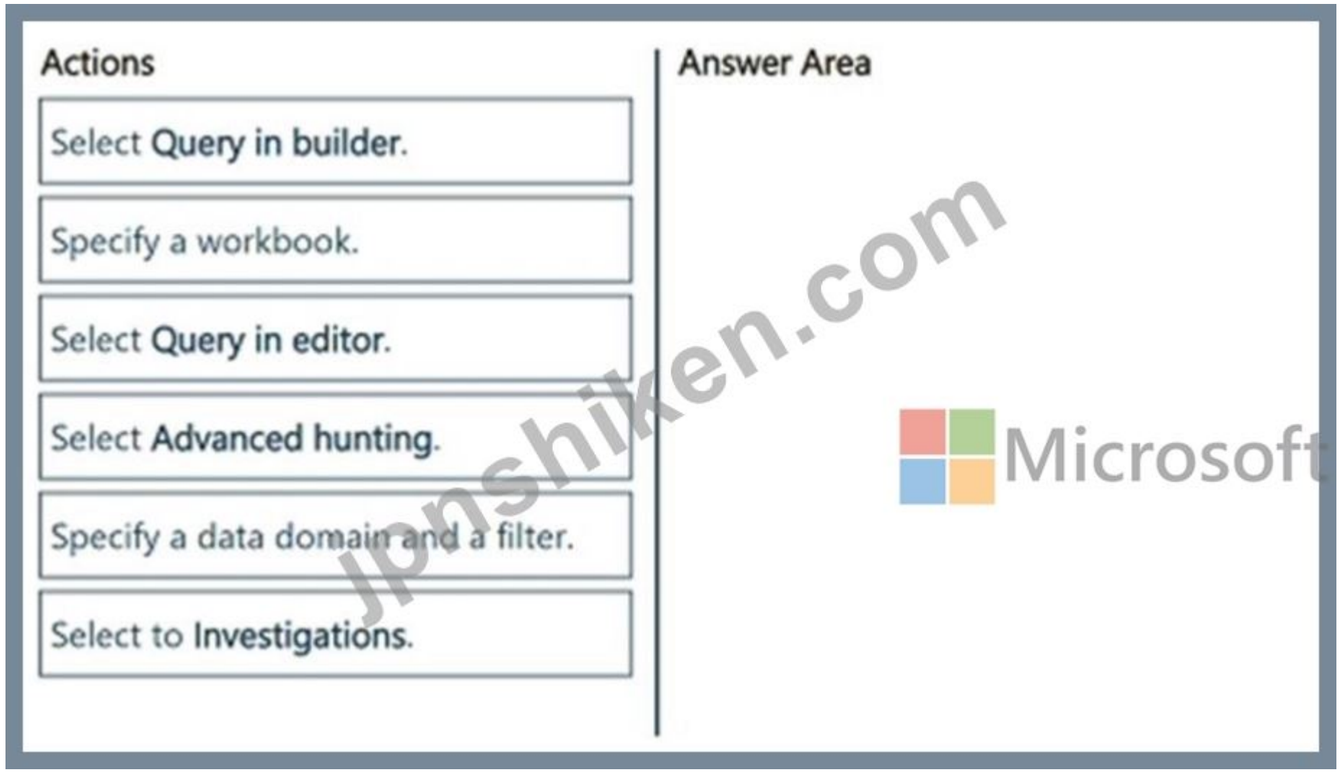
質問: **143**

ドラッグアンドドロップ問題

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で、その中にUser1という名前のユーザーが存在します。

セキュリティインシデントの影響を受けたデバイス上のエンドポイントの脆弱性を、ユーザー1が特定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、ユーザー1がKQLの知識を持っていることを要求してはなりません。

ユーザー1は、Microsoft Defenderポータルでどの3つの操作を順番に実行すべきでしょうか？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、正しい順序に並べ替えてください。



正解:

Actions	Answer Area
	Select **Advanced hunting**.
Specify a workbook.	Select **Query in builder**.
Select **Query in editor**.	Specify a data domain and a filter.
Select to **Investigations**.	

質問: 144

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

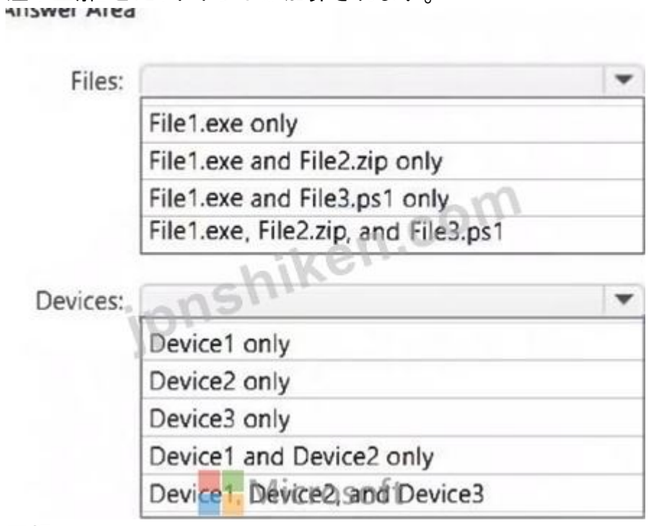
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。

Azure セキュリティ センターを使用します。

セキュリティ センターでセキュリティ警告を受け取ります。

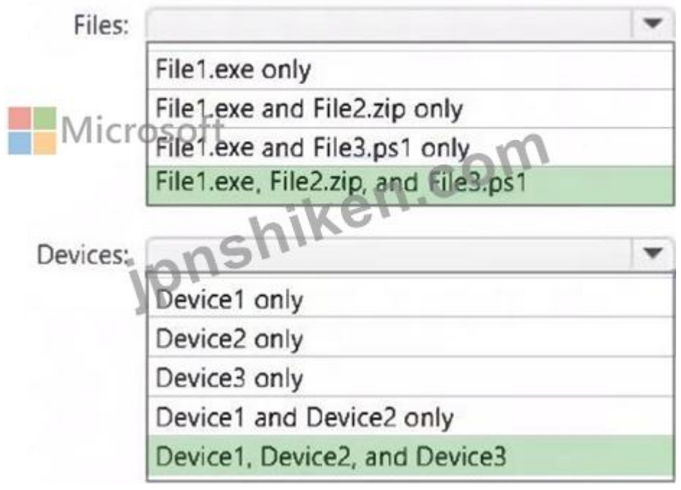
Security Center でアラートを解決するには、推奨事項を表示する必要があります。
解決策: [セキュリティ アラート] からアラートを選択し、[アクションの実行] を選択して、[脅威の軽減] セクションを展開します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **A** (コメントを発表する)
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

質問: **145**
ホットスポットに関する質問
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、以下のデバイスが含まれています。
- デバイス1 :Windows 11 Proを実行
- デバイス2 :Windows Serverを実行
- デバイス3 :Ubuntu Linuxを実行
File1.exe、File2.zip、File3.ps1という名前の3つの不審なファイルを特定しました。
詳細な分析を用いてファイルを調査する必要があります。
どのデバイスが詳細分析に対応しており、どのファイルを詳細分析に提出できますか？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



Explanation:

Box 1: File1.exe, File2.zip, and File3.ps1

Microsoft Defender for Endpoint supports deep analysis for executable (.exe), script (.ps1), and compressed (.zip) files, as well as other common file types like DLLs, Office documents, and PDFs. Deep file analysis works by submitting these files for detailed examination of their content, behavior, and context to detect advanced and zero-day threats.

Box 2: Device1, Device2, and Device3

Microsoft Defender for Endpoint supports deep analysis on Windows 11 Pro, Windows Server, and Ubuntu Linux. All listed operating systems are supported because they can run a Defender for Endpoint agent, enabling capabilities like Endpoint Detection and Response (EDR), vulnerability management, and automated investigation and remediation (AIR).

Reference:

https://learn.microsoft.com/en-us/defender-endpoint/supported-capabilities-by-platform

https://learn.microsoft.com/en-us/defender-endpoint/investigate-files

質問: **146**

お客様の環境には、Microsoft Defender for Endpoint にオンボーディングされたオンプレミスの Windows 11 Pro デバイスが 1,000 台あります。

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。

攻撃者がデバイス上で以下の操作を実行したことを確認しました。

レジストリベースのウイルス対策除外のファイルシステムパスを変更しました

ファイルシステムパスに悪意のあるファイルをダウンロードしました

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。

悪意のあるファイルを削除する必要があります。

どのコマンドを実行すればよいですか？

A. 収集

B. getfile

C. 元に戻す

D. 修復する

正解: **D** (コメントを発表する)

Advanced commands
The following commands are available for user roles that are granted the ability to run advanced live response commands.
* remediate
Remediates an entity on the device. The remediation action varies, depending on the entity type:
- File: delete
- Process: stop, delete image file
- Service: stop, delete image file
- Registry entry: delete
- Scheduled task: remove
- Startup folder item: delete file
Reference:
https://learn.microsoft.com/en-us/defender-endpoint/live-response

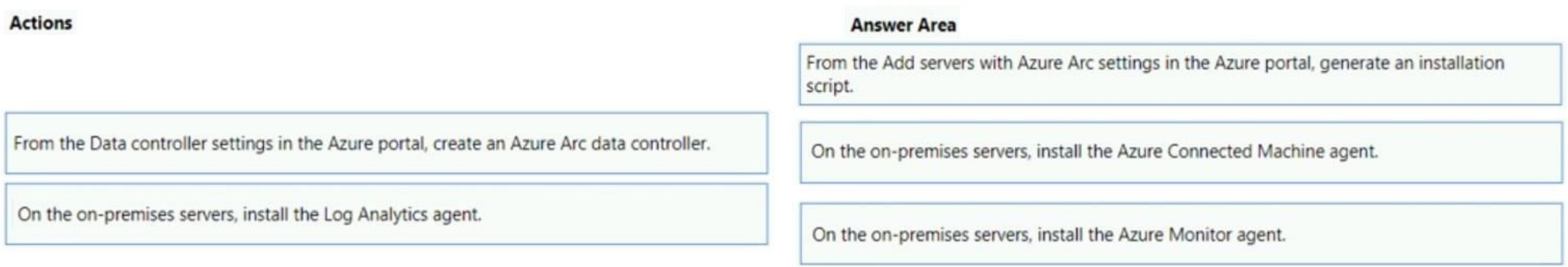
質問**: 147**
Microsoft 365 Defender ポータルを使用して、悪意のある可能性のあるドキュメントに関連する複数段階のインシデントの調査を行っています。詳細を確認した結果、悪意のある可能性のあるドキュメントに関連付けられたアラートが、環境内の別のインシデントにも関連していることが判明しました。ただし、このアラートは現在、その2番目のインシデントの一部としては表示されていません。
警報に関する調査は継続中であり、関連する2件の事件に関する調査も同様に継続中です。
アラートを適切に分類し、それが2番目のインシデントに関連付けられていることを確認する必要があります。
調査のこの部分を完了するために、「アラートの管理」ペインで実行すべき2つの操作は何ですか？
(2つ選択)
A. ステータスを「進行中」に設定する
B. ステータスを新規に設定する
C. 分類を真のアラートに設定する
D. コメント欄に、関連するインシデントのインシデントIDを入力してください。
E. 「アラートを別のインシデントにリンクする」オプションを選択します。
正解**: (**正解を表示します**)**
The correct action to classify the alert would be to set the status to In progress. While the alert may seem to be legitimate as it is linked to another incident, until a final determination is reached, you should set the status to In progress to ensure that others know it is being worked on. Once a determination is reached, you can then change it to Resolved and select the appropriate classification (True alert or False alert).
The correct action to correlate the alert to the other incident would be to select the Link alert to another incident option. While ideally, the alert would automatically be included in both incidents that are not always the case. If you notice an alert that is not linked to an incident that it is clearly connected to, using the Link alert to another incident option ensures they are tied together.
You should not set the classification to True alert. While a point can be made that it seems this malicious file involved in multiple incidents is likely to be a True alert, you cannot yet make that determination. It is also not the time to classify it as a false alert. The best practice while continuing an investigation would be not to change the classification at all, which means leaving it as the default Not set classification.
You should not enter the Incident ID of the related incident in the Comment section. While this might be helpful from an administrative perspective, it creates no link to the other incident.
You should not set the status to New. This is the default status of any alert. The question specifically seeks to ensure your peers know the alert is being investigated, so setting (or leaving) the status as New would make it impossible to differentiate from other uninvestigated alerts.
All of the actions mentioned in the options can be found in the Manage alert pane, which can be reached via the Alerts tab in the Incidents section of the Microsoft 365 Defender portal.
References:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide
質問**: 148**
Sub1という名前のAzureサブスクリプションがあり、そこではMicrosoft Defender for Cloudが使用されています。

PCI DSS 4.0イニシアチブをSub1に割り当て、Defender for Cloudの規制遵守ダッシュボードにそのイニシアチブが表示されるようにする必要があります。
環境設定のセキュリティポリシーを確認すると、業界標準や規制基準を追加するオプションが利用できないことがわかります。
まず最初に何をすべきでしょうか？
A. サブスクリプションに対してクラウドセキュリティ態勢管理(CSPM)プランを有効にします。
B. Azure Event Hubs の継続的エクスポート設定を構成します。
C. Microsoft Cloud Security Benchmark (MCSB) の割り当てを無効にします。
D. Log Analytics の継続的エクスポート設定を構成します。
正解: **(**正解を表示します**)**

質問: **149**
お客様は、Microsoft 365 Defender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。
Microsoft Defender からハンティングクエリを作成する予定です。
サブスクリプションの脅威状態を評価するために使用する、カスタム追跡クエリを作成する必要があります。
Microsoft 365 Defender ポータルからクエリを作成するには、どのページを使用すればよいですか？
A. 脅威分析
B. 上級狩猟
C. エクスプローラー
D. ポリシーとルール
正解: **B (**コメントを発表する**)**
"Use Advance mode if you're comfortable creating custom queries."
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-overview?view=o365-worldwide
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-modes?view=o365-worldwide#get-started-with-guided-hunting-mode

質問: **150**
ドラッグアンドドロップ問題
オンプレミスサーバーが50台あります。
お客様は、Microsoft Defender for Cloud を使用する Azure サブスクリプションをご利用中です。Defender for Cloud の展開では、Microsoft Defender for Servers と自動プロビジョニングが有効になっています。
オンプレミスサーバーをサポートするには、Defender for Cloudを構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。
脅威および脆弱性管理を提供する。
- データ収集ルールをサポートする。
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:
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection
https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm

質問: **151**
お客様は、500台の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されています。
お使いのMicrosoft Defender for Endpointの展開環境には、以下の設定が含まれています。
- 発見モード: 基本
- ライブレスポンス：無効
- ブロックモードでEDRを有効にする :オフ

- 改ざん防止機能: オフ
Microsoft Defender XDRで自動攻撃阻止機能を実装する必要があります。
あなたはどうすべきでしょうか？
A. 検出モードを標準検出に変更します。
B. ライブレスポンスをオンに設定します。
C. 改ざん防止機能をオンに設定します。
D. ブロックモードでEDRを有効にする設定をオンにします。
正解: **(**正解を表示します**)**
EDR in block mode should be enabled or in passive mode for it to function correctly with the full automated remediation capabilities of Microsoft Defender XDR. EDR in block mode provides a crucial layer of protection for Microsoft Defender Antivirus, and while it's most beneficial when MDE is running in passive mode, it is necessary for automatic attack disruption to work effectively.
Reference:
https://learn.microsoft.com/en-us/defender-xdr/configure-attack-disruption

質問: **152**
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。このワークスペースには、Microsoft Defender for Cloudデータコネクタが含まれています。
特定のイベントに対してアラートを作成する際に、どの詳細情報を含めるかをカスタマイズする必要があります。
あなたはどうすべきでしょうか？
A. ユーザーおよびエンティティ行動分析(UEBA)を有効にする。
B. データ収集ルール(DCR)を作成します。
C. コネクタのプロパティを変更します。
D. スケジュールされたクエリルールを作成します。
正解: **(**正解を表示します**)**
To customize which details will be included when an alert is created for a specific event in Microsoft Sentinel, you can modify the properties of the Microsoft Defender for Cloud data connector.
https://learn.microsoft.com/en-us/azure/sentinel/customize-alert-details

質問: **153**
ホットスポットに関する質問
contoso.com という名前の Microsoft 365 サブスクリプションがあり、その中に Device1 という名前の Windows 11 デバイスが含まれています。Device1 は Microsoft Defender for Endpoint に登録されています。
あなたは以下の操作を実行します。
- Defender for Endpoint から、以下に示すデバイス グループを作成します。
以下の表をご覧ください。

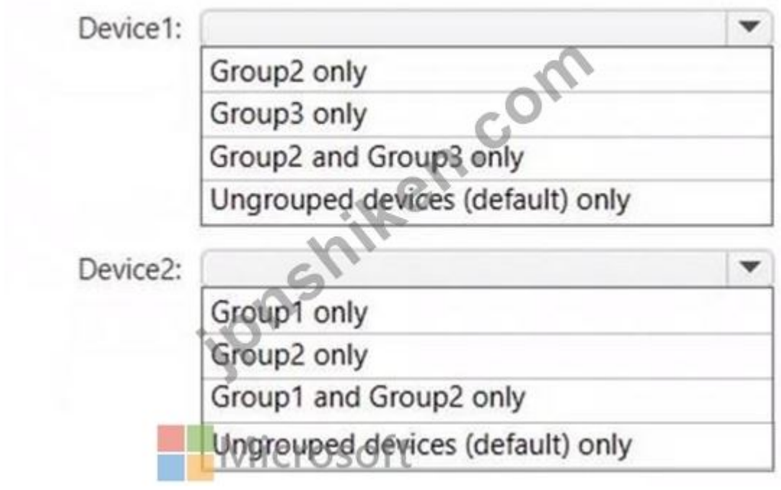
Rank	Name	Matching rule
1	Group1	OS In Android
2	Group2	Name Starts with Device
3	Group3	Name Starts with Device AND Domain Equals contoso.com

- Device2という名前のAndroidデバイスをDefender for Endpointにオンボーディングします。

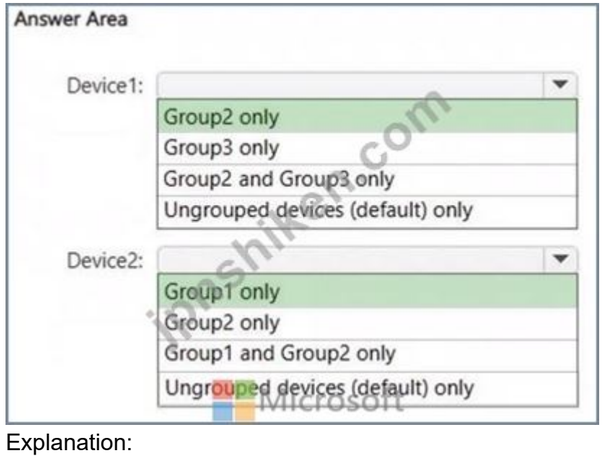
各デバイスはどのデバイスグループに追加されますか？回答するには、回答欄で適切なオプションを選択してください。

注：正解ごとに1ポイントが加算されます。

Answer Area



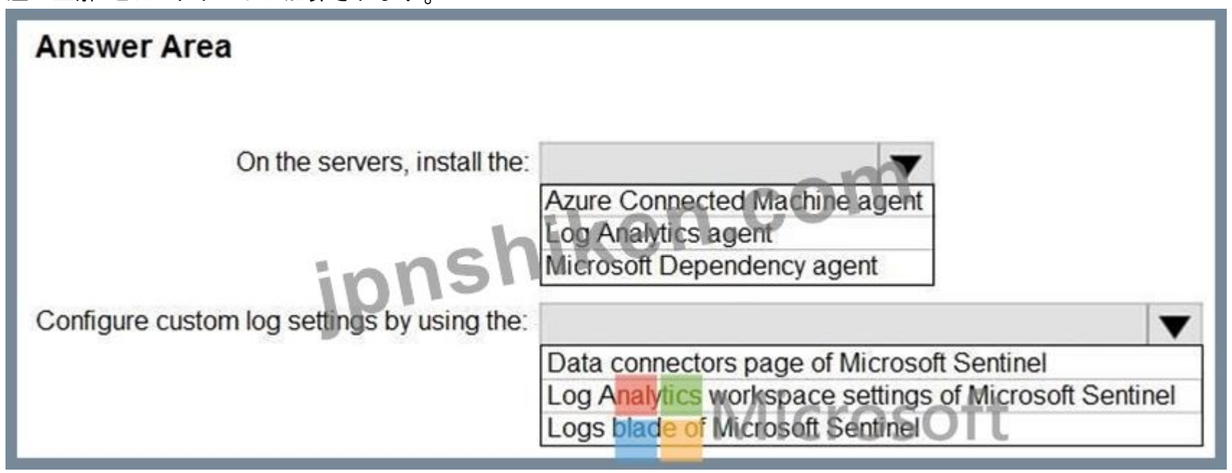
正解:



Explanation:

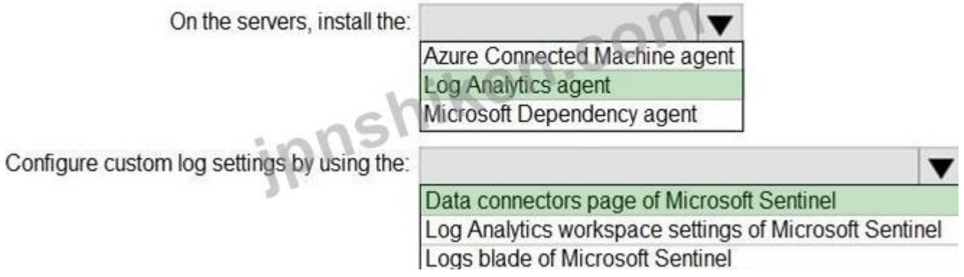
Box 1: Group2 only.
Device1 is a Windows 11.
The Rank 2 matching rule is matching, and Device1 is added to Group2.
Box 2: Group1 only.
Device2 is using Android
The Rank 1 matching rule is matching, and Device2 is added to Group1.
Note: Microsoft Defender applies rules and policies based on a priority order, where a lower numerical value indicates a higher priority; policies are processed in order, and the first matching rule determines the outcome for a recipient, stopping further processing for that item. Predefined preset security policies and custom policies are applied before a default policy, but preset policies must be enabled to take effect.
Reference:
https://learn.microsoft.com/en-us/defender-office-365/how-policies-and-protections-are-combined

質問**: 154**
ホットスポットに関する質問
お客様のオンプレミスネットワークには、Windows Serverを実行するサーバーが100台あります。
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションをお持ちです。
オンプレミスサーバーからカスタムログをMicrosoft Sentinelにアップロード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:

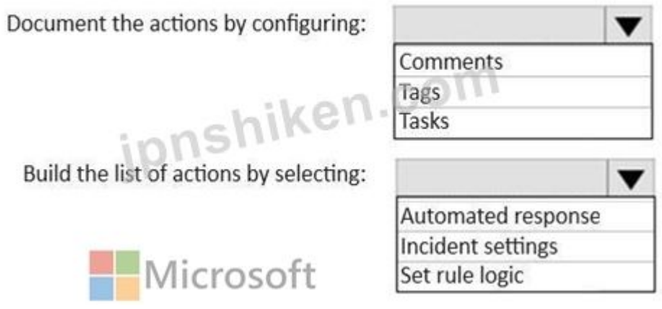
Answer Area



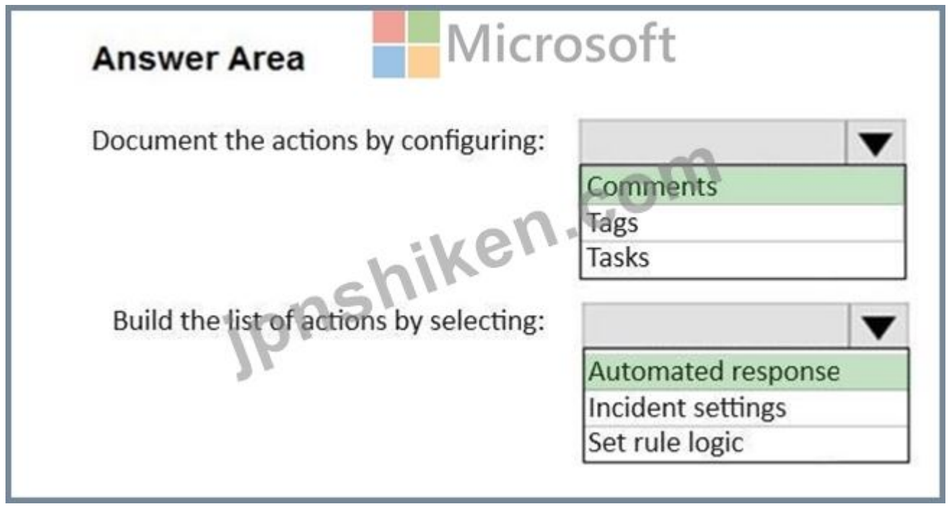
Explanation:
https://learn.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG

質問: **155**
ホットスポットに関する質問
お客様は、WS1 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。
WS1のインシデントには、実行しなければならないアクションのリストが含まれていることを確認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。
- それぞれのインシデントの種類に応じて、個別の対応策リストを作成できることを確認してください。
・管理業務の手間を最小限に抑える。
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:



質問: **156**
VM1 という名前の仮想マシンを含み、Azure Defender を使用する Azure サブスクリプションがあります。Azure Defender では自動プロビジョニングが有効になっています。
VM1 上の PowerShell の不審な使用に対する誤検知アラートを抑制するカスタム アラート抑制ルールを作成する必要があります。
まず何をすべきでしょうか?
A. Azure Security Center から、ワークフロー自動化を追加します。
B. VM1 で、Get-MPThreatCatalog コマンドレットを実行します。
C. VM1 で PowerShell アラートをトリガーします。
D. Azure Security Center から、アラートを Log Analytics ワークスペースにエクスポートします。
正解: **(**正解を表示します**)**
For a rule to suppress an alert on a specific subscription, that alert type has to have been triggered at least once before the rule is created.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule

質問: **157**
Microsoft Sentinel ワークスペースがあります。
アカウントへのサインイン試行に失敗すると、複数のアラートを受け取ります。
あなたは、アラートが誤検知であることを特定しました。
アカウントに対して追加のサインイン失敗アラートが生成されないようにする必要があります。ソリューションは次の要件を満たしている必要があります。
* 他のアカウントに対して失敗したサインインのアラートが生成されるようにします。
* 管理労力を最小限に抑える
何をすべきでしょうか?
A. 自動化ルールを作成します。
B. ウォッチリストを作成します。
C. 分析ルールを変更します。
D. アクティビティ テンプレートをエンティティの動作に追加します。
正解: **A (**コメントを発表する**)**

Two methods for avoiding false positives:
Automation rules create exceptions without modifying analytics rules.
Scheduled analytics rules modifications permit more detailed and permanent exceptions.
https://learn.microsoft.com/en-us/azure/sentinel/false-positives

質問: **158**
事例研究4 - Litware Inc.
概要
アダタム -コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境
オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。
ライセンス状況
Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。
クラウド環境
クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境
オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

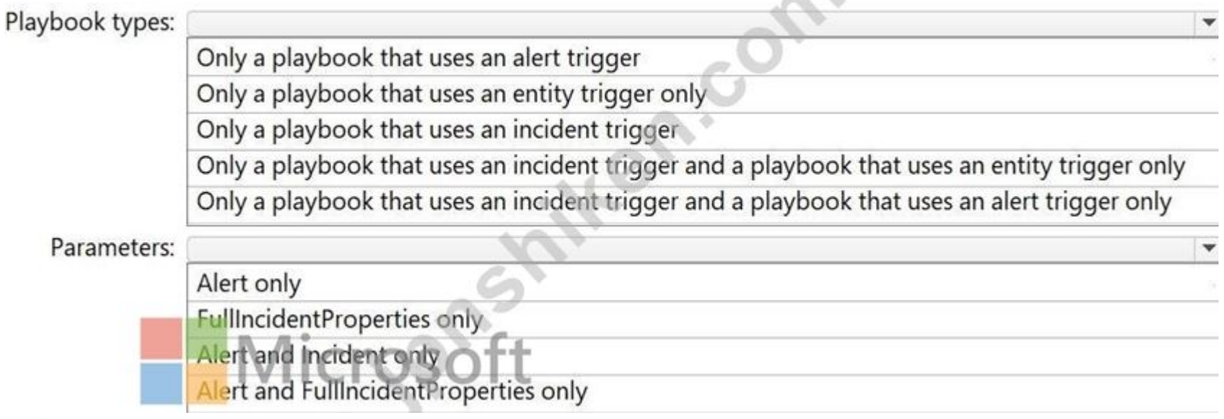
要件
計画されている変更
Adatum社は以下の変更を実施する予定です。
- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

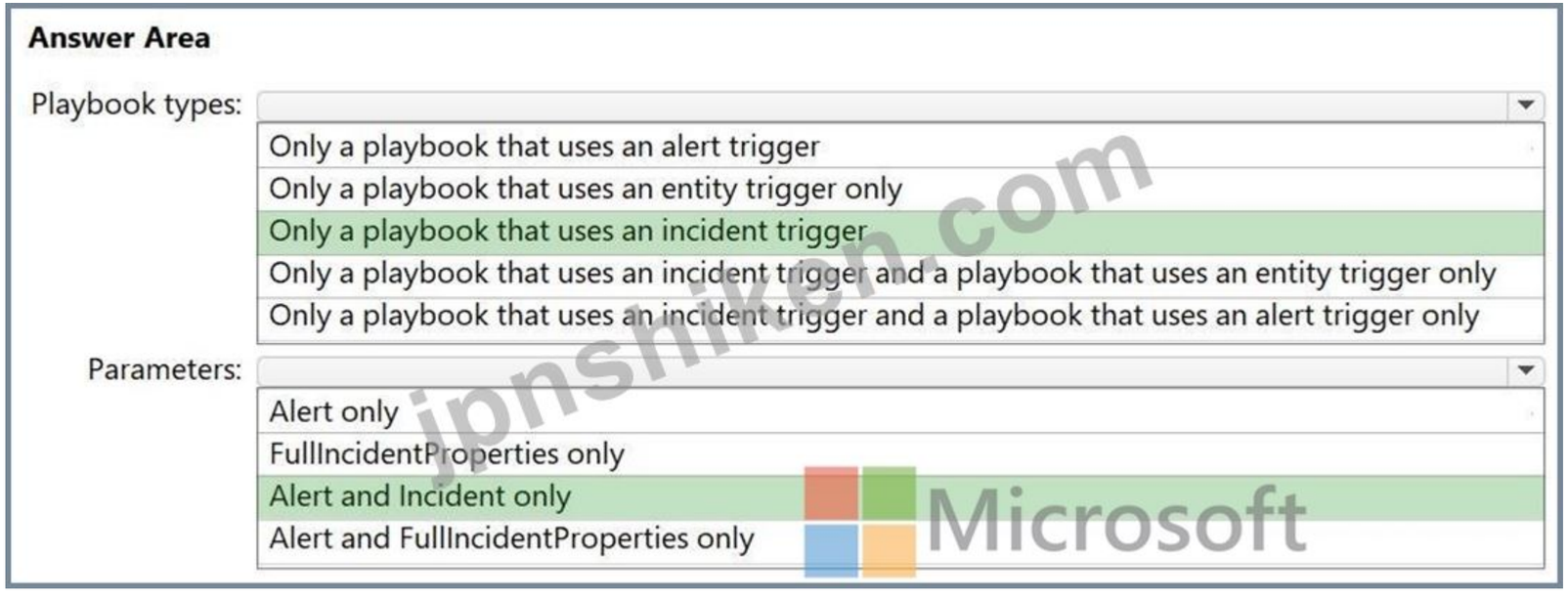
- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。
Microsoft Defender for Cloud の要件
Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。
グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。
- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。
Microsoft Sentinelの要件
Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。
- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。
可能な限り、ASIMに組み込まれているパーサーを使用してください。
ビジネス要件
Adatumは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則に従うこと。
可能な限り管理業務を最小限に抑える。
Group1のメンバーがMicrosoft Sentinelの要件を満たしていることを確認する必要があります。
グループ1にはどの役割を割り当てるべきですか？
A. Microsoft Sentinel Playbook Operator
B. Logic App の貢献者
C. 自動化オペレーター
D. Microsoft Sentinel Automation 貢献者
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/azure/sentinel/roles
質問: **159**
あなたは、127 件を超えるアラートを含む Azure Sentinel のインシデントを調査しています。
このインシデントで、さらなる調査が必要な 8 つのアラートを発見しました。
アラートを別の Azure Sentinel 管理者にエスカレーションする必要があります。
管理者にアラートを送信するにはどうすればよいですか?
A. Microsoft インシデント作成ルールを作成する
B. インシデントの URL を共有します
C. スケジュールされたクエリ ルールを作成します。
D. インシデントを割り当てます

正解: **D** (コメントを発表する)
Incidents can be assigned to a specific user or to a group. For each incident you can assign an owner, by setting the Owner field. All incidents start as unassigned. You can also add comments so that other analysts will be able to understand what you investigated and what your concerns are around the incident.
https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

質問: **160**
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。
以下の要件を満たすプレイブックを作成する必要があります。
自動化ルールを使用して、エンティティに対するアクションをトリガーします。
- エンティティを呼び出す - ホストを取得するアクション。
どのタイプのプレイブックを使用すべきか、またどのパラメータを指定すべきか？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。
Answer Area



正解:

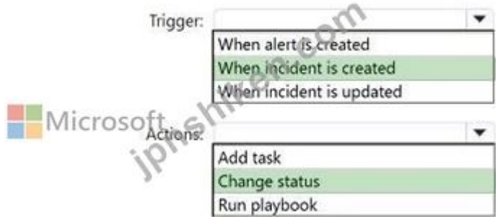


質問: 161
ホットスポットに関する質問
Microsoft Sentinelワークスペースをお持ちです。
Microsoft Defenderコネクタによって生成されたインシデントを一時的に抑制するように、Fusion Analyticsルールを構成する必要があります。このソリューションは、以下の要件を満たす必要があります。
- 多段階攻撃の検出能力への影響を最小限に抑える。
- 管理業務の手間を最小限に抑える。

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:

Answer Area



質問: **162**
Azure Active Directory (Azure AD) ユーザーをブロックするために使用される既存の Azure ロジック アプリがあります。ロジック アプリは手動でトリガーされます。
Azure Sentinel をデプロイします。
既存のロジック アプリを Azure Sentinel のプレイブックとして使用する必要があります。まず何をすべきでしょうか?
A. 新しいスケジュールされたクエリ 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 Threat Intelligence コネクタを構成します。
D. ロジック アプリでトリガーを変更します。
正解: **D (**コメントを発表する**)**
You must modify existing Logic App and choose Azure Sentinel actions either the following ones:
- When a response to an Azure Sentinel Alert is triggered
- When Azure Sentinel incident creation rule was triggered
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: **163**
ホットスポットに関する質問
Workspace1 という名前の Log Analytics 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。
AzureアクティビティログとMicrosoft Entra IDログをWorkspace1に転送するように構成します。
リスクの高いユーザーによって照会または変更されたAzureリソース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。

正解:

質問: **164**

サインインログに対して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。

対話型サインインの失敗を確実に検出する必要があります。また、管理作業を最小限に抑えるソリューションが求められます。

何を使うべきでしょうか？

A. 狩猟に関する質問

B. UEBAアクティビティテンプレート

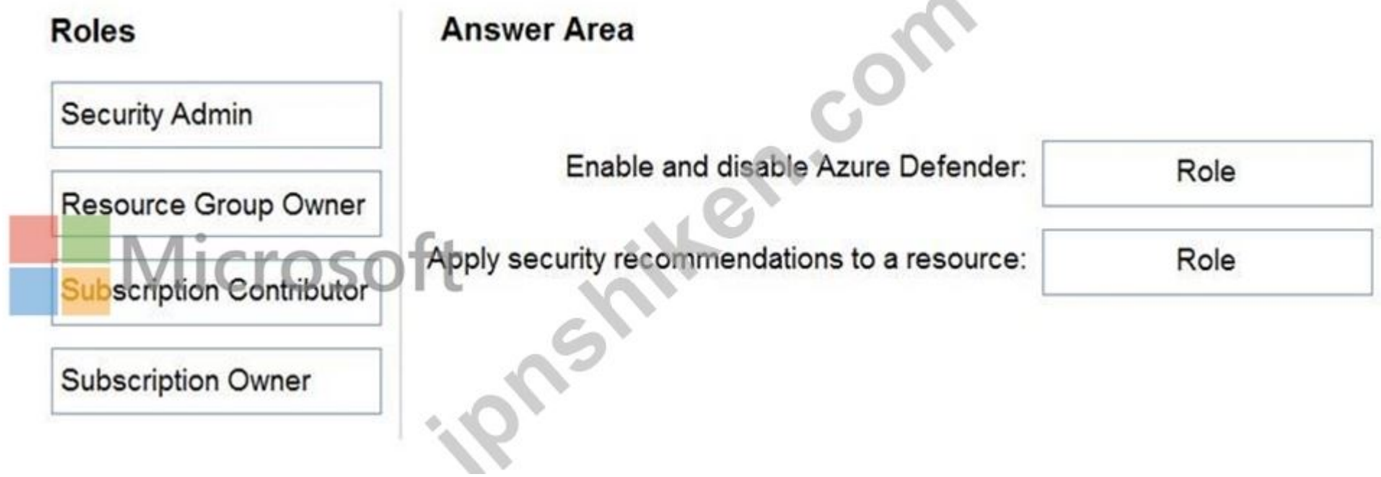
C. スケジュールされたアラートクエリ

D. アクティビティログデータコネクタ

正解: **(**正解を表示します**)**

質問: **165**

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:

Roles

Subscription Contributor

Subscription Owner

Answer Area

Enable and disable Azure Defender: Security Admin

Apply security recommendations to a resource: Resource Group Owner

Explanation:
Box 1: Security Admin
Box 2: Resource Group Owner
This has lower privilege than subscription contributor and can still apply security recommendations.
Reference:
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**: 166**
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 :ExcelからFile1.csvの既存の列にフィルターを適用してJSONプロパティの数を減らし、その後Get 8t Transform Data操作を実行してAuditData列を解析します。
これは要件を満たしていますか？
A. はい

B. いいえ
正解: (正解を表示します)
No, this solution will not ensure that Excel generates columns for specific JSON properties in the AuditData column. Applying filters in Excel will only help reduce data quantity but won't address the issue of correctly parsing the JSON data in the AuditData column into separate columns for each JSON property.

質問: **167**
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。
SecurityEvent 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。
- イベントの発生件数を日ごとに時系列グラフで表示する。
ワークブック1には何を追加すべきですか？
A. 質問
B. 指標
C. グループ
D. リンクまたはタブ
正解: (正解を表示します)
A query allows you to retrieve specific data from the SecurityEvent table.
You can write a query that filters events based on the past week's timestamp and aggregates the count of events by day.
The timechart visualization will display this aggregated data over time, showing the event count trends.

質問: **168**
ドラッグアンドドロップ問題
Azure Sentinel を使用して脅威ハンティングを行っています。ドメインコントローラー上の特定のイベントを識別するためのクエリを作成しました。
複数のドメインコントローラーがあり、それぞれのクエリを個別に管理する必要があるため、類似したクエリを複数作成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ものでなければなりません。
クエリを複製するには、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、可能な操作のリストから適切な操作を回答欄に移動し、正しい順序に並べ替えてください。

Possible actions

- On the Create custom query page, make your edits then click the Create button.
- On the Hunting page of Azure Sentinel, select New query.
- Choose Clone query by clicking the ellipsis icon at the end of the row.
- On the Hunting page of Azure Sentinel, find the query you wish to clone.
- Select the ellipsis in the line of the query you want to modify, and select Edit query.

Actions in order

正解:

Possible actions

- On the Hunting page of Azure Sentinel, select New query.
- Select the ellipsis in the line of the query you want to modify, and select Edit query.

Actions in order

- On the Hunting page of Azure Sentinel, find the query you wish to clone.
- Choose Clone query by clicking the ellipsis icon at the end of the row.
- On the Create custom query page, make your edits then click the Create button.

Explanation:
You should perform the following tasks in order:
On the Hunting page of Azure Sentinel, find the query you wish to clone.
Choose Clone query by clicking the ellipsis icon at the end of the row.
On the Create custom query page, make your edits then click the Create button.
First, you should find the query you wish to clone. You will do this by navigating to the Hunting page within Azure Sentinel and then looking through the list of queries. This will allow you to ensure the right initial query is cloned in the next step.
Next, you should choose the Clone query option. This is accessible via the ellipsis at the end of the row for the query you found in step one. This will make a copy of the query you identified in the first step and will take you to the page where you can make changes to that copy.
Finally, you should make your edits then click the Create button. These edits will be made on the Create custom query page, which is the page you are taken to after selecting Clone query in step two. This will allow you to tweak the copy to your needs. When you click Create, the initial query you copied will still exist in its original state, and a new query with the changes you make in this step will be generated/saved.
This process would allow you, for example, to alter the IP or hostname in the query to match your other domain controllers (DCs) but keep the rest of the query the same. As mentioned above, it also leaves the original query untouched/as-is. This is a fast, efficient way to make several queries that are related but require minor tweaks to meet the desired outcome. Starting each query from scratch would take much longer and would be more likely to result in human error in the query syntax.
You should not select New query on the Hunting page of Azure Sentinel. While this option could ultimately be chosen to generate the queries for your other DCs, as mentioned above, you would be starting from scratch. If you only need to change a few minor things in your query, going to New query is a waste of time as the clone option gives you a better starting point.
You should not select the ellipsis in the line of the query you want to modify, and select Edit query. This would allow you to edit an existing query, but it would not create a copy of it. Any edits made here would alter the original query. With the Clone query option, you leave the original unaltered, while efficiently creating new queries based on it.

質問**: 169**
Workbook1 という名前のカスタム Microsoft Sentinel ワークブックがあります。
Workbook1にグリッドを追加する必要があります。グリッドの行数は最大100行に制限する必要があります。
あなたはどうすべきでしょうか？
A. クエリ エディタのインターフェースで、設定を構成します。
B. クエリ エディターのインターフェースで、詳細エディターを選択します。
C. グリッドクエリにプロジェクト演算子を含めます。
D. グリッドクエリに take 演算子を含めます。
正解**: D (**コメントを発表する**)**
The take operator allows you to limit the number of rows returned by a query. By including the take operator in the grid query and specifying a maximum of 100 rows, you can ensure that the grid in Workbook1 contains a maximum of 100 rows.
https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/takeoperator

質問**: 170**
事例研究2 - Litware Inc.
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。

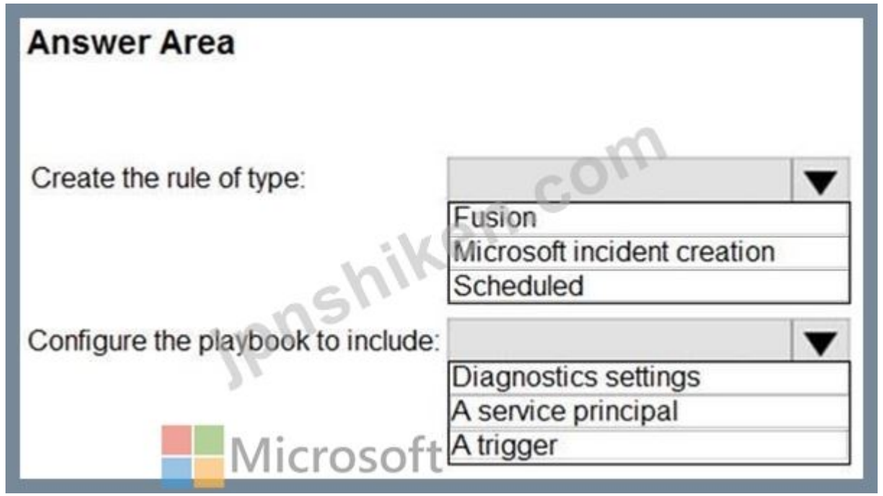
* カスタムクエリに基づいて Azure Sentinel 分析ルールを作成します。このルールは、プレイブックの実行を自動的に開始する必要があります。
* 特定のIPアドレスからのデータアクセスを表すイベントにメモを追加し、調査グラフをナビゲートする際にIPアドレスを参照できるようにします。
* Azure ADテストユーザーアカウントによるMicrosoft Office 365への受信アクセスが検出された場合にアラートを生成するテストルールを作成します。ルールによって生成されたアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。

ホットスポットに関する質問

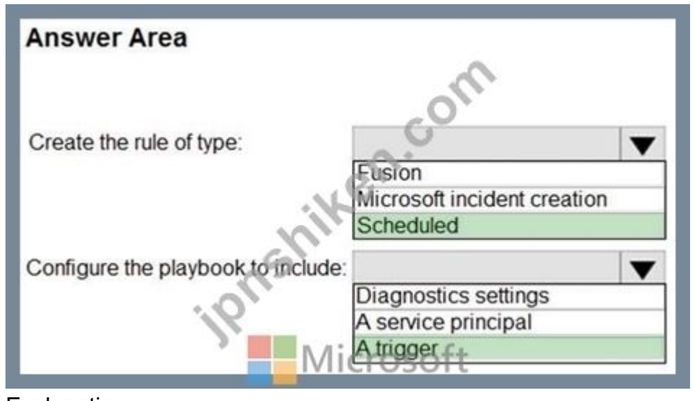
Azure Sentinelの要件を満たすには、分析ルールを作成する必要があります。

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:

Fusion rules are pre-built and cannot be custom.

None of the playbook options can be used except trigger so it must be trigger.

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and-create-the-rule

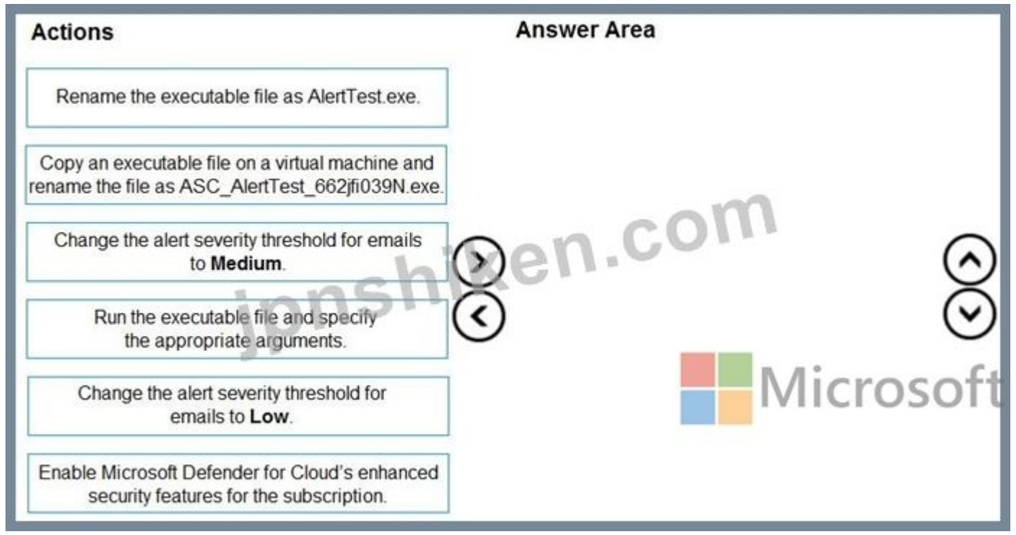
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

質問: 171

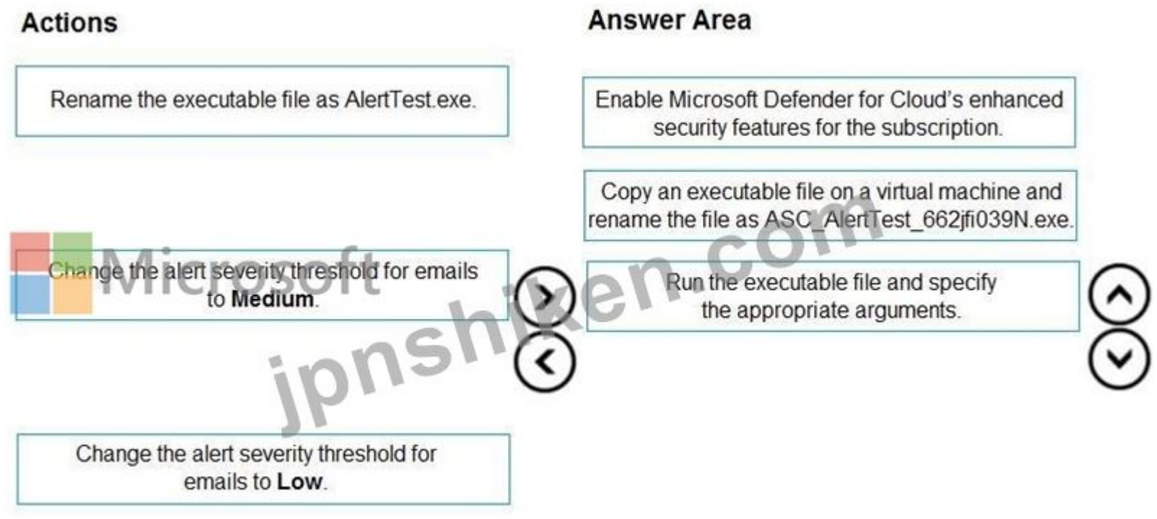
sub1という名前のAzureサブスクリプションを作成します。
sub1では、workspace1という名前のLog Analyticsワークスペースを作成します。
Azure Security Center を有効にし、ワークスペース 1 を使用するように Security Center を構成します。
Security Centerが、workspace1にレポートを送信するAzure仮想マシンからのイベントを処理するようにする必要があります。
あなたはどうすべきでしょうか？
A. セキュリティセンターからデータ収集を有効にする
B. サブ1でプロバイダーを登録します。
C. セキュリティセンターからワークフロー自動化を作成します。
D. workspace1 でワークブックを作成します。
正解**: (**正解を表示します**)**
Data collection
Store additional raw data - Windows security events
To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

質問**: 172**
Azure Defender を使用しています。
機密情報を含む Azure ストレージ アカウントをお持ちです。
誰かが不審な IP アドレスからストレージ アカウントにアクセスした場合は、PowerShell スクリプトを実行する必要があります。
どの 2 つのアクションを実行する必要がありますか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. Azure Security Center から、ワークフローの自動化を有効にします。
B. 手動トリガーを持つ Azure ロジック アプリを作成します
C. Azure Security Center アラート トリガーを持つ Azure ロジック アプリを作成します。
D. HTTP トリガーを持つ Azure ロジック アプリを作成します。
E. Azure Active Directory (Azure AD) から、アプリの登録を追加します。
正解**: (**正解を表示します**)**
You want a security trigger for the login and you use this trigger to start the automation workflow with the powershellscript.
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage- configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

質問**: 173**
ドラッグアンドドロップ問題
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。
Microsoft Defender for Cloudが、Windows Serverを実行しているAzure仮想マシン上に悪意のあるファイルが存在する場合にアラートをトリガーすること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:



質問: **174**

お客様は、Device1という名前のWindowsデバイスと、User1およびUser2という名前の2人のユーザーを含むMicrosoft 365サブスクリプションを所有しています。Device1はMicrosoft Defender for Endpointに登録されています。

デバイス1上で自動攻撃阻止が作動し、阻止期間中、ユーザー1は隔離される。

User2がUser1の隔離を解除できるようにする必要があります。解決策は最小権限の原則に従う必要があります。

User2にはどの役割を割り当てるべきですか？

A. ユーザー管理者

B. セキュリティ管理者
C. セキュリティリーダー
D. グローバル管理者
正解**: (**正解を表示します**)**
To undo a user containment or release a contained device triggered by attack disruption, user2 must be assigned the Security Administrator role. This role provides the necessary least privilege to manage and approve remediation actions in the Microsoft Defender portal without elevating to a global administrator.
Reference:
https://learn.microsoft.com/en-us/defender-xdr/automatic-attack-disruption

質問**: 175**
事例研究4 - Litware Inc.
概要
アダタム -コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境
オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。
ライセンス状況
Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。
クラウド環境
クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境
オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件
計画されている変更
Adatum社は以下の変更を実施する予定です。
- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```


- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。

Microsoft Defender for Cloud の要件

Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。

グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。

- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。

Microsoft Sentinelの要件

Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。

- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。

可能な限り、ASIMに組み込まれているパーサーを使用してください。

ビジネス要件

Adatumは、以下のビジネス要件を特定しました。

可能な限り、最小権限の原則に従うこと。

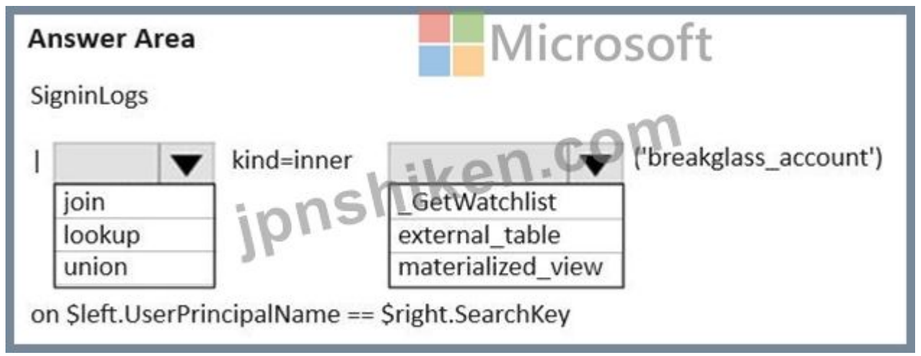
可能な限り管理業務を最小限に抑える。

ホットスポットに関する質問

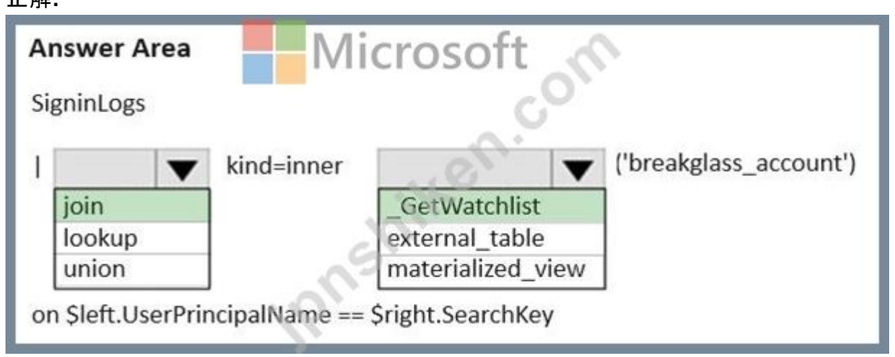
指定された緊急時アカウントを監視するには、Microsoft Sentinel NRTルールを実装する必要があります。ソリューションは、Microsoft Sentinelの要件を満たしている必要があります。

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:



質問: **176**

Microsoft Sentinelデータレイクに接続されたWorkspace1という名前のMicrosoft Sentinelワークスペースがあります。Workspace1は、データレイク層に12年分の履歴データを保持しています。

複数のテーブルを結合し、データレイク内のデータに直接アクセスする高度なハンティングクエリを実行する予定です。

調査中やスケジュールに基づいて、必要に応じてクエリを実行できることを確認する必要があります。ソリューションは、クエリが非同期で実行できることを保証しなければなりません。

何を使うべきでしょうか？

A. 要約ルール

B. 分析層のみを照会するスケジュール済み分析ルール

C. 求人検索

D. KQLジョブ

正解: **(**正解を表示します**)**

To meet your exact investigative requirements, you should use KQL jobs in the Microsoft Sentinel data lake.

Direct Data Lake Access: KQL jobs run natively against the long-term data lake tier to process massive historical datasets spanning up to 12 years.

Advanced Multi-Table Joins: Unlike standard Search jobs (which typically prioritize single-table lookups or strict hydration scenarios), KQL jobs allow you to execute complex Kusto Query Language (KQL) scripts involving multi-table joins and data aggregations.

Asynchronous Execution: Jobs naturally decouple compute from your real-time session. They run entirely in the background, preventing timeout limits commonly found in interactive queries.

On-Demand & Scheduled Support: You can execute a KQL job explicitly on-demand when conducting a live investigation, or configure it on a recurring schedule to promote findings continuously into a target table.

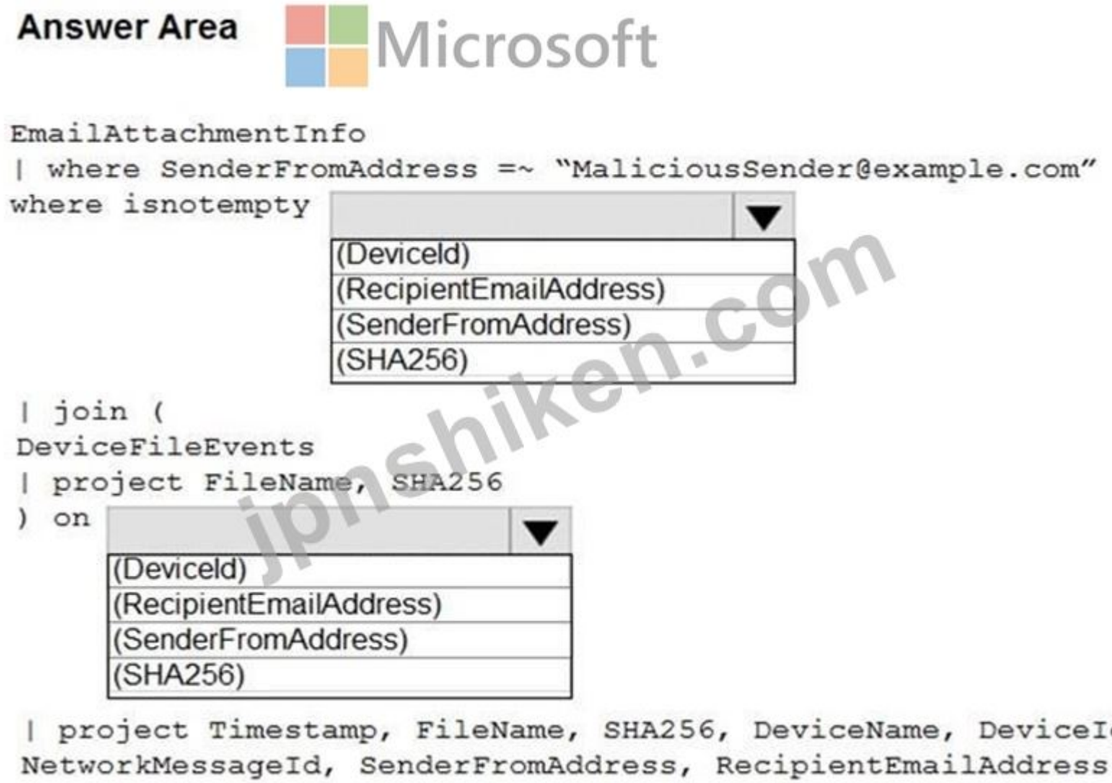
Reference:

https://learn.microsoft.com/en-us/azure/sentinel/datalake/kql-jobs

質問: **177**

ホットスポットに関する質問
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。

Answer Area



正解:

Answer Area

```
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:
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your- devices

質問: **178**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Active Directory との ID 統合のために Microsoft Defender を構成しています。
Microsoft Defender for ID ポータルから、攻撃者が悪用できるようにいくつかのアカウントを構成する必要があります。
解決策: 各アカウントを機密アカウントとして追加します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

質問: **179**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合があり

ますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Azure Sentinel を構成しています。
悪意のある IP アドレスからの Azure 仮想マシンへのサインインが検出された場合は、Azure Sentinel でインシデントを作成する必要があります。
解決策: データ コネクタ用のスケジュールされたクエリ ルールを作成します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**
You can create scheduled rules from Data connector pages (Next steps tab). But the bottom line is whoever wrote this question should be fired on the spot.

質問: **180**
Azure Sentinel で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。
ルールが断続的に失敗することがわかりました。
失敗の考えられる 2 つの原因は何ですか?それぞれの正解は、解決策の一部を示しています。
注: 正しく選択するたびに 1 ポイントの価値があります。
A. ルール クエリの実行に時間がかかりすぎてタイムアウトになります。
B. 対象のワークスペースが削除されました。
C. ルール クエリのデータ ソースへの権限が変更されました。
D. データ ソースと Log Analytics の間に接続の問題があります。
正解: **(**正解を表示します**)**
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom#troubleshooting

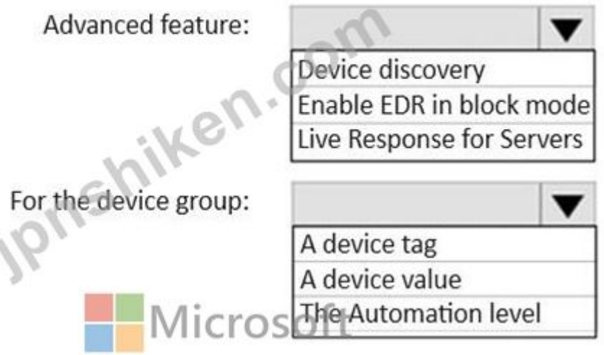
質問: **181**
Azure Sentinel で脅威を検出するためのカスタム分析ルールがあります。
分析ルールの実行が停止したことがわかります。ルールは無効になっており、ルール名には AUTO DISABLED というプレフィックスが付いています。
問題の考えられる原因は何ですか?
A. データ ソースと Log Analytics の間に接続の問題があります。
B. アラートの数が 2 分以内に 10,000 を超えました。
C. ルール クエリの実行に時間がかかりすぎてタイムアウトになります。
D. ルール クエリのデータ ソースの 1 つに対する権限が変更されました。
正解: **(**正解を表示します**)**
Permanent failure - rule auto-disable due to the following reasons
The target workspace (on which the rule query operated) has been deleted.
The target table (on which the rule query operated) has been deleted.
Microsoft Sentinel had been removed from the target workspace.

A function used by the rule query is no longer valid; it has been either modified or removed.
Permissions to one of the data sources of the rule query were changed.
One of the data sources of the rule query was deleted or disconnected.
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name

質問**: 182**
注 :このセクションには、同じシナリオと問題に関する複数の質問セットが含まれています。各質問には、問題に対する固有の解決策が提示されています。提示された解決策が、提示された目標を満たしているかどうかを判断する必要があります。セット内の複数の解決策が問題を解決できる場合もあります。また、セット内のどの解決策も問題を解決でき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、前のセクションに戻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。
あなたはMicrosoft 365のサブスクリプションをお持ちです。
サードパーティ製のウイルス対策ソフトがインストールされ、Microsoft Defenderウイルス対策ソフトがパッシブモードで動作しているWindowsデバイスが1,000台あります。
サードパーティ製のウイルス対策製品では検出されなかった悪意のあるファイルからデバイスが保護されていることを確認する必要があります。
解決策：自動調査対応(AIR)を有効にします。
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**: B (**コメントを発表する**)**
Enabling automated investigation and response (AIR) alone does not meet the goal. While AIR can investigate and respond to threats, it requires that Microsoft Defender Antivirus is active or that other components of Microsoft Defender for Endpoint, such as endpoint detection and response (EDR), are operational.
Since Microsoft Defender Antivirus is in passive mode, it cannot actively scan and detect malicious artifacts that were missed by the third-party antivirus. To achieve the goal, you need to enable EDR in block mode in addition to AIR. EDR in block mode works even when Microsoft Defender Antivirus is in passive mode, allowing Microsoft Defender for Endpoint to detect and remediate threats that the third-party antivirus missed.
Thus, simply enabling AIR is not sufficient to protect the devices in this scenario.

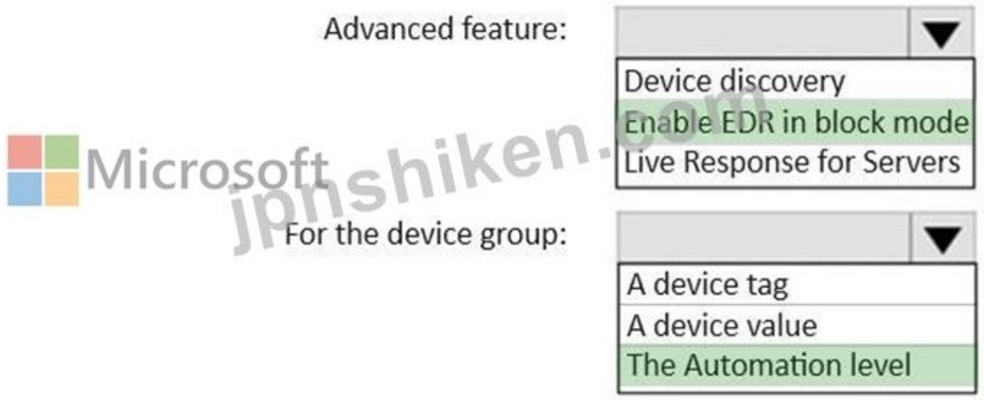
質問**: 183**
ホットスポットに関する質問
お客様は、Microsoft 365 Defender for Endpointを使用するMicrosoft 365 E5サブスクリプションをご利用中です。
Microsoft 365 Defenderポータルを使用して、Windowsサーバーへのリモートシェル接続を開始できることを確認する必要があります。
何を設定すればよいですか？回答するには、回答欄で適切なオプションを選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area



正解:

Answer Area



質問: **184**
XYZ社で複数の誤検知アラートが発生しています。XYZ社のセキュリティ運用アナリストは、アラートを減らすために実行可能ファイル(c:\myxyzapp\myxyzwinapp.exe)を除外する必要があります。どの除外タイプを使用すればよいでしょうか？
A. 拡張機能
B. フォルダ
C. ファイル
D. 登録
正解: (正解を表示します)
File will exclude only this specific file, whereas extension would exclude all files with the extensions, and folder would exclude all files in a folder. Registry exclusion doesn't happen.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-extension-file-exclusions-microsoft-defender-antivirus?view=o365-worldwide

質問: **185**
事例研究1 - Contoso Ltd
概要
Contoso Ltd.という会社は、北米各地に本社と5つの支店を構えています。本社はシアトルにあり、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アラートを受信している。セキュリティチームは、どのサイバーセキュリティアラートが正当な脅威で、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る。
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る。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複数発生している。
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
Azure仮想マシンの技術要件を満たす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. ジャストインタイム(JIT)アクセス
B. アズールディフェンダー
C. Azure Firewall
D. Azure Application Gateway

正解: **B** (コメントを発表する)
Defender for Cloud helps you limit exposure to brute force attacks.
https://docs.microsoft.com/en-us/azure/security-center/azure-defender

質問: **186**
お客様は、Microsoft 365 Defender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。
自動調査における修復措置として、複数のデバイス間でファイルが隔離されます。
デバイス上でファイルを安全としてマークし、隔離状態から削除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. アクションセンターの履歴タブから、操作を元に戻します。
B. 調査ページから、AIRプロセスを確認します。
C. レビューページの隔離からルールを変更します。
D. 脅威トラッカーからクエリを確認します。
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide#undo-completed-actions

質問: **187**
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションをお持ちです。
脅威ハンティングクエリを使用することで、新たな脅威を検出できます。
Microsoft Sentinelが脅威を自動的に検出するようにする必要があります。また、管理作業を最小限に抑えるソリューション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. 分析ルールを作成します。
B. クエリをワークブックに追加します。
C. ウォッチリストを作成します。
D. プレイブックを作成する。
正解: **A** (コメントを発表する)
Creating an analytics rule in Microsoft Sentinel is the best way to ensure that the system automatically detects the threat with minimal administrative effort. Analytics rules allow you to create custom detections based on specific events or patterns that you want to monitor.

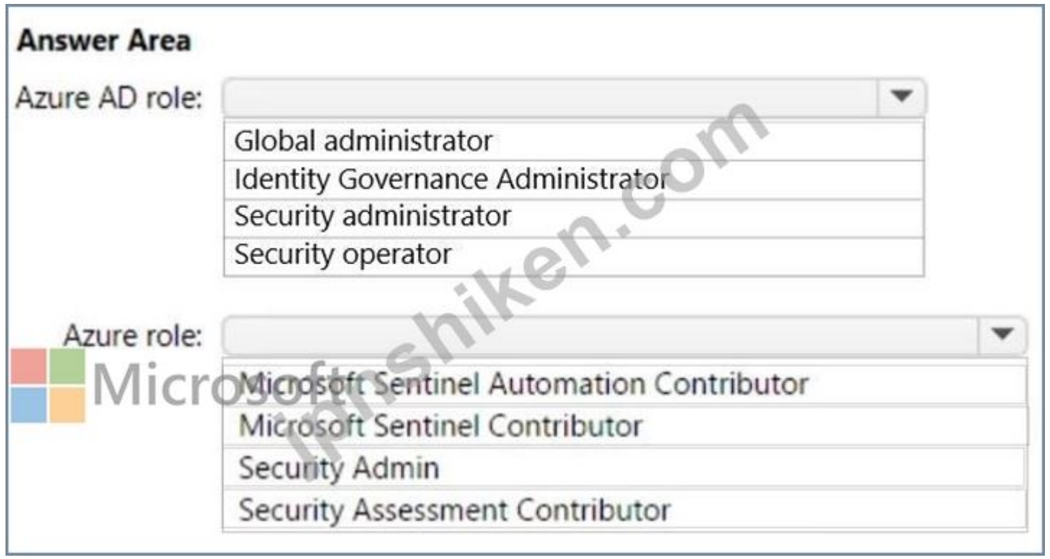
質問: **188**
Azure Sentinel を使用しています。
組み込みロールを使用して、セキュリティ アナリストにカスタム Azure Sentinel ブックのクエリを編集する機能を提供する必要があります。ソリューションでは、最小特権の原則を使用する必要があります。
アナリストにはどの役割を割り当てるべきですか?
A. Azure Sentinel の貢献者
B. セキュリティ管理者
C. Azure Sentinel レスポンダー
D. ロジック アプリのコントリビューター
正解: **A** (コメントを発表する)
Azure Sentinel Contributor can create and edit workbooks, analytics rules, and other Azure Sentinel resources.
Reference:

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

質問: **189**
お客様は、VM1 という名前の仮想マシンを含む Azure サブスクリプションを所有しており、その仮想マシンは Microsoft Defender for Cloud を使用しています。
Microsoft Defender for Cloud は、Azure Monitor Agent を使用するように自動プロビジョニングが構成されています。
VM1上でPowerShellの不審な使用に関する誤検知アラートを抑制するカスタムアラート抑制ルールを作成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. Microsoft Defender for Cloud から、アラートを Log Analytics ワークスペースにエクスポートします。
B. Microsoft Defender for Cloud からワークフロー自動化を追加します。
C. VM1 上で PowerShell アラートをトリガーします。
D. VM1 で Get-MPThreatCatalog コマンドレットを実行します。
正解: **(**正解を表示します**)**
You must trigger the alert before deploying a suppression rule.

質問: **190**
Microsoft Sentinelワークスペースをお持ちです。
2つ以上の警告またはアクティビティで構成される高度な多段階攻撃を検出するために使用されるルールを特定する必要があります。ソリューションは、管理作業を最小限に抑える必要があります。
どのルールタイプを照会すべきですか？
A. 融合
B. マイクロソフトセキュリティ
C. ML行動分析
D. 予定
正解: **A (**コメントを発表する**)**
Microsoft Sentinel uses Fusion, a correlation engine based on scalable machine learning algorithms, to automatically detect multistage attacks.
https://learn.microsoft.com/en-us/azure/sentinel/fusion

質問: **191**
ホットスポットに関する質問
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Azure AD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:

質問: **192**

ホットスポットに関する質問

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。

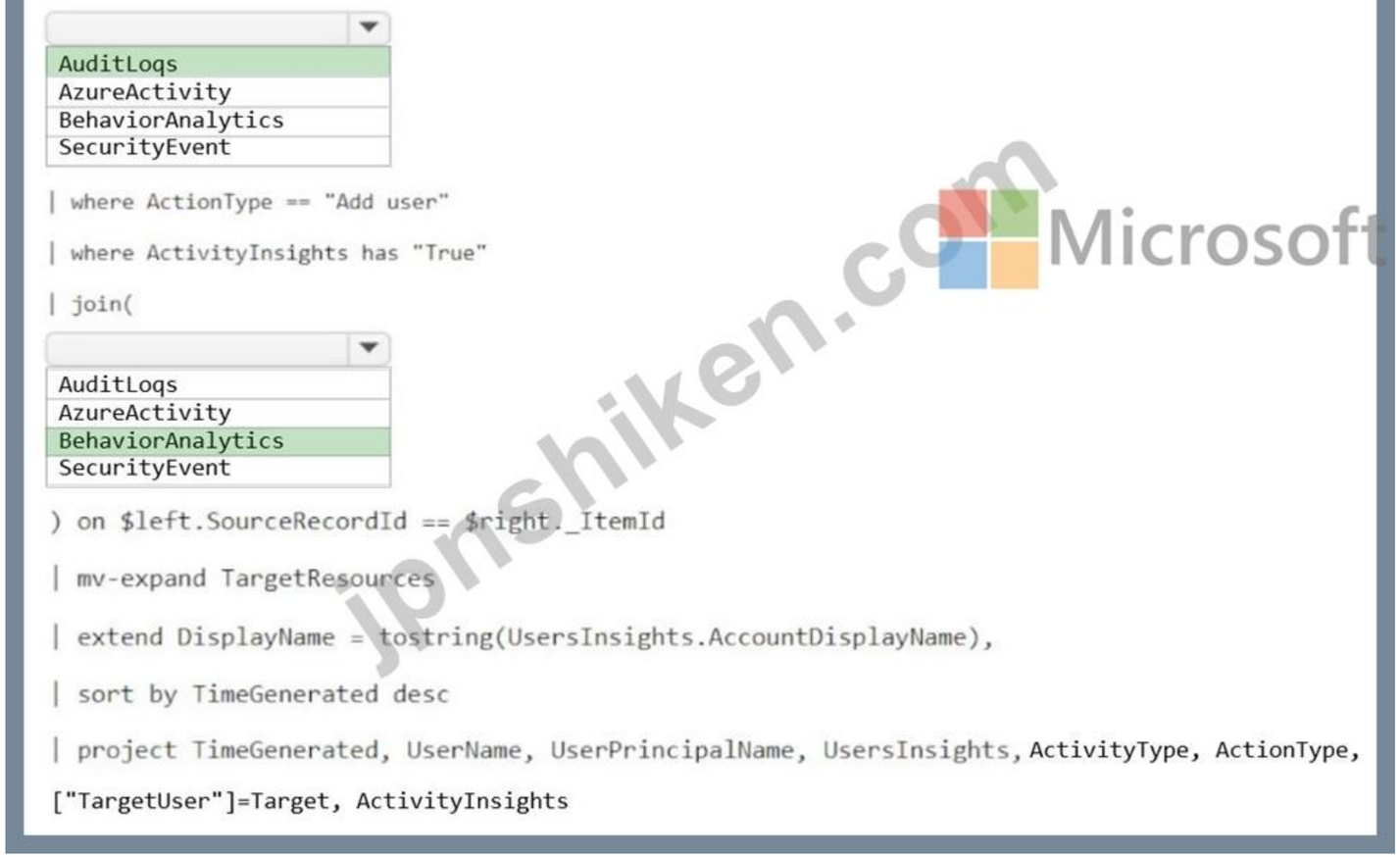
注：正解ごとに1ポイントが加算されます。

Answer Area

```
[ AuditLogs | AzureActivity | BehaviorAnalytics | SecurityEvent ]
| where ActionType == "Add user"
| where ActivityInsights has "True"
| join(
[ AuditLogs | AzureActivity | BehaviorAnalytics | SecurityEvent ]
) on $left.SourceRecordId == $right._ItemId
| mv-expand TargetResources
| extend DisplayName = tostring(UsersInsights.AccountDisplayName),
| sort by TimeGenerated desc
| project TimeGenerated, UserName, UserPrincipalName, UsersInsights, ActivityType, ActionType,
["TargetUser"]=Target, ActivityInsights
```

正解:

Answer Area



質問: **193**

お客様は、Microsoft Security Copilot 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。

以下の表に示すファイルをお持ちです。

Name	Size
File1.docx	4 MB
File2.pdf	2 MB
File3.txt	128 KB

各ファイルには、貴社のコンプライアンスポリシーのコピーが含まれています。

Security Copilotの応答がコンプライアンスポリシーに基づいていることを確認する必要があります。

Security Copilotにアップロードできるファイルはどれですか？

A. ファイル1.docxのみ

B. ファイル3.txtのみ

C. ファイル1.docxとファイル3.txtのみ

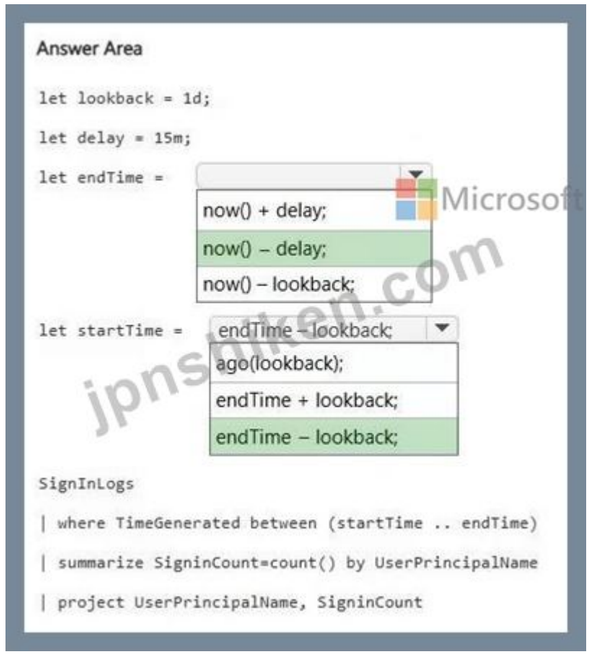
D. ファイル2.pdfとファイル3.txtのみ
E. File1.docx、File2.pdf、およびFile3.txt
正解**: (**正解を表示します**)**
File1.docx is too large.
Each uploaded file must not exceed 3 MB.
Reference:
https://learn.microsoft.com/sv-se/copilot/security/upload-file

質問**: 194**
ホットスポットに関する質問
Microsoft Sentinelデータレイクに接続されたMicrosoft Sentinelワークスペースをお持ちです。
新たに取り込まれたデータがデータレイク内でクエリ可能になるまでには、最大15分かかる場合があります。
脅威ハンターが使用するサマリーテーブルにデータを入力するKQLジョブを、毎日午前0時10分に実行するようにスケジュール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。
- 各実行では、15分後に終了する固定の24時間ウィンドウに対してクエリを実行する必要があります。
ジョブ実行前に。
- 日々の運行において、二重計上を防止する必要がある。
遅れて到着した記録も要約に含める必要があります。
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

```
let lookback = 1d;
let delay = 15m;
let endTime =
let startTime =
SignInLogs
| where TimeGenerated between (startTime .. endTime)
| summarize SigninCount=count() by UserPrincipalName
| project UserPrincipalName, SigninCount
```

- let endTime =
  - now() + delay;
  - now() – delay;
  - now() – lookback;
- let startTime = endTime – lookback;
  - ago(lookback);
  - endTime + lookback;
  - endTime – lookback;

正解:



質問: **195**

お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。

Rule1という名前のカスタム検出ルールがあり、デバイス上で5つ以上のウイルス対策ソフトが検出された場合にアラートを生成します。Rule1のルックバック期間は12時間です。

参照期間を48時間に変更する必要があります。

ルール1については、何を変更すべきでしょうか？

A. 範囲

B. KQLクエリの要約演算子

C. 周波数

D. KQLクエリのwhere演算子

正解: **(**正解を表示します**)**

Microsoft Defender XDR, Create and manage custom detections rules

Rule frequency

When you save a new rule, it runs and checks for matches from the past 30 days of data. The rule then runs again at fixed intervals, applying a lookback period based on the frequency you choose:

Every 24 hours - Runs every 24 hours, checking data from the past 30 days.

Every 12 hours - Runs every 12 hours, checking data from the past 48 hours.

Every 3 hours - Runs every 3 hours, checking data from the past 12 hours.

Every hour - Runs hourly, checking data from the past 4 hours.

Continuous (NRT) - Runs continuously, checking data from events as they're collected and processed in near real-time (NRT), see Continuous (NRT) frequency.

Reference:

https://learn.microsoft.com/en-us/defender-xdr/custom-detection-rules

質問: **196**
Microsoft 365 Defenderデータコネクタを使用するMicrosoft Sentinelワークスペースをお持ちです。
Microsoft Sentinel から、Microsoft 365 のインシデントを調査します。
Microsoft Defender for Cloud Apps によって生成されたアラートを含めるように、インシデントを更新する必要があります。
何を使うべきでしょうか？
A. Microsoft Sentinel のタイムライン カードのエンティティ サイド パネル
B. Microsoft Sentinel のインシデントページのタイムライン タブ
C. Microsoft Sentinel のインシデントページにある調査グラフ
D. Microsoft 365 Defender ポータルのアラート ページ
正解: **(**正解を表示します**)**
Open the Microsoft 365 Defender portal and select Alerts.
Find the alert that you want to add to the incident and select it.
In the alert details page, select Add to existing incident.
In the Add alert to incident pane, select the incident that you want to update and then select Add.
This will add the alert to the incident in both Microsoft 365 Defender and Microsoft Sentinel portals. Any changes you make to the incident in Microsoft 365 Defender will be synchronized to the same incident in Microsoft Sentinel

質問: **197**
お客様はMicrosoft 365サブスクリプションをご利用中です。このサブスクリプションではMicrosoft 365 Defenderが使用されており、集約アラートが構成されたデータ損失防止(DLP)ポリシーが設定されています。
集約されたアラートの中で、影響を受けるエンティティを特定する必要があります。
Microsoft 365コンプライアンスセンターのDLPアラート管理ダッシュボードでは、どのような項目を確認すべきでしょうか？
A. アラートのイベントタブ
B. アラートの 機密情報タイプ」タブ
C. 管理ログ
D. アラートの詳細タブ
正解: **(**正解を表示します**)**
In order to identify the impacted entities in an aggregated alert, you should review the "Events" tab of the DLP alert management dashboard in the Microsoft 365 compliance center. This tab will display a list of all the events that triggered the alert, including the specific entities (e.g. files, emails, etc.) that were affected. You can further investigate each event to identify the specific user, device and action that caused the alert to be triggered.
https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts- policies?view=o365-worldwide

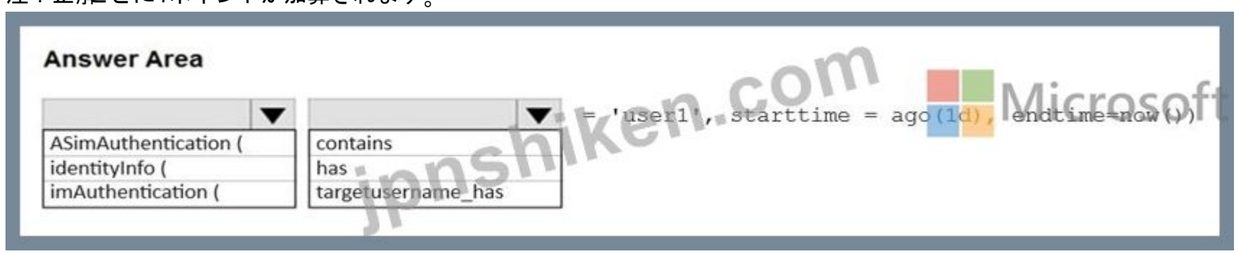
質問: **198**
お客様は、Microsoft Defender XDRを使用するMicrosoft 365サブスクリプションをご利用されています。

Name	Tactic
Tactic1	Conditional Access policy reconnaissance
Tactic2	Mailbox reconnaissance
Tactic3	Invites guest users to the tenant

とが知られている攻撃者を調査しています。攻撃者は、次の表に示す戦術を実行します。

組織内で悪意のある活動がないか調査する必要があります。
MicrosoftGraphActivityLogsテーブルを使用して、どのような戦術を分析できますか？
A. 戦術1、戦術2、戦術3
B. 戦術2と戦術3のみ
C. 戦術2のみ
D. 戦術1と戦術2のみ
正解: **A** (コメントを発表する)

質問: **199**
ホットスポットに関する質問
ユーザー「User1」と「WS1」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。
WS1に高度セキュリティ情報モデル(ASIM)認証パーサーをデプロイします。
パーサーを使用して、User1が過去24時間以内に生成した認証イベントを照会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。



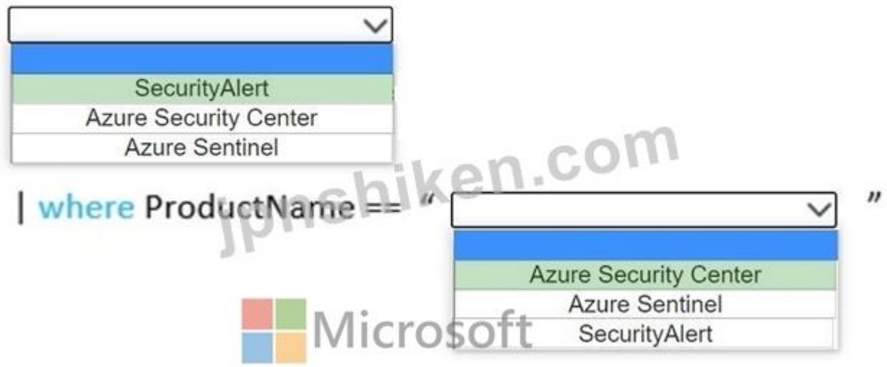
正解:

質問: **200**
お客様は、Microsoft Sentinelを使用するAzureサブスクリプションをお持ちです。
時間の経過に伴うサインイン情報を視覚化するカスタムレポート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. 狩猟に関する質問
B. ワークブック
C. ノート
D. プレイブック
正解: **B** (コメントを発表する)

A Workbook is a collection of visualizations and data that can be used to analyze and report on data in Azure Sentinel. It can be used to create custom reports that visualize sign-in information over time.
https://learn.microsoft.com/en-us/azure/sentinel/monitor-your-data

質問: **201**
ホットスポットに関する質問
お客様は、クラウドワークロードを保護し、環境を監視するために、Azure DefenderとAzure Sentinelを使用しています。
Azure Defender のアラートを識別するクエリを作成するには、Kusto クエリ言語 (KQL) を使用する必要があります。
この要件を満たすには、どのようなクエリを作成すればよいでしょうか？回答するには、ドロップダウンメニューから適切なオプションを選択してクエリを完成させてください。

正解:

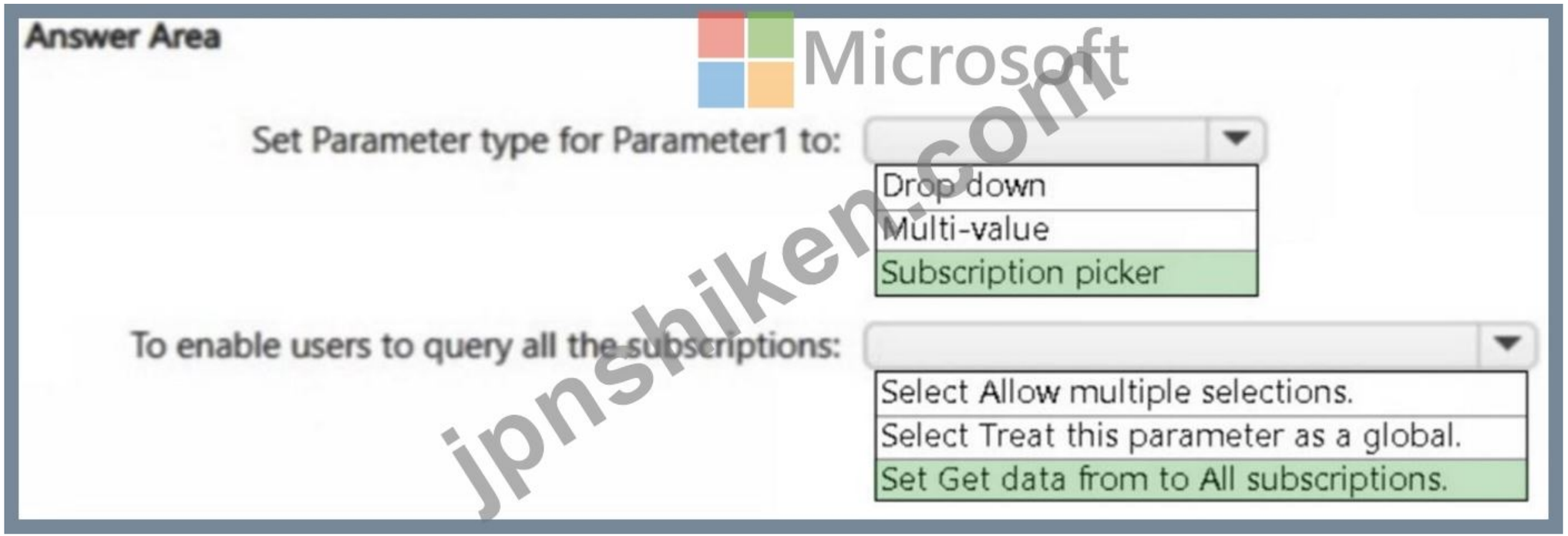


Explanation:
You should complete the query as follows:
SecurityAlert
| where ProductName == "Azure Security Center"
This completes a basic query to identify all security alerts in Azure Security Center. Placing SecurityAlert first queries the SecurityAlert table, and then using | where ProductName == "Azure Security Center" afterwards ensures that in that SecurityAlert table you are only looking for entries where the ProductName column has a value of Azure Security Center. From here, you can expand. For example, you could use KQL to specify time frames or specific devices to query.

Kusto Query Language (KQL) is the language you will use when building queries in Azure Sentinel. Queries serve as a way to search through the massive amount of data Azure Sentinel has access to.
You should not begin the query with Azure Security Center. The structure of a query requires that you first identify the key table you will be querying. The SecurityAlert table includes the security alerts that are being digested by Azure Sentinel. You should first query this table, then narrow the search to the alerts coming from the Azure Security Center product.
You should not begin the query with Azure Sentinel. Again, the structure of a query requires that you first identify the key table you will be querying. In this case, that would be the SecurityAlert table. More importantly, while Azure Sentinel is the solution aggregating this data and performing the query, it should not be used as the ProductName. This should be specified as the Azure Security Center.
You should not end the query with Azure Sentinel. As mentioned in the paragraph above, the ProductName (solution source) for the SecurityAlert (alerts) table you should query is Azure Security Center. The query would be run in Azure Sentinel, but do not confuse the solution being queried with the one running the query.
You should not end the query with SecurityAlert. Here you need to name the solution you want to query. In this case, that is Azure Security Center. SecurityAlert would not be a valid ProductName.

質問: **202**
ホットスポットに関する質問
Azure 環境には、Sub1 という名前のサブスクリプションを含む 50 個のサブスクリプションがあります。Sub1 には、他のサブスクリプションからログを収集する Workspace1 という名前の Microsoft Sentinel ワークスペースが含まれています。Workspace1 には、WB1 という名前のワークブックが含まれています。
WB1に、Item1という名前のパラメータ項目を追加します。Item1に、Parameter1という名前のパラメータを追加します。
Parameter1のドロップダウンメニューを以下の要件を満たすように設定する必要があります。
ユーザーがクエリ対象のサブスクリプションを1つ以上選択できるようにする。
ユーザーがすべての購読情報を照会できる単一のオプションを提供する。
解決策は、WB1へのデータ入力にかかる時間を最小限に抑える必要がある。また、管理上の手間も最小限に抑える必要がある。
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:



質問: **203**
Azure Defender for Key Vault のアラートに応答するのはお客様の責任です。
アラートの調査中に、Tor 出口ノードからキー コンテナーへの不正なアクセスの試みを発見しました。
脅威を軽減するには何を構成する必要がありますか?
A. Key Vault ファイアウォールと仮想ネットワーク
B. Azure Active Directory (Azure AD) のアクセス許可
C. キー コンテナーのロールベースのアクセス制御 (RBAC)
D. キー コンテナーのアクセス ポリシー設定
正解: **(**正解を表示します**)**
To be able to prevent unauthorized access to the key vault through suspicious IPs you have to change the networking settings under the key vault resource.
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

質問: **204**
事例研究2 - Litware Inc.
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。

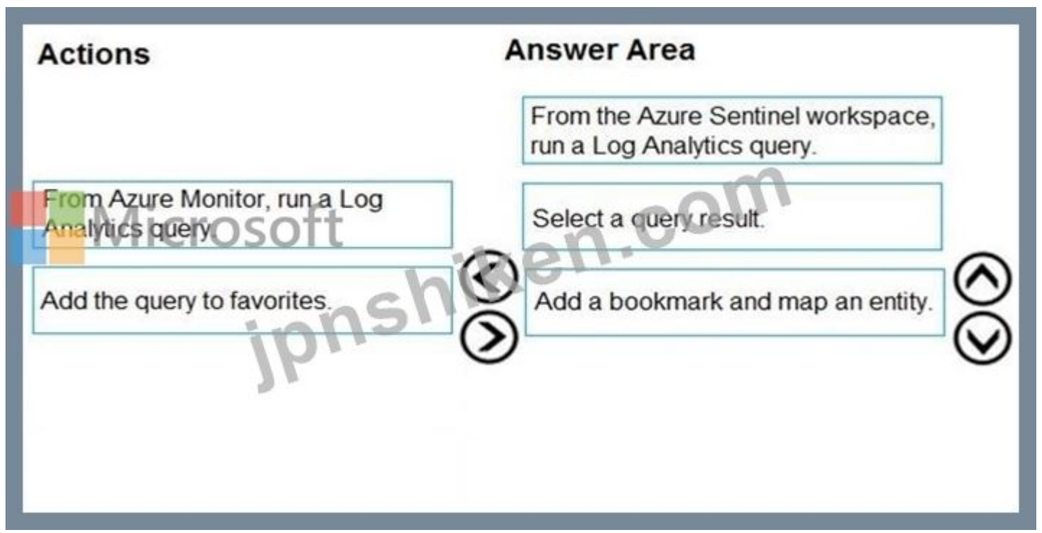
* admin1 という名前のユーザーが Azure Sentinel プレイブックを構成できることを確認してください。
* カスタムクエリに基づいて Azure Sentinel 分析ルールを作成します。このルールは、プレイブックの実行を自動的に開始する必要があります。
* 特定のIPアドレスからのデータアクセスを表すイベントにメモを追加し、調査グラフをナビゲートする際にIPアドレスを参照できるようにします。
* Azure ADテストユーザーアカウントによるMicrosoft Office 365への受信アクセスが検出された場合にアラートを生成するテストルールを作成します。ルールによって生成されたアラートは、テストユーザーアカウントごとに1つのインシデントとしてグループ化する必要があります。

ドラッグアンドドロップ問題

Azure Sentinelの要件を満たすには、イベントにメモを追加する必要があります。

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:

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

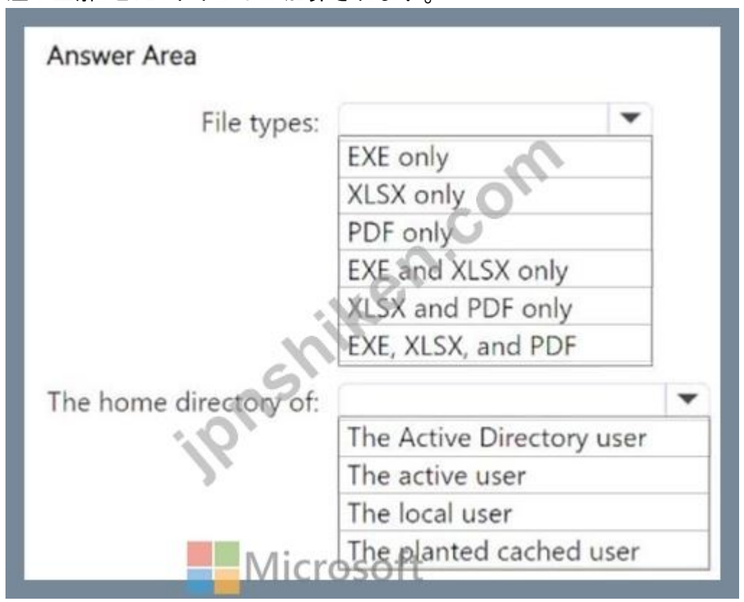
質問: **205**
お客様は、Microsoft Defender XDR を使用する Microsoft 365 サブスクリプションをご利用中です。このサブスクリプションには、Microsoft Defender ウイルス対策を使用する Windows 11 デバイスが 100 台含まれています。これらのデバイスは、単一の Microsoft Defender for Endpoint デバイス グループに属しています。
デバイス上で潜在的に悪意のあるファイルをブロックできるように、「ファイルの許可」または 「ファイルのブロック」オプションを使用する必要があります。
Microsoft Defender ポータルから、「ファイルの許可またはブロック」を 「オン」に設定します。
次に何をすべきでしょうか？
A. デバイス自動応答の設定
B. インジケーターを追加します。
C. アセットルートを作成する
D. 是正レベルを割り当てる。
正解: **(**正解を表示します**)**
After enabling the Allow or block file setting in the Microsoft Defender portal, the next step to block potentially malicious files is to create file indicators for the specific file hashes you want to block.
You can add these indicators by following these steps in the Microsoft Defender portal:
Navigate to Indicators: Go to Settings > Endpoints > Indicators (under the Rules section).
Add File Hashes: Select the File hashes tab and click Add item.
Define the Indicator: Enter the file's hash (MD5, SHA1, or SHA256) and set the Action to Block execution or Block and remediate.
Set the Scope: Choose the organizational scope. Since you have a single device group including all devices, you can apply the indicator to that specific group or the entire organization.
Requirements for Blocking to Work:
Active Mode: Microsoft Defender Antivirus must be running in Active mode on the devices.
Cloud Protection: Cloud-delivered protection must be enabled to allow the endpoint to communicate with the service for real-time blocking.
Reference:
https://learn.microsoft.com/en-us/defender-endpoint/indicator-file

質問: **206**
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中です。このサブスクリプションには、Microsoft Entra に参加し、Microsoft Defender for Endpoint の既定のデバイス グループに属し、Microsoft Intune を使用して管理されている 500 台のデバイスが含まれています。
Microsoft Defenderの脆弱性管理を導入する必要があります。ソリューションは、管理作業を最小限に抑えるものでなければなりません。
Microsoft Defenderポータルで最初に何をすべきですか？
A. 構成管理から、適用範囲の設定を構成します。
B. デフォルトのデバイスグループに対して自動修復を設定します。
C. Microsoft Intune の接続をオンに設定します。
D. ライブレスポンスをオンに設定します。
正解: **(**正解を表示します**)**
To get Defender Vulnerability Management (TVM) working with Intune-managed devices, first enable the Intune connection in the Defender portal (Settings > Endpoints > Advanced features) and then use Endpoint Security Policies (Configuration profiles) in Intune or the Defender portal to deploy security settings and onboard devices, creating device groups in Entra ID to target these policies effectively for vulnerabilities and remediation.
Here are the key configuration steps:
In the Microsoft Defender Portal (security.microsoft.com):
*-> 1. Connect to Intune: Go to Settings > Endpoints > Advanced features, find the "Microsoft Intune connection," and turn the toggle On, then Save.
3. Use Device Groups: Navigate to Endpoints > Device groups, create/manage groups (e.g., for Windows 11) to filter vulnerability data and apply specific settings.
2. Check Device Onboarding: Verify devices appear in the Assets > Devices inventory, showing their risk, exposure, and management status.
In Microsoft Intune (Microsoft Endpoint Manager admin center):

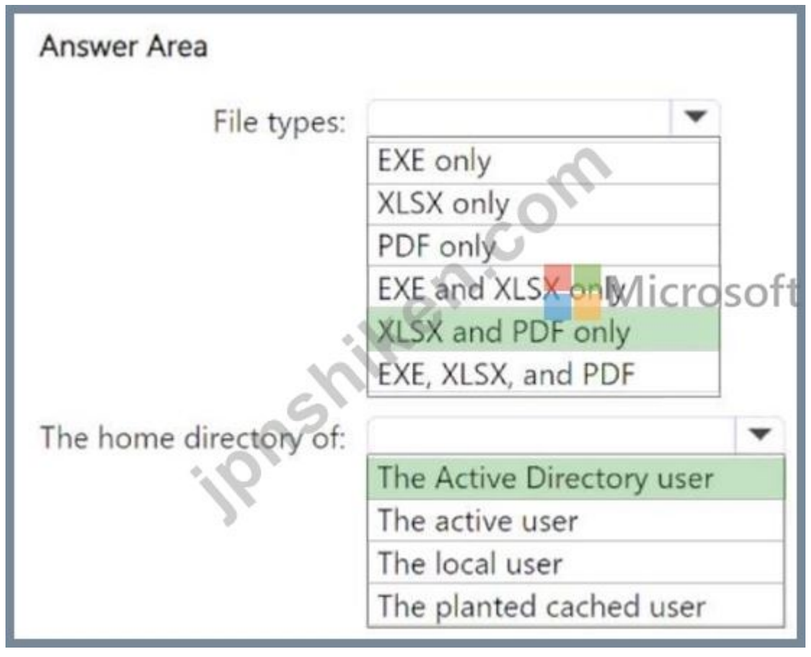
1. Onboard Devices
2. Deploy Security Settings
3. Create Remediation Tasks

Reference:
https://learn.microsoft.com/en-us/intune/intune-service/protect/microsoft-defender-integrate

質問**: 207**
ホットスポットに関する質問
お客様は、Microsoft Defender XDRを使用するMicrosoft 365 E5サブスクリプションをご利用されています。
あなたは欺瞞行為に関するルールを適用しています。
カスタムルアーファイルを提供する必要があります。
カスタムルアーの場合は、植え付けパスをHOMEに設定します。
カスタムルアーにはどのような種類のファイルを使用できますか？また、そのファイルはデバイス上のどのホームディレクトリに配置すればよいですか？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: 208

Device1という名前のWindowsデバイスがあり、Microsoft Defender for Endpointに登録されています。
Policy1 という名前の攻撃対象領域縮小 (ASR) ポリシーを作成し、すべての Office アプリケーションが子プロセスを作成することをブロックするように設定して、ブロックします。
デバイス1では、必須のMicrosoft Officeプラグインであるplugin1が失敗します。
Policy1がDevice1上のPlugin1の不具合を引き起こしているかどうかを検証する必要があります。解決策は、管理上の手間を最小限に抑えるものでなければなりません。
まず最初に何をすべきでしょうか？

A. Microsoft Defender ポータルから、デバイス1の選択的隔離モードを有効にします。
B. Microsoft Defender ポータルから、デバイス1のトラブルシューティングモードを有効にします。
C. Device1 で、Set-MpPreference -DisableTamperProtection $true コマンドレットを実行します。
D. Device1 で、Set-MpPreference -AttackSurfaceReductionRules_Ids E5AF940AB-401D-41FC-AADC-AD5F3C50679A AttackSurfaceReductionRules_Actions コマンドレットを実行します。

正解: (正解を表示します)

The best first step is to enable troubleshooting mode on the device from the Microsoft Defender portal.
Enabling Troubleshooting Mode allows a security administrator to temporarily bypass or modify security settings directly on a targeted endpoint. This lets you test whether security features like Attack Surface Reduction (ASR) or real-time antivirus protection are causing an application or plugin to break. It keeps administration low because the mode automatically terminates after 4 hours, reverting the device back to its original centralized management state without needing a policy overhaul.
Incorrect:
[Not A]
Selective Isolation Mode: This feature isolates a compromised device from the network to contain threats while allowing specific tools or applications to communicate. It is used for incident response containment, not for local policy debugging or troubleshooting false-positive application blocks.
[Not C]
Using Set-MpPreference -DisableTamperProtection $true: Under normal operation, Microsoft Defender's Tamper Protection actively prevents local administrators or scripts from modifying endpoint security preferences. Running this

command on a standard onboarded device will be blocked by Tamper Protection unless Troubleshooting Mode has already been initiated from the cloud portal.
[Not D]
Using Set-MpPreference to modify ASR IDs manually: Attempting to alter specific ASR rules on the machine locally using PowerShell will also fail or be overridden by central policies and Tamper Protection. Modifying individual policies directly for a single test introduces higher administrative overhead compared to the 1-click cloud troubleshooting session.
Reference:
https://www.indefent.com/troubleshooting-performance-bottlenecks-in-microsoft-defender-for-endpoint/

質問: **209**
Azure Defender から Key Vault のアラートを受け取ります。
複数の不審な IP アドレスからアラートが生成されていることがわかりました。
問題を調査する際に、Key Vault のシークレットが漏洩する可能性を減らす必要があります。ソリューションはできるだけ早く実装する必要があり、正規ユーザーへの影響を最小限に抑える必要があります。
まず何をすべきでしょうか?
A. キー コンテナーのアクセス制御設定を変更します。
B. Key Vault ファイアウォールを有効にします。
C. アプリケーション セキュリティ グループを作成します。
D. キー コンテナーのアクセス ポリシーを変更します。
正解: **(正解を表示します)**
You create firewall rules and adds trusted range to ensure Key Vault can only be accessed from those trusted IP addresses while you are doing investigation.
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

質問: **210**
ホットスポットに関する質問
複数のAzureサブスクリプションがあり、それぞれに複数のMicrosoft Sentinelワークスペースが含まれています。
AzureActivity テーブルへの参照を含む Microsoft Sentinel ワークブックを作成しています。
以下の操作を実行するKQLクエリを作成する必要があります。
- 各ワークスペースにAzureActivityテーブルが存在するかどうかを確認します。
テーブルが存在する場合は、isMissing を持つ単一の行を返します。
列が0に設定されました。
- テーブルが存在しない場合は、
isMissing列が1に設定されます。
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。

Answer Area

正解:

質問: **211**

事例研究3 - Litware Inc.

概要

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。

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、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。

Microsoft 365環境

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を実装し、ログコレクターを有効にします。

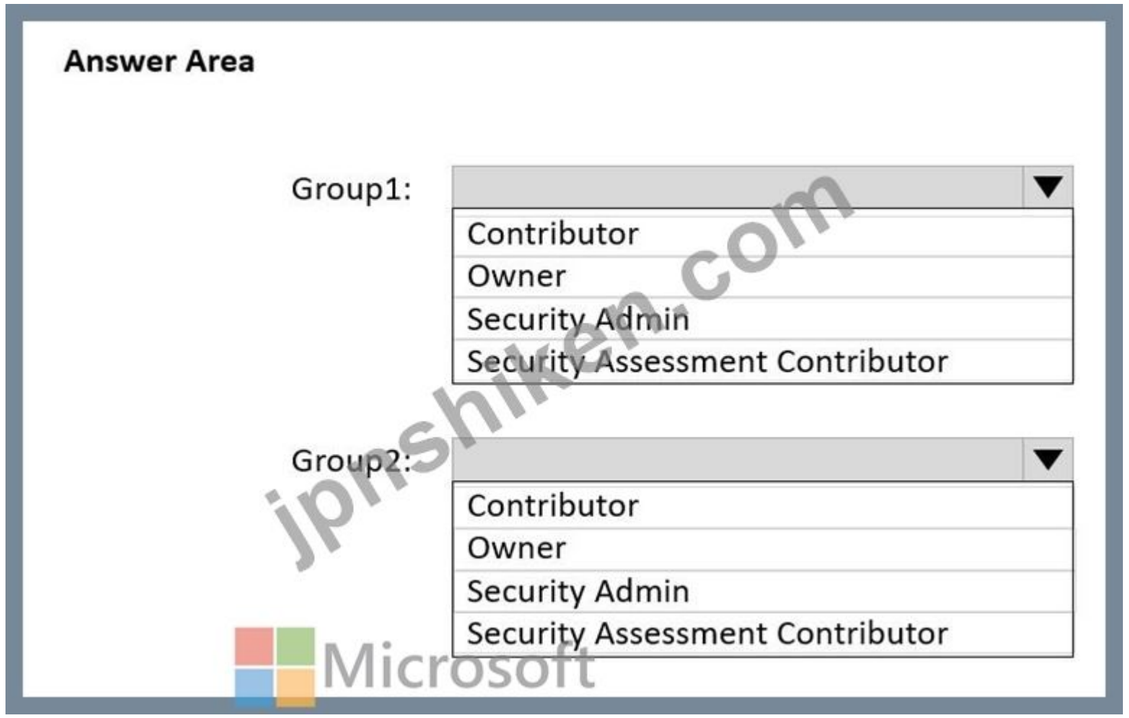
Azure環境

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。

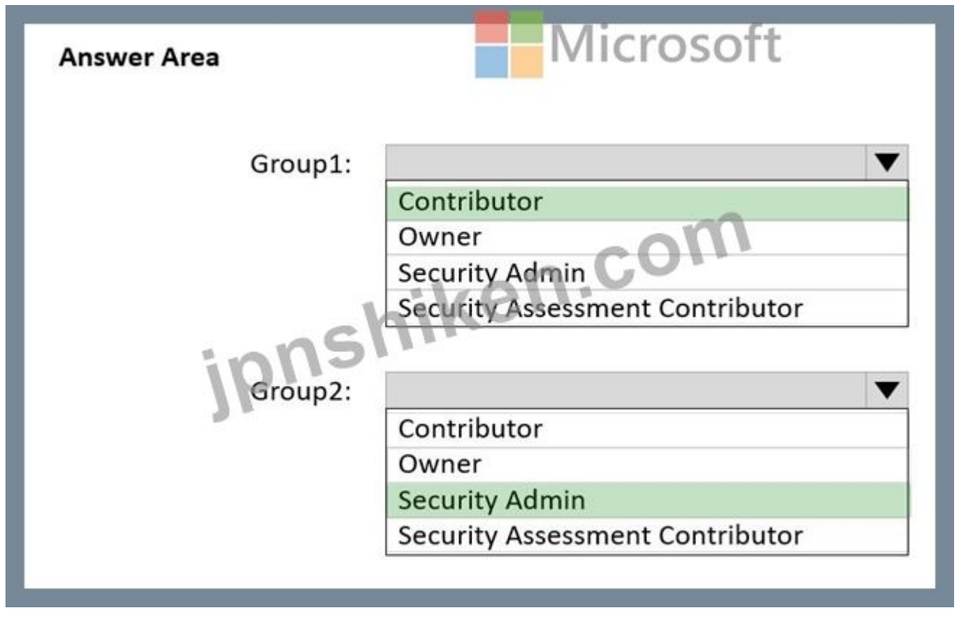
Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics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

Amazon Web Services (AWS) 環境
FabrikamはAccount1という名前のAmazon Web Services(AWS)アカウントを持っています。Account1には
カスタム版Windows Server 2022を実行するAmazon Elastic Compute Cloud(EC2)インスタンス100台。
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。
最新の課題
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」に関する警告を大量に発生させます。
Defender for Identityは、DCSync攻撃の疑いに関するアラートを大量に発生させますが、その多くは誤検知です。
要件
計画されている変更
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
ビジネス要件
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。
Microsoft Defender for Cloud Apps の要件
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。
Microsoft Defender for ID の要件
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。
Microsoft Defender for Cloud の要件
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する。

- 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。
Microsoft Sentinelの要件
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の平均解決時間を特定します。
- 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、Pool1に対して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。
ホットスポットに関する質問
Microsoft Defender for Cloudの要件とビジネス要件を満たすには、Group1とGroup2にロールベースアクセス制御(RBAC)ロールを割り当てる必要があります。
各グループにどのような役割を割り当てるべきでしょうか？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。

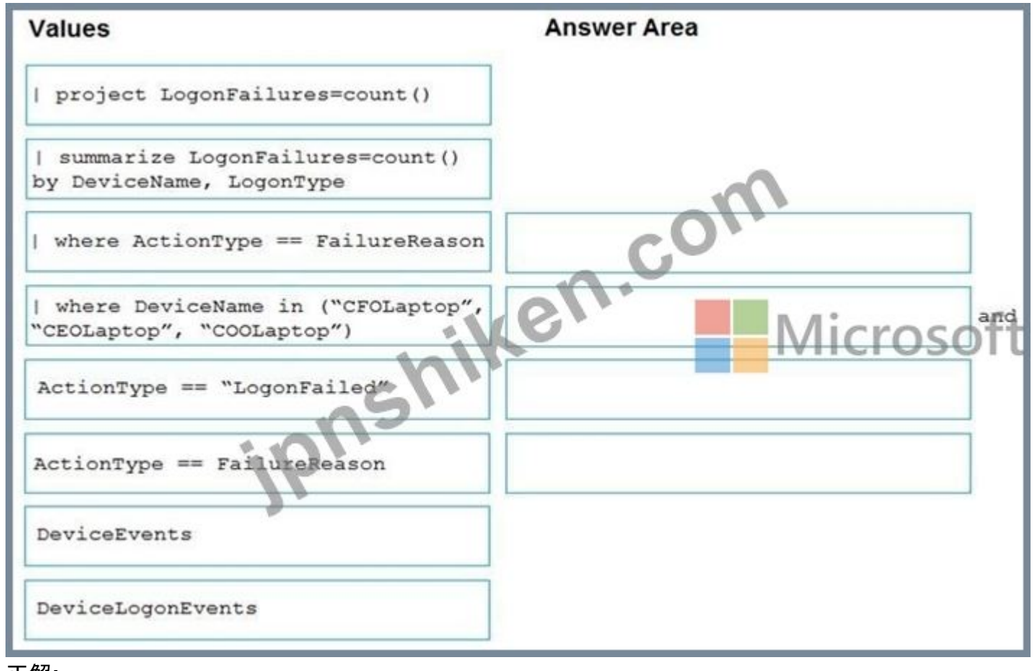

Answer Area
Group1:
Contributor
Owner
Security Admin
Security Assessment Contributor
Group2:
Contributor
Owner
Security Admin
Security Assessment Contributor
jpnshiken.com
Microsoft

正解:

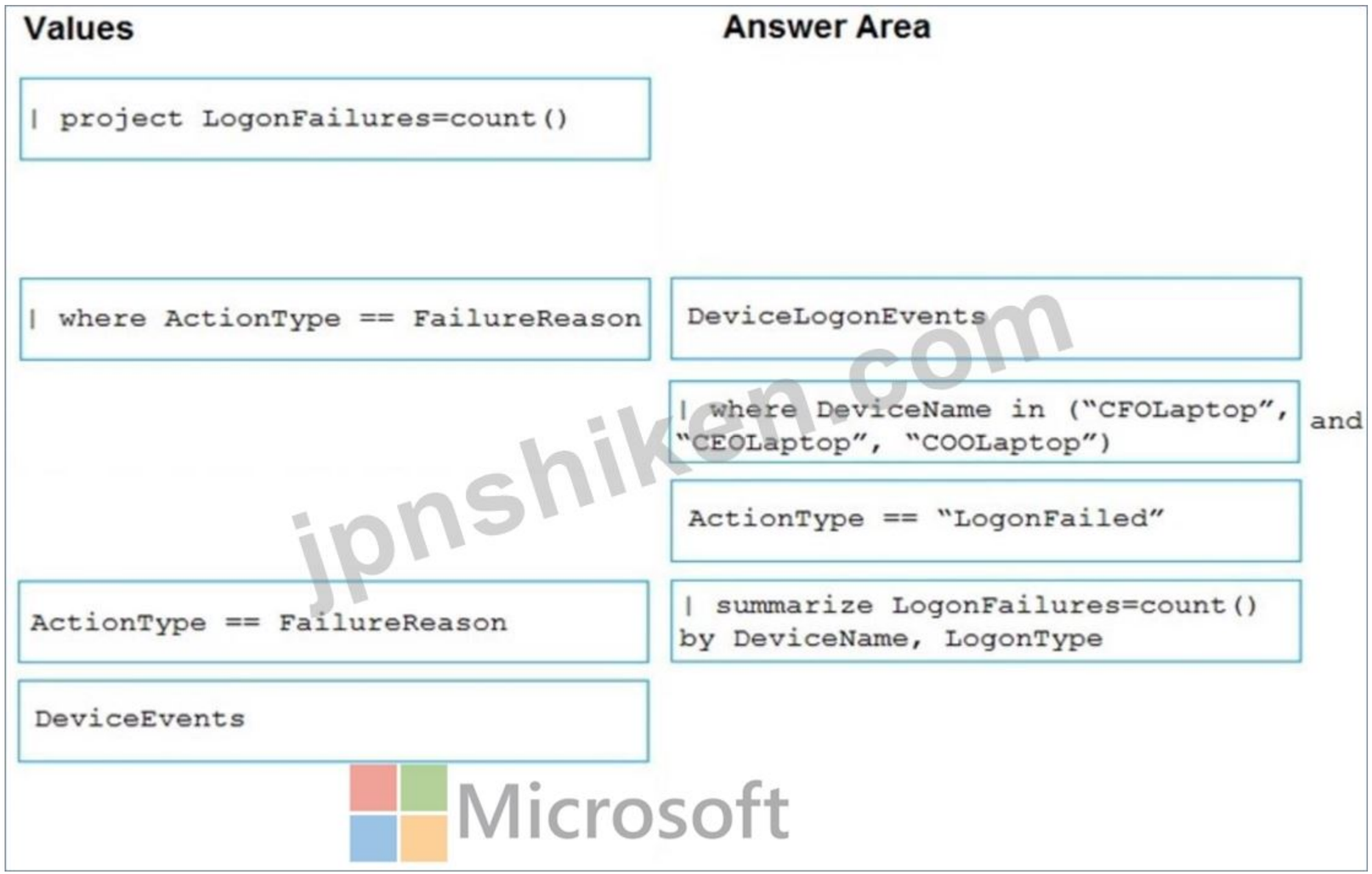

Answer Area
Microsoft
Group1:
Contributor
Owner
Security Admin
Security Assessment Contributor
jpnshiken.com
Group2:
Contributor
Owner
Security Admin
Security Assessment Contributor

質問: **212**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできません。そのため、これらの質問はレビュー画面には表示されません。
Azure Sentinel を構成しています。
悪意のある IP アドレスからの Azure 仮想マシンへのサインインが検出された場合は、Azure Sentinel でインシデントを作成する必要があります。
解決策: データ コネクタ用の Microsoft インシデント作成ルールを作成します。
これは目標を達成していますか?
A. はい
B. いいえ
正解: **A** (コメントを発表する)
As this kind of alert is generated by ASC, so we need the Microsoft incident creation rule to create incidents from ASC into sentinel.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference

質問: **213**
ドラッグアンドドロップ問題
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。



正解:

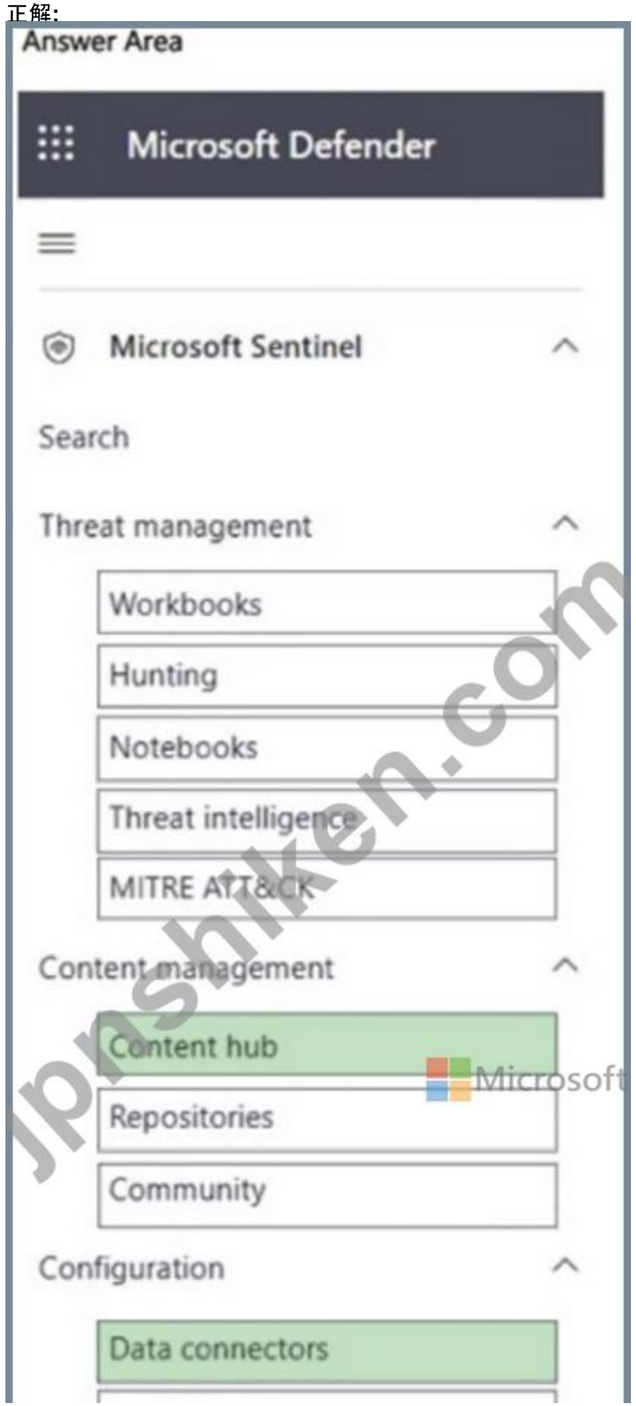


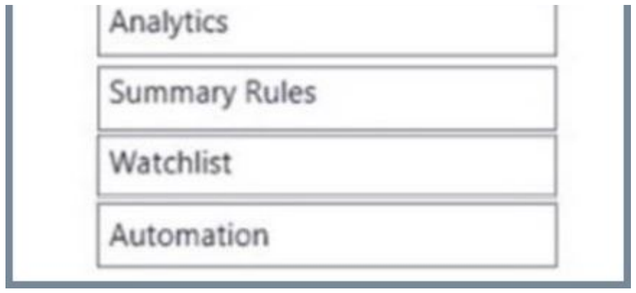
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/reference/tables/devicelogonevents

質問**: 214**
ホットスポットに関する質問
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
Microsoft Entraからログを収集するように、Microsoft Sentinelを設定する必要があります。
Microsoft Defender ポータルで使用すべきノードはどれですか？回答するには、回答欄で適切なノード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


Microsoft Defender
Microsoft Sentinel
Search
Threat management
Workbooks
Hunting
Notebooks
Threat intelligence
MITRE ATT&CK
Content management
Content hub
Repositories
Community
Configuration
Data connectors
Analytics
Summary Rules
Watchlist
Automation

正解:


Answer Area
Microsoft Defender
Microsoft Sentinel
Search
Threat management
Workbooks
Hunting
Notebooks
Threat intelligence
MITRE ATT&CK
Content management
Content hub
Repositories
Community
Configuration
Data connectors



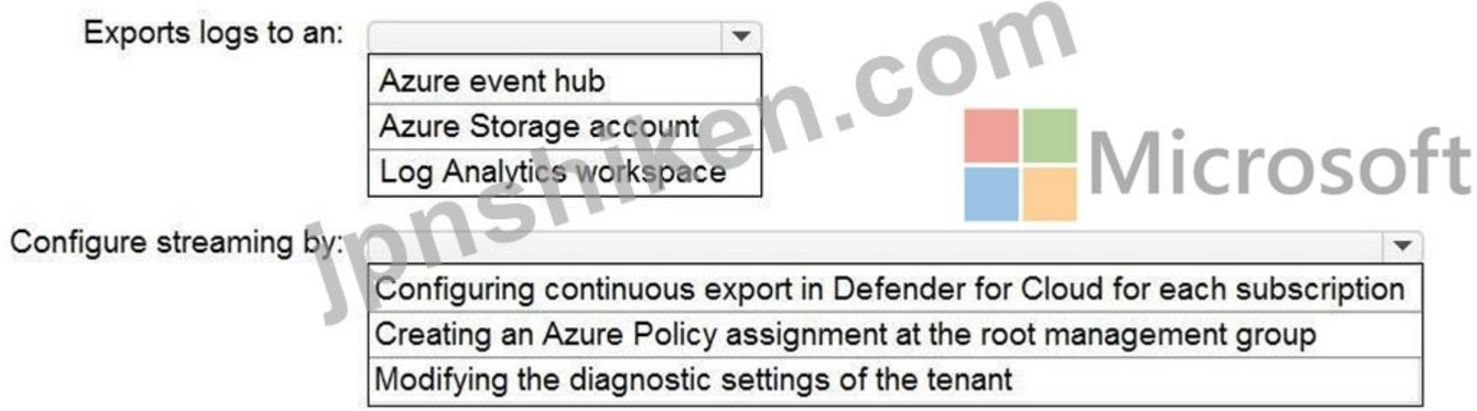
質問: **215**
お客様は、User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションをご利用中です。このサブスクリプションでは、Microsoft 365 Copilot for Security が使用されています。Copilot for Security は Sentinel プラグインを使用しています。
ユーザー1には、コパイロット貢献者の役割が割り当てられています。
調査中に、ユーザー1がプロンプトを送信すると、セキュリティコンピューティングユニット(SCU)の使用量がプロビジョニングされた容量制限に近づいているため、Copilot for Security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. 1時間待ってから、プロンプトを再送信してください。
B. プロビジョニングされたSCUを更新します。
C. Microsoft Sentinel 最適化ワークブックを実行します。
D. 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。
正解: **(正解を表示します)**
Manage usage of security compute units in Security Copilot
Nearing and crossing security compute unit limit
When the usage in your organization is nearing the limit, you are notified of it when submitting the prompts. To avoid disruption, you can contact the Azure capacity owner or contributor to increase the security compute units or limit the number of prompts.
Reference:
https://learn.microsoft.com/en-us/copilot/security/manage-usage

質問: **216**
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
攻撃者が特定のデバイスに接続しようとした際に、Microsoft Defender XDRでアラートが生成されるようにする必要があります。また、管理作業を最小限に抑えるソリューションを採用する必要があります。
Microsoft Defenderポータルでは、どのような操作を行うべきですか？
A. 誘惑を含む欺瞞ルールを作成します。
B. おとりを含む欺瞞ルールを作成します。
C. 既存のデバイスをハニートークンエンティティとしてタグ付けします。
D. 既存のデバイスを機密エンティティとしてタグ付けします。
正解: **(正解を表示します)**

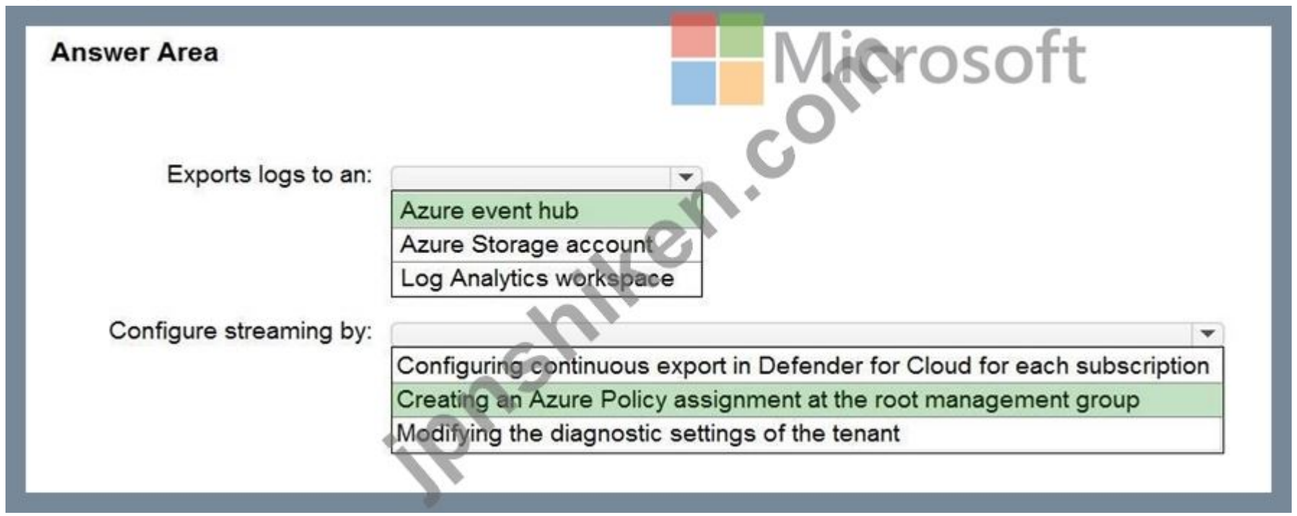
質問: **217**

ホットスポットに関する質問
Microsoft Defender for Cloud の強化されたセキュリティ機能が有効になっている Azure サブスクリプションが 100 件あります。
すべてのサブスクリプションは、単一のAzure Active Directory(Azure AD)テナントに紐付けられています。
Defender for Cloudのログをsyslogサーバーにストリーミングする必要があります。ソリューションは管理作業を最小限に抑えるものでなければなりません。
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。

Answer Area



正解:



Explanation:
Box 1: Azure Event hub
To stream alerts into //Syslog servers// ,and other monitoring solutions, connect Defender for Cloud using continuous export and Azure Event Hubs.

Box 2: Azure Policy
Note:
To stream alerts at the tenant level, use this //Azure policy// and set the scope at the root management group.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/export-to-siem#stream-alerts-with-continuous-export
https://docs.microsoft.com/en-us/azure/defender-for-cloud/continuous-export?tabs=azure-policy#configure-continuous-export-at-scale-using-the-supplied-policies

質問: 218
事例研究4 - Litware Inc.
概要
アダタム -コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。
既存の環境
アイデンティティ環境
オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。
ライセンス状況
Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。
クラウド環境
クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境
オンプレミスネットワークには、次の表に示すリソースが含まれています。

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件
計画されている変更
Adatum社は以下の変更を実施する予定です。
- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```


- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。
Microsoft Defender for Cloud の要件
Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。
グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。
- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。
Microsoft Sentinelの要件
Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。
- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。
可能な限り、ASIMに組み込まれているパーサーを使用してください。
ビジネス要件
Adatumは、以下のビジネス要件を特定しました。
可能な限り、最小権限の原則に従うこと。
可能な限り管理業務を最小限に抑える。
HuntingQuery1 の構成が Microsoft Sentinel の要件を満たしていることを確認する必要があります。
あなたはどうすべきでしょうか？
A. ライブストリームにHuntingQuery1を追加します。
B. ウォッチリストを作成します。
C. Azure Automation ルールを作成します。
D. HuntingQuery1 をお気に入りに追加します。
正解**: D (**コメントを発表する**)**
Favorites are automatically run when opening hunting page.
Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.

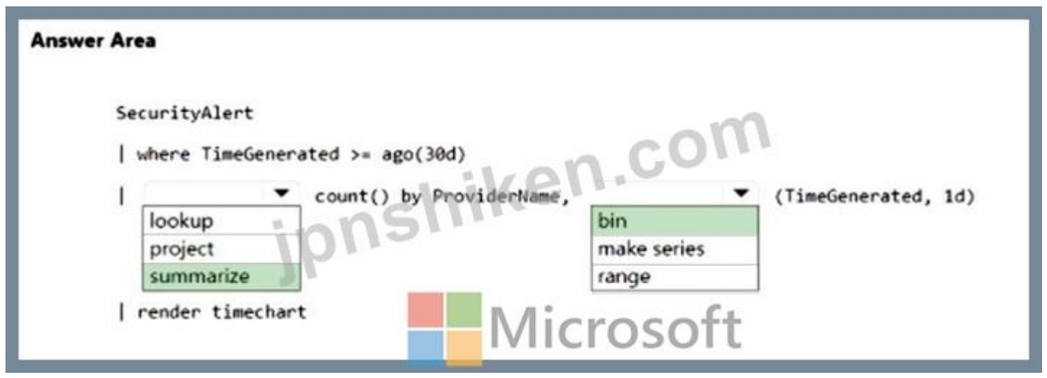
質問: **219**
注 :このセクションには、同じシナリオと問題に関する複数の質問セットが含まれています。各質問には、問題に対する固有の解決策が提示されています。提示された解決策が、提示された目標を満たしているかどうかを判断する必要があります。セット内の複数の解決策が問題を解決できる場合もあります。また、セット内のどの解決策も問題を解決できない場合もあります。
このセクションの質問に回答すると、前のセクションに戻ることはできません。そのため、これらの質問は復習画面には表示されません。
あなたはMicrosoft 365のサブスクリプションをお持ちです。
サードパーティ製のウイルス対策ソフトがインストールされ、Microsoft Defenderウイルス対策ソフトがパッシブモードで動作しているWindowsデバイスが1,000台あります。
すべてのWindowsデバイスは、Microsoft Defender for Endpointにオンボーディングされています。
サードパーティ製のウイルス対策製品では検出されなかった悪意のあるファイルからデバイスが保護されていることを確認する必要があります。
解決策 :ライブレスポンスを有効にします。
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: **B** (コメントを発表する)

質問: **220**
Microsoft 365 Defender が有効になっている Microsoft 365 サブスクリプションがあります。
過去 7 日間に機密ラベルに加えられたすべての変更を特定する必要があります。
何を使えばいいのでしょうか？
A. Microsoft 365 Defender ポータルのインシデント ブレード
B. Microsoft 365 コンプライアンス センターのデータ損失防止ブレードのアラート設定
C. Microsoft 365 コンプライアンス センターのアクティビティ エクスプローラー
D. Microsoft 365 Defender ポータルの [電子メールとコラボレーション] ブレードのエクスプローラー設定
正解: (正解を表示します)
Labeling activities are available in Activity explorer.
For example:
Sensitivity label applied
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.
It is captured at the time of save in Office native applications and web applications. It is captured at the time of occurrence in Azure Information protection add-ins. Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.
Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity- explorer-available-events?view=o365-worldwide

質問: **221**
ホットスポットに関する質問
カスタムワークブックを含む Microsoft Sentinel ワークスペースがあります。
1日あたりのセキュリティアラートの数を照会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30日間に発生したアラートを特定します。
結果を時系列グラフで表示する。
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ポイントが加算されます。

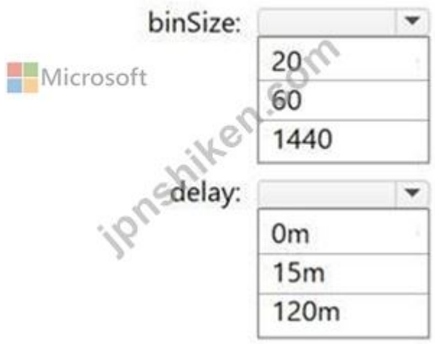
Answer Area

正解:



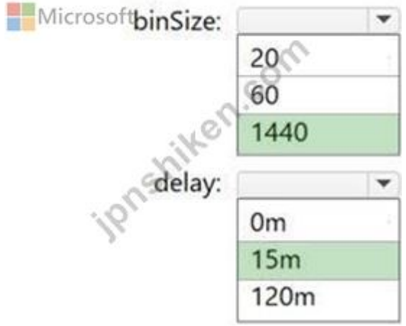
質問: **222**
ホットスポットに関する質問
Microsoft Sentinel ワークスペース 「Workspace1」があり、1 TB/日のファイアウォールイベントを Microsoft Sentinel データレイク層に取り込んでいます。Workspace1 には、「Workbook1」という名前のワークブックが含まれており、毎日午前 6:00 に更新されます。
イベントは最大10分遅れて到着する場合があります。
アナリストは午前6時30分にワークブック1のレビューを開始し、それまでに更新作業を完了させる必要がある。
遅延して到着するイベントを見逃すことなく、完全な日次サマリーを生成するサマリールールスケジュールを設定する必要があります。このソリューションは、サマリールールの実行コストを最小限に抑える必要があります。
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。

Answer Area



正解:

Answer Area



質問: **223**

ホットスポットに関する質問

以下の表に示すAzureサブスクリプションをお持ちです。

Name	Resource group
Sub1	RG1
Sub2	• RG2 • RG3

お客様のMicrosoft Entraテナントには、以下の表に示すユーザーが含まれています。

Name	Role
User1	Security Operator
User2	Security Administrator
User3	Global Administrator

ユーザーには、次の表に示すAzureロールが付与されています。

User	Role	Scope
User1	Owner	Sub1
User2	Reader	Sub2
User3	Owner	RG2

Microsoft Copilot for Security の機能は、次の表に示すように構成します。

Name	Resource group
Capacity1	RG1
Capacity2	RG3

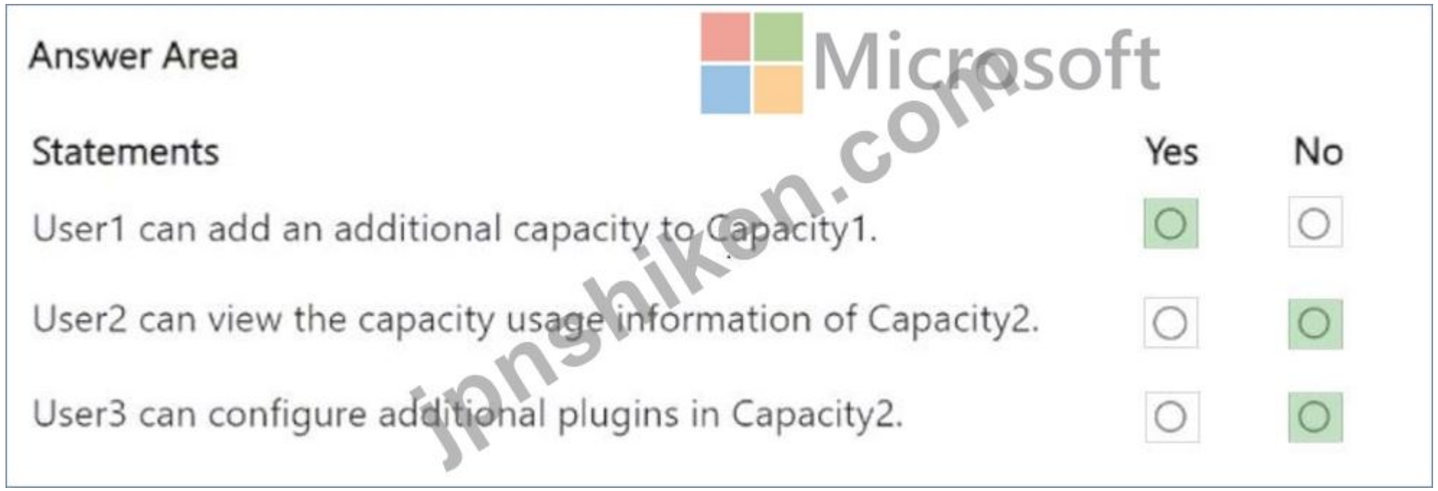
以下の各記述について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注：正解ごとに1ポイントが加算されます。

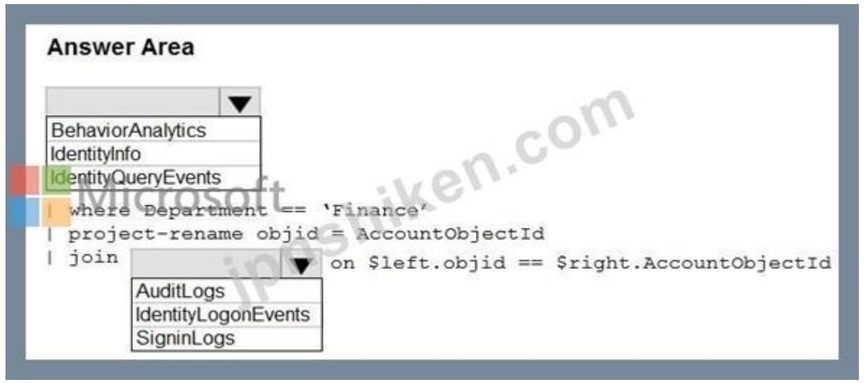
Answer Area

Statements	Yes	No
User1 can add an additional capacity to Capacity1.	○	○
User2 can view the capacity usage information of Capacity2.	○	○
User3 can configure additional plugins in Capacity2.	○	○

正解:



質問: **224**
ホットスポットに関する質問
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。



正解:

Answer Area

Explanation:
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitylogonevents-table?view=o365-worldwide

質問: **225**
お客様は、Microsoft Security Copilot 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。
あなたはCopilot用のカスタムGPTプラグインを設定する予定です。
どのGPTモデルを使用すべきですか？
A. gpt-4o
B. o1-mini
C. davinci-002
D. gpt-35-turbo
正解: **(正解を表示します)**
GPT plugins in Microsoft Security Copilot
Available model names
gpt-4o only.
Reference:
https://learn.microsoft.com/en-us/copilot/security/plugin-gpt

質問: **226**
事例研究2 - Litware Inc.
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たアラートは、テストユーザーアカウントごとに1つ

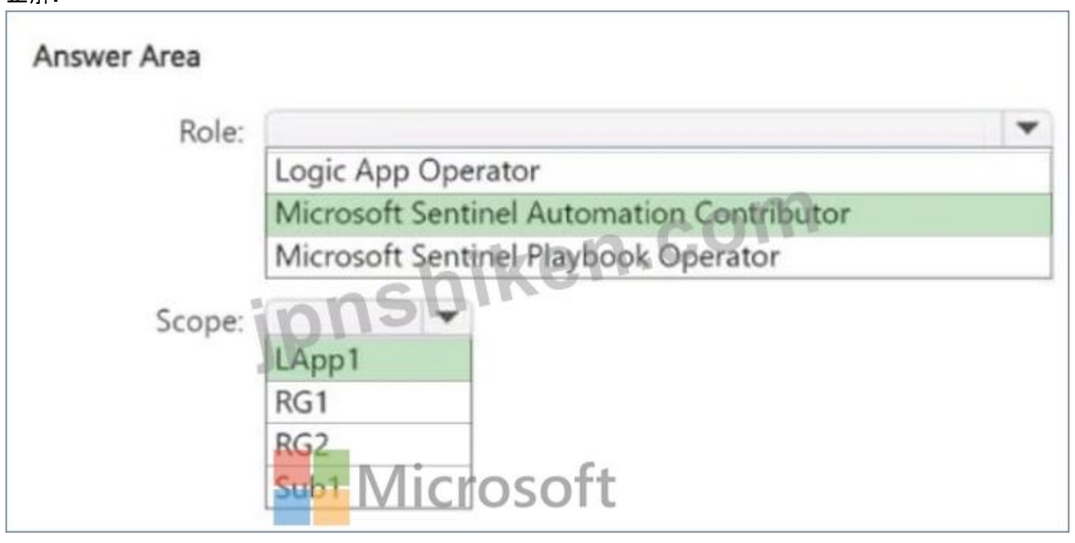
のインシデントとしてグループ化する必要があります。
Microsoft Defender for Endpointの要件を満たすには、CLIENT1上で実行されるクラウドアプリを制限する必要があります。
どの2つの設定を変更すべきでしょうか？それぞれの正解は、解決策の一部を示しています。
注：正解ごとに1ポイントが加算されます。
A. Microsoft Defender Security Center のデバイス管理にあるオンボーディング設定
B. クラウドアプリセキュリティ異常検知ポリシー
C. Microsoft Defender セキュリティ センターの 設定」にある高度な機能
D. 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)
All Cloud App Security unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.
You can also add URLs/Domains to block directly from Defender - Settings - Endpoints - Indicators - URLs/Domains tab - Add items --> to add cloud apps to block.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/mde-govern

質問: **227**
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、そこには次の表に示すリソースが含まれています。

Name	Type	Resource group	Description
WS1	Microsoft Sentinel workspace	RG1	Contains a scheduled query rule named Rule1
LApp1	Azure logic app	RG2	Contains a Microsoft Sentinel incident trigger

インシデントが発生した際にLapp1がトリガーされるように、Rule1を設定する予定です。
WS1に割り当てるべきロールベースアクセス制御(RBAC)ロールと、そのロールを割り当てる範囲を推奨する必要があります。解決策は最小権限の原則に従う必要があります。
何を推奨しますか？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:



質問: **228**

Log Analytics ワークスペースを含む Azure サブスクリプションがあります。

Azure リソースのジャストインタイム (JIT) VM アクセスとネットワーク検出を有効にする必要があります。

Azure Defender をどこで有効にすればよいですか?

A. サブスクリプション レベル

B. ワークスペース レベル

C. リソースレベルで

正解: **(**正解を表示します**)**

Enabling it at the workspace level doesn't enable just-in-time VM access, adaptive application controls, and network detections for Azure resources. In addition, the only Microsoft Defender plans available at the workspace level are Microsoft Defender for servers and Microsoft Defender for SQL servers on machines.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security

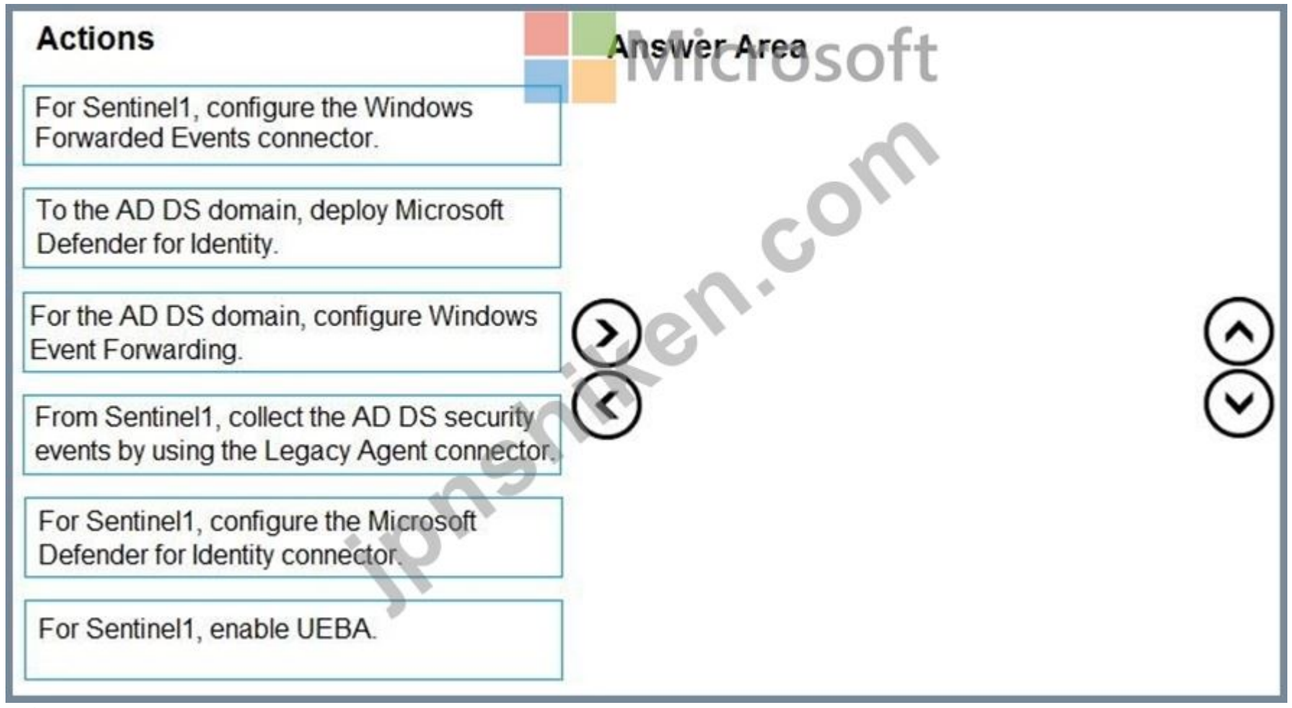
質問: **229**
Microsoft 365 Defender ポータルを使用して、悪意のある可能性のあるドキュメントに関連する複数段階のインシデントの調査を行っています。詳細を確認した結果、この潜在的に悪意のあるドキュメントに関連付けられたアラートが、環境内の別のインシデントにも関連していることが判明しました。ただし、このアラートは現在、その2番目のインシデントの一部としてはリストされていません。アラートに関する調査は継続中であり、関連する2つのインシデントに関する調査も継続中です。
アラートを適切に分類し、それが2番目のインシデントに関連付けられていることを確認する必要があります。
調査のこの部分を完了するために、「アラートの管理」ペインで実行すべき2つの操作は何ですか？
それぞれの正解は、解答の一部を示しています。
A. 「アラートを別のインシデントにリンクする」オプションを選択します。
B. 分類を「真のアラート」に設定します。
C. ステータスを新規に設定します。
D. ステータスを「進行中」に設定します。
E. コメント欄に、関連するインシデントのインシデントIDを入力してください。
正解: **(**正解を表示します**)**
The correct action to classify the alert would be to set the status to In progress. While the alert may seem to be legitimate as it is linked to another incident, until a final determination is reached, you should set the status to In progress to ensure that others know it is being worked on. Once a determination is reached, you can then change it to Resolved and select the appropriate classification (True alert or False alert).
The correct action to correlate the alert to the other incident would be to select the Link alert to another incident option. While ideally the alert would automatically be included in both incidents, that is not always the case. If you notice an alert that is not linked to an incident that it is clearly connected to, using the Link alert to another incident option ensures they are tied together.
You should not set the classification to True alert. While a point can be made that it seems this malicious file involved in multiple incidents is likely to be a True alert, you are not yet able to make that determination. It also is not time to classify it as a false alert. The best practice while continuing an investigation would be not to change the classification at all, which means leaving it as the default Not set classification.
You should not enter the Incident ID of the related incident in the Comment section. While this might be helpful from an administrative perspective, it creates no link to the other incident.
You should not set the status to New. This is the default status of any alert. The question specifically seeks to ensure your peers know the alert is being investigated, so setting (or leaving) the status as New would make it impossible to differentiate from other uninvestigated alerts.
All of the actions mentioned in the options can be found in the Manage alert pane, which can be reached via the Alerts tab in the Incidents section of the Microsoft 365 Defender portal. This is an excellent central location from which you can manage incidents, and the components that make them up, including alerts.

質問: **230**
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。
Microsoft Defender for Cloud Apps の統合監査ログのデータを使用して脅威を調査できることを確認する必要があります。
最初に何を設定すべきですか？
A. ユーザーエンリッチメント設定
B. Azureコネクタ
C. Office 365 コネクタ
D. 自動ログアップロード設定
正解: **C (**コメントを発表する**)**
https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365
質問: **231**
ホットスポットに関する質問
お客様の環境には、Windows Serverが稼働しているものの、インターネット接続のないオンプレミスサーバーが100台あります。

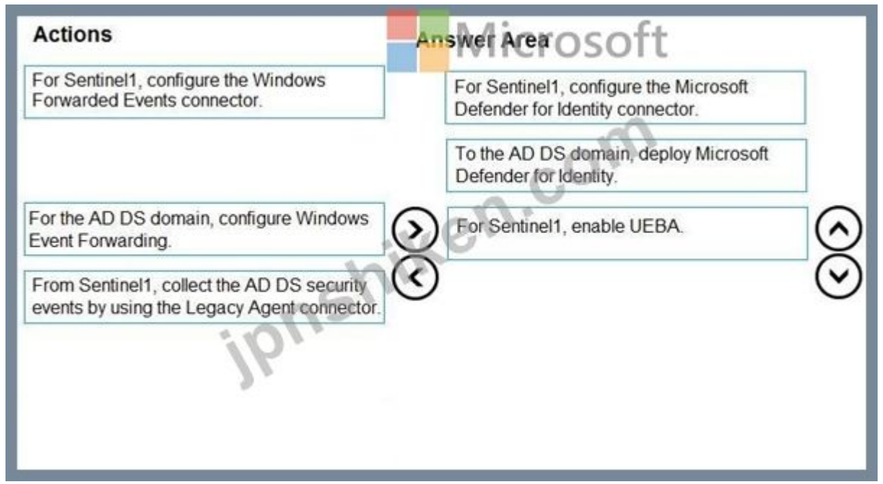
お客様は、専用の監視サーバーを含むAzureサブスクリプションをお持ちです。
Workspace1という名前のMicrosoft Sentinelワークスペースがあります。
オンプレミスサーバーからWindowsイベントログをWorkspace1に取り込む必要があります。
どうすればよいですか？回答するには、回答欄で適切な選択肢を選んでください。
注：正解ごとに1ポイントが加算されます。

正解:

質問: **232**
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:

For Sentinel1, configure the Microsoft defender for identity connector.

This will allow you to sync user entities from on-premises Active Directory, using Microsoft Defender for Identity.

To the AD DS Domain, deploy Microsoft Defender for Identity.

You need to install the MDI sensor on your Active Directory domain controller to enable UEBA to collect security events from your on-premises AD DS domain.

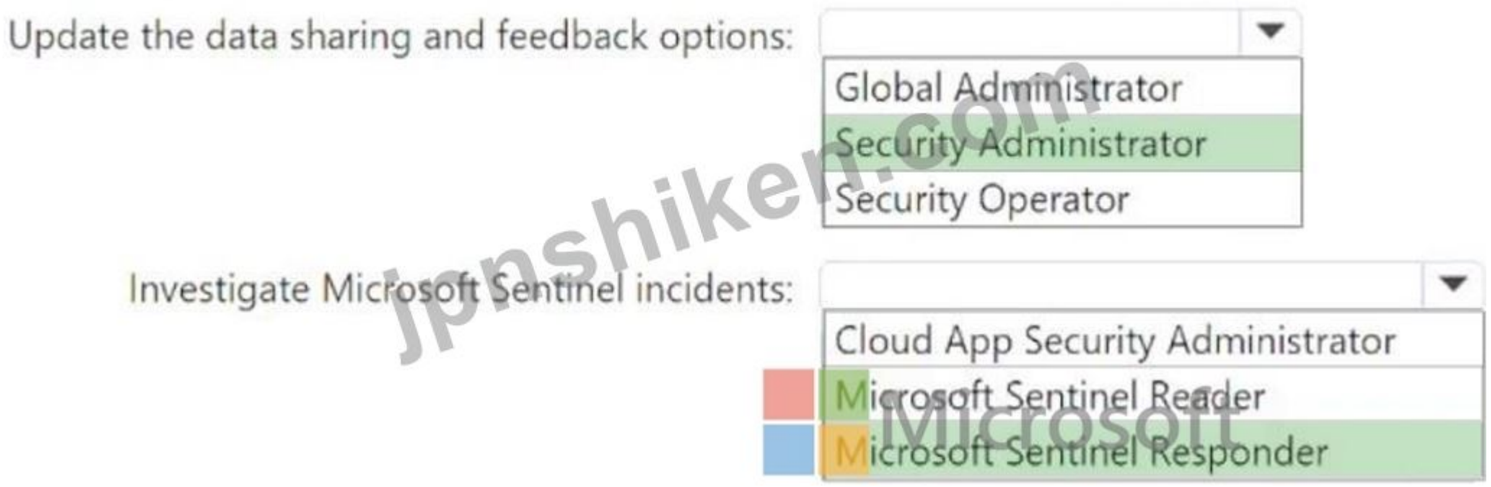
For Sentinel1, enable UEBA.

You need to switch the toggle to On and select the data sources on which you want to enable UEBA.

質問: **233**
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、それが contoso.com という名前の Microsoft Entra テナントにリンクされています。contoso.com には User1 という名前のユーザーが存在します。Sub1 には Microsoft Sentinel ワークスペースが含まれています。
Microsoft Copilot for Securityの機能をプロビジョニングします。
User1がCopilot for Securityを使用して以下のタスクを実行できるようにする必要があります。
- データ共有とフィードバックのオプションを更新します。
- Microsoft Sentinel関連のインシデントを調査する。
解決策は最小権限の原則に従わなければならない。
各タスクにおいて、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:

Answer Area



質問: 234

事例研究4 - Litware Inc.

概要

アダタム -コーポレーションは、米国に本社を置く金融サービス会社で、ニューヨーク、シカゴ、サンフランシスコに地域オフィスを構えている。

既存の環境

アイデンティティ環境

オンプレミスネットワークには、corp.adatum.com という名前の Active Directory ドメインサービス (AD DS) フォレストがあり、これは adatum.com という名前の Azure AD テナントと同期しています。すべてのユーザーおよびグループ管理タスクは corp.adatum.com で実行されます。corp.adatum.com ドメインには、adatum.com と同期する Group1 という名前のグループが含まれています。

ライセンス状況

Adatumの全ユーザーには、Microsoft 365 ESライセンスとAzure Active Directory Premium P2ライセンスが割り当てられています。

クラウド環境

クラウド環境には、Microsoft 365 サブスクリプション、adatum.com テナントにリンクされた Azure サブスクリプション、および次の表に示すリソースが含まれています。

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

オンプレミス環境

オンプレミスネットワークには、次の表に示すリソースが含まれています。

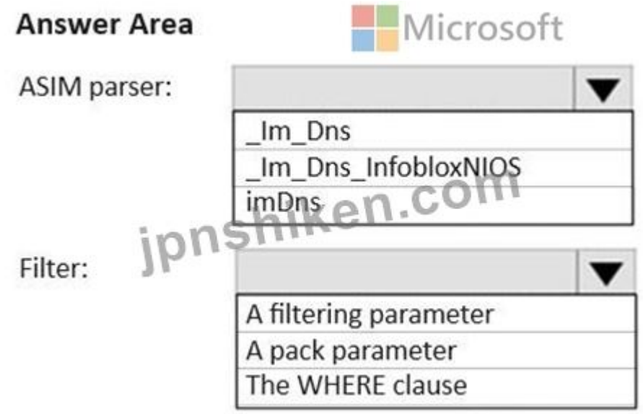
Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

要件
計画されている変更
Adatum社は以下の変更を実施する予定です。
- 以下の KQL クエリを含む rulequery1 という名前のクエリを実装します。

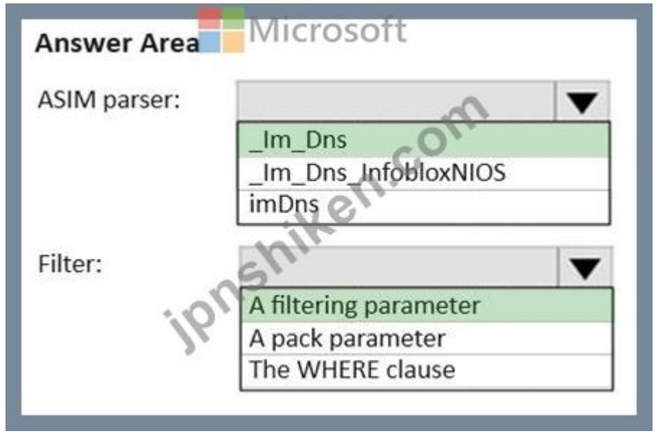
```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

- ルールクエリ1に基づいてインシデントを生成するMicrosoft Sentinelのスケジュール済みルールを実装します。
Microsoft Defender for Cloud の要件
Adatumは、Microsoft Defender for Cloudの要件として以下のものを挙げています。
グループ1のメンバーは、Defender for Cloudプランを有効にし、規制遵守のための取り組みを適用できる必要があります。
- すべてのAzure仮想マシンでMicrosoft Defender for Serversプラン2を有効にする必要があります。
- Server2はエージェントレススキャンから除外する必要があります。
Microsoft Sentinelの要件
Adatumは、Microsoft Sentinelに関する以下の要件を特定しています。
- Infoblox1 から NXDOMAIN 応答が返される DNS リクエストの数を返す Advanced Security Information Model (ASIM) クエリを実装します。
- 1人のユーザーがAzure Cloud Shellを複数回起動したことに応答してrulequery1によって生成された複数のアラートが、単一のインシデントとして統合されるようにします。
- Microsoft Sentinel 用の AMA コネクタを介して Windows セキュリティ イベントを実装し、Server1 のセキュリティ イベント ログを監視するように構成します。
- 会社のセキュリティ運用チームがAzure Cloud Shellを起動した場合、rulequery1によって生成されたインシデントが自動的にクローズされるようにします。
- Webapp1 からデータを動的に取得するクエリを含む、Workbook1 という名前のカスタム Microsoft Sentinel ワークブックを実装します。
- 指定された緊急対応アカウントへのサインインを検出する、Microsoft Sentinelのニアリアルタイム(NRT)分析ルールを実装します。
- Azure ポータルの Microsoft Sentinel のハンティング ページにアクセスした際に、HuntingQuery1 が自動的に実行されるようにします。
- corp.adatum.comのユーザーアカウントに対するパスワードリセットの件数が通常よりも多い場合、それを検出します。
- ASIMパーサーを使用するクエリに関連するオーバーヘッドを最小限に抑える。
- Group1のメンバーがプレイブックを作成および編集できることを確認してください。
可能な限り、ASIMに組み込まれているパーサーを使用してください。
ビジネス要件
Adatumは、以下のビジネス要件を特定しました。

可能な限り、最小権限の原則に従うこと。
可能な限り管理業務を最小限に抑える。
ホットスポットに関する質問
DNSリクエストに対してASIM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の要件を満たしている必要があります。
クエリ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。



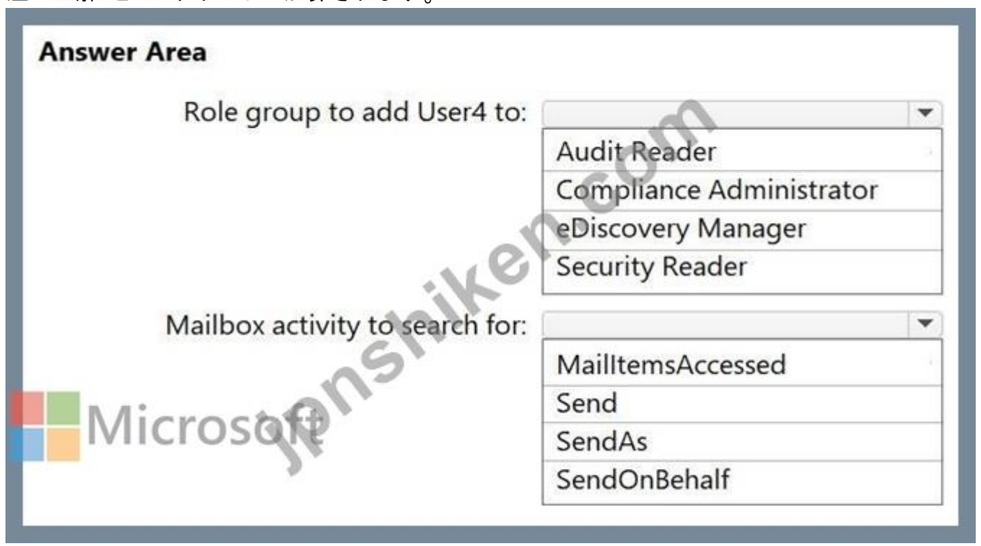
正解:



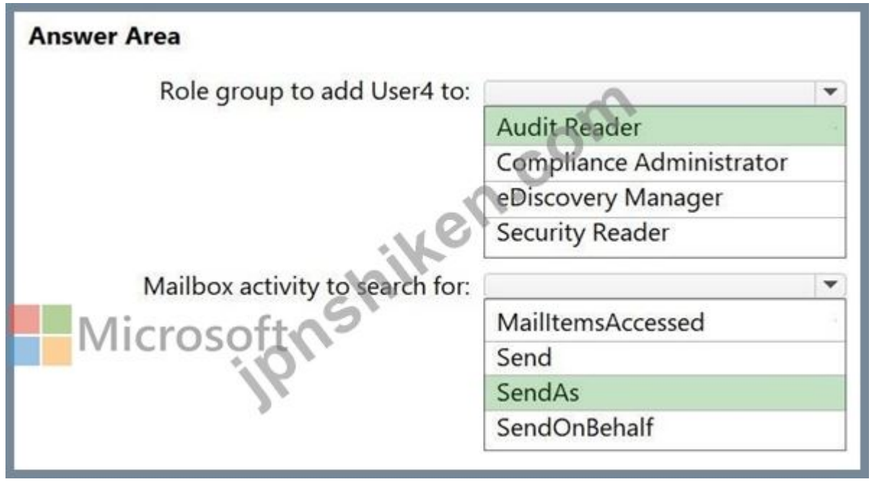
Explanation:
https://learn.microsoft.com/en-us/azure/sentinel/normalization-about-parsers

質問: **235**
ホットスポットに関する質問
お客様は、User1、User2、User3、User4という名前の4人のユーザーを含むMicrosoft 365 E5サブスクリプションをご利用になっています。このサブスクリプションでは、Microsoft Purview AuditとMicrosoft Defender XDRが使用されています。
ユーザー2とユーザー3は、ユーザー1のメールボックスへのアクセス権を委任されています。
User1のメールボックスから、送信者がUser1であることを示すフィッシングメールが送信されました。

User4が監査機能を使用して、フィッシングメールを送信したのがUser2かUser3かを特定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。
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:



質問: **236**
あなたはMicrosoft 365 E5のサブスクリプションをお持ちです。
Windowsデバイス上でPowerShellを使用して、Microsoft Purviewの監査ログを検索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. Microsoft Graph PowerShellモジュールをインストールします。
B. PowerShellリモート処理を有効にする。
C. Microsoft Exchange Online PowerShell モジュールをインストールします。

D. TrustedHosts リストを変更します。
正解**: C (**コメントを発表する**)**
Step 1: Load the Exchange Online PowerShell module
Microsoft Purview, Use a PowerShell script to search the audit log
Connect to Exchange Online PowerShell
After you've installed the module, open a PowerShell window and load the module by running the following command:
Import-Module ExchangeOnlineManagement
Reference:
https://learn.microsoft.com/en-us/purview/audit-log-search-script
https://learn.microsoft.com/en-us/powershell/exchange/connect-to-exchange-online-powershell